Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Journal of Algebra 301 (2006) 425–445

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

The centre of quantum $\mathfrak{sl}_n$ at a root of unity

Rudolf Tange

School of Mathematics, University of Southampton, Highfield, SO17 1BJ, UK

Received 5 May 2005

Available online 13 February 2006

Communicated by Corrado de Concini

Summary

It is proved that the centre Z of the simply connected quantised universal enveloping algebra over $\mathbb{C}$, $U_{\varepsilon,P}(\mathfrak{sl}_n)$, ε a primitive lth root of unity, l an odd integer > 1, has a rational field of fractions. Furthermore it is proved that if l is a power of an odd prime, Z is a unique factorisation domain.

Introduction

In [8] de Concini, Kac and Procesi introduced the simply connected quantised universal enveloping algebra $U = U_{\varepsilon,P}(\mathfrak{g})$ over $\mathbb{C}$ at a primitive lth root of unity ε associated to a simple finite-dimensional complex Lie algebra $\mathfrak{g}$. The importance of the study of the centre Z of U and its spectrum $\mathrm{Maxspec}(Z)$ is pointed out in [7,8].

In this article we consider the following two conjectures concerning the centre Z of U in the case $\mathfrak{g} = \mathfrak{sl}_n$:

(1) Z has a rational field of fractions.
(2) Z is a unique factorisation domain (UFD).

The same conjectures can be made for the universal enveloping algebra $U(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ of a reductive group over an algebraically closed field of positive characteristic.

E-mail address: rtange@maths.soton.ac.uk.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2005.11.036

In [16] these conjectures were proved for $\mathfrak{g} = \mathfrak{gl}_n$ and for $\mathfrak{g} = \mathfrak{sl}_n$ under the condition that n is non-zero in the field.

The second conjecture was made by Braun and Hajarnavis in [1] for the universal enveloping algebra $U(\mathfrak{g})$ and suggested for $U = U_{\varepsilon,P}(\mathfrak{g})$. There it was also proved that Z is locally a UFD. In Section 3 below, this conjecture is proved for $\mathfrak{sl}_n$ under the condition that l is a power of a prime ($\neq 2$). The auxiliary results and Step 1 of the proof of Theorem 4, however, hold without extra assumptions on l.

The first conjecture was posed as a question by J. Alev for the universal enveloping algebra $U(\mathfrak{g})$. It can be considered as a first step towards a proof of a version of the Gelfand–Kirillov conjecture for U. Indeed the Gelfand–Kirillov conjecture for $\mathfrak{gl}_n$ and $\mathfrak{sl}_n$ in positive characteristic[1] was proved recently by J.-M. Bois in his PhD thesis [4] using results in [16] on the centres of their universal enveloping algebras (for $\mathfrak{sl}_n$ it was required that $n \neq 0$ in the field). It should be noted that the Gelfand–Kirillov conjecture for $U(\mathfrak{g})$ in characteristic 0 (and in positive characteristic) is still open for $\mathfrak{g}$ not of type A.

As in [16], a certain semi-invariant d for a maximal parabolic subgroup of GL_n will play an important rôle. Later we learned that (a version of) this semi-invariant already appeared before in the literature, see [10]. For quantum versions, see [12,13].

1. Preliminaries

In this section we recall some basic results, mostly from [8], that are needed to prove the main results (Theorems 3 and 4) of this article. Short proofs are added in case the results are not explicitly stated in [8].

1.1. Elementary definitions

Let $\mathfrak{g}$ be a simple finite-dimensional Lie algebra over $\mathbb{C}$ with Cartan subalgebra $\mathfrak{h}$, let Φ be its root system relative to $\mathfrak{h}$, let $(\alpha_1, \dots, \alpha_r)$ be a basis of Φ and let $(\cdot|\cdot)$ be the symmetric bilinear form on $\mathfrak{h}^*$ which is invariant for the Weyl group W and satisfies $(\alpha|\alpha) = 2$ for all short roots α. Put $d_i = (\alpha_i|\alpha_i)/2$. The root lattice and the weight lattice of Φ are denoted by respectively Q and P. Note that $(\cdot|\cdot)$ is integral on $Q \times P$.

Mostly we will be in the situation where $\mathfrak{g} = \mathfrak{sl}_n$. In this case $r = n - 1$ and all the d_i are equal to 1. We then take $\mathfrak{h}$ the subalgebra that consists of the diagonal matrices in $\mathfrak{sl}_n$ and we take $\alpha_i = A \mapsto A_{ii} - A_{i+1\,i+1} : \mathfrak{h} \to \mathbb{C}$.

Let l be an odd integer > 1 and coprime to all the d_i, let ε be a primitive lth root of unity and let Λ be a lattice between Q and P. Let $U = U_{\varepsilon,\Lambda}(\mathfrak{g})$ be the quantised universal enveloping algebra of $\mathfrak{g}$ at the root of unity ε defined in [8] and denote the centre of U by Z. Since U has no zero divisors (see [7, 1.6–1.8]), Z is an integral domain. Let U^+, U^-, U^0 be the subalgebras of U generated by respectively the E_i, the F_i and the K_λ with $\lambda \in \Lambda$. Then the multiplication $U^- \otimes U^0 \otimes U^+ \to U$ is an isomorphism of vector spaces. We

[1] The *Gelfand–Kirillov conjecture* for a Lie algebra $\mathfrak{g}$ over K states that the fraction field of $U(\mathfrak{g})$ is isomorphic to a Weyl skew field $D_n(L)$ over a purely transcendental extension L of K.

identify U^0 with the group algebra $\mathbb{C}\Lambda$ of Λ. Note that W acts on U^0, since it acts on Λ. Let T be the complex torus $\mathrm{Hom}(\Lambda, \mathbb{C}^\times)$. Then T can be identified with $\mathrm{Maxspec}(U^0) = \mathrm{Hom}_{\mathbb{C}\text{-}\mathrm{Alg}}(U^0, \mathbb{C})$ and for the action of T on $U^0 = \mathbb{C}[T]$ by translation we have $t \cdot K_\lambda = t(\lambda)K_\lambda$.

The *braid group* $\mathcal{B}$ acts on U by automorphisms. See [8, 0.4]. The subalgebra Z_0 of U is defined as the smallest $\mathcal{B}$-stable subalgebra containing the elements K_λ^l, $\lambda \in \Lambda$, and E_i^l, F_i^l, $i = 1, \dots, r$. We have $Z_0 \subseteq Z$. Put $z_\lambda = K_\lambda^l$ and let Z_0^0 be the subalgebra of Z_0 spanned by the z_λ. Then the identification of U^0 with $\mathbb{C}\Lambda$ gives an identification of Z_0^0 with $\mathbb{C}l\Lambda$. If we replace K_λ by z_λ in foregoing remarks, then we obtain an identification of T with $\mathrm{Maxspec}(Z_0^0)$. Put $Z_0^\pm = Z_0 \cap U^\pm$. Then the multiplication $Z_0^- \otimes Z_0^0 \otimes Z_0^+ \to Z_0$ is an isomorphism (of algebras). See e.g. [7, 3.3].

1.2. The Harish-Chandra centre Z_1 and the quantum restriction theorem

Let $Q^\vee$ be the dual root lattice, that is, the $\mathbb{Z}$-span of the dual root system $\Phi^\vee$. We have $Q^\vee \cong P^* \hookrightarrow \Lambda^*$. Denote the image of $Q^\vee$ under the homomorphism $f \mapsto (\lambda \mapsto (-1)^{f(\lambda)}) : \Lambda^* \to T$ by $Q_2^\vee$. Then the elements $\neq 1$ of $Q_2^\vee$ are of order 2 and $U^{0Q_2^\vee} = \mathbb{C}(\Lambda \cap 2P)$. Since $Q_2^\vee$ is W-stable, we can form the semi-direct product $\tilde{W} = W \ltimes Q_2^\vee$ and then $U^{0\tilde{W}} = (\mathbb{C}(\Lambda \cap 2P))^W$.

Let $h' : U = U^- \otimes U^0 \otimes U^+ \to U^0$ be the linear map taking $x \otimes u \otimes y$ to $\epsilon_U(x)u\epsilon_U(y)$, where ϵ_U is the counit of U. Then h' is a projection of U onto U^0. Furthermore $h'(Z_0) = Z_0^0 = \mathbb{C}l\Lambda$ and $h'|_{Z_0} : Z_0 \to Z_0^0$ has a similar description as h' and is a homomorphism of algebras. Define the shift automorphism γ of $U^{0Q_2^\vee}$ by setting $\gamma(K_\lambda) = \varepsilon^{(\rho|\lambda)}K_\lambda$ for $\lambda \in \Lambda \cap 2P$. Here ρ is the half sum of the positive roots. Note that $\gamma = \mathrm{id}$ on $Z_0^{0Q_2^\vee} = \mathbb{C}l(\Lambda \cap 2P)$. In [8, p. 174] and [7, §2], there was constructed an injective homomorphism $\bar{h} : U^{0\tilde{W}} \to Z$, whose image is denoted by Z_1, such that $h'(Z_1) \subseteq U^{0Q_2^\vee}$ and the inverse

$$h : Z_1 \xrightarrow{\sim} U^{0\tilde{W}}$$

of $\bar{h}$ is equal to $\gamma^{-1} \circ h'$. Note that $h = h'$ on $Z_0 \cap Z_1$ and that $h'|_{Z_1}$ is a homomorphism of algebras. Since $\mathrm{Ker}(h')$ is stable under left and right multiplication by elements of U^0 and under multiplication by elements of Z, we can conclude that the restriction of h' to the subalgebra generated by Z_0 and Z_1 is a homomorphism of algebras.

From now on we assume that $\Lambda = P$. Let G be the simply connected almost simple complex algebraic group with Lie algebra $\mathfrak{g}$ and let T be a maximal torus of G. We identify Φ and W with the root system and the Weyl group of G relative to T. Note that the character group $X(T)$ of T is equal to P. In case $\mathfrak{g} = \mathfrak{sl}_n$ we take T the subgroup of diagonal matrices in SL_n.

1.3. Generators for $\mathbb{C}[G]^G$ and Z_1

We denote the fundamental weights corresponding to the basis $(\alpha_1, \dots, \alpha_r)$ by $\varpi_1, \dots, \varpi_r$. As is well known, they form a basis of P. Let $\mathbb{C}[G]$ be the algebra of regular functions on G. Then the restriction homomorphism $\mathbb{C}[G] \to \mathbb{C}[T] = \mathbb{C}P$ induces an isomorphism $\mathbb{C}[G]^G \xrightarrow{\sim} \mathbb{C}[T]^W = (\mathbb{C}P)^W$, see [17, §6]. For $\lambda \in P$ denote the basis element of $\mathbb{C}P$ corresponding to λ by $e(\lambda)$, denote the W-orbit of λ by $W \cdot \lambda$ and put $\mathrm{sym}(\lambda) = \sum_{\mu \in W\cdot\lambda} e(\mu)$. Then the $\mathrm{sym}(\varpi_i)$, $i = 1, \dots, r$, are algebraically independent generators of $(\mathbb{C}P)^W$. See [3, No. VI.3.4, Théorème 1].

