THE CENTRE OF QUANTUM $\mathfrak{sl}_n$ AT A ROOT OF UNITY

RUDOLF TANGE

Summary. It is proved that the centre $Z$ of the simply connected quantised universal enveloping algebra $U_{\varepsilon,P}(\mathfrak{sl}_n)$, $\varepsilon$ a primitive $l$-th 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] DeConcini, Kac and Procesi introduced the simply connected quantised universal enveloping algebra $U = U_{\varepsilon,P}(\mathfrak{g})$ over $\mathbb{C}$ at a primitive $l$-th root of unity $\varepsilon$ 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 Maxspec$(Z)$ is also pointed out in [7].

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. 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 nonzero 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\footnote{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 $K$.} 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 [10], 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] and [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 $\Phi$ be its root system relative to $\mathfrak{h}$, let $(\alpha_1, \ldots, \alpha_r)$ be a basis of $\Phi$ and let $(\langle . | . \rangle)$ be the symmetric bilinear form on $\mathfrak{h}^* \ast$ which is invariant for the Weyl group $W$ and satisfies $\langle \alpha | \alpha \rangle = 2$ for all short roots $\alpha$. Put $d_i = (\alpha_i | \alpha_i)/2$. The root lattice and the weight lattice of $\Phi$ are denoted by resp. $Q$ and $P$. Note that $(\langle . | . \rangle)$ 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 $\varepsilon$ be a primitive $l$-th root of unity and let $\Lambda$ 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 $\varepsilon$ defined in [7] 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 resp. the $E_i$, the $F_i$ and the $K_\lambda$ with $\lambda \in \Lambda$. Then the multiplication $U^- \otimes U^0 \otimes U^+ \to U$ is an isomorphism of vector spaces. We identify $U^0$ with the group algebra $\mathbb{C}\Lambda$ of $\Lambda$. Note that $W$ acts on $U^0$, since it acts on $\Lambda$. Let $T$ be the complex torus $\text{Hom}(\Lambda, \mathbb{C}^\times)$. Then $T$ can be identified with $\text{Maxspec}(U^0) = \text{Hom}_{\mathbb{C}\text{-Alg}}(U^0, \mathbb{C})$ 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 $K_\lambda^l$, $\lambda \in \Lambda$ and $E_i^l, F_i^l$, $i = 1, \ldots, r$. We have $Z_0 \subseteq Z$. Put $z_\lambda = K_\lambda^l$ and let $Z_0^l$ be the subalgebra of $Z_0$ spanned by the $z_\lambda$. Then the identification of $U^0$ with $\mathbb{C}\Lambda$ gives an identification of $Z_0^l$ with $\mathbb{C}z\Lambda$. If we replace $K_\lambda$ by $z_\lambda$ in foregoing remarks, then we obtain an identification of $T$ with $\text{Maxspec}(Z_0^l)$. 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 $f \mapsto (\lambda \mapsto (-1)^{f(\lambda)}) : \Lambda^* \to Q_2^\vee$. 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 $\varepsilon_U(x)u \varepsilon_U(y)$, where $\varepsilon_U$ is de counit of $U$. Then $h'$ is a projection of $U$ onto $U^0$. Furthermore $h'(Z_0) = Z_0^0 = \mathbb{C} \Lambda$ 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 $\gamma$ of $U^{0Q_2^\vee}$ by setting $\gamma(K_\lambda) = \varepsilon^{(\rho,\lambda)} K_\lambda$ for $\lambda \in \Lambda \cap 2P$. Here $\rho$ is the half sum of the positive roots. Note that $\gamma = \text{id}$ on $Z_0^{0Q_2^\vee} = \mathbb{C}(\Lambda \cap 2P)$. In [8] p 174 and [21], §2, there was constructed an injective homomorphism $\overline{h} : U^{0\tilde{W}} \to \tilde{Z}$, whose image is denoted by $Z_1$, such that $h'(Z_1) \subseteq U^{0Q_2^\vee}$ and the inverse 

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

of $\overline{h}$ 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 $\text{Ker}(h')$ 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 $\Phi$ 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 $\text{SL}_n$.

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

We denote the fundamental weights corresponding to the basis $(\alpha_1, \ldots, \alpha_r)$ by $\varpi_1, \ldots, \varpi_r$. 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 $\mathbb{C}[G]^G \cong \mathbb{C}[T]^W = (\mathbb{C}P)^W$, see [17] §6. For $\lambda \in P$ denote the basis element of $\mathbb{C}P$ corresponding to $\lambda$ by $e(\lambda)$, denote the $W$-orbit of $\lambda$ by $W \cdot \lambda$ and put $\text{sym}(\lambda) = \sum_{\mu \in W \lambda} e(\mu)$. Then the $\text{sym}(\varpi_i), i = 1, \ldots, r$ are algebraically independent generators of $(\mathbb{C}P)^W$. See [3] no. VI.3.4, Thm. 1.

For a field $K$, we denote the vector space of all $n \times n$ matrices over $K$ by $\text{Mat}_n = \text{Mat}_n(K)$. Now assume that $K = \mathbb{C}$. In this section we denote the restriction to $\text{SL}_n$ of the standard coordinate functionals on $\text{Mat}_n$ by $\xi_{ij}, 1 \leq i, j \leq n$. Furthermore, for $i \in \{1, \ldots, n - 1\}$, $s_i \in \mathbb{C}[\text{SL}_n]$ is defined by $s_i(A) = \text{tr}(\Lambda^i A)$, where $\Lambda^i A$ denotes the $i$-th exterior power of $A$ and tr denotes the trace. Then $\varpi_i = (\xi_{11} \cdots \xi_{ii})|_{T}$ and therefore $\text{sym}(\varpi_i) = s_i|_T \ (\ast)$, the $i$-th 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 \( s_1, \ldots, s_r \) are algebraically independent generators of \( \mathbb{C}[G]^G \).

Identifying \( U^0 \) and \( CP \), we have \( U^0W = (\mathbb{C}2P)^W \). Put \( u_i = \overline{\eta}(\text{sym}(2\varpi_i)) \). Then \( h(u_i) = \text{sym}(2\varpi_i) \) and \( u_1, \ldots, u_r \) are algebraically independent generators of \( Z_1 \).

1.4. The cover \( \pi \) and the intersection \( Z_0 \cap Z_1 \).

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

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

In [8] §4 there was constructed an unramified cover \( \pi : \Omega \to O \) of degree \( 2^r \). I give a short description of the construction of \( \pi \). Put \( \Omega^\pm = \text{Maxspec}(\tilde{Z}_0^\pm) \). 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 \( \Omega^\pm \cong U_\pm \) and \( \pi \) is defined as \( YZ^2X \) (multiplication in \( G \)). This means: \( \pi(x) = Y(x)Z(x)^2X(x) \).

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

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

(i) \( Z_0^G = Z_1 \). \(^3\)

(ii) \( \pi^{co} \) induces an isomorphism \( \mathbb{C}[G]^G \cong Z_0^G = Z_0 \cap Z_1 \).

(iii) The monomorphism \( (\mathbb{C}P)^W \cong (\mathbb{C}P)^W \) 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 \( h(Z_0 \cap Z_1) = (\mathbb{C}2lP)^W \).

\(^2\)In [8] \( Z_2^G \) 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.

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

\[
\begin{array}{ccc}
G & \xrightarrow{\pi} & \Omega \\
\downarrow & & \downarrow \\
T & \overset{t \mapsto t^2}{\longrightarrow} & T
\end{array}
\]

Expressed in terms of the comorphisms this reads: $(x \mapsto 2x) \circ \text{res}_{G,T} = \text{res}_{\Omega,T} \circ \pi^0$, where $\text{res}_{G,T}$ and $\text{res}_{\Omega,T}$ 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 $(x \mapsto lx) \circ \text{res}_{G,T} = h'|_{Z_0} : Z_0 \to U^0 = \mathbb{C}P$ we obtain $(x \mapsto 2lx) \circ \text{res}_{G,T} = h' \circ \pi^0$. 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 1.5. 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 $u_1^{k_1} \cdots u_r^{k_r}$, $0 \leq k_i < l$ as a basis.

