ON QUASITRIANGULAR QUASI-HOPF ALGEBRAS
AND A GROUP CLOSELY CONNECTED WITH Gal(Q/𝑄)

V. G. DRIÑFEL'D

ABSTRACT. A previously announced theorem is proved concerning the structure of quasitriangular quasi-Hopf algebras in the framework of the theory of perturbations with respect to the Planck constant. In the process we use the pro-unipotent version of a group defined by Grothendieck that contains Gal(Q/𝑄).

§1. Introduction

This paper is devoted primarily to the proof of a theorem announced in [1] concerning the structure of quasitriangular quasi-Hopf algebras in the framework of the theory of perturbations with respect to the Planck constant ℏ.

As a technical tool we use the pro-unipotent version of a group introduced by Grothendieck in [2] — a group of enormous interest because of its close connection with Gal(𝐐/𝐐).

Let us recall the basic definitions of [1]. A quasi-Hopf algebra differs from a Hopf algebra in that the coassociativity axiom is replaced by a weaker condition. More precisely, a quasi-Hopf algebra over a commutative ring k, as defined in [1], is a set (A, Δ, ε, Φ), where A is an associative k-algebra with unity, Δ a homomorphism A → A ⊗ A, ε a homomorphism A → k (we assume that Δ(1) = 1, ε(1) = 1), and Φ an invertible element of A ⊗ A ⊗ A, all these satisfying

\begin{align*}
(id ⊗ Δ)(Δ(a)) &= Φ · (Δ ⊗ id)(Δ(a)) · Φ^{-1}, \quad a ∈ A, \\
(id ⊗ id ⊗ Δ)(Φ) · (Δ ⊗ id ⊗ id)(Φ) &= (1 ⊗ Φ) · (id ⊗ Δ ⊗ id)(Φ) · (Φ ⊗ 1), \\
(ε ⊗ id) ◦ Δ &= id = (id ⊗ ε) ◦ Δ, \\
(id ⊗ ε ⊗ id)(Φ) &= 1,
\end{align*}

(together with an axiom which in the Hopf case, i.e., for Φ = 1, reduces to existence and bijectivity of an antipode. In the situation of the present paper, when (A, Δ, ε, Φ) is a deformation of a Hopf algebra depending on an “infinitely small” parameter ℏ, this axiom is satisfied automatically by Theorem 1.6 of [1]. As in the Hopf case, Δ is called the comultiplication, and ε the counit.

The paper [1] generalized to the quasitriangular Hopf algebra defined in §10 of [3] and inspired by the quantum method for the inverse problem [4]. Specifically, a quasitriangular quasi-Hopf algebra is a set (A, Δ, ε, Φ, R), where (A, Δ, ε, Φ) is a quasi-Hopf algebra and R an


Key words and phrases. Hopf algebras, quantum groups, conformal field theory, Galois group of the rationals, braid groups, Lie algebras.
invertible element of \( A \otimes A \) such that

\[
\Delta'(a) = R \Delta(a) R^{-1}, \quad a \in A, \tag{1.5}
\]

\[
(\Delta \otimes \text{id})(R) = \Phi^{312} R^{13} (\Phi^{132})^{-1} R^{23} \Phi. \tag{1.6a}
\]

\[
(\text{id} \otimes \Delta)(R) = (\Phi^{231})^{-1} R^{13} \Phi^{213} R^{12} \Phi^{-1}. \tag{1.6b}
\]

Here \( \Delta' = \sigma \circ \Delta \), where \( \sigma : A \otimes A \to A \otimes A \) interchanges the tensor factors. If

\[
R = \sum_i a_i \otimes b_i
\]

then by definition \( R^{12} = \sum_i a_i \otimes b_i \otimes 1 \), \( R^{13} = \sum_i a_i \otimes 1 \otimes b_i \), and \( R^{23} = \sum_i 1 \otimes a_i \otimes b_i \). We also need to explain that, for example, if \( \Phi = \sum_j x_j \otimes y_j \otimes z_j \), then \( \Phi^{312} = \sum_j y_j \otimes z_j \otimes x_j \).