For a field K, we denote the vector space of all $n \times n$ matrices over K by $\mathrm{Mat}_n = \mathrm{Mat}_n(K)$. Now assume that $K = \mathbb{C}$. In this section we denote the restriction to SL_n of the standard coordinate functionals on Mat_n by ξ_{ij}, $1 \leqslant i, j \leqslant n$. Furthermore, for $i \in \{1, \dots, n-1\}$, $s_i \in \mathbb{C}[\mathrm{SL}_n]$ is defined by $s_i(A) = \mathrm{tr}(\bigwedge^i A)$, where $\bigwedge^i A$ denotes the ith exterior power of A and tr denotes the trace. Then $\varpi_i = (\xi_{11} \cdots \xi_{ii})|_T$ and therefore

$$\mathrm{sym}(\varpi_i) = s_i|_T, \tag{$*$}$$

the ith elementary symmetric function in the $\xi_{jj}|_T$. See [16, 2.4].

In the general case we use the restriction theorem for $\mathbb{C}[G]$ and define $s_i \in \mathbb{C}[G]^G$ by $(*)$. So then $s_1, \dots, s_r$ are algebraically independent generators of $\mathbb{C}[G]^G$.

Identifying U^0 and $\mathbb{C}P$, we have $U^{0\tilde{W}} = (\mathbb{C}2P)^W$. Put $u_i = \bar{h}(\mathrm{sym}(2\varpi_i))$. Then $h(u_i) = \mathrm{sym}(2\varpi_i)$ and $u_1, \dots, u_r$ are algebraically independent generators of Z_1.

1.4. The cover π and the intersection $Z_0 \cap Z_1$

Let Φ^+ be the set of positive roots corresponding to the basis $(\alpha_1, \dots, \alpha_r)$ of Φ and let U_+ respectively U_- be the maximal unipotent subgroup of G corresponding to Φ^+ respectively $-\Phi^+$. If $\mathfrak{g} = \mathfrak{sl}_n$, then U_+ and U_- consist of the upper respectively lower triangular matrices in SL_n with ones on the diagonal. Put $\mathcal{O} = U_- T U_+$. Then $\mathcal{O}$ is a non-empty open and therefore dense subset of G. Furthermore, the group multiplication defines an isomorphism $U_- \times T \times U_+ \xrightarrow{\sim} \mathcal{O}$ of varieties. Put $\Omega = \mathrm{Maxspec}(Z_0)$.

In [7, (3.4)–(3.6)] there was constructed a group $\tilde{G}$ of automorphisms of $\hat{U} = \hat{Z}_0 \otimes_{Z_0} U$, where $\hat{Z}_0$ denotes the algebra of holomorphic functions on the complex analytic variety Ω. The group $\tilde{G}$ leaves $\hat{Z}_0$ and $\hat{Z} = \hat{Z}_0 \otimes_{Z_0} Z$ stable. In particular it acts by automorphisms on the complex analytic variety Ω. In [8] this action is called the "quantum coadjoint action."

In [8, §4] there was constructed an unramified cover $\pi : \Omega \to \mathcal{O}$ of degree 2^r. I give a short description of the construction of π. Put $\Omega^\pm = \mathrm{Maxspec}(Z_0^\pm)$. Then we have $\Omega = \Omega^- \times T \times \Omega^+$. Now $Z : \Omega \to T$ is defined as the projection on T, $X : \Omega \to U_+$ and $Y : \Omega \to U_-$ as the projection on $\Omega^\pm$ followed by some isomorphism $\Omega^\pm \xrightarrow{\sim} U_\pm$ and π is defined as YZ^2X (multiplication in G).[2] This means: $\pi(x) = Y(x)Z(x)^2X(x)$.

The following theorem says something about how $\tilde{G}$ and π are related to the "Harish-Chandra centre" Z_1 and the conjugation action of G on $\mathbb{C}[G]$. For more precise statements see [8, 5.4, 5.5 and §6].

Theorem 1. [8, Proposition 6.3, Theorem 6.7] *Consider π as a morphism to G. Then the comorphism $\pi^{\mathrm{co}} : \mathbb{C}[G] \to Z_0$ is injective and the following holds*:

[2] In [8] Z^2 is denoted by Z. The notation here comes from [9]. The centre of U is denoted by the same letter, but this will cause no confusion.

(i) $Z^{\tilde{G}} = Z_1$.[3]
(ii) π^{co} *induces an isomorphism* $\mathbb{C}[G]^G \xrightarrow{\sim} Z_0^{\tilde{G}} = Z_0 \cap Z_1$.
(iii) *The monomorphism* $(\mathbb{C}P)^W \xrightarrow{\sim} (\mathbb{C}P)^W$ *obtained by combining the isomorphism in* (ii) *with the restriction homomorphism* $\mathbb{C}[G] \to \mathbb{C}[T] = \mathbb{C}P$ *and* $h : Z_1 \to U^0 = \mathbb{C}P$, *is given by* $x \mapsto 2lx : P \to P$. *In particular* $h(Z_0 \cap Z_1) = (\mathbb{C}2lP)^W$.

I will give the proof of (iii). If we identify Z_0^0 with $\mathbb{C}[T]$, then the homomorphism $h'|_{Z_0} : Z_0 \to Z_0^0$ is the comorphism of a natural embedding $T \hookrightarrow \Omega$. Now we have a commutative diagram

$$\begin{array}{ccc} G & \xleftarrow{\pi} & \Omega \\ \uparrow & & \uparrow \\ T & \xleftarrow{t \mapsto t^2} & T \end{array}$$

Expressed in terms of the comorphisms this reads: $(x \mapsto 2x) \circ \mathrm{res}_{G,T} = \mathrm{res}_{\Omega,T} \circ \pi^{\mathrm{co}}$, where $\mathrm{res}_{G,T}$ and $\mathrm{res}_{\Omega,T}$ are the restrictions to T and the comorphism of the morphism between the tori is denoted by its restrictions to the character groups. Now we identify U^0 with $\mathbb{C}[T]$. Composing both sides on the left with $x \mapsto lx$ and using $(x \mapsto lx) \circ \mathrm{res}_{\Omega,T} = h'|_{Z_0} : Z_0 \to U^0 = \mathbb{C}P$ we obtain $(x \mapsto 2lx) \circ \mathrm{res}_{G,T} = h' \circ \pi^{\mathrm{co}}$. If we restrict both sides of this equality to $\mathbb{C}[G]^G$, then we can replace h' by h and we obtain the assertion.

1.5. Z_0 and Z_1 generate Z

Theorem 2. [8, Proposition 6.4, Theorem 6.4] *Let $u_1, \ldots, u_r$ be the elements of Z_1 defined in Subsection* 1.3. *Then the following holds*:

(i) *The multiplication $Z_1 \otimes_{Z_0 \cap Z_1} Z_0 \to Z$ is an isomorphism of algebras.*
(ii) *Z is a free Z_0-module of rank l^r with the restricted monomials $u_1^{k_1} \cdots u_r^{k_r}$, $0 \leqslant k_i < l$, as a basis.*

I give a proof of (ii). In [8, Proposition 6.4] it is proved that $(\mathbb{C}P)^W$ is a free $(\mathbb{C}lP)^W$-module of rank l^r with the restricted monomials (exponents $< l$) in the $\mathrm{sym}(\varpi_i)$ as a basis. The same holds then of course for $(\mathbb{C}2P)^W$, $(\mathbb{C}2lP)^W$ and the $\mathrm{sym}(2\varpi_i)$. But then the same holds for Z_1, $Z_0 \cap Z_1$ and the u_i by (iii) of Theorem 1. So the result follows from (i).

Recall that $\Omega = \Omega^- \times T \times \Omega^+$ and that $\Omega^\pm \cong U_\pm$. So Z_0 is a polynomial algebra in $\dim(\mathfrak{g})$ variables with r variables inverted. In particular its Krull dimension (which coincides with the transcendence degree of its field of fractions) is $\dim(\mathfrak{g})$. The same holds then for Z, since it is a finitely generated Z_0-module.

[3] $\tilde{G}$ is a group of automorphisms of the algebra $\hat{U}$ and does not leave Z stable. However, $S^{\tilde{G}}$ can be defined in the obvious way for every subset S of $\hat{U}$.

Let Z'_0 be a subalgebra of Z_0 containing $Z_1 \cap Z_0$. Then the multiplication $Z_1 \otimes_{Z_0 \cap Z_1} Z'_0 \to Z'_0 Z_1$ is an isomorphism of algebras by the above theorem. This gives us a way to determine generators and relations for $Z'_0 Z_1$: Let $s_1, \dots, s_r$ be the generators of $\mathbb{C}[G]^G$ defined in Subsection 1.3. Then $\pi^{\mathrm{co}}(s_1), \dots, \pi^{\mathrm{co}}(s_r)$ are generators of $Z_0 \cap Z_1 = Z'_0 \cap Z_1$ by Theorem 1(ii). Now assume that we have generators and relations for Z'_0. We use for Z_1 the generators $u_1, \dots, u_r$ defined in Subsection 1.3. For each $i \in \{1, \dots, r\}$ we can express $\pi^{\mathrm{co}}(s_i)$ as a polynomial g_i in the generators of Z'_0 and as a polynomial f_i in the u_j. Then the generators and relations for Z'_0 together with the u_i and the relations $f_i = g_i$ form a presentation of $Z'_0 Z_1$.[4]

The f_i can be determined as follows. Write $\mathrm{sym}(l\varpi_i)$ as a polynomial f_i in the $\mathrm{sym}(\varpi_j)$. Then $\mathrm{sym}(2l\varpi_i)$ is the same polynomial in the $\mathrm{sym}(2\varpi_j)$ and $\pi^{\mathrm{co}}(s_i) = f_i(u_1, \dots, u_r)$ by Theorem 1(iii).

Note that $\pi^{\mathrm{co}}(\mathbb{C}[\mathcal{O}]) = Z_0^- \mathbb{C}(2lP) Z_0^+$ and that $Z_0 = \pi^{\mathrm{co}}(\mathbb{C}[\mathcal{O}])[z_{\varpi_1}, \dots, z_{\varpi_r}]$.

Now assume that $G = \mathrm{SL}_n$. For $f \in \mathbb{C}[\mathrm{SL}_n]$ denote $f \circ \pi$ by $\tilde{f}$ and put $\tilde{Z}_0 = \pi^{\mathrm{co}}(\mathbb{C}[\mathrm{SL}_n])$. Then $\tilde{Z}_0$ is generated by the $\tilde{\xi}_{ij}$; it is a copy of $\mathbb{C}[\mathrm{SL}_n]$ in Z_0. Now $\mathcal{O}$ consists of the matrices $A \in \mathrm{SL}_n$ that have an LU-decomposition (without row permutations), that is, whose principal minors $\Delta_1(A), \dots, \Delta_{n-1}(A)$ are non-zero. So $\mathbb{C}[\mathcal{O}] = \mathbb{C}[\mathrm{SL}_n][\Delta_1^{-1}, \dots, \Delta_{n-1}^{-1}]$, $\pi^{\mathrm{co}}(\mathbb{C}[\mathcal{O}]) = \tilde{Z}_0[\tilde{\Delta}_1^{-1}, \dots, \tilde{\Delta}_{n-1}^{-1}]$ and

$$Z_0 = \tilde{Z}_0[z_{\varpi_1}, \dots, z_{\varpi_{n-1}}]\big[\tilde{\Delta}_1^{-1}, \dots, \tilde{\Delta}_{n-1}^{-1}\big].$$

Let $\mathrm{pr}_{\mathcal{O},T}$ be the projection of $\mathcal{O}$ on T. An easy computation shows that $\Delta_i|_{\mathcal{O}} = (\xi_{11} \cdots \xi_{ii}) \circ \mathrm{pr}_{\mathcal{O},T} = \varpi_i \circ \mathrm{pr}_{\mathcal{O},T}$ for $i = 1, \dots, n-1$.[5] So $\tilde{\Delta}_i = \varpi_i \circ \mathrm{pr}_{\mathcal{O},T} \circ \pi = \varpi_i \circ (t \mapsto t^2) \circ \mathrm{pr}_{\Omega,T} = 2\varpi_i \circ \mathrm{pr}_{\Omega,T} = z_{\varpi_i}^2$. In Subsection 3.3 we will determine generators and relations for $Z'_0 Z_1$, where $Z'_0 = \tilde{Z}_0[z_{\varpi_1}, \dots, z_{\varpi_{n-1}}]$ using the method mentioned above.