I give a proof of (ii). In [8] Prop. 6.4 it is proved that $(\mathbb{C}P)^W$ is a free $(\mathbb{C}I)P)^W$-module of rank $l^r$ with the restricted monomials (exponents $< l$) in the $\text{sym}(\pi_i)$ as a basis. The same holds then of course for $(\mathbb{C}2P)^W$, $(\mathbb{C}2I)P)^W$ and the $\text{sym}(2\pi_i)$. 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 $\Omega^\pm \simeq U_\pm$. So $Z_0$ is a polynomial algebra in $\dim(g)$ variables with $r$ variables inverted. In particular it’s Krull dimension (which coincides with the transcendence degree of its field of fractions) is $\dim(g)$.

The same holds then for $Z$, since it is a finitely generated $Z_0$-module.

Let $Z_0'$ be a subalgebra of $Z_0$ containing $Z_1 \cap Z_0$. Then the multiplication $Z_1 \otimes_{Z_0 \cap Z_1} Z_0' \to Z_0' \cap Z_1$ 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 $s_1, \ldots, s_r$ be the generators of $\mathbb{C}[G]^G$ defined in Subsection 1.5. Then $\pi^0(s_1), \ldots, \pi^0(s_r)$ 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 $u_1, \ldots, u_r$ defined in Subsection 1.5. For each $i \in \{1, \ldots, r\}$ we can express $\pi^0(s_i)$ 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 $Z_0'Z_1$.

The $f_i$ can be determined as follows. Write $\text{sym}(l\pi_i)$ as a polynomial $f_i$ in the $\text{sym}(\pi_i)$. Then $\text{sym}(2l\pi_i)$ is the same polynomial in the $\text{sym}(2\pi_j)$ and $\pi^{co}(s_i) = f_i(u_1, \ldots, u_n)$ by Theorem $\text{	extbf{III}}$.

Note that $\pi^{co}(C[O]) = Z_0 - C(2lP)Z_0^+$ and that $Z_0 = \pi^{co}(C[O])[z_{w_1}, \ldots, z_{w_r}]$.

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

$$Z_0 = \tilde{Z}_0[z_{w_1}, \ldots, z_{w_{n-1}}][\tilde{\Delta}_1^{-1}, \ldots, \tilde{\Delta}_{n-1}^{-1}].$$

Let $pr_{O,T}$ be the projection of $O$ on $T$. An easy computation shows that $\Delta_i|_O = (\xi_{11} \cdots \xi_{ii}) \circ pr_{O,T} = \pi \circ pr_{O,T}$ for $i = 1, \ldots, n - 1$. So $\tilde{\Delta}_i = \pi \circ pr_{O,T}$ and $\pi = \pi \circ (t \mapsto t^2) \circ pr_{O,T} = 2\pi_i \circ pr_{O,T} = 2z_{w_i}$. In Subsection 3.3 we will determine generators and relations for $Z_0'Z_1$, where $Z_0' = \tilde{Z}_0[z_{w_1}, \ldots, z_{w_{n-1}}]$ using the method mentioned above.

2. Rationality

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

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

To prove theorem below we need to look at the expressions of the functions $s_i$ in terms of the $\xi_{ij}$. We use that those equations are linear in $\xi_{11}, \xi_{22}, \ldots, \xi_{nn}$. The treatment is completely analogous to that in [16] 4.1 (we use the same symbols $R$, $M$, $d$ and $x_a$) to which we refer for more explanation. Let $R$ be the $Z$-subalgebra of $\mathbb{C}[\text{Mat}_n]$ generated by all $\xi_{ij}$ with $j \neq n$.

---

4This method was also used by Krylyuk in [13] to determine generators and relations for the centre of the universal enveloping algebra $U(g)$ of $g$. Our homomorphism $\pi^{co} : C[G] \rightarrow Z_0$ plays the rôle of Krylyuk’s $G$-equivariant isomorphism $\eta : S(g)^{(1)} \rightarrow Z_p$, where we use the notation of [16].

5For two $n \times n$ matrices $A$ and $B$ we have $\wedge^k(AB) = \wedge^k(A) \wedge^k(B)$. From this it follows that if either $A$ is lower triangular or $B$ is upper triangular, then $\Delta_k(AB) = \Delta_k(A)\Delta_k(B)$.
Then the matrix $M$ has entries in $R$ and the following vector equation holds:

\[(1)\quad M \cdot \mathbf{c} = \mathbf{s} + \mathbf{r}, \quad \text{where } \mathbf{r} \in R^n.\]

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

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

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 $\dim(Q(\mathfrak{sl}_n)) = n^2 - 1$ over $\mathbb{C}$ and that it is generated as a field by the $n^2 + 2(n - 1)$ variables $\xi_{ij}, u_1, \ldots, u_{n-1}$ and $z_{\varpi_1}, \ldots, z_{\varpi_{n-1}}$. To prove the assertion we will show that $Q(Z)$ is generated by the $n^2 - 1$ elements $\xi_{ij}, i \neq j, j \neq n, u_1, \ldots, u_{n-1}$ and $z_{\varpi_1}, \ldots, z_{\varpi_{n-1}}$. We will first eliminate the $n$ generators $\xi_{1n}, \ldots, \xi_{nn}$ and then the $n - 1$ generators $\xi_{11}, \ldots, \xi_{n-1,n-1}$.

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

\[(2)\quad \tilde{M} \cdot \tilde{\mathbf{c}} = \tilde{\mathbf{s}} + \tilde{\mathbf{r}}, \quad \text{where } \tilde{\mathbf{r}} \in \tilde{R}^n.\]

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 resp. 1, and $\tilde{R}$ is the $\mathbb{Z}$-subalgebra of $Z_0$ generated by all $\xi_{ij}$ with $j \neq n$. Choosing $\mathbf{a}$ such that $a_n = (-1)^{n-1}$ we have $x_\mathbf{a} \in \text{SL}_n$. Since $d(x_\mathbf{a}) = 1$, we have $d' \neq 0$ and therefore $\det(\tilde{M}) = \tilde{d} \neq 0$. Furthermore, for $i = 1, \ldots, n - 1$, $(\tilde{s}_i, i = \tilde{s}_i \in Z_0 \cap Z_1$ and $Z_1$ is generated by $u_1, \ldots, u_{n-1}$. It follows that $\xi_{1n}, \ldots, \xi_{nn}$ are in the subfield of $Q(Z)$ generated by the $\xi_{ij}$ with $j \neq n$ and $u_1, \ldots, u_{n-1}$.

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

\[z_{\varpi_1}^2 = \tilde{\Delta}_1 = \tilde{\xi}_{11} \]
and for $k = 2, \ldots, n - 1$ we have, by the Laplace expansion rule,
\[
z_i^2 = \bar{\Delta}_k = \tilde{\xi}_{kk} \bar{\Delta}_{k-1} + t_k = \tilde{\xi}_{kk} z_{i,k}^2 + t_k,
\]
where $t_k$ is in the $\mathbb{Z}$-subalgebra of $\mathbb{Z}$ generated by the $\tilde{\xi}_{ij}$ with $i, j \leq k$ and $(i, j) \neq (k, k)$. It follows by induction $k$ that for $k = 1, \ldots, n - 1$, $\tilde{\xi}_{ii}, \ldots, \tilde{\xi}_{kk}$ are in the subfield of $\mathbb{Q}(\mathbb{Z})$ generated by the $z_{i,j}$ with $i \leq k$ and the $\tilde{\xi}_{ij}$ with $i, j \leq k$ and $i \neq j$.