The gist of the axioms (1.1)-(1.6) is that the representations of a quasitriangular quasi-Hopf algebra \( A \) form a quasitensor category in the sense of [5] (see also §3 of [1]). This means that, firstly, there exists in the category of representations of \( A \) a tensor-product functor: given two representations of \( A \), in \( k \)-modules \( V_i \) and \( V_j \), the representation of \( A \) in \( V_i \otimes V_j \) is defined as the composite \( A \xrightarrow{\Delta} A \otimes A \to \text{End}_k(V_i \otimes V_j) \). Secondly, there exist functorial isomorphisms of commutativity \( c : V_i \otimes V_j \xrightarrow{\sim} V_j \otimes V_i \) and associativity \( a : (V_i \otimes V_j) \otimes V_k \xrightarrow{\sim} V_i \otimes (V_j \otimes V_k) \) where the \( V_i \) are representations of \( A \).

Namely, \( c \) is the operator in \( V_i \otimes V_j \otimes V_k \) corresponding to \( \Phi \), and \( a \) is the composite of the operator in \( V_i \otimes V_j \) corresponding to \( R \) with the usual isomorphism \( \sigma : V_i \otimes V_j \xrightarrow{\sim} V_j \otimes V_i \). Thirdly, there exists an identity representation \( k \) and isomorphisms \( V \otimes k \xrightarrow{\sim} V \) and \( k \otimes V \xrightarrow{\sim} V \) for any representation \( V \).

Finally, (1.2), (1.4), and (1.6) guarantee the commutativity of the diagrams

\[
\begin{array}{ccc}
(V_i \otimes (V_j \otimes V_k)) \otimes V_4 & \xrightarrow{\sim} & V_1 \otimes ((V_2 \otimes V_3) \otimes V_4) \\
\downarrow & & \downarrow \\
(V_i \otimes (V_2 \otimes V_3)) \otimes V_4 & \xrightarrow{\sim} & V_1 \otimes ((V_2 \otimes V_3) \otimes V_4)
\end{array}
\]

\[
(1.7)
\]

\[
\begin{array}{ccc}
V_i \otimes V_2 & \xrightarrow{\sim} & V_1 \otimes (V_2 \otimes V_3) \\
\downarrow & & \downarrow \\
V_i \otimes (V_2 \otimes V_3) & \xrightarrow{\sim} & V_i \otimes (k \otimes V_k)
\end{array}
\]

\[
(1.8)
\]

We note that in general \( R^{21} \neq R^{-1} \), and consequently the commutativity isomorphism is not involutory (a point of difference between quasitensor categories and tensored [6]).
If \((A, \Delta, \varepsilon, \Phi, R)\) is a quasitriangular quasi-Hopf algebra, and \(F\) an invertible element of \(A \otimes A\) such that \((\text{id} \otimes \varepsilon)(F) = 1 = (\varepsilon \otimes \text{id})(F)\), then putting
\[
\tilde{\Delta}(a) = F \cdot \Delta(a) \cdot F^{-1},
\]
\[
\tilde{\Phi} = F^{23} \cdot (\text{id} \otimes \Delta)(F) \cdot \Phi \cdot (\Delta \otimes \text{id})(F^{-1}) \cdot (F^{12})^{-1},
\]
\[
\tilde{R} = R^{21} \cdot R \cdot F^{-1},
\]
we obtain a new quasitriangular quasi-Hopf algebra \((A, \tilde{\Delta}, \varepsilon, \tilde{\Phi}, \tilde{R})\); we say it is obtained from \((A, \Delta, \varepsilon, \Phi, R)\) by twisting via \(F\). The quasitensor categories that correspond to \((A, \Delta, \varepsilon, \Phi, R)\) and \((A, \tilde{\Delta}, \varepsilon, \tilde{\Phi}, \tilde{R})\) are equivalent. It is therefore natural to refer to the twisting as a “gauge transformation”.