2. Rationality

We use the notation of Section 1 with the following modifications. The functions ξ_{ij}, $1 \leqslant i, j \leqslant n$, now denote the standard coordinate functionals on Mat_n and for $i \in \{1, \dots, n\}$, $s_i \in K[\mathrm{Mat}_n]$ is defined by $s_i(A) = \mathrm{tr}(\bigwedge^i A)$ for $A \in \mathrm{Mat}_n$. Then $\det(x\,\mathrm{id} - A) = x^n + \sum_{i=1}^n (-1)^i s_i(A) x^{n-i}$. This notation is in accordance with [16].

For $f \in \mathbb{C}[\mathrm{Mat}_n]$ we denote its restriction to SL_n by f' and we denote $\pi^{\mathrm{co}}(f')$ by $\tilde{f}$. So now $s'_1, \dots, s'_{n-1}$ and ξ'_{ij} are the functions $s_1, \dots, s_{n-1}$ and ξ_{ij} of Subsection 1.3 and the $\tilde{\xi}_{ij}$ are the same.

To prove the theorem below we need to look at the expressions of the functions s_i in terms of the ξ_{ij}. We use that those equations are linear in $\xi_{1n}, \xi_{2n}, \dots, \xi_{nn}$. The treatment

[4] This method was also used by Krylyuk in [14] to determine generators and relations for the centre of the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$. Our homomorphism $\pi^{\mathrm{co}} : \mathbb{C}[G] \to Z_0$ plays the rôle of Krylyuk's G-equivariant isomorphism $\eta : S(\mathfrak{g})^{(1)} \to Z_p$, where we use the notation of [16].

[5] For two $n \times n$ matrices A and B we have $\bigwedge^k(AB) = \bigwedge^k(A) \bigwedge^k(B)$. From this it follows that if either A is lower triangular or B is upper triangular, then $\Delta_k(AB) = \Delta_k(A)\Delta_k(B)$.

is completely analogous to that in [16, 4.1] (we use the same symbols R, M, d and $x_{\mathbf{a}}$) to which we refer for more explanation. Let R be the $\mathbb{Z}$-subalgebra of $\mathbb{C}[\mathrm{Mat}_n]$ generated by all ξ_{ij} with $j \neq n$.

Let ∂_{ij} denote differentiation with respect to the variable ξ_{ij} and set

$$M = \begin{bmatrix} \partial_{1n}(s_1) & \partial_{2n}(s_1) & \dots & \partial_{nn}(s_1) \\ \partial_{1n}(s_2) & \partial_{2n}(s_2) & \dots & \partial_{nn}(s_2) \\ \vdots & \vdots & \ddots & \vdots \\ \partial_{1n}(s_n) & \partial_{2n}(s_n) & \dots & \partial_{nn}(s_n) \end{bmatrix}, \qquad \mathbf{c} = \begin{bmatrix} \xi_{1n} \\ \xi_{2n} \\ \vdots \\ \xi_{nn} \end{bmatrix}, \qquad \mathbf{s} = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix}.$$

Then the matrix M has entries in R and the following vector equation holds:

$$M \cdot \mathbf{c} = \mathbf{s} + \mathbf{r}, \quad \text{where } \mathbf{r} \in R^n. \tag{1}$$

We denote the determinant of M by d. For $\mathbf{a} = (a_1, \dots, a_n) \in K^n$ we set

$$x_{\mathbf{a}} = \begin{bmatrix} 0 & \cdots & 0 & 0 & a_n \\ 1 & \cdots & 0 & 0 & a_{n-1} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & a_2 \\ 0 & \cdots & 0 & 1 & a_1 \end{bmatrix}.$$

Then the minimal polynomial of $x_{\mathbf{a}}$ equals $x^n - \sum_{i=1}^n a_i x^{n-i}$, $\det(x_{\mathbf{a}}) = (-1)^{n-1} a_n$ and $d(x_{\mathbf{a}}) = 1$ (compare Lemma 3 in [16]).

Theorem 3. *Z has a rational field of fractions.*

Proof. Denote the field of fractions of Z by $Q(Z)$. From Subsection 1.5 it is clear that $Q(Z)$ has transcendence degree $\dim(\mathfrak{sl}_n) = n^2 - 1$ over $\mathbb{C}$ and that it is generated as a field by the $n^2 + 2(n-1)$ variables $\tilde{\xi}_{ij}, u_1, \dots, u_{n-1}$ and $z_{\varpi_1}, \dots, z_{\varpi_{n-1}}$. To prove the assertion we will show that $Q(Z)$ is generated by the $n^2 - 1$ elements $\tilde{\xi}_{ij}$, $i \neq j$, $j \neq n$, $u_1, \dots, u_{n-1}$ and $z_{\varpi_1}, \dots, z_{\varpi_{n-1}}$. We will first eliminate the n generators $\tilde{\xi}_{1n}, \dots, \tilde{\xi}_{nn}$ and then the $n-1$ generators $\tilde{\xi}_{11}, \dots, \tilde{\xi}_{n-1\,n-1}$.

Applying the homomorphism $f \mapsto \tilde{f} = \pi^{\mathrm{co}} \circ (f \mapsto f') : \mathbb{C}[\mathrm{Mat}_n] \to Z_0$ to both sides of (1) we obtain the following equations in the $\tilde{\xi}_{ij}$ and $\tilde{s}_1, \dots, \tilde{s}_{n-1}$

$$\tilde{M} \cdot \tilde{\mathbf{c}} = \tilde{\mathbf{s}} + \tilde{\mathbf{r}}, \quad \text{where } \tilde{\mathbf{r}} \in \tilde{R}^n. \tag{2}$$

Here $\tilde{M}, \tilde{\mathbf{c}}, \tilde{\mathbf{s}}, \tilde{\mathbf{r}}$ have the obvious meaning, except that we put the last component of $\tilde{\mathbf{s}}$ and $\tilde{\mathbf{r}}$ equal to 0 respectively 1, and $\tilde{R}$ is the $\mathbb{Z}$-subalgebra of Z_0 generated by all $\tilde{\xi}_{ij}$ with $j \neq n$. Choosing $\mathbf{a}$ such that $a_n = (-1)^{n-1}$ we have $x_{\mathbf{a}} \in \mathrm{SL}_n$. Since $d(x_{\mathbf{a}}) = 1$, we have $d' \neq 0$ and therefore $\det(\tilde{M}) = \tilde{d} \neq 0$. Furthermore, for $i = 1, \dots, n-1$, $(\tilde{\mathbf{s}})_i = \tilde{s}_i \in Z_0 \cap Z_1$ and Z_1 is generated by $u_1, \dots, u_{n-1}$. It follows that $\tilde{\xi}_{1n}, \dots, \tilde{\xi}_{nn}$ are in the subfield of $Q(Z)$ generated by the $\tilde{\xi}_{ij}$ with $j \neq n$ and $u_1, \dots, u_{n-1}$.

Now we will eliminate the generators $\tilde{\xi}_{11}, \dots, \tilde{\xi}_{n-1\,n-1}$. We have

$$z_{\varpi_1}^2 = \tilde{\Delta}_1 = \tilde{\xi}_{11}$$

and for $k = 2, \dots, n-1$ we have, by the Laplace expansion rule,

$$z_{\varpi_k}^2 = \tilde{\Delta}_k = \tilde{\xi}_{kk}\tilde{\Delta}_{k-1} + t_k = \tilde{\xi}_{kk} z_{\varpi_{k-1}}^2 + t_k,$$

where t_k is in the $\mathbb{Z}$-subalgebra of Z generated by the $\tilde{\xi}_{ij}$ with $i, j \leqslant k$ and $(i, j) \neq (k, k)$. It follows by induction on k that for $k = 1, \dots, n-1$, $\tilde{\xi}_{11}, \dots, \tilde{\xi}_{kk}$ are in the subfield of $Q(Z)$ generated by the z_{ϖ_i} with $i \leqslant k$ and the $\tilde{\xi}_{ij}$ with $i, j \leqslant k$ and $i \neq j$. $\square$

3. Unique factorisation

Recall that *Nagata's lemma* asserts the following: If x is a non-zero prime element of a Noetherian integral domain S such that $S[x^{-1}]$ is a UFD, then S is a UFD. See [11, Lemma 19.20]. Here an element is called prime if it generates a prime ideal. The non-zero prime elements of an integral domain are always irreducible and in a UFD the converse holds. In Theorem 4 we will see that, by Nagata's lemma, it suffices to show that the algebra $Z/(\tilde{d})$ is an integral domain in order to prove that Z is a UFD. To prove this we will show by induction that the two sequences of algebras (to be defined later):

$$K[\mathrm{SL}_n]/(d') \cong \bar{A}(K) = \bar{B}_{0,0}(K) \subseteq \bar{B}_{0,1}(K) \subseteq \cdots \subseteq \bar{B}_{0,n-1}(K) = \bar{B}_0(K)$$

in characteristic p and

$$\bar{B}_0(\mathbb{C}) \subseteq \bar{B}_1(\mathbb{C}) \subseteq \cdots \subseteq \bar{B}_{n-1}(\mathbb{C}) = \bar{B}(\mathbb{C})$$

over $\mathbb{C}$, consist of integral domains. Lemma 2 is, among other things, needed to show that $\bar{A}(K) \cong K[\mathrm{SL}_n]/(d')$ is an integral domain. Lemmas 3 and 4 are needed to obtain bases over $\mathbb{Z}$ (see Proposition $\bar{1}$), which, in turn, is needed to pass to fields of positive characteristic and to apply mod p reduction (see Lemma 6).

3.1. The case $n = 2$

In this subsection we show that the centre of $U_{\varepsilon,P}(\mathfrak{sl}_2)$ is always a UFD, without any extra assumptions on l. The standard generators for $U = U_{\varepsilon,P}(\mathfrak{sl}_2)$ are E, F, K_ϖ and K_ϖ^{-1}. Put $K = K_\alpha = K_\varpi^2$, $z_1 = z_\varpi = K_\varpi^l$, $z = z_\alpha = z_1^2 = K^l$. Furthermore, following [8, 3.1], we put $c = (\varepsilon - \varepsilon^{-1})^l$, $x = -cz^{-1}E^l$, $y = cF^l$. Then x, y and z_1 are algebraically independent over $\mathbb{C}$ and $Z_0 = \mathbb{C}[x, y, z_1][z_1^{-1}]$ (see [8, §3]).