3. Unique Factorisation

Recall that Nagata’s lemma asserts the following: If $x$ is a prime element of a Noetherian integral domain $S$ such that $S[x^{-1}]$ is a UFD, then $S$ is a UFD. See Lemma 19.20. In Theorem 4.1 we will see that, by Nagata’s lemma, it suffices to show that the algebra $\mathbb{Z}/(\bar{d})$ is an integral domain in order to prove that $\mathbb{Z}$ is a UFD. To prove this we will show by induction that the two sequences of algebras (to be defined later):
\[
K[SL_n]/(d') \cong \overline{A}(K) = \overline{B}_0,0(K) \subseteq \overline{B}_0,1(K) \subseteq \cdots \subseteq \overline{B}_{0,n-1}(K) = \overline{B}_0(K)
\]
in characteristic $p$ and
\[
\overline{B}_0(\mathbb{C}) \subseteq \overline{B}_1(\mathbb{C}) \subseteq \cdots \subseteq \overline{B}_{n-1}(\mathbb{C}) = \overline{B}(\mathbb{C})
\]
consist of integral domains. Lemma’s 2 and 3 are, among other things, needed to obtain bases over $\mathbb{C}$ in the subfield of $\mathbb{C}$ in $\mathbb{Q}$ for $\mathbb{C}$. Identifying $SL_n$ with $C$ in characteristic $p$ and for $\mathbb{Z}$, we put $\tilde{\xi}_E, \tilde{\xi}_F, \tilde{\xi}_K$ and $\tilde{\xi}_z$ are algebraically independent over $\mathbb{C}$ and for $\mathbb{Q}[\mathbb{Z}]$, we have sym$(2\mathbb{Z}) = \mathbb{K} + \mathbb{K}^{-1}$.

3.1. The case $n = 2$

In this subsection we show that the centre of $U_{\epsilon, p}(sl_2)$ is always a UFD, without any extra assumptions on $l$. The standard generators for $U_{\epsilon, p}(sl_2)$ are $E, F, K_\infty$ and $K_\infty^{-1}$. Put $K = K_\alpha = K_\infty^2$, $z_1 = z_\infty = K_\infty^l$, $z = z_\alpha = z_\infty^2 = K_\infty$. Furthermore, following 3.1, we put $c = (\epsilon - \epsilon^{-1})^l$, $x = -cz^{-1}E$, $y = cF^l$. 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 §3).

We have $U^0 = \mathbb{C}[K_\infty, K_\infty^{-1}]$ and $U^{\overline{W}} = \mathbb{C}[K, K^{-1}]^{\overline{W}} = \mathbb{C}[K + K^{-1}]$. Identifying $U^0$ and $\mathbb{C}P$, we have sym$(2\mathbb{Z}) = K + K^{-1}$ and sym$(2\mathbb{Z}) = z + z^{-1}$. Put $u = \overline{h}(\text{sym}(2\mathbb{Z}))$. By the restriction theorem for $U$, $Z_1$ is a polynomial algebra in $u$. Denote the trace map on Mat$_2$ by tr. Then $tr|_T = \text{sym}(2\mathbb{Z})$. By the restriction theorem for $\mathbb{C}[G]$ and Theorem §2, $\text{tr}$ generates $Z_0 \cap Z_1$. Furthermore $\text{tr} = \overline{h}(z + z^{-1})$, by Theorem §3. Let $f \in \mathbb{C}[u]$ be the polynomial with $z + z^{-1} = f(K + K^{-1})$. Then $\text{tr} = f(u)$. From the formula’s in 5.2 it follows that $\text{tr} = -zxy + z + z^{-1}$.

By the construction from Subsection 1.2 (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 $-z^2xy + z^2 + z^{-2} - f(u)$. 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 \( \mathbb{C}[z_1, u] \) 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. \( \text{SL}_n \) and the function \( d \).

Part (i) of the next lemma is needed for the proof of Lemma 2 and part (ii) is needed for the proof of Theorem 4. The Jacobian matrices below consist of the partial derivatives of the functions in question with respect to the variables \( \xi_{ij} \).

**Lemma 1.**

(i) There exists a matrix \( A \in \text{SL}_n(\mathbb{Z}) \) such that \( \Delta_{n-1}(A) = 0 \) and such that some second order minor of the Jacobian matrix of \( (\det, \Delta_{n-1}) \) is \( \pm 1 \) at \( A \).

(ii) If \( n \geq 3 \), then there exists a matrix \( A \in \text{SL}_n(\mathbb{Z}) \) 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 \( \pm 1 \) 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 \( (\xi_{ij}) \) and for an \( n \times n \) matrix \( B = (b_{ij}) \) and \( \Lambda_1, \Lambda_2 \subseteq \{1, \ldots, n\} \) we denote by \( B_{\Lambda_1, \Lambda_2} \) 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

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

where \( n_1(i) \) denotes the position in which \( i \) occurs in \( \Lambda_1 \) and similarly for \( n_2(j) \).

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

(i) We let \( A \) be the following \( n \times n \)-matrix:

\[
A = \begin{bmatrix}
0 & 0 & \cdots & 0 & -1 \\
0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 \\
1 & 0 & \cdots & 0 & 0
\end{bmatrix}.
\]
Clearly \( \det(A) = 1 \) and \( \Delta_{n-1}(A) = 0 \). From the above two facts it is easy to deduce that
\[
\begin{bmatrix}
\partial_{1n} \det & \partial_{11} \det \\
\partial_{1n} \Delta_{n-1} & \partial_{11} \Delta_{n-1}
\end{bmatrix}
\] is equal to
\[
\begin{bmatrix}
\pm 1 & 0 \\
0 & \pm 1
\end{bmatrix}
\] at \( A \).

(ii). Put \( \alpha = ((11), (22), (23), \ldots, (2n-1), (nn), (n-1n), \ldots, (2n), (21), (12)) \), and let \( \alpha_i \) denote the \( i \)-th component of \( \alpha \). We let \( A \) be the following \( n \times n \)-matrix:

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

The columns of the Jacobian matrix are indexed by the pairs \((i, j)\) with \( 1 \leq i, j \leq n \). Let \( M_{\alpha} \) be the \( 2n \)-square submatrix of the Jacobian matrix consisting of the columns with indices from \( \alpha \). 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 nonzero at \( A \).

First we consider the \( \Delta_k \), \( k \in \{1, \ldots, n-1\} \). 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:

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

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

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

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

- \( i, n \in \Lambda \);
- \( j \in \Lambda \Rightarrow j - 1 \in \Lambda \) for all \( j \) with \( 4 \leq j \leq n \) 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 \( 3 \leq j \leq n - 1 \), since otherwise there would be a zero column.

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

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 \( \partial_{1n}(\det(\mathcal{X}_{\Lambda, \Lambda}))(A) = (-1)^{1+n-1} = (-1)^n \).

In the second case we have \( \partial_{1n}(\det(\mathcal{X}_{\Lambda, \Lambda}))(A) = (-1)^{2+n} = (-1)^n \).

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 \( \partial_{1n}(\det(\mathcal{X}_{\Lambda, \Lambda}))(A) = (-1)^{1+n-1} = (-1)^n \).

In the second case we have \( \partial_{1n}(\det(\mathcal{X}_{\Lambda, \Lambda}))(A) = (-1)^{1+n} - 1 = (-1)^n \).
So for $i \in \{1, \ldots, n-1\}$ and $k \in \{1, \ldots, n\}$ we have:

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

It follows from the above equalities that in $M(A)$ the first 2 columns are equal. So $\partial_{1}A \equiv 0$.