We shall study quasitriangular quasi-Hopf algebras in the framework of the theory of perturbations with respect to \(h\), restricting ourselves to the case of characteristic 0. These words are given a precise meaning by the following definition (QUE is short for “quantized universal enveloping”).

**Definition.** Let \(k\) be a field of characteristic 0. By a quasitriangular quasi-Hopf QUE-algebra over \(k[[h]]\) is meant a topological quasitriangular quasi-Hopf algebra \((A, \Delta, \varepsilon, \Phi, R)\) over \(k[[h]]\) such that \(A/hA\) is a universal enveloping algebra with the standard comultiplication, and \(A\), as a topological \(k[[h]]\)-module, is isomorphic to \(V[[h]]\) for some vector space \(V\) over \(k\).

**Remark.** Since \(A/hA\) is a universal enveloping algebra, it follows from (1.4) and the invertibility of \(\Phi\) that \(\Phi \equiv 1 \mod h\). Similarly, \(R \equiv 1 \mod h\), and for a twisting of quasitriangular quasi-Hopf QUE-algebras, \(F \equiv 1 \mod h\).

Inspired by [7],[9], the following method was proposed in [1] for constructing quasitriangular quasi-Hopf QUE-algebras. Let \(g\) be a Lie algebra over \(k[[h]]\) which as a \(k[[h]]\)-module is isomorphic to \(V[[h]]\) for some vector space \(V\) over \(k\). (This condition on \(g\) means that \(g\) is a deformation of a Lie algebra \(g_0\) over \(k\), where \(g_0 = g/hg\); such algebras \(g\) will therefore be called deformation algebras.) Suppose given a symmetric \(g\)-invariant tensor \(t \in g \otimes g\), where \(\otimes\) is the complete tensor product. Put \(A = U_g\), where \(U_g\) means the \(h\)-adic completion of the universal enveloping algebra. Define in the usual way \(e: A \rightarrow k[[h]]\) and \(\Delta: A \rightarrow A \otimes A\) (where \(\otimes\) is the complete tensor product), and put \(R = e^{hR/2}\). Then (1.3)–(1.5) are satisfied, and it remains to find \(\Phi \in A \otimes A \otimes A\) satisfying (1.1), (1.2), (1.4), and (1.6) (note that (1.1) means in this situation the \(g\)-invariance of \(\Phi\)). The first main result of the present paper is:

**Theorem A.** Such a \(\Phi\) exists, and is unique up to twisting via symmetric \(g\)-invariant elements \(F \in A \otimes A\).

**Remarks.** a) If \(\Delta\) is the usual comultiplication in \(A = U_g\) and \(R = e^{hR/2}\), and \(\Delta\) and \(R\) are defined by formulas (1.10) and (1.12), then the equalities \(\tilde{\Delta} = \Delta\) and \(\tilde{R} = R\) are equivalent to \(g\)-invariance and symmetry of \(F\) (\(t\) commutes with the \(g\)-invariant elements of \(A \otimes A\), since \(t = (\Delta(C) - C \otimes 1 - 1 \otimes C)/2\), where \(C \in U_g\) is the Casimir element).

b) Together with Theorem A we prove that if the condition \(R = e^{hR/2}\) is replaced by the at first sight weaker conditions of symmetry and \(g\)-invariance of \(R\), then automatically \(R = e^{hR/2}\) for some \(t \in g \otimes g\).

Uniqueness in Theorem A is proved simply enough (see Propositions 3.2 and 3.4). For \(k = C\), what is proposed in [1] is an explicit but transcendental construction for \(\Phi\) by means of the Knizhnik-Zamolodchikov system of equations
(for short: the KZ system) that arises in conformal field theory [10]. This $\Phi$, hereafter denoted by $\Phi_{KZ}$, is expressed in terms of $\tau = ht$ by means of a "C-universal formula"; i.e., if we write $\Phi_{KZ}$ in the form

$$\Phi_{KZ} = \sum_{m,n,p} a^{i_1 \cdots i_m j_1 \cdots j_n l_1 \cdots l_p}_{m,n,p} e_{i_1 \cdots i_m} \otimes e_{j_1 \cdots j_n} \otimes e_{l_1 \cdots l_p},$$