We have $U^0 = \mathbb{C}[K_\varpi, K_\varpi^{-1}]$ and $U^{0\tilde{W}} = \mathbb{C}[K, K^{-1}]^W = \mathbb{C}[K + K^{-1}]$. Identifying U^0 and $\mathbb{C}P$, we have $\mathrm{sym}(2\varpi) = K + K^{-1}$ and $\mathrm{sym}(2l\varpi) = z + z^{-1}$. Put $u = \bar{h}(\mathrm{sym}(2\varpi))$. By the restriction theorem for U, Z_1 is a polynomial algebra in u. Denote the trace map on Mat_2 by tr. Then $\mathrm{tr}|_T = \mathrm{sym}(\varpi)$. By the restriction theorem for $\mathbb{C}[G]$ and Theorem 1(ii),

$\tilde{\mathrm{tr}}$ generates $Z_0 \cap Z_1$. Furthermore $\tilde{\mathrm{tr}} = \bar{h}(z + z^{-1})$, by Theorem 1(iii). Let $f \in \mathbb{C}[u]$ be the polynomial with $z + z^{-1} = f(K + K^{-1})$. Then $\tilde{\mathrm{tr}} = f(u)$. From the formulas in [8, 5.2] it follows that $\tilde{\mathrm{tr}} = -zxy + z + z^{-1}$.

By the construction from Subsection 1.5 (we take $Z_0' = Z_0$), Z is isomorphic to the quotient of the localised polynomial algebra $\mathbb{C}[x, y, z_1, u][z_1^{-1}]$ by the ideal generated by $-z_1^2xy + z_1^2 + z_1^{-2} - f(u)$. Clearly x, u and z_1 generate the field of fractions of Z. In particular they are algebraically independent. So $Z[x^{-1}]$ is isomorphic to the localised polynomial algebra $\mathbb{C}[x, z_1, u][z_1^{-1}, x^{-1}]$ and therefore a UFD. By Nagata's lemma it suffices to show that x is a prime element in Z. But $Z/(x)$ is isomorphic to the quotient of $\mathbb{C}[y, z_1, u][z_1^{-1}]$ by the ideal generated by $z_1^2 + z_1^{-2} - f(u)$. This ideal is also generated by $z_1^4 - f(u)z_1^2 + 1$. So it suffices to show that $z_1^4 - f(u)z_1^2 + 1$ is irreducible in $\mathbb{C}[y, z_1, u][z_1^{-1}]$. From the fact that f is of odd degree $l > 0$ (see e.g. Lemma 4 below), one easily deduces that $z_1^4 - f(u)z_1^2 + 1$ is irreducible in $\mathbb{C}[z_1, u]$ and therefore also in $\mathbb{C}[y, z_1, u]$. Clearly $z_1^4 - f(u)z_1^2 + 1$ is not invertible in $\mathbb{C}[y, z_1, u][z_1^{-1}]$, so it is also irreducible in this ring.

3.2. SL_n *and the function d*

The next lemma is needed for the proof of Theorem 4. The Jacobian matrix below consists of the partial derivatives of the functions in question with respect to the variables ξ_{ij}.

Lemma 1. *If $n \geqslant 3$, then there exists a matrix $A \in \mathrm{SL}_n(\mathbb{Z})$ such that $d(A) = 0$ and such that some $2n$-th order minor of the Jacobian matrix of $(s_1, \ldots, s_n, d, \Delta_1, \ldots, \Delta_{n-1})$ is ± 1 at A.*

Proof. The computations below are very similar to those in [16, Section 6]. We denote by $\mathcal{X}$ the $(n \times n)$-matrix (ξ_{ij}) and for an $(n \times n)$-matrix $B = (b_{ij})$ and $\Lambda_1, \Lambda_2 \subseteq \{1, \ldots, n\}$ we denote by B_{Λ_1, Λ_2} the matrix $(b_{ij})_{i \in \Lambda_1, j \in \Lambda_2}$, where the indices are taken in the natural order.

In the computations below we will use the following two facts:

For $\Lambda_1, \Lambda_2 \subseteq \{1, \ldots, n\}$ with $|\Lambda_1| = |\Lambda_2|$ we have

$$\partial_{ij}\big(\det(\mathcal{X}_{\Lambda_1, \Lambda_2})\big) = \begin{cases} (-1)^{n_1(i)+n_2(j)} \det(\mathcal{X}_{\Lambda_1 \setminus \{i\}, \Lambda_2 \setminus \{j\}}) & \text{when } (i, j) \in (\Lambda_1 \times \Lambda_2), \\ 0 & \text{when } (i, j) \notin (\Lambda_1 \times \Lambda_2), \end{cases}$$

where $n_1(i)$ denotes the position in which i occurs in Λ_1 and similarly for $n_2(j)$.

For $k \leqslant n$ we have $s_k = \sum_\Lambda \det(\mathcal{X}_{\Lambda, \Lambda})$ where the sum ranges over all k-subsets Λ of $\{1, \ldots, n\}$.

Put $\alpha = ((1\,1), (2\,2), (2\,3), \ldots, (2\,n-1), (n\,n), (n-1\,n), \ldots, (2\,n), (2\,1), (1\,2))$, and let α_i denote the ith component of α. We let A be the following $(n \times n)$-matrix:

$$A = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & (-1)^n \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}.$$

The columns of the Jacobian matrix are indexed by the pairs (i, j) with $1 \leqslant i, j \leqslant n$. Let M_α be the $2n$-square submatrix of the Jacobian matrix consisting of the columns with indices from α. By permuting in A the first row to the last position and interchanging the first two columns, we see that $\det(A) = 1$. We will show that $d(A) = 0$ and that the minor $d_\alpha := \det(M_\alpha)$ of the Jacobian matrix is ± 1 at A.

First we consider the Δ_k, $k \in \{1, \ldots, n-1\}$. By inspecting the matrix A and using the fact that $\partial_{ij}\Delta_k = 0$ if $i > k$ or $j > k$, we deduce the following facts:

$$(\partial_{2i}\Delta_k)(A) = \begin{cases} \pm 1 & \text{if } i = k, \\ 0 & \text{if } i > k, \end{cases} \quad \text{for } i, k \in \{1, \ldots, n-1\},\ i \neq 1,$$

$$(\partial_{11}\Delta_1)(A) = 1,$$

$$(\partial_{12}\Delta_k)(A) = (\partial_{21}\Delta_k)(A) = 0 \quad \text{for all } k \in \{1, \ldots, n-1\},$$

and

$$(\partial_{in}\Delta_k)(A) = 0 \quad \text{for all } k \in \{1, \ldots, n-1\} \text{ and all } i \in \{1, \ldots, n\}.$$

Now we consider the s_k. Let $i \in \{1, \ldots, n\}$ and let $\Lambda \subseteq \{1, \ldots, n\}$. Assume that $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))$ is non-zero at A. Then we have:

- $i, n \in \Lambda$;
- $j \in \Lambda \Rightarrow j - 1 \in \Lambda$ for all j with $4 \leqslant j \leqslant n$ and $j \neq i$, since otherwise there would be a zero row (in $\mathcal{X}_{\Lambda\setminus\{i\},\Lambda\setminus\{n\}}(A) = A_{\Lambda\setminus\{i\},\Lambda\setminus\{n\}}$);
- $j \in \Lambda \Rightarrow j + 1 \in \Lambda$ for all j with $3 \leqslant j \leqslant n - 1$, since otherwise there would be a zero column.

First assume that $i \geqslant 3$ and that $|\Lambda| \leqslant n - i + 1$. Then it follows that $\Lambda = \{i, \ldots, n\}$ and that $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))(A) = \pm 1$.

Next assume that $i = 2$. Then it follows that either $\Lambda = \{2, \ldots, n\}$ or $\Lambda = \{1, \ldots, n\}$. In the first case we have $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))(A) = (-1)^{1+n-1} = (-1)^n$. In the second case we have $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))(A) = (-1)^{2+n} = (-1)^n$.

Now assume that $i = 1$. Then it follows that either $\Lambda = \{1, 3, \ldots, n\}$ or $\Lambda = \{1, \ldots, n\}$. In the first case we have $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))(A) = (-1)^{1+n-1} = (-1)^n$. In the second case we have $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))(A) = (-1)^{1+n} \cdot (-1) = (-1)^n$.

So for $i, k \in \{1, \dots, n\}$ we have:

$$(\partial_{in} s_k)(A) = \begin{cases} \pm 1 & \text{if } i \geqslant 3 \text{ and } i + k = n + 1, \\ 0 & \text{if } i \geqslant 3 \text{ and } i + k < n + 1, \\ (-1)^n & \text{if } i \in \{1, 2\} \text{ and } k \in \{n - 1, n\}, \\ 0 & \text{if } i \in \{1, 2\} \text{ and } k < n - 1. \end{cases}$$

It follows from the above equalities that in $M(A)$ the first 2 columns are equal. So $d(A) = \det(M(A)) = 0$.

Let $\Lambda \subseteq \{1, \dots, n\}$. Assume that $\partial_{12}(\det(\mathcal{X}_{\Lambda,\Lambda}))$ is non-zero at A. Then $1, 2 \in \Lambda$ and the first row is zero. A contradiction. So $\partial_{12}(\det(\mathcal{X}_{\Lambda,\Lambda}))$ is zero at A. Now assume that $\partial_{21}(\det(\mathcal{X}_{\Lambda,\Lambda}))$ is non-zero at A. Then

- $1, 2 \in \Lambda$;
- $n \in \Lambda$, since otherwise the first row would be zero;
- $j \in \Lambda \Rightarrow j - 1 \in \Lambda$ for all j with $4 \leqslant j \leqslant n$, since otherwise there would be a zero row.

So $\Lambda = \{1, \dots, n\}$ and $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))(A) = \pm 1$. Thus we have $(\partial_{12} s_k)(A) = 0$ for all $k \in \{1, \dots, n\}$ and

$$(\partial_{21} s_k)(A) = \begin{cases} \pm 1 & \text{if } k = n, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we consider the function d. Let $i \in \{1, \dots, n\}$, let $\Lambda \subseteq \{1, \dots, n\}$ and assume that $\partial_{12}\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))$ is non-zero at A. Then we have:

- $1, 2, i, n \in \Lambda$ and $i \neq 1$;
- $i = 2$, since otherwise the first row would be zero;
- $j \in \Lambda \Rightarrow j - 1 \in \Lambda$ for all j with $4 \leqslant j \leqslant n$, since otherwise there would be a zero row.

It follows that $i = 2$, $\Lambda = \{1, \dots, n\}$ and $\partial_{12}\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda})) = \pm 1$. So for $i, k \in \{1, \dots, n\}$ we have:

$$(\partial_{12}\partial_{in} s_k)(A) = \begin{cases} \pm 1 & \text{if } (i, k) = (2, n), \\ 0 & \text{if } (i, k) \neq (2, n). \end{cases}$$

We have

$$d = \sum_{\pi \in \mathfrak{S}_n} \operatorname{sgn}(\pi) \partial_{\pi(1)n}(s_1) \cdots \partial_{\pi(n)n}(s_n). \tag{3}$$

So, by the above,

$$(\partial_{12} d)(A) = \Big(\sum \operatorname{sgn}(\pi) \partial_{\pi(1)n}(s_1) \partial_{\pi(2)n}(s_2) \cdots \partial_{\pi(n-1)n}(s_{n-1}) \partial_{12}\partial_{2n}(s_n)\Big)(A),$$

where the sum is over all $\pi \in \mathfrak{S}_n$ with $\pi(n) = 2$. From what we know about the $\partial_{in} s_k$ we deduce that the only permutation that survives in the above sum is given by $(\pi(1), \dots, \pi(n)) = (n, n-1, \dots, 3, 1, 2)$ and that $(\partial_{12} d)(A) = \pm 1$.