Let $\Lambda \subseteq \{1, \ldots, n\}$. Assume that $\partial_{12}(\det(\mathcal{X}_{\Lambda,A}))$ is nonzero at $A$. Then $1, 2 \in \Lambda$ and the first row is zero. A contradiction. So $\partial_{12}(\det(\mathcal{X}_{\Lambda,A}))$ is zero at $A$. Now assume that $\partial_{21}(\det(\mathcal{X}_{\Lambda,A}))$ is nonzero 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 $4 \leq j \leq n$, since otherwise there would be a zero row.

So $\Lambda = \{1, \ldots, n\}$ and $\partial_{m}(\det(\mathcal{X}_{\Lambda,A}))(A) = \pm 1$. Thus we have $(\partial_{12}s_{k})(A) = 0$ for all $k \in \{1, \ldots, n\}$ 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 $i \in \{1, \ldots, n\}$, let $\Lambda \subseteq \{1, \ldots, n\}$ and assume that $\partial_{12}\partial_{m}(\det(\mathcal{X}_{\Lambda,A}))$ is nonzero 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 $4 \leq j \leq n$, since otherwise there would be a zero row.

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

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

We have

$$
(3) \quad d = \sum_{\pi \in \mathfrak{S}_{n}} \text{sgn}(\pi) \partial_{\pi(1),n}(s_{1}) \cdots \partial_{\pi(n),n}(s_{n}).
$$

So, by the above, $(\partial_{12}d)(A) = \left(\sum_{\pi \in \mathfrak{S}_{n}} \text{sgn}(\pi)\partial_{\pi(1),n}(s_{1})\partial_{\pi(2),n}(s_{2}) \cdots \partial_{\pi(n-1),n}(s_{n-1})\partial_{12}\partial_{2n}(s_{n})\right)(A)$, where the sum is over all $\pi \in \mathfrak{S}_{n}$ with $\pi(n) = 2$. From what we know about the $\partial_{m}s_{k}$ we deduce that the only permutation that survives in the above sum is given by $(\pi(1), \ldots, \pi(n)) = (n, n - 1, \ldots, 3, 1, 2)$ and that $(\partial_{12}d)(A) = \pm 1$. 

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

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

It is well known that the algebra of regular functions $K[G]$ of a simply connected semi-simple algebraic group $G$ is a UFD (see [15], the corollary to Proposition 1), but the elementary proof below provides a way to show that $d'$ and the $\Delta_i$ are irreducible elements of $K[\text{SL}_n]$. I did not know how to use the fact that $K[\text{SL}_n]$ is a UFD to simplify the proof that $\Delta_{n-1}'$ is irreducible.

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 $\varphi_i$.

**Lemma 2.** $K[\text{SL}_n]$ is a unique factorisation domain and $\Delta_{n-1}'$ is an irreducible element of $K[\text{SL}_n]$.

**Proof.** From the Laplace expansion for det with respect to the last row or the last column it is clear that we can eliminate $\xi_{nn}$ using the relation det $= 1$, if we make $\Delta_{n-1}'$ invertible. So we have an isomorphism of $K[\text{SL}_n][\Delta_{n-1}']$ with the localised polynomial algebra $K[(\xi_{ij})_{(i,j)\neq (n,n)}][\Delta_{n-1}']$. Since the latter algebra is a UFD, it suffices, by Nagata’s lemma, to prove that $\Delta_{n-1}'$ is prime in $K[\text{SL}_n]$, i.e. that $(\Delta_{n-1}', \det - 1)$ generates a prime ideal in $K[\text{Mat}_n]$. First we show that the closed subvariety $V$ of $\text{Mat}_n$ defined by this ideal is irreducible.

Let $X$ the matrix introduced above and let $\alpha_1, \ldots, \alpha_{n-2}$ be variables. For a matrix $A$ denote by $A^{(i,j)}$ the matrix which is obtained from $A$ by deleting the $i$-th row and the $j$-th column. Let $X'_\alpha$ be the $n \times n$ matrix which is obtained by replacing in $X$ the $(n-1)$-th column of $X^{(n,n)}$ by the linear combination $\sum_{j=1}^{n-2} \alpha_j \xi_{ij}$, of the first $n - 2$ columns of $X^{(n,n)}$. Then $\det(X'^{(n,j)}_\alpha) = \pm \alpha_j \det(X^{(n,n-1)})$ for all $j \in \{1, \ldots, n - 2\}$ and $\det(X'^{(n,n)}_\alpha) = 0$. So, by the Laplace expansion rule

$$
\det(X'_\alpha) - 1 = \sum_{j=1}^{n-1} \pm \xi_{nj} \det(X'^{(n,j)}_\alpha) - 1
$$

$$
= \pm \xi_{nn-1} \det(X^{(n,n-1)}) + \sum_{j=1}^{n-2} \pm \alpha_j \xi_{nj} \det(X^{(n,n-1)}) - 1
$$

Let $K[X_\alpha]$ be the polynomial ring in the variables that occur in $X_\alpha$. If we consider $\det(X_\alpha) - 1$ as a polynomial in the variable $\xi_{n,n-1}$, then it is linear and its leading coefficient is $\pm \det(X^{(n,n-1)})$ which is irreducible and does not divide the constant term $\sum_{j=1}^{n-2} \pm \alpha_j \xi_{nj} \det(X^{(n,n-1)}) - 1$. So $\det(X_\alpha) - 1$ is irreducible in $K[X_\alpha]$ and
it defines an irreducible closed subvariety $V_1$ of an $n^2-1$ dimensional affine space with coordinate functionals $\xi_{ij}$, $j \neq n-1$, $\xi_{n,n-1}$, $\alpha_1, \ldots, \alpha_{n-2}$.

Let $H$ be the algebraic group of $n \times n$ matrices $(a_{ij})$ of determinant 1 with $a_{nn} = 1$ and $a_{ni} = a_{ni} = 0$ for all $i \in \{1, \ldots, n-1\}$. Then $H \cong \text{SL}_n$ and for every $A \in V$ there exists an $S \in H$ such that in $(AS)^{(n,n)}$ the last column is a linear combination of the others. So the morphism of varieties $(u, S) \mapsto X_u(u)S : V_1 \times H \rightarrow \text{Mat}_n$ has image $V$. Now the irreducibility of $V$ follows from the irreducibility of $V_1 \times H$.

It remains to show that $(\det -1, \Delta_{n-1})$ is a radical ideal of $K[\text{Mat}_n]$, i.e. that $K[\text{Mat}_n]/(\det -1, \Delta_{n-1})$ is reduced. We know that $\Delta_{n-1} \neq 0$ on the irreducible variety $\text{SL}_n$, so $\dim(V) = n^2-2$ and $K[\text{Mat}_n]/(\det -1, \Delta_{n-1})$ is Cohen-Macaulay (see [11] Proposition 18.13). By Theorem 18.15 in [11] it suffices to show that the closed subvariety of $V$ defined by the Jacobian ideal of $\det -1, \Delta_{n-1}$ is of codimension $\geq 1$. Since $V$ is irreducible this follows from Lemma [11](i).

Lemma 3. (i) $d$ is an irreducible element of $K[\text{Mat}_n]$.

(ii) The invertible elements of $K[\text{SL}_n]$ are the nonzero scalars.

(iii) $d', \Delta'_1, \ldots, \Delta'_{n-1}$ is are mutually inequivalent irreducible elements of $K[\text{SL}_n]$.

Proof. (i). The proof of this is completely analogous to that of Proposition 3 in [10]. One now has to work with the maximal parabolic subgroup $P$ of $\text{GL}_n$ 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 $\xi_{nn}$ (the restriction of this weight to the maximal torus of diagonal matrices is $n\overline{\omega}_{n-1}$).