where the $e_i$ are a basis of $g$ as a topological $\mathbb{C}[[h]]$-module and the tensors $a^{i_1 \cdots i_m j_1 \cdots j_n l_1 \cdots l_p}_{m,n,p}$ are symmetric in each group of indices $i$, $j$, $l$, then the $a^{i_1 \cdots i_m j_1 \cdots j_n l_1 \cdots l_p}_{m,n,p}$ are expressed in terms of the structural constants $c^i_{rs}$ of the algebra $g$ and the components $e^a_{i}$ of the tensor $\tau$ in accordance with the rules of acyclic tensor calculus with coefficients in $\mathbb{C}$, while (1.1), (1.2), (1.4), and (1.6) follow, in accordance with the rules of acyclic tensor calculus, from the fact that the $c^i_{rs}$ are the structural constants of a Lie algebra and $\tau$ is symmetric and invariant.

(Acyclicity means, for example, exclusion of the expression $c^i_{rs} c^s_{lj} c^l_{ir}$, where $r, s, l$ form a "cycle".) Among the coefficients of the $\mathbb{C}$-universal formula occur (see (2.15) and (2.18)) the numbers $\zeta((2m+1)/(2\pi i))^{2m+1}$, $m \in \mathbb{N}$, which are imaginary and probably transcendental. Thus, for $k \not= \mathbb{C}$ the existence part of Theorem A cannot follow from the construction of $\Phi_{KZ}$. However, it is proved in §3, in conjunction with the following theorem.

**Theorem A'.** There exists a $\mathbb{Q}$-universal formula expressing the element $\Phi$ of Theorem A in terms of $\tau = ht$. It is unique up to twisting via a symmetric $\mathbb{Q}$-universal $F = F(\tau)$.

The quasitriangular quasi-Hopf algebras supplied by Theorem A will be called the standard algebras.

**Theorem B.** Any quasitriangular quasi-Hopf QUE-algebra can be made standard by a suitable twist.

The $\mathbb{C}$-universal formula expressing $\Phi_{KZ}$ in terms of $\tau = ht$ is of the form $\Phi_{KZ} = exp P_{KZ}(t^{12}, t^{23})$ where $P_{KZ}$ is a Lie (i.e., commutator) formal series with coefficients in $\mathbb{C}$ (see §2). Theorem A can be strengthened as follows.

**Theorem A''.'** There exists a Lie formal series $P$ with coefficients in $\mathbb{Q}$ such that the $\Phi$ of Theorem A can be taken as $exp P(ht^{12}, ht^{23})$.

If $\Phi$ has the form $exp P(ht^{12}, ht^{23})$ where $P$ is a Lie formal series, then the $\Phi$ defined by formula (1.11) is not, in general, of the same form. However, on the set of Lie series $P$ over $k$ such that $\Phi = exp P(ht^{12}, ht^{23})$ and $R = e^{ht/2}$ satisfy (2.2) and (1.6) we can define (see §4) a natural transitive action of a certain group, which we call the Grothendieck-Teichmüller group and denote by $GT(k)$. This action forms the basis of the proof of Theorem A'''. The definition of $GT(k)$ is in essence borrowed from [2], where, in particular, it is shown how to construct a canonical homomorphism $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GT(\mathbb{Q})$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and $l$ is a prime number.

The plan of the paper is as follows. §2 is devoted to $\Phi_{KZ}$. In §3, the methods of [1] are used to prove Theorems A, A', and B. In §4 we define the Grothendieck-Teichmüller group (in several versions) and explain its connection with $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In §5 we prove Theorem A''', and also reduce the study of $GT(k)$ to the study of an infinite-dimensional graded Lie algebra $\mathfrak{g} r _{\mathbb{C}} (k)$.
In §6 we gather together certain facts about this algebra. §4 is independent of §§2 and 3, and §§5 and 6 are independent of §3.

The author thanks A. A. Bellinson, G. V. Belyt, Yu. I. Manin, and G. B. Shabat for calling his attention to the papers [2], [11]–[15].