If we permute the rows of $M_\alpha(A)$ in the order given by $\Delta_1, \dots, \Delta_{n-1}, s_1, \dots, s_n, d$ and take the columns in the order given by α, then the resulting matrix is lower triangular with ± 1's on the diagonal. So we can conclude that $d_\alpha(A) = \det(M_\alpha(A)) = \pm 1$. $\square$

In the remainder of this subsection K denotes an algebraically closed field.

Lemma 2.

(i) *d is an irreducible element of $K[\mathrm{Mat}_n]$.*
(ii) *$K[\mathrm{SL}_n]$ is a UFD.*
(iii) *The invertible elements of $K[\mathrm{SL}_n]$ are the non-zero scalars.*
(iv) *$d', \Delta'_1, \dots, \Delta'_{n-1}$ is are mutually inequivalent irreducible elements of $K[\mathrm{SL}_n]$.*

Proof. (i) The proof of this is completely analogous to that of Proposition 3 in [16]. One now has to work with the maximal parabolic subgroup P of GL_n that consists of the invertible matrices (a_{ij}) with $a_{ni} = 0$ for all $i < n$. The element d is then a semi-invariant of P with the weight $\det \cdot \xi_{nn}^{-n}$ (the restriction of this weight to the maximal torus of diagonal matrices is $n\varpi_{n-1}$).

(ii) In fact it is well known that the algebra of regular functions $K[G]$ of a simply connected semi-simple algebraic group G over K is a UFD. See [15, the corollary to Proposition 1].

(iii) and (iv). Since Δ'_{n-1} is not everywhere non-zero on SL_n, it is not invertible in $K[\mathrm{SL}_n]$. From the Laplace expansion for det with respect to the last row or the last column it is clear that we can eliminate ξ_{nn} using the relation $\det = 1$, if we make Δ_{n-1} invertible. So we have an isomorphism $K[\mathrm{SL}_n][\Delta'^{-1}_{n-1}] \cong K[(\xi_{ij})_{(i,j)\neq(n,n)}][\Delta^{-1}_{n-1}]$. It maps $d', \Delta'_1, \dots, \Delta'_{n-1}$ to respectively $d, \Delta_1, \dots, \Delta_{n-1}$, since these polynomials do not contain the variable ξ_{nn}. The invertible elements of $K[(\xi_{ij})_{(i,j)\neq(n,n)}][\Delta^{-1}_{n-1}]$ are the elements $\alpha\Delta^k_{n-1}$, $\alpha \in K \setminus \{0\}$, $k \in \mathbb{Z}$, since Δ_{n-1} is irreducible in $K[(\xi_{ij})_{(i,j)\neq(n,n)}]$. So the invertible elements of $K[\mathrm{SL}_n][\Delta'^{-1}_{n-1}]$ are the elements $\alpha\Delta'^k_{n-1}$, $\alpha \in K \setminus \{0\}$, $k \in \mathbb{Z}$. This shows that Δ'_{n-1} is irreducible in $K[\mathrm{SL}_n]$, since otherwise there would be more invertible elements in $K[\mathrm{SL}_n][\Delta'^{-1}_{n-1}]$. So the invertible elements of $K[\mathrm{SL}_n]$ are the non-zero scalars. Since d and the Δ_i are not scalar multiples of each other, all that remains is to show that d' and $\Delta'_1, \dots, \Delta'_{n-2}$ are irreducible. We only do this for d', the argument for the Δ'_i is completely similar. Since d is prime in $K[(\xi_{ij})_{(i,j)\neq(n,n)}]$ and d does not divide Δ_{n-1}, it follows that d is prime in $K[(\xi_{ij})_{(i,j)\neq(n,n)}][\Delta^{-1}_{n-1}]$ and therefore that d' is prime in $K[\mathrm{SL}_n][\Delta'^{-1}_{n-1}]$. To show that d' is prime in $K[\mathrm{SL}_n]$ it suffices to show that for every $f \in K[\mathrm{SL}_n]$, $\Delta'_{n-1} f \in (d')$ implies $f \in (d')$. So assume that

$$\Delta'_{n-1} f = g d' \qquad (*)$$

for some $f, g \in K[\mathrm{SL}_n]$. If we take $\mathbf{a} \in K^n$ such that $a_n = (-1)^{n-1}$, then we have $x_{\mathbf{a}} \in \mathrm{SL}_n$, $d'(x_{\mathbf{a}}) = 1$ and $\Delta'_{n-1}(x_{\mathbf{a}}) = 0$. So Δ'_{n-1} does not divide d'. But then Δ'_{n-1} divides g, since Δ'_{n-1} is irreducible. Cancelling a factor Δ'_{n-1} on both sides of $(*)$, we obtain that $f \in (d')$. $\square$

3.3. Generators and relations and a $\mathbb{Z}$-form for $\tilde{Z}_0[z_{\varpi_1}, \ldots, z_{\varpi_{n-1}}]Z_1$

For the basics about monomial orderings and Gröbner bases I refer to [5].

Lemma 3. *If we give the monomials in the variables ξ_{ij} the lexicographic monomial ordering for which $\xi_{nn} > \xi_{n\,n-1} > \cdots > \xi_{n1} > \xi_{n-1\,n} > \cdots > \xi_{n-1\,1} > \cdots > \xi_{11}$, then* det *has leading term $\pm\xi_{nn} \cdots \xi_{22}\xi_{11}$ and d has leading term $\pm\xi_{n\,n-1}^{n-1} \cdots \xi_{32}^2\xi_{21}$.*

Proof. I leave the proof of the first assertion to the reader. For the second assertion we use the notation and the formulas of Subsection 3.2. The leading term of a non-zero polynomial f is denoted by $\mathrm{LT}(f)$. Let $i \in \{1, \ldots, n\}$ and $\Lambda \subseteq \{1, \ldots, n\}$ with $|\Lambda| = k \geqslant 2$ and assume that $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda})) \neq 0$. Then $i, n \in \Lambda$. Now we use the fact that no monomial in $\partial_{in}(\det(\mathcal{X}_{\Lambda,\Lambda}))$ contains a variable with row index equal to i or with column index equal to n or a product of two variables which have the same row or column index.

First assume that $i > n - k + 1$. Then

$$\mathrm{LT}\big(\partial_{in}\big(\det(\mathcal{X}_{\Lambda,\Lambda})\big)\big) \leqslant \pm\xi_{n\,n-1} \cdots \xi_{i+1\,i}\xi_{i-1\,i-1} \cdots \xi_{n-k+1\,n-k+1}$$

with equality if and only if $\Lambda = \{n, n-1, \ldots, n-k+1\}$. Now assume that $i = n - k + 1$. Then

$$\mathrm{LT}\big(\partial_{in}\big(\det(\mathcal{X}_{\Lambda,\Lambda})\big)\big) \leqslant \pm\xi_{n\,n-1} \cdots \xi_{n-k+2\,n-k+1}$$

with equality if and only if $\Lambda = \{n, n-1, \ldots, n-k+1\}$. Finally assume that $i < n-k+1$. Then

$$\mathrm{LT}\big(\partial_{in}\big(\det(\mathcal{X}_{\Lambda,\Lambda})\big)\big) \leqslant \pm\xi_{n\,n-1} \cdots \xi_{n-k+3\,n-k+2}\xi_{n-k+2\,i}$$

with equality if and only if $\Lambda = \{n, n-1, \ldots, n-k+2, i\}$.

So for $i, k \in \{1, \ldots, n\}$ with $k \geqslant 2$ we have:

$$\mathrm{LT}(\partial_{in}s_k) = \begin{cases} \pm\xi_{n\,n-1} \cdots \xi_{i+1\,i}\xi_{i-1\,i-1} \cdots \xi_{n-k+1\,n-k+1} & \text{if } i + k > n + 1, \\ \pm\xi_{n\,n-1} \cdots \xi_{n-k+2\,n-k+1} & \text{if } i + k = n + 1, \\ \pm\xi_{n\,n-1} \cdots \xi_{n-k+3\,n-k+2}\xi_{n-k+2\,i} & \text{if } i + k < n + 1. \end{cases}$$

In particular $\mathrm{LT}(\partial_{in}s_k) \leqslant \pm\xi_{n\,n-1} \cdots \xi_{n-k+1\,n-k+1}$ with equality if and only if $i + k = n + 1$. But then, by Eq. (3), $\mathrm{LT}(d) = \mathrm{LT}(\partial_{nn}s_1)\mathrm{LT}(\partial_{n-1\,n}s_2) \cdots \mathrm{LT}(\partial_{1n}s_n) = \pm\xi_{n\,n-1}^{n-1} \cdots \xi_{32}^2\xi_{21}$. $\square$

Recall that the degree reverse lexicographical ordering on the monomials $u^\alpha = u_1^{\alpha_1} \cdots u_k^{\alpha_k}$ in the variables $u_1, \ldots, u_k$ is defined as follows: $u^\alpha > u^\beta$ if $\deg(u^\alpha) > \deg(u^\beta)$ or $\deg(u^\alpha) = \deg(u^\beta)$ and $\alpha_i < \beta_i$ for the last index i with $\alpha_i \neq \beta_i$.

Lemma 4. *Let $f_i \in \mathbb{Z}[u_1, \dots, u_{n-1}]$ be the polynomial such that* $\mathrm{sym}(l\varpi_i) = f_i(\mathrm{sym}(\varpi_1), \dots, \mathrm{sym}(\varpi_{n-1}))$. *If we give the monomials in the u_i the degree reverse lexicographic monomial ordering for which $u_1 > \dots > u_{n-1}$, then f_i has leading term u_i^l. Furthermore, the monomials that appear in $f_i - u_i^l$ are of total degree $\leqslant l$ and have exponents $< l$.*[6]

Proof. Let σ_i be the ith elementary symmetric function in the variables $x_1, \dots, x_n$ and let $\lambda_i \in P = X(T)$ be the character $A \mapsto A_{ii}$ of T. Then $\mathrm{sym}(\varpi_i) = \sigma_i(e(\lambda_1), \dots, e(\lambda_n))$ for $i \in \{1, \dots, n-1\}$. So the f_i can be found as follows. For $i \in \{1, \dots, n-1\}$, determine $F_i \in \mathbb{Z}[u_1, \dots, u_n]$ such that $\sigma_i(x_1^l, \dots, x_n^l) = F_i(\sigma_1, \dots, \sigma_n)$. Then $f_i = F_i(u_1, \dots, u_{n-1}, 1)$. It now suffices to show that for $i \in \{1, \dots, n-1\}$, $F_i - u_i^l$ is a $\mathbb{Z}$-linear combination of monomials in the u_j that have exponents $< l$, are of total degree $\leqslant l$ and that contain some u_j with $j > i$ (the monomials that contain u_n will become of total degree $< l$ when u_n is replaced by 1).

Fix $i \in \{1, \dots, n-1\}$. Consider the following properties of a monomial in the x_j:

(x1) the monomial contains at least $i+1$ variables;
(x2) the exponents are $\leqslant l$;
(x3) the number of exponents equal to l is $\leqslant i$;

and the following properties of a monomial in the u_j:

(u1) the monomial contains a variable u_j for some $j > i$;
(u2) the total degree is $\leqslant l$;
(u3) the exponents are $< l$.