(ii) and (iii). Consider the isomorphism $K[\text{SL}_n][\Delta'_{n-1}] \cong K[(\xi_{ij})_{(i,j)\neq(n,n)}][\Delta_{n-1}]$ from the proof of the above lemma. It maps $d', \Delta'_1, \ldots, \Delta'_{n-1}$ to respectively $d, \Delta_1, \ldots, \Delta_{n-1}$, since these polynomials do not contain the variable $\xi_{nn}$. The invertible elements of $K[(\xi_{ij})_{(i,j)\neq(n,n)}][\Delta_{n-1}]$ are the elements $\alpha \Delta_{n-1}^k, \alpha \in K \setminus \{0\}$, $k \in \mathbb{Z}$, since $\Delta_{n-1}$ is irreducible in $K[(\xi_{ij})_{(i,j)\neq(n,n)}]$.

So the invertible elements of $K[\text{SL}_n][\Delta'_{n-1}]$ are the elements $\alpha \Delta_{n-1}^k$, $\alpha \in K \setminus \{0\}$, $k \in \mathbb{Z}$. By Lemma [2] $\Delta'_{n-1}$ is irreducible in $K[\text{SL}_n]$, so the invertible elements of $K[\text{SL}_n]$ are the nonzero scalars. Since $d$ and the $\Delta_i$ are not scalar multiples of each other, all that remains is to show that $d'$ and $\Delta'_1, \ldots, \Delta'_{n-2}$ are irreducible. We only do this for $d'$, the argument for the $\Delta'_i$ is completely similar. Since $d$ is prime in $K[(\xi_{ij})_{(i,j)\neq(n,n)}]$ and $d$ does not divide $\Delta_{n-1}$, it follows that $d$ is prime in $K[(\xi_{ij})_{(i,j)\neq(n,n)}][\Delta_{n-1}]$ and therefore that $d'$ is prime in $K[\text{SL}_n][\Delta'_{n-1}]$. To show that $d'$ is prime in $K[\text{SL}_n]$ it suffices to show that for every $f \in K[\text{SL}_n]$, $\Delta_{n-1}' f \in (d')$ implies $f \in (d')$. So assume that $\Delta_{n-1}' f = gd'$ for some $f, g \in K[\text{SL}_n]$. If we take $a \in \mathbb{K}^n$ such that $a_n = (-1)^{n-1}$, then we have $x_n \in \text{SL}_n$, $d'(x_n) = 1$ and $\Delta_{n-1}'(x_n) = 0$. So $\Delta_{n-1}'$ does not divide $d'$. But then, by Lemma [2] $\Delta'_{n-1}$ divides $g$. Cancelling a factor $\Delta_{n-1}'$ on both sides of $(*), we obtain that $f \in (d')$.

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

For the basics about monomial orderings and Gröbner bases I refer to [3].
Lemma 4. If we give the monomials in the variables $\xi_{ij}$ the lexicographic monomial ordering for which $\xi_{nn} > \xi_{n-1n} \cdots > \xi_{n1} > \xi_{n-1n} \cdots > \xi_{11}$, then det has leading term $\pm \xi_{nn} \cdots \xi_{22} \xi_{11}$ and $d$ has leading term $\pm s_{n1}^{-1} \cdots \xi_{22}^2 \xi_{21}$.

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 nonzero polynomial $f$ is denoted by $\text{LT}(f)$. Let $i \in \{1, \ldots, n\}$ and $\Lambda \subseteq \{1, \ldots, n\}$ with $|\Lambda| = k \geq 2$ and assume that $\partial_{i n}(\det(X_{\Lambda,n})) \neq 0$. Then $i, n \in \Lambda$. Now we use the fact that no monomial in $\partial_{i n}(\det(X_{\Lambda,n}))$ 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

$$\text{LT}(\partial_{i n}(\det(X_{\Lambda,n}))) \leq \pm \xi_{n1} \cdots \xi_{i+1} \xi_{i-1} \cdots \xi_{n-k+1}$$

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

$$\text{LT}(\partial_{i n}(\det(X_{\Lambda,n}))) \leq \pm \xi_{n1} \cdots \xi_{n-k+2}$$

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

$$\text{LT}(\partial_{i n}(\det(X_{\Lambda,n}))) \leq \pm \xi_{n1} \cdots \xi_{n-k+2} \xi_{n-k+2}$$

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

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

$$\text{LT}(\partial_{i n} s_k) = \begin{cases} \pm \xi_{n1} \cdots \xi_{i+1} \xi_{i-1} \cdots \xi_{n-k+1} \xi_{n-k+1} & \text{if } i + k > n + 1, \\ \pm \xi_{n1} \cdots \xi_{n-k+2} & \text{if } i + k = n + 1, \\ \pm \xi_{n1} \cdots \xi_{n-k+3} \xi_{n-k+2} \xi_{n-k+2} & \text{if } i + k < n + 1. \end{cases}$$

In particular $\text{LT}(\partial_{i n} s_k) \leq \pm \xi_{n1} \cdots \xi_{n-k+1} \xi_{n-k+1}$ with equality if and only if $i + k = n + 1$. But then, by equation (3), $\text{LT}(d) = \text{LT}(\partial_{i n} s_1) \text{LT}(\partial_{n1} s_2) \cdots \text{LT}(\partial_{i n} s_n) = \pm \xi_{n1}^{-1} \cdots \xi_{22}^2 \xi_{21} \square$

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 5. Let $f_i \in \mathbb{Z}[u_1, \ldots, u_{n-1}]$ be the polynomial such that $\text{sym}(l \omega_i) = f_i(\text{sym}(\omega_1), \ldots, \text{sym}(\omega_{n-1}))$. If we give the monomials in the $u_i$ the degree reverse lexicographic monomial ordering for which $u_1 > \cdots > u_{n-1}$, then $f_i$ has leading term $u_i^l$. Furthermore, the monomials that appear in $f_i - u_i^l$ are of total degree $\leq l$ and have exponents $< l$. 6
Proof. Let \( \sigma_i \) be the \( i \)-th elementary symmetric function in the variables \( x_1, \ldots, x_n \) and let \( \lambda_i \in P = X(T) \) be the character \( A \mapsto A_{\lambda_i} \) of \( T \). Then \( \text{sym}(\lambda_i) = \sigma_i(e(\lambda_1), \ldots, e(\lambda_n)) \) for \( i \in \{1, \ldots, n-1\} \). So the \( f_i \) can be found as follows. For \( i \in \{1, \ldots, n-1\} \), determine \( F_i \in \mathbb{Z}[u_1, \ldots, u_n] \) such that \( \sigma_i(x_1^l, \ldots, x_n^l) = F_i(\sigma_1, \ldots, \sigma_n) \). Then \( f_i = F_i(u_1, \ldots, u_{n-1}, 1) \). It now suffices to show that for \( i \in \{1, \ldots, n-1\} \), \( F_i - u_i^l \) is a \( \mathbb{Z} \)-linear combination of monomials in the \( u_j \) that have exponents \( < l \), are of total degree \( \leq l \) 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 \( i \in \{1, \ldots, n-1\} \). Consider the following properties of a monomial in the \( x_j \):

- (x1) the monomial contains at least \( i+1 \) variables.
- (x2) the exponents are \( \leq l \).
- (x3) the number of exponents equal to \( l \) is \( \leq i \).