§2. Construction of $\Phi_{KZ}$

$\Phi_{KZ}$ is most easily defined by the formula $\Phi_{KZ} = G_1^{-1}G_2$ where $G_1$ and $G_2$ are the solutions of the differential equation

$$G'(x) = \hbar \left( \frac{t^{12}}{x} + \frac{t^{23}}{x - 1} \right) G(x), \quad \hbar = \hbar/2\pi i,$$

that are defined for $0 < x < 1$ and have the asymptotic properties $G_1(x) \sim x^{\hbar/2i}$ for $x \to 0$ and $G_2(x) \sim (1 - x)^{\hbar/2i}$ for $x \to 1$. Here $t^{12} = t \otimes 1 \in (Ug)^{\otimes 3}$ and $t^{23} = 1 \otimes t \in (Ug)^{\otimes 3}$, where $g$ is a deformation Lie algebra over $\mathbb{C}[[\hbar]]$ and the tensor $t \in g \otimes g$ is symmetric and $g$-invariant. The $G$ in equation (2.1) must be an analytic function $(0, 1) \to (Ug)^{\otimes 3}$; i.e., for any $n$ the image of $G(x)$ in $(Ug)^{\otimes 3}/\hbar^n(Ug)^{\otimes 3}$ must be of the form $\sum_{i=0}^{N} a_i(x) \cdot u_i$, where $u_i \in (Ug)^{\otimes 3}/\hbar^n(Ug)^{\otimes 3}$, the $a_i$ are analytic functions $(0, 1) \to C$, and $N$ depends in general on $n$. In the most important case, when $g = g_0[[\hbar]]$ (i.e., $g$ is the trivial deformation of $g_0$), this means that $G(x) = \sum_{i=0}^{\infty} g_i(x)\hbar^i$, where each $g_i$ is an analytic function with values in some finite-dimensional subspace $V_i \subset (Ug_0)^{\otimes 3}$. Of course, $x^{\hbar/2i}$ should be understood as $\exp(\hbar \ln x \cdot t^{12}) = 1 + \hbar \ln x \cdot t^{12} + \cdots$. The notation $G_1(x) \sim x^{\hbar/2i}$ means that $G_1(x)x^{-\hbar/2i}$ has an analytic continuation into a neighborhood of the point $x = 0$ and becomes 1 at that point. Existence and uniqueness of $G_1$ and $G_2$ are proved without difficulty.

The KZ system has the form

$$\frac{\partial W}{\partial z_i} = \hbar \sum_{j \neq i} \frac{t^{1j}}{z_i - z_j} \cdot W, \quad i = 1, 2, \ldots, n,$$

where $W(z_1, \ldots, z_n) \in (Ug)^{\otimes n}$ and $t^{1j}$ is the image of $t$ under the $(i, j)$th imbedding $Ug \otimes Ug \to (Ug)^{\otimes n}$. For us it is essential that, as indicated in [10], the system (2.2) is self-consistent; i.e., the curvature of the corresponding connection is 0. Since $\partial W/\partial z_i + \cdots + \partial W/\partial z_n = 0$, the function $W$ depends only on the differences $z_i - z_j$. Furthermore, $\sum_{i=1}^{n} z_i \partial W/\partial z_i = \hbar \sum_{i=1}^{n} t^{1i}W$, so that (2.2) reduces to a system of equations for a function of $n - 2$ variables. In particular, for $n = 3$ the solutions of (2.2) are of the form

$$\Phi_{KZ} = (z_2 - z_1)^{\hbar/2i} G((z_2 - z_1)/(z_3 - z_1)),$$

with asymptotics $W_1 \sim (z_2 - z_1)^{\hbar/2i} (z_3 - z_1)^{\hbar/2i} (z_3 - z_1)^{\hbar/2i}$ for $z_2 - z_1 \ll z_3 - z_1$, and $W_2 \sim (z_2 - z_1)^{\hbar/2i} (z_3 - z_1)^{\hbar/2i}$ for $z_3 - z_2 \ll z_3 - z_1$.