Let h be a symmetric polynomial in the x_i and let H be the polynomial in the u_i such that $h = H(\sigma_1, \dots, \sigma_n)$. Give the monomials in the x_i the lexicographic monomial ordering for which $x_1 > \dots > x_n$. We will show by induction on the leading monomial of h that if each monomial that appears in h has property (x1) respectively property (x2) respectively properties (x1), (x2) and (x3), then each monomial that appears in H has property (u1) respectively property (u2) respectively properties (u1), (u2) and (u3). Let $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the leading monomial of h. Then $\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_n$. Put $\beta = (\alpha_1 - \alpha_2, \dots, \alpha_{n-1} - \alpha_n, \alpha_n)$. Let k be the last index for which $\alpha_k \neq 0$. Then $\beta = (\alpha_1 - \alpha_2, \dots, \alpha_{k-1} - \alpha_k, \alpha_k, 0, \dots, 0)$. If x^α has property (x1), then $k \geqslant i+1$, u^β has property (u1) and the monomials that appear in σ^β have property (x1), since σ_k appears in σ^β.

If x^α has property (x2), then $\alpha_1 \leqslant l$, u^β is of total degree $\alpha_1 \leqslant l$ and the monomials that appear in σ^β have exponents $\leqslant \beta_1 + \dots + \beta_k = \alpha_1 \leqslant l$. Now assume that x^α has properties (x1), (x2) and (x3). For $j < k$ we have $\beta_j = \alpha_j - \alpha_{j+1} < l$, since $\alpha_{j+1} \neq 0$. So we have to show that $\beta_k = \alpha_k < l$. If α_k were equal to l, then we would have $\alpha_1 = \dots = \alpha_k = l$, by (x2). This contradicts (x3), since we have $k \geqslant i+1$ by (x1). Finally we show that the

[6] So our f_i are related to the polynomials $P_i = x_i^l - \sum_\mu d_{i\mu} x_\mu$ from the proof of Proposition 6.4 in [8] as follows: $P_i = f_i(x_1, \dots, x_{n-1}) - \mathrm{sym}(l\varpi_i)$. In particular $d_{i0} = \mathrm{sym}(l\varpi_i)$ and $d_{i\mu} \in \mathbb{Z}$ for all $\mu \in P \setminus \{0\}$ (we are, of course, in the situation that $\mathfrak{g} = \mathfrak{sl}_n$).

monomials that appear in σ^β have property (x3). If $\alpha_1 < l$, then all these monomials have exponents $< l$. So assume $\alpha_1 = l$. Let j be the smallest index for which $\beta_j \neq 0$. Then the number of exponents equal to l in a monomial that appears in σ^β is $\leqslant j$. On the other hand, $\alpha_1 = \cdots = \alpha_j = l$. So we must have $j \leqslant i$, since x^α has property (x3).

Now we can apply the induction hypothesis to $h - c\sigma^\beta$, where c is the leading coefficient of h.

The assertion about $F_i - u_i^l$ now follows, because the monomials that appear in $\sigma_i(x_1^l, \dots, x_n^l) - \sigma_i^l$ have the properties (x1), (x2) and (x3). □

From now on we denote z_{ϖ_i} by z_i.[7] Let $\mathbb{Z}[\mathrm{SL}_n]$ be the $\mathbb{Z}$-subalgebra of $\mathbb{C}[\mathrm{SL}_n]$ generated by the ξ'_{ij} and A be the $\mathbb{Z}$-subalgebra of Z generated by the $\tilde{\xi}_{ij}$. So $A = \pi^{\mathrm{co}}(\mathbb{Z}[\mathrm{SL}_n])$. Let B be the $\mathbb{Z}$-subalgebra generated by the elements $\tilde{\xi}_{ij}, u_1, \dots, u_{n-1}$ and $z_1, \dots, z_{n-1}$. For a commutative ring R we put $A(R) = R \otimes_{\mathbb{Z}} A$ and $B(R) = R \otimes_{\mathbb{Z}} B$. Clearly we can identify $A(\mathbb{C})$ with $\tilde{Z}_0$. In the proposition below "natural homomorphism" means a homomorphism that maps ξ_{ij} to $\tilde{\xi}_{ij}$ and, if this applies, the variables u_i and z_i to the equally named elements of Z. The polynomials f_i below are the ones defined in Lemma 4.

Proposition 1. *The following holds*:

- (i) *The kernel of the natural homomorphism from the polynomial algebra* $\mathbb{Z}[(\xi_{ij})_{ij}, u_1, \dots, u_{n-1}, z_1, \dots, z_{n-1}]$ *to* B *is generated by the elements* $\det - 1, f_1 - s_1, \dots, f_{n-1} - s_{n-1}, z_1^2 - \Delta_1, \dots, z_{n-1}^2 - \Delta_{n-1}$.
- (ii) *The homomorphism* $B(\mathbb{C}) \to Z$*, given by the universal property of ring transfer, is injective.*
- (iii) A *is a free* $\mathbb{Z}$*-module and* B *is a free* A*-module with the monomials* $u_1^{k_1} \cdots u_{n-1}^{k_{n-1}} z_1^{m_1} \cdots z_{n-1}^{m_{n-1}}$, $0 \leqslant k_i < l$, $0 \leqslant m_i < 2$*, as a basis.*
- (iv) $A[z_1, \dots, z_{n-1}] \cap Z_1 = A \cap Z_1 = \mathbb{Z}[\tilde{s}_1, \dots, \tilde{s}_{n-1}]$ *and* $B \cap Z_1$ *is a free* $A \cap Z_1$*-module with the monomials* $u_1^{k_1} \cdots u_{n-1}^{k_{n-1}}$, $0 \leqslant k_i < l$*, as a basis.*

Proof. Let Z'_0 be the $\mathbb{C}$-subalgebra of Z generated by the $\tilde{\xi}_{ij}$ and $z_1, \dots, z_{n-1}$. As we have seen in Subsection 1.5, the z_i satisfy the relations $z_i^2 = \tilde{\Delta}_i$. The $\tilde{\Delta}_i$ are part of a generating transcendence basis of the field of fractions $\mathrm{Fr}(\tilde{Z}_0)$ of $\tilde{Z}_0$ by arguments very similar to those at the end of the proof of Theorem 3. This shows that the monomials $z_1^{m_1} \cdots z_{n-1}^{m_{n-1}}$, $0 \leqslant m_i < 2$, form a basis of $\mathrm{Fr}(Z'_0)$ over $\mathrm{Fr}(\tilde{Z}_0)$ and of Z'_0 over $\tilde{Z}_0$. It follows that the kernel of the natural homomorphism from the polynomial algebra $\mathbb{C}[(\xi_{ij})_{ij}, z_1, \dots, z_{n-1}]$ to Z'_0 is generated by the elements $\det - 1, z_1^2 - \Delta_1, \dots, z_{n-1}^2 - \Delta_{n-1}$. So we have generators and relations for Z'_0. By the construction from Subsection 1.5 we then obtain that the kernel I of the natural homomorphism from the polynomial algebra $\mathbb{C}[(\xi_{ij})_{ij}, u_1, \dots, u_{n-1}, z_1, \dots, z_{n-1}]$ to $Z'_0 Z_1$ is generated by the elements $\det - 1, f_1 - s_1, \dots, f_{n-1} - s_{n-1}, z_1^2 - \Delta_1, \dots, z_{n-1}^2 - \Delta_{n-1}$.

[7] In [8,9] z_{α_i} is denoted by z_i.

Now we give the monomials in the variables $(\xi_{ij})_{ij}, u_1, \dots, u_{n-1}, z_1, \dots, z_{n-1}$ a monomial ordering which is the lexicographical product of an arbitrary monomial ordering on the monomials in the z_i, the monomial ordering of Lemma 4 on the monomials in the u_i and the monomial ordering of Lemma 3 on the ξ_{ij}.[8] Then the ideal generators mentioned above have leading monomials $\xi_{nn}\cdots\xi_{22}\xi_{11}, u_1^l, \dots, u_{n-1}^l, z_1^2, \dots, z_{n-1}^2$ and the leading coefficients are all ± 1. Since the leading monomials have gcd 1, the ideal generators form a Gröbner basis; see [5, Chapter 2, §9, Theorem 3 and Proposition 4], for example. Since the leading coefficients are all ± 1, it follows from the division with remainder algorithm that the ideal of $\mathbb{Z}[(\xi_{ij})_{ij}, u_1, \dots, u_{n-1}, z_1, \dots, z_{n-1}]$ generated by these elements consists of the polynomials in I that have integral coefficients and that it has the $\mathbb{Z}$-span of the monomials that are not divisible by any of the above leading monomials as a direct complement. This proves (i) and (ii).

(iii) The canonical images of the above monomials form a $\mathbb{Z}$-basis of B. These monomials are the products of the monomials in the ξ_{ij} that are not divisible by $\xi_{nn}\cdots\xi_{22}\xi_{11}$ and the restricted monomials mentioned in the assertion. The canonical images of the monomials in the ξ_{ij} that are not divisible by $\xi_{nn}\cdots\xi_{22}\xi_{11}$ form a $\mathbb{Z}$-basis of A.

(iv) As we have seen, the monomials with exponents < 2 in the z_i form a basis of the $\tilde{Z}_0$-module Z_0'. So $A[z_1, \dots, z_{n-1}] \cap \tilde{Z}_0 = A$. Therefore, by Theorem 1(ii), $A[z_1, \dots, z_{n-1}] \cap Z_1 = A \cap Z_1 = \pi^{\mathrm{co}}(\mathbb{Z}[\mathrm{SL}_n]^{\mathrm{SL}_n})$. Now $(\mathbb{Z}P)^W = \mathbb{Z}[\mathrm{sym}(\varpi_1), \dots, \mathrm{sym}(\varpi_{n-1})]$ (see [3, No. VI.3.4, Theorem 1]) and the s_i' are in $\mathbb{Z}[\mathrm{SL}_n]$, so $\mathbb{Z}[\mathrm{SL}_n]^{\mathrm{SL}_n} = \mathbb{Z}[s_1', \dots, s_{n-1}']$ by the restriction theorem for $\mathbb{C}[\mathrm{SL}_n]$. This proves the first assertion. From the proof of Theorem 2 we know that the given monomials form a basis of Z_1 over $Z_0 \cap Z_1$ and a basis of Z over Z_0. So an element of Z is in Z_1 if and only if its coefficients with respect to this basis are in $Z_0 \cap Z_1$. The second assertion now follows from (iii). □

By (ii) of the above proposition we may identify $B(\mathbb{C})$ with $\tilde{Z}_0[z_1, \dots, z_{n-1}]Z_1$ and $B(\mathbb{C})[\tilde{\Delta}_1^{-1}, \dots, \tilde{\Delta}_{n-1}^{-1}]$ with Z.

Put $\bar{Z} = Z/(\tilde{d})$. For the proof of Theorem 4 we need a version for $\bar{Z}$ of Proposition 1. First we introduce some more notation. For $u \in Z$ we denote the canonical image of u in $\bar{Z}$ by $\bar{u}$. For $f \in \mathbb{C}[\mathrm{Mat}_n]$ we write $\bar{f}$ instead of $\bar{\tilde{f}}$. Let $\bar{A}$ be the $\mathbb{Z}$-subalgebra of $\bar{Z}$ generated by the $\bar{\xi}_{ij}$ and let $\bar{B}$ be the $\mathbb{Z}$-subalgebra generated by the elements $\bar{\xi}_{ij}, \bar{u}_1, \dots, \bar{u}_{n-1}$ and $\bar{z}_1, \dots, \bar{z}_{n-1}$. For a commutative ring R we put $\bar{A}(R) = R \otimes_{\mathbb{Z}} \bar{A}$ and $\bar{B}(R) = R \otimes_{\mathbb{Z}} \bar{B}$.