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 \( \leq l \).
- (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 \( h = H(\sigma_1, \ldots, \sigma_n) \). Give the monomials in the \( x_i \) the lexicographic monomial ordering for which \( x_1 > \cdots > x_n \). We will show by induction on the leading monomial of \( h \) that if each monomial that appears in \( h \) has property (x1) resp. property (x2) resp. properties (x1), (x2) and (x3), then each monomial that appears in \( H \) has property (u1) resp. property (u2) resp. properties (u1), (u2) and (u3). Let \( x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n} \) be the leading monomial of \( h \). Then \( \alpha_1 \geq \alpha_2 \cdots \geq \alpha_n \). Put \( \beta = (\alpha_1 - \alpha_2, \ldots, \alpha_{n-1} - \alpha_n, \alpha_n) \). Let \( k \) be the last index for which \( \alpha_k \neq 0 \). Then \( \beta = (\alpha_1 - \alpha_2, \ldots, \alpha_{k-1} - \alpha_k, \alpha_k, 0, \ldots, 0) \). If \( x^\alpha \) has property (x1), then \( k \geq i+1 \), \( \beta^\beta \) has property (u1) and the monomials that appear in \( \sigma^\beta \) have property (x1), since \( \sigma_k \) appears in \( \sigma^\beta \). If \( x^\alpha \) has property (x2), then \( \alpha_1 \leq l \), \( \beta^\beta \) is of total degree \( \alpha_1 \leq l \) and the monomials that appear in \( \sigma^\beta \) have exponents \( \leq \beta_1 + \cdots + \beta_k = \alpha_1 \leq l \). Now assume that \( x^\alpha \) 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 \( \alpha_k \) were equal to \( l \), then we would have \( \alpha_1 = \cdots = \alpha_l = l \), by (x2). This contradicts (x3), since we have \( k \geq i+1 \) by (x1). Finally we show that the monomials that appear in \( \sigma^\beta \) 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 \( \sigma^\beta \) is \( \leq j \). On the other hand \( \alpha_1 = \cdots = \alpha_j = l \). So we must have \( j \leq i \), since \( x^\alpha \) has property (x3).

\(^6\)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 [S] as follows: \( P_i = f_i(x_1, \ldots, x_{n-1}) = \text{sym}(l(\lambda_i)) \). In particular \( d_{i0} = \text{sym}(l(\lambda_i)) \) and \( d_{i\mu} \in \mathbb{Z} \) for all \( \mu \in P \setminus \{0\} \) (we are, of course, in the situation that \( g = \mathfrak{sl}_n \)).
Proposition 1. The following holds:

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

(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
\[ u_1^{k_1} \cdots u_{n-1}^{k_{n-1}} z_1^{m_1} \cdots z_{n-1}^{m_{n-1}}, 0 \leq k_i < l, 0 \leq m_i < 2 \] as a basis.

(iv) \( A[z_1, \ldots, z_{n-1}] \cap Z_1 = A \cap Z_1 = \mathbb{Z}[\tilde{s}_1, \ldots, \tilde{s}_{n-1}] \) and \( B \cap Z_1 \) is a free \( A \cap Z_1 \)-module with the monomials
\[ u_1^{k_1} \cdots u_{n-1}^{k_{n-1}}, 0 \leq k_i < l \] as a basis.

Proof. Let \( Z'_0 \) be the \( \mathbb{C} \)-subalgebra of \( Z \) generated by the \( \tilde{\xi}_{ij} \) and \( z_1, \ldots, z_{n-1} \). As we have seen in Subsection 1.3, 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 \( \text{Fr}(Z_0) \) of \( Z_0 \) by arguments very similar to those at the end of the proof of Theorem 3. This shows that the monomials \( z_1^{m_1} \cdots z_{n-1}^{m_{n-1}}, 0 \leq m_i < 2 \), form a basis of \( \text{Fr}(Z'_0) \) over \( \text{Fr}(Z_0) \) and of \( Z'_0 \) over \( Z_0 \). It follows that the kernel of the natural homomorphism from the polynomial algebra \( \mathbb{C}[(\xi_{ij})_{ij}, z_1, \ldots, z_{n-1}] \) to \( Z'_0 \) is generated by the elements \( \det -1, z_1^2 - \Delta_1, \ldots, z_{n-1}^2 - \Delta_{n-1} \). So we have generators and relations for \( Z'_0 \). By the construction from Subsection 1.3 we then obtain that the kernel \( I \) 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 \( Z'_0 \) is generated by the elements \( \det -1, f_1 - s_1, \ldots, f_{n-1} - s_{n-1}, z_1^2 - \Delta_1, \ldots, z_{n-1}^2 - \Delta_{n-1} \).

Now we give the monomials in the variables \( (\xi_{ij})_{ij}, u_1, \ldots, u_{n-1}, z_1, \ldots, z_{n-1} \) 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 5 on the monomials in the \( u_i \) and the monomial ordering of Lemma 4 on the \( \xi_{ij} \).

7In \[8\] and \[9\] \( z_n \) is denoted by \( z_i \).

8So the \( z_i \) are greater than the \( u_i \) which are greater than the \( \xi_{ij} \).
Then the ideal generators mentioned above have leading monomials \( \xi_{n,n} \cdots \xi_{22} \xi_{11} \), \( u_{1}^{i_{1}} \cdots u_{n-1}^{i_{n-1}}, z_{1}^{2}, \ldots, z_{n-1}^{2} \) and the leading coefficients are all \( \pm 1 \). Since the leading monomials have gcd 1, the ideal generators form a Gröbner basis; see [3] Ch. 2 § 9 Theorem 3 and Proposition 4, for example. Since the leading coefficients are all \( \pm 1 \), it follows from the division with remainder algorithm that the ideal of \( \mathbb{Z}[(\xi_{ij})_{ij}, u_{1}, \ldots, u_{n-1}, z_{1}, \ldots, z_{n-1}] \) 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 \( \xi_{ij} \) that are not divisible by \( \xi_{n,n} \cdots \xi_{22} \xi_{11} \) and the restricted monomials mentioned in the assertion. The canonical images of the monomials in the \( \xi_{ij} \) that are not divisible by \( \xi_{n,n} \cdots \xi_{22} \xi_{11} \) 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 \( A[z_{1}, \ldots, z_{n-1}] \cap \tilde{Z}_{0} = A \). Therefore, by Theorem 1(ii), \( A[z_{1}, \ldots, z_{n-1}] \cap Z_{1} = A \cap Z_{1} = \pi^{co}(\mathbb{Z}[\text{SL}_{n}]^{\text{SL}_{n}}) \). Now \( \mathbb{Z}[\pi] = \mathbb{Z}[\text{sym}(\varpi_{1}), \ldots, \text{sym}(\varpi_{n-1})] \) (see [3] no. VI.3.4, Thm. 1.) and the \( s'_{i} \) are in \( \mathbb{Z}[\text{SL}_{n}] \), so \( \mathbb{Z}[\text{SL}_{n}]^{\text{SL}_{n}} = \mathbb{Z}[s'_{1}, \ldots, s'_{n-1}] \) by the restriction theorem for \( \mathbb{C}[\text{SL}_{n}] \). This proves the first assertion. From the proof of Theorem 2 we know that the given monomials form a basis of \( Z_{1} \) over \( \mathbb{Z} \cap Z_{1} \) and a basis of \( Z \) over \( \mathbb{Z} \). So an element of \( Z \) is in \( Z_{1} \) if and only if its coefficients with respect to this basis are in \( \mathbb{Z} \cap Z_{1} \). The second assertion now follows from (iii).\( \square \)

By (ii) of the above proposition we may identify \( B(\mathbb{C}) \) with \( \tilde{Z}_{0}[z_{1}, \ldots, z_{n-1}]Z_{1} \) and \( B(\mathbb{C})[\Delta_{1}^{-1}, \ldots, \Delta_{n-1}^{-1}] \) with \( Z \).

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

**Proposition 1** The following holds:

(i) The kernel of the natural homomorphism from the polynomial algebra \( \mathbb{Z}[(\xi_{ij})_{ij}, u_{1}, \ldots, u_{n-1}, z_{1}, \ldots, z_{n-1}] \) to \( \overline{B} \) is generated by the elements \( \det -1, d, f_{1} - s_{1}, \ldots, f_{n-1} - s_{n-1}, z_{1}^{2} - \Delta_{1}, \ldots, z_{n-1}^{2} - \Delta_{n-1} \).

(ii) The kernel of the natural homomorphism \( \mathbb{Z}[\text{Mat}_{n}] \to \overline{A} \) is \( (\det -1, d) \).