This definition of $\Phi_{KZ}$ in terms of the system (2.2) is convenient, in particular, for verifying (1.2) and (1.6) (equality (1.1), equivalent to $g$-invariance
of $\Phi_{\varepsilon}$ is obvious). To prove (1.6), we consider (2.2) for $n = 4$ in the region 
$(z_1, z_2, z_3, z_4) \in \mathbb{R}^4 \mid z_1 < z_2 < z_3 < z_4$ and distinguish five zones:

1) $z_2 - z_1 \ll z_3 - z_1 \ll z_4 - z_1$,
2) $z_3 - z_2 \ll z_3 - z_1 \ll z_4 - z_1$,
3) $z_3 - z_2 \ll z_4 - z_2 \ll z_4 - z_1$,
4) $z_4 - z_3 \ll z_4 - z_2 \ll z_4 - z_1$.

These zones correspond to the “vertices” of the pentagon (1.7) in accordance with the following rule: if $V_i$ and $V_j$ fall between any two corresponding parentheses and $V_k$ is outside these parentheses, then $|z_i - z_j| \ll |z_i - z_k|$; for example, $(V_1 \otimes (V_2 \otimes V_3)) \otimes V_4$ corresponds to the second zone.

**Lemma.** There exist unique solutions $W_1, \ldots, W_5$ of the system (2.2) with the following asymptotic behaviors in the corresponding zones:

$$W_1 \sim (z_2 - z_1)^{h_{12}} (z_3 - z_1)^{h_{12} + h_{13} + h_{14}} (z_4 - z_1)^{h_{12} + h_{13} + h_{14} + h_{15}},$$

$$W_2 \sim (z_3 - z_2)^{h_{23}} (z_3 - z_1)^{h_{12} + h_{13}} (z_4 - z_1)^{h_{12} + h_{13} + h_{14} + h_{15}},$$

$$W_3 \sim (z_4 - z_3)^{h_{34}} (z_4 - z_2)^{h_{12} + h_{14}} (z_4 - z_1)^{h_{12} + h_{13} + h_{14} + h_{15}},$$

$$W_4 \sim (z_4 - z_3)^{h_{34}} (z_4 - z_2)^{h_{12} + h_{14}} (z_4 - z_1)^{h_{12} + h_{13} + h_{14} + h_{15}},$$

$$W_5 \sim (z_2 - z_1)^{h_{12}} (z_3 - z_2)^{h_{23}} (z_4 - z_1)^{h_{12} + h_{13} + h_{14} + h_{15}}.$$

It is to be understood here that, e.g., for $W_5$ this means that

$$W_5 = f(u, v)(z_2 - z_1)^{h_{12}} (z_3 - z_2)^{h_{23}} (z_4 - z_1)^{h_{12} + h_{13} + h_{14} + h_{15}},$$

where $u = (z_2 - z_1)/(z_4 - z_1)$, $v = (z_4 - z_2)/(z_4 - z_1)$, $f$ is analytic in a neighborhood of $(0, 0)$, and $f(0, 0) = 1$.

**Proof.** Consider, say, the fifth zone. Make the substitution $W = g(u, v) \times (z_4 - z_1)^{h_{14}}$, where $T = t^{12} + t^{13} + t^{14} + t^{23} + t^{24} + t^{34}$, $u = (z_2 - z_1)/(z_4 - z_1)$, and $v = (z_4 - z_2)/(z_4 - z_1)$. Then for $g$ we obtain a system of equations of the form

$$\frac{\partial g}{\partial u} = h \left( \frac{A}{u} + R(U, v) \right) \cdot g(u, v),$$

$$\frac{\partial g}{\partial v} = h \left( \frac{B}{v} + S(u, v) \right) \cdot g(u, v),$$

where the functions $R$ and $S$, with values in $(Ug)^{\otimes 3}$, are analytic in a neighborhood of $(0, 0)$, while $A, B \in (Ug)^{\otimes 3}$ are independent of $u$ and $v$ (note