Proposition $\bar{1}$. *The following holds*:

(i) *The kernel of the natural homomorphism from the polynomial algebra* $\mathbb{Z}[(\xi_{ij})_{ij}, u_1, \dots, u_{n-1}, z_1, \dots, z_{n-1}]$ *to* $\bar{B}$ *is generated by the elements* $\det -1, d, f_1 - s_1, \dots, f_{n-1} - s_{n-1}, z_1^2 - \Delta_1, \dots, z_{n-1}^2 - \Delta_{n-1}$.

(ii) *The kernel of the natural homomorphism* $\mathbb{Z}[\mathrm{Mat}_n] \to \bar{A}$ *is* $(\det -1, d)$.

(iii) *The homomorphism* $\bar{B}(\mathbb{C}) \to \bar{Z}$, *given by the universal property of ring transfer, is injective.*

[8] So the z_i are greater than the u_i which are greater than the ξ_{ij}.

(iv) *$\bar{A}$ is a free $\mathbb{Z}$-module and $\bar{B}$ is a free $\bar{A}$-module with the monomials $\bar{u}_1^{k_1} \cdots \bar{u}_{n-1}^{k_{n-1}} \bar{z}_1^{m_1} \cdots \bar{z}_{n-1}^{m_{n-1}}$, $0 \leqslant k_i < l$, $0 \leqslant m_i < 2$, as a basis.*

(v) *The $\bar{A}$-span of the monomials $\bar{u}_1^{k_1} \cdots \bar{u}_{n-1}^{k_{n-1}}$, $0 \leqslant k_i < l$, is closed under multiplication.*

Proof. From Lemma 2(iii) we deduce that $(A(\mathbb{C})[\tilde{\Delta}_1^{-1}, \ldots, \tilde{\Delta}_{n-1}^{-1}]\tilde{d}) \cap A(\mathbb{C}) = A(\mathbb{C})\tilde{d}$. From this it follows, using the $A(\mathbb{C})$-basis of $B(\mathbb{C})$, that $(Z\tilde{d}) \cap B(\mathbb{C})$, which is the kernel of the natural homomorphism $B(\mathbb{C}) \to \bar{Z}$, equals $B(\mathbb{C})\tilde{d}$. From (i) and (ii) of Proposition 1 or from its proof it now follows that the kernel of the natural homomorphism from the polynomial algebra $\mathbb{C}[(\xi_{ij})_{ij}, u_1, \ldots, u_{n-1}, z_1, \ldots, z_{n-1}]$ to $\bar{Z}$ is generated by the elements $\det - 1, d, f_1 - s_1, \ldots, f_{n-1} - s_{n-1}, z_1^2 - \Delta_1, \ldots, z_{n-1}^2 - \Delta_{n-1}$.

Again using the $A(\mathbb{C})$-basis of $B(\mathbb{C})$ we obtain that $(B(\mathbb{C})\tilde{d}) \cap A(\mathbb{C}) = A(\mathbb{C})\tilde{d}$. From this it follows that the kernel of the natural homomorphism $\mathbb{C}[\mathrm{Mat}_n] \to \bar{Z}$ is generated by $\det - 1$ and d.

By Lemma 3 we have $\mathrm{LT}(d) = \pm\xi_{n\,n-1}^{n-1} \cdots \xi_{32}^2 \xi_{21}$ which has gcd 1 with the leading monomials of the other ideal generators, so the ideal generators mentioned above form a Gröbner basis over $\mathbb{Z}$. Now (i)–(iv) follow as in the proof of Proposition 1.

(v) This follows from the fact that the remainder modulo the Gröbner basis of a polynomial in $\mathbb{Z}[(\xi_{ij})_{ij}, u_1, \ldots, u_{n-1}]$ is again in $\mathbb{Z}[(\xi_{ij})_{ij}, u_1, \ldots, u_{n-1}]$. $\square$

By (ii) and (iii) of the above proposition $\bar{A}$ and $\bar{B}(\mathbb{C})[\bar{\Delta}_1^{-1}, \ldots, \bar{\Delta}_{n-1}^{-1}]$ can be identified with respectively $\mathbb{Z}[\mathrm{Mat}_n]/(\det - 1, d)$ and $\bar{Z}$. From (iv) it follows that, for any commutative ring R, $\bar{A}(R)$ embeds in $\bar{B}(R)$.

3.4. The theorem

Lemma 5. *Let A be an associative algebra with 1 over a field F and let L be an extension of F. Assume that for every finite extension F' of F, $F' \otimes_F A$ has no zero divisors. Then the same holds for $L \otimes_F A$.*

Proof. Assume that there exist $a, b \in L \otimes_F A \setminus \{0\}$ with $ab = 0$. Let $(e_i)_{i \in I}$ be an F-basis of A and let $c_{ij}^k \in F$ be the structure constants. Write $a = \sum_{i \in I} \alpha_i e_i$ and $b = \sum_{i \in I} \beta_i e_i$. Let I_a respectively I_b be the set of indices i such that $\alpha_i \neq 0$ respectively $\beta_i \neq 0$ and let J be the set of indices k such that $c_{ij}^k \neq 0$ for some $(i, j) \in I_a \times I_b$. Then I_a and I_b are non-empty and I_a, I_b and J are finite. Take $i_a \in I_a$ and $i_b \in I_b$. Since $ab = 0$, the following equations over F in the variables x_i, $i \in I_a$, y_i, $i \in I_b$, u and v have a solution over L:

$$\sum_{i \in I_a,\, j \in I_b} c_{ij}^k x_i y_j = 0 \quad \text{for all } k \in J,$$

$$x_{i_a} u = 1, \qquad y_{i_b} v = 1.$$

But then they also have a solution over a finite extension F' of F by Hilbert's Nullstellensatz. This solution gives us non-zero elements $a', b' \in F' \otimes_F A$ with $a'b' = 0$. $\square$

Lemma 6. *Let R be the valuation ring of a non-trivial discrete valuation of a field F and let K be its residue class field. Let A be an associative algebra with* 1 *over R which is free as an R-module and let L be an extension of F. Assume that for every finite extension K' of K, $K' \otimes_R A$ has no zero divisors. Then the same holds for $L \otimes_R A$.*

Proof. Assume that there exist $a, b \in L \otimes_R A \setminus \{0\}$ with $ab = 0$. By the above lemma we may assume that $a, b \in F' \otimes_R A \setminus \{0\}$ for some finite extension F' of F. Let $(e_i)_{i\in I}$ be an R-basis of A. Let ν be an extension to F' of the given valuation of F, let R' be the valuation ring of ν, let K' be the residue class field and let $\delta \in R'$ be a uniformiser for ν. Note that R' is a local ring and a principal ideal domain (and therefore a UFD) and that K' is a finite extension of K (see e.g. [6, Chapter 8, Theorem 5.1]). By multiplying a and b by suitable integral powers of δ we may assume that their coefficients with respect to the basis $(e_i)_{i\in I}$ are in R' and not all divisible by δ (in R'). By passing to the residue class field K we then obtain non-zero $a', b' \in K' \otimes_{R'} (R' \otimes_R A) = K' \otimes_R A$ with $a'b' = 0$. $\square$

Remark. The above lemmas also hold if we replace "zero divisors" by "non-zero nilpotent elements."

For $t \in \{0, \ldots, n-1\}$ let $\bar{B}_t$ be the $\mathbb{Z}$-subalgebra generated by the elements $\bar{\xi}_{ij}$, $\bar{u}_1, \ldots, \bar{u}_{n-1}$ and $\bar{z}_1, \ldots, \bar{z}_t$. So $\bar{B}_{n-1} = \bar{B}$. For a commutative ring R we put $\bar{B}_t(R) = R \otimes_{\mathbb{Z}} \bar{B}_t$. From (iv) and (v) of Proposition $\bar{1}$ we deduce that the monomials $\bar{u}_1^{k_1} \cdots \bar{u}_{n-1}^{k_{n-1}} \times \bar{z}_1^{m_1} \cdots \bar{z}_t^{m_t}$, $0 \leqslant k_i < l$, $0 \leqslant m_i < 2$, form a basis of $\bar{B}_t$ over $\bar{A}$. So for any commutative ring R we have bases for $\bar{B}_t(R)$ over $\bar{A}(R)$ and over R. Note that $\bar{B}_t(R)$ embeds in $\bar{B}(R)$, since the $\mathbb{Z}$-basis of $\bar{B}_t$ is part of the $\mathbb{Z}$-basis of $\bar{B}$.

Modifying the terminology of [11, §16.6], we define the *Jacobian ideal* of an m-tuple of polynomials $\varphi_1, \ldots, \varphi_m$ as the ideal generated by the $k \times k$ minors of the Jacobian matrix of $\varphi_1, \ldots, \varphi_m$, where k is the height of the ideal generated by the φ_i.

Theorem 4. *If l is a power of an odd prime p, then Z is a unique factorisation domain.*

Proof. We have seen in Subsection 3.1 that for $n = 2$ it holds without any extra assumptions on l, so assume that $n \geqslant 3$. For the elimination of variables in the proof of Theorem 3 we only needed the invertibility of $\tilde{d}$, so $Z[\tilde{d}^{-1}]$ is isomorphic to a localisation of a polynomial algebra and therefore a UFD. So, by Nagata's lemma, it suffices to prove that $\tilde{d}$ is a prime element of Z, i.e. that $\bar{Z} = Z/(\tilde{d})$ is an integral domain. We do this in 5 steps.

Step 1. $\bar{B}(K)$ is reduced for any field K.

We may assume that K is algebraically closed. Since $\bar{B}(K)$ is a finite $\bar{A}(K)$-module it follows that $\bar{B}(K)$ is integral over $\bar{A}(K) \cong K[\mathrm{Mat}_n]/(\det -1, d)$. So its Krull dimension is $n^2 - 2$. By Proposition $\bar{1}$(i), $\bar{B}(K)$ is isomorphic to the quotient of a polynomial ring over K in $n^2 + 2(n-1)$ variables by an ideal I which is generated by

$2n$ elements.[9] So $\bar{B}(K)$ is Cohen–Macaulay (see [11, Proposition 18.13]). Let $\mathcal{V}$ be the closed subvariety of $(n^2+2(n-1))$-dimensional affine space defined by I. Then, by [11, Corollary 18.14], $\mathcal{V}$ is equidimensional of dimension n^2-2. By Theorem 18.15 in [11] it suffices to show that the closed subvariety of $\mathcal{V}$ defined by the Jacobian ideal of $\det-1, d, f_1-s_1, \dots, f_{n-1}-s_{n-1}, z_1^2-\Delta_1, z_{n-1}^2-\Delta_{n-1}$ does not contain any of the irreducible components of $\mathcal{V}$. This amounts to showing that this subvariety is of codimension $\geqslant 1$ in $\mathcal{V}$, since $\mathcal{V}$ equidimensional.