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

(iv) \( \overline{A} \) is a free \( \mathbb{Z} \)-module and \( \overline{B} \) is a free \( \overline{A} \)-module with the monomials \( \overline{u}_{1}^{k_{1}} \cdots \overline{u}_{n-1}^{l} \overline{z}_{1}^{m_{1}} \cdots \overline{z}_{n-1}^{m_{n-1}}, 0 \leq k_{i} < l, 0 \leq m_{i} < 2 \) as a basis.
(v) The $\overline{A}$-span of the monomials $\overline{\pi}_1^{k_1} \cdots \overline{\pi}_{n-1}^{k_{n-1}}$, $0 \leq k_i < l$, is closed under multiplication.

Proof. From Lemma 3(iii) we deduce that $(A(\mathbb{C})[\Delta_1^{-1}, \ldots, \Delta_{n-1}^{-1}]d) \cap A(\mathbb{C}) = A(\mathbb{C})d$. From this it follows, using the $A(\mathbb{C})$-basis of $B(\mathbb{C})$, that $(Zd) \cap B(\mathbb{C})$, which is the kernel of the natural homomorphism $B(\mathbb{C}) \to \overline{\mathbb{Z}}$, equals $B(\mathbb{C})d$.

From (i) and (ii) of Proposition 4 or from its proof it now follows that the kernel of the natural homomorphism $\mathbb{C}[\text{Mat}_n] \to \overline{\mathbb{Z}}$ is generated by $\det -1, d, f_1 - s_1, \ldots, f_{n-1} - s_{n-1}, z_1^2 - \Delta_1, \ldots, z_{n-1}^2 - \Delta_{n-1}$.

Again using the $A(\mathbb{C})$-basis of $B(\mathbb{C})$ we obtain that $(B(\mathbb{C})d) \cap A(\mathbb{C}) = A(\mathbb{C})d$.

By Lemma 4 we have $\text{LT}(d) = \pm \xi_{n,n-1}^2 \cdots \xi_{3,21}^2$ 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 4.

(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 $\overline{A}$ and $\overline{B(\mathbb{C})}[\Delta_1^{-1}, \ldots, \Delta_{n-1}^{-1}]$ can be identified with respectively $\mathbb{Z}[\text{Mat}_n]/(\det -1, d)$ and $\overline{\mathbb{Z}}$. From (iv) it follows that, for any commutative ring $R$, $\overline{A(R)}$ embeds in $\overline{B(R)}$.

3.4. The theorem.

Lemma 6. 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 $I_a$ resp. $I_b$ be the set of indices $i$ such that $\alpha_i \neq 0$ resp. $\beta_i \neq 0$ 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 nonempty 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 $L$:

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

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

But then they also have a solution over a finite extension $F'$ of $F$ by Hilbert’s Nullstellensatz. This solution gives us nonzero elements $a', b' \in F' \otimes_F A$ with $a'b' = 0$. $\square$
Lemma 7. Let $R$ be the valuation ring of a nontrivial 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 $\nu$ be an extension to $F'$ of the given valuation of $F$, let $R'$ be the valuation ring of $\nu$, let $K'$ be the residue class field and let $\delta \in R'$ be a uniformiser for $\nu$. 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. Chapter 8 Theorem 5.1). By multiplying $a$ and $b$ by suitable integral powers of $\delta$ we may assume that their coefficients with respect to the basis $(e_i)_{i \in I}$ are in $R'$ and not all divisible by $\delta$ (in $R'$). By passing to the residue class field $K$ we then obtain nonzero $a', b' \in K' \otimes_{R'} (R' \otimes_R A) = K' \otimes_R A$ with $a'b' = 0$. □

Remark. The above lemmas also hold if we replace ”zero divisors” by ”nonzero nilpotent elements”.

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

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 of Proposition 1 that for $n = 2$ it holds without any extra assumptions on $l$, so assume that $n \geq 3$. 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 $\overline{Z} = Z/(\tilde{d})$ is an integral domain. We do this in 5 steps.

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

We may assume that $K$ is algebraically closed. Since $\overline{B}(K)$ is a finite $\overline{A}(K)$-module it follows that $\overline{B}(K)$ is integral over $\overline{A}(K) \cong K[\text{Mat}_n]/(\det - 1, d)$. So it its Krull dimension is $n^2 - 2$. By Proposition 1 $\overline{B}(K)$ 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. So $\overline{B}(K)$ is Cohen-Macaulay (see Proposition 18.13). Let $\mathcal{V}$ be the closed subvariety of $n^2 + 2(n - 1)$-dimensional affine space defined by $I$. By Theorem 18.15 in [11] it suffices to show that the
closed subvariety of \( V \) defined by the Jacobian ideal of \( -1, d, f_1-s_1, \ldots, f_{n-1}-s_{n-1}, z_1^2-\Delta_1, z_{n-1}^2-\Delta_{n-1} \) is of codimension \( \geq 1 \).

By Lemmas 3 and 2, \((\det -1, d)\) is a prime ideal of \( K[\text{Mat}_n]\). So we have an embedding \( K[\text{Mat}_n]/(\det -1, d) \to K[V] \) which is the comorphism of a finite surjective morphism of varieties \( V \to V(\det -1, d) \), where \( V(\det -1, d) \) is the closed subvariety of \( \text{Mat}_n \) that consists of the matrices of determinant 1 on which \( d \) vanishes. This morphism maps the closed subvariety of \( V \) defined by the Jacobian ideal of \( -1, d, f_1-s_1, \ldots, f_{n-1}-s_{n-1}, z_1^2-\Delta_1, z_{n-1}^2-\Delta_{n-1} \) 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 \((s_1, \ldots, s_n, \Delta_1, \ldots, \Delta_{n-1})\) with respect to the variables \( \xi_{ij} \). 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 \( \Delta_i \). Since finite morphisms preserve dimension (see e.g. Corollary 9.3), it suffices to show that the latter variety is of codimension \( \geq 1 \) in \( V(\det -1, d) \). Since \( V(\det -1, d) \) is irreducible, this follows from Lemma 1(ii).

2. \( \mathcal{B}_0(K) \) 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 3) and the additivity of the \( p \)-th power map in characteristic \( p \) it follows that \( f_i = u_i^p \mod p \). So the kernel of the natural homomorphism from the polynomial algebra \( K[\xi_{ij}, u_1, \ldots, u_{n-1}, z_1, \ldots, z_{n-1}] \) to \( \mathcal{B}(K) \) is generated by the elements \( \det -1, d, u_1^p - s_1, \ldots, u_{n-1}^p - s_{n-1} \) and the \( \mathcal{A}(K) \)-span of the monomials \( \overline{u}_1^{k_1} \cdots \overline{u}_k^{k_k}, 0 \leq k_i < l, \) is closed under multiplication for each \( t \in \{0, \ldots, n-1\} \). We show by induction on \( t \) that \( \mathcal{B}_{0,t}(K) = \mathcal{A}(K)[\overline{u}_1, \ldots, \overline{u}_t] \) is an integral domain for \( t = 0, \ldots, n-1 \). For \( t = 0 \) this follows from Lemma 3 and Proposition 1(ii). Let \( t \in \{1, \ldots, n-1\} \) and assume that it holds for \( t - 1 \). Clearly \( \mathcal{B}_{0,t}(K) = \mathcal{B}_{0,t-1}(K)[\overline{u}_t] \cong \mathcal{B}_{t-1}(K)[x]/(x^t - \overline{x}_t) \). So it suffices to prove that \( x^t - \overline{x}_t \) is irreducible over the field of fractions of \( \mathcal{B}_{0,t-1}(K) \). By the Vahlen-Capelli criterion or a more direct argument, it suffices to show that \( \overline{x}_t \) is not a \( p \)-th power in the field of fractions of \( \mathcal{B}_{0,t-1}(K) \). So assume that \( \overline{x}_t = (v/w)^p \) for some \( v, w \in \mathcal{B}_{0,t-1}(K) \) with \( w \neq 0 \). Then we have \( v^p = \overline{x}_tw^p = \overline{u}_tw^p \). So with \( l = \text{lcm}(p, t) \), we have \( v^l = \overline{x}_t^lw^l = 0 \). But then \( v - \overline{u}_tw = 0 \) by Step 1. Now recall that \( v \) and \( w \) can be expressed uniquely as \( \mathcal{A}(K) \)-linear combinations of monomials in \( \overline{u}_1, \ldots, \overline{u}_{t-1} \) with exponents \( < l \). If such a monomial appears with a nonzero coefficient in \( w \), then \( \overline{u}_t^l \) times this monomial appears with the same coefficient in the expression of \( 0 = v - \overline{u}_tw \) as an \( \mathcal{A}(K) \)-linear combination of restricted monomials in \( \overline{u}_1, \ldots, \overline{u}_{t-1} \). Since this is impossible, we must have \( w = 0 \). A contradiction.

3. \( \mathcal{B}_0(\mathbb{C}) \) is an integral domain.

This follows immediately from Step 2 and Lemma 7 applied to the \( p \)-adic valuation of \( \mathbb{Q} \) and with \( L = \mathbb{C} \).

4. \( \mathcal{B}_t(\mathbb{C}) \) 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 $\overline{B}_t(\mathbb{C}) = \overline{B}_{t-1}(\mathbb{C})[\tau_t] \cong \overline{B}_{t-1}(\mathbb{C})[x]/(x^2 - \Delta_t)$. So it suffices to prove that $x^2 - \Delta_t$ is irreducible over the field of fractions of $\overline{B}_{t-1}(\mathbb{C})$. Assume that $x^2 - \Delta_t$ has a root in this field, i.e. that $\Delta_t = (v/w)^2$ for some $v, w \in \overline{B}_{t-1}(\mathbb{C})$ with $w \neq 0$. By the same arguments as in the proof of Lemma 3 we may assume that for some finite extension $F$ of $\mathbb{Q}$ there exist $v, w \in \overline{B}_{t-1}(F)$ with $w \neq 0$ and $w^2 \Delta_t = v^2$.

Let $\nu_2$ be an extension to $F$ of the 2-adic valuation of $\mathbb{Q}$, let $S_2$ be the valuation ring of $\nu_2$, let $K$ be the residue class field and let $\delta \in S_2$ be a uniformiser for $\nu_2$. We may assume that the coefficients of $v$ and $w$ with respect to the $\mathbb{Z}$-basis of $\overline{B}_{t-1}$ mentioned earlier are in $S_2$. Assume that the coefficients of $w$ are all divisible by $\delta$ (in $S_2$). Then $w = 0$ in $\overline{B}_{t-1}(K)$ and therefore $v^2 = 0$ in $\overline{B}_{t-1}(K)$.

But by Step 1, $\overline{B}_{t-1}(K)$ is reduced, so $v = 0$ in $\overline{B}_{t-1}(K)$ and all coefficients of $v$ are divisible by $\delta$. So, by cancelling a suitable power of $\delta$ in $w$ and $v$, we may assume that not all coefficients of $w$ are divisible by $\delta$. By passing to the residue class field $K$ we then obtain $v, w \in \overline{B}_{t-1}(K)$ with $w \neq 0$ and $w^2 \Delta_t = v^2$. But then $(w\bar{\tau}_t - v)^2 = 0$ in $\overline{B}_t(K)$, since $\bar{\tau}_t^2 = \Delta_t$ and $K$ is of characteristic 2. The reducedness of $\overline{B}_t(K)$ (Step 1) now gives $w\bar{\tau}_t - v = 0$ in $\overline{B}_t(K)$.

Now recall that $v$ and $w$ can be expressed uniquely as $A(K)$-linear combinations of the monomials $u_{k_1} \cdots u_{k_{n-1}} \bar{\tau}_1 \cdots \bar{\tau}_{t-1}$, $0 \leq k_i < l$, $0 \leq m_i < 2$. We then obtain a contradiction in the same way as at the end of Step 2.

5. $\mathbb{Z}/(d)$ is an integral domain.

Since $\mathbb{Z} = \overline{B}(\mathbb{C})[\Delta_1^{-1}, \ldots, \Delta_{n-1}^{-1}]$ and the $\Delta_i$ are nonzero in $\overline{A}(\mathbb{C}) \cong \mathbb{C}[SL_n]/(d')$ by Lemma 3 this follows from Step 4.

\textbf{Remarks.}

1. Note that we didn’t prove that $\overline{B}(K)$ is an integral domain for $K$ some algebraically closed field of positive characteristic.

2. 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.

\textbf{References}

[1] A. Braun, C. R. Hajarnavis, \textit{Smooth polynomial identity algebras with almost factorial centers}, Warwick preprint: 7/2003.

[2] A. Borel, \textit{Linear algebraic groups}, Second edition, Graduate Texts in Mathematics 126, Springer-Verlag, New York, 1991.

[3] N. Bourbaki, \textit{Groupes et Algèbres de Lie}, Chaps. 4, 5 et 6, Hermann, Paris, 1968.

[4] J.-M. Bois, \textit{Corps enveloppants des algèbres de Lie en dimension infinie et en caractéristique positive}, Thesis, University of Rheims, 2004.

[5] D. Cox, J. Little, D. O’Shea, \textit{Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra}, Second edition, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997.

[6] P. M. Cohn, \textit{Algebra}, Vol. 2, Second edition, John Wiley & Sons, Ltd., Chichester, 1982.
[7] C. De Concini, V. G. Kac, *Representations of quantum groups at roots of 1*, Operator algebras, unitary representations, enveloping algebras, and invariant theory (Paris, 1989), 471-506, Progr. Math. 92, Birkhäuser Boston, MA, 1990.
[8] C. De Concini, V. G. Kac, C. Procesi, *Quantum coadjoint action*, J. Amer. Math. Soc. 5 (1992), no. 1, 151-189.
[9] C. De Concini, C. Procesi, *Quantum groups, D-modules, representation theory, and quantum groups* (Venice, 1992), 31-140, Lecture Notes in Math. 1565, Springer, Berlin, 1993.
[10] J. Dixmier, *Sur les algèbres enveloppantes de sl(n, C) et af(n, C)*, Bull. Sci. Math. (2) 100 (1976), no. 1, 57-95.
[11] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Math., vol. 150, Springer, New York, 1995.
[12] F. Fauquant-Millet, *Sur une algèbre parabolique P de U_q(sl_{n+1}) et ses semi-invariants par l'action adjointe de P*, Bull. Sci. Math. 122 (1998), no. 7, 495-519.
[13] F. Fauquant-Millet, *Quantification de la localisation de Dixmier de U(sl_{n+1}(C))*, J. Algebra 218 (1999), no. 1, 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) (1986), no. 4, 475-487 (Russian); Math. USSR Sbornik 58 (1987), no. 2, 477-490 (English translation).
[15] V. L. Popov, *Picard groups of homogeneous spaces of linear algebraic groups and one-dimensional homogeneous vector fiberings*, Izv. Akad. Nauk SSSR Ser. Mat. 38 (1974), 294-322 (Russian); Math. USSR Izvestija 8 (1974), no. 2, 301-327 (English translation).
[16] A. A. Premet and R. H. Tange, *Zassenhaus varieties of general linear Lie algebras*, to appear in J. Algebra.
[17] R. Steinberg, *Regular elements of semi-simple algebraic groups*, Inst. Hautes Études Sci. Publ. Math. 25 (1965), 49-80.

Department of Mathematics, The University of Manchester, Oxford Road, M13 9PL, UK
E-mail address: rudolf.h.tange@stud.man.ac.uk