By Lemma 2, $(\det-1, d)$ is a prime ideal of $K[\mathrm{Mat}_n]$. So we have an embedding $K[\mathrm{Mat}_n]/(\det-1,d) \to K[\mathcal{V}]$ which is the comorphism of a finite surjective morphism of varieties $\mathcal{V} \to V(\det-1,d)$, where $V(\det-1,d)$ is the closed subvariety of Mat_n that consists of the matrices of determinant 1 on which d vanishes. This morphism maps the closed subvariety of $\mathcal{V}$ defined by the Jacobian ideal of $\det-1, d, f_1-s_1, \dots, f_{n-1}-s_{n-1}, z_1^2-\Delta_1, \dots, z_{n-1}^2-\Delta_{n-1}$ into the closed subvariety of $V(\det-1,d)$ defined by the ideal generated by the $2n$th order minors of the Jacobian matrix of $(s_1, \dots, s_n, d, \Delta_1, \dots, \Delta_{n-1})$ with respect to the variables ξ_{ij}. This follows easily from the fact that $s_n = \det$ and that the z_j and u_j do not appear in the s_i and Δ_i. Since finite morphisms preserve dimension (see e.g. [11, Corollary 9.3]), it suffices to show that the latter variety is of codimension $\geqslant 1$ in $V(\det-1,d)$. Since $V(\det-1,d)$ is irreducible, this follows from Lemma 1(ii).

Step 2. $\bar{B}_0(K)$ is an integral domain for any field K of characteristic p.

We may assume that K is algebraically closed. From the construction of the f_i (see the proof of Lemma 4) and the additivity of the pth power map in characteristic p it follows that $f_i \equiv u_i^l \bmod p$. So the kernel of the natural homomorphism from the polynomial algebra $K[(\xi_{ij})_{ij}, u_1, \dots, u_{n-1}, z_1, \dots, z_{n-1}]$ to $\bar{B}(K)$ is generated by the elements $\det-1, d, u_1^l-s_1, \dots, u_{n-1}^l-s_{n-1}$ and the $\bar{A}(K)$-span of the monomials $\bar{u}_1^{k_1}\cdots\bar{u}_t^{k_t}$, $0 \leqslant k_i < l$, is closed under multiplication for each $t \in \{0, \dots, n-1\}$. We show by induction on t that $\bar{B}_{0,t}(K) := \bar{A}(K)[\bar{u}_1, \dots, \bar{u}_t]$ is an integral domain for $t = 0, \dots, n-1$. For $t=0$ this follows from Lemma 2 and Proposition $\bar{1}$(ii). Let $t \in \{1, \dots, n-1\}$ and assume that it holds for $t-1$. Clearly $\bar{B}_{0,t}(K) = \bar{B}_{0,t-1}(K)[\bar{u}_t] \cong \bar{B}_{t-1}(K)[x]/(x^l-\bar{s}_t)$. So it suffices to prove that $x^l-\bar{s}_t$ is irreducible over the field of fractions of $\bar{B}_{0,t-1}(K)$. By the Vahlen–Capelli criterion or a more direct argument, it suffices to show that $\bar{s}_t$ is not a pth power in the field of fractions of $\bar{B}_{0,t-1}(K)$. So assume that $\bar{s}_t = (v/w)^p$ for some $v, w \in \bar{B}_{0,t-1}(K)$ with $w \neq 0$. Then we have $v^p = \bar{s}_t w^p = \bar{u}_t^l w^p$. So with $l' = l/p$, we have $(v - \bar{u}_t^{l'} w)^p = 0$. But then $v - \bar{u}_t^{l'} w = 0$ by Step 1. Now recall that v and w can be expressed uniquely as $\bar{A}(K)$-linear combinations of monomials in $\bar{u}_1, \dots, \bar{u}_{t-1}$ with exponents $< l$. If such a monomial appears with a non-zero coefficient in w, then $\bar{u}_t^{l'}$ times this monomial appears with the same coefficient in the expression of $0 = v - \bar{u}_t^{l'} w$ as an $\bar{A}(K)$-linear combination of restricted monomials in $\bar{u}_1, \dots, \bar{u}_{n-1}$. Since this is impossible, we must have $w = 0$. A contradiction.

[9] The statement in Proposition $\bar{1}$(i) is only for $\bar{B}$, but the fact that $\bar{B}(K) = K \otimes_{\mathbb{Z}} \bar{B}$ has the same presentation, the coefficients of the ideal generators reduced mod p, holds for very general reasons. See e.g. [2, No. II.3.6, Proposition 5 and its corollary].

Step 3. $\bar{B}_0(\mathbb{C})$ is an integral domain.

This follows immediately from Step 2 and Lemma 6 applied to the p-adic valuation of $\mathbb{Q}$ and with $L = \mathbb{C}$.

Step 4. $\bar{B}_t(\mathbb{C})$ is an integral domain for $t = 0, \ldots, n-1$.

We prove this by induction on t. For $t = 0$ it is the assertion of Step 3. Let $t \in \{1, \ldots, n-1\}$ and assume that it holds for $t-1$. Clearly $\bar{B}_t(\mathbb{C}) = \bar{B}_{t-1}(\mathbb{C})[\bar{z}_t] \cong \bar{B}_{t-1}(\mathbb{C})[x]/(x^2 - \bar{\Delta}_t)$. So it suffices to prove that $x^2 - \bar{\Delta}_t$ is irreducible over the field of fractions of $\bar{B}_{t-1}(\mathbb{C})$. Assume that $x^2 - \bar{\Delta}_t$ has a root in this field, i.e. that $\bar{\Delta}_t = (v/w)^2$ for some $v, w \in \bar{B}_{t-1}(\mathbb{C})$ with $w \neq 0$. By the same arguments as in the proof of Lemma 5 we may assume that for some finite extension F of $\mathbb{Q}$ there exist $v, w \in \bar{B}_{t-1}(F)$ with $w \neq 0$ and $w^2\bar{\Delta}_t = v^2$. Let ν_2 be an extension to F of the 2-adic valuation of $\mathbb{Q}$, let S_2 be the valuation ring of ν_2, let K be the residue class field and let $\delta \in S_2$ be a uniformiser for ν_2. We may assume that the coefficients of v and w with respect to the $\mathbb{Z}$-basis of $\bar{B}_{t-1}$ mentioned earlier are in S_2. Assume that the coefficients of w are all divisible by δ (in S_2). Then $w = 0$ in $\bar{B}_{t-1}(K)$ and therefore $v^2 = 0$ in $\bar{B}_{t-1}(K)$. But by Step 1, $\bar{B}_{t-1}(K)$ is reduced, so $v = 0$ in $\bar{B}_{t-1}(K)$ and all coefficients of v are divisible by δ. So, by cancelling a suitable power of δ in w and v, we may assume that not all coefficients of w are divisible by δ. By passing to the residue class field K we then obtain $v, w \in \bar{B}_{t-1}(K)$ with $w \neq 0$ and $w^2\bar{\Delta}_t = v^2$. But then $(w\bar{z}_t - v)^2 = 0$ in $\bar{B}_t(K)$, since $\bar{z}_t^2 = \bar{\Delta}_t$ and K is of characteristic 2. The reducedness of $\bar{B}_t(K)$ (Step 1) now gives $w\bar{z}_t - v = 0$ in $\bar{B}_t(K)$. Now recall that v and w can be expressed uniquely as $\bar{A}(K)$-linear combinations of the monomials $\bar{u}_1^{k_1} \cdots \bar{u}_{n-1}^{k_{n-1}} \bar{z}_1^{m_1} \cdots \bar{z}_{t-1}^{m_{t-1}}$, $0 \leqslant k_i < l$, $0 \leqslant m_i < 2$. We then obtain a contradiction in the same way as at the end of Step 2.

Step 5. $Z/(d)$ is an integral domain.

Since $\bar{Z} = \bar{B}(\mathbb{C})[\bar{\Delta}_1^{-1}, \ldots, \bar{\Delta}_{n-1}^{-1}]$ and the $\bar{\Delta}_i$ are non-zero in $\bar{A}(\mathbb{C}) \cong \mathbb{C}[\mathrm{SL}_n]/(d')$ by Lemma 2, this follows from Step 4. $\square$

Remark. To attempt a proof for arbitrary odd $l > 1$ I have tried the filtration with $\deg(\xi_{ij}) = 2l$, $\deg(z_i) = li$ and $\deg(u_i) = 2i$. But the main problem with this filtration is that it does not simplify the relations $s_i = f_i(u_1, \ldots, u_{n-1})$ enough.

References

[1] A. Braun, C.R. Hajarnavis, Smooth polynomial identity algebras with almost factorial centers, Warwick preprint: 7/2003.
[2] N. Bourbaki, Algèbre, Chapitres 1, 2 et 3, Hermann, Paris, 1970.
[3] N. Bourbaki, Groupes et Algèbres de Lie, Chapitres 4, 5 et 6, Hermann, Paris, 1968.
[4] J.-M. Bois, Corps enveloppantes des algèbres de Lie en dimension infinie et en charactéristique positive, Thesis, University of Rheims, 2004.

[5] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, second ed., Undergrad. Texts Math., Springer-Verlag, New York, 1997.
[6] P.M. Cohn, Algebra, vol. 2, second ed., Wiley, Chichester, 1982.
[7] C. de Concini, V.G. Kac, Representations of quantum groups at roots of 1, in: Operator Algebras, Unitary Representations, Enveloping Algebras, and Invariant Theory, Paris, 1989, in: Progr. Math., vol. 92, Birkhäuser, Boston, MA, 1990, pp. 471–506.
[8] C. de Concini, V.G. Kac, C. Procesi, Quantum coadjoint action, J. Amer. Math. Soc. 5 (1) (1992) 151–189.
[9] C. de Concini, C. Procesi, Quantum groups, in: D-Modules, Representation Theory, and Quantum Groups, Venice, 1992, in: Lecture Notes in Math., vol. 1565, Springer-Verlag, Berlin, 1993, pp. 31–140.
[10] J. Dixmier, Sur les algèbres enveloppantes de $\mathfrak{sl}(n, \mathbb{C})$ et $\mathfrak{af}(n, \mathbb{C})$, Bull. Sci. Math. (2) 100 (1) (1976) 57–95.
[11] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Grad. Texts in Math., vol. 150, Springer-Verlag, New York, 1995.
[12] F. Fauquant-Millet, Sur une algèbre parabolique P de $\check{U}_q(\mathfrak{sl}_{n+1})$ et ses semi-invariants par l'action adjointe de P, Bull. Sci. Math. 122 (7) (1998) 495–519.
[13] F. Fauquant-Millet, Quantification de la localisation de Dixmier de $U(\mathfrak{sl}_{n+1}(\mathfrak{C}))$, J. Algebra 218 (1) (1999) 93–116.
[14] Ya.S. Krylyuk, The Zassenhaus variety of a classical semi-simple Lie algebra in finite characteristic, Mat. Sb. (N.S.) 130(172) (4) (1986) 475–487 (in Russian); English translation: Math. USSR Sb. 58 (2) (1987) 477–490.
[15] V.L. Popov, Picard groups of homogeneous spaces of linear algebraic groups and one-dimensional homogeneous vector bundles, Izv. Akad. Nauk SSSR Ser. Mat. 38 (1974) 294–322 (in Russian); English translation: Math. USSR Izv. 8 (2) (1974) 301–327.
[16] A.A. Premet, R.H. Tange, Zassenhaus varieties of general linear Lie algebras, J. Algebra 294 (1) (2005) 177–195.
[17] R. Steinberg, Regular elements of semi-simple algebraic groups, Inst. Hautes Études Sci. Publ. Math. 25 (1965) 49–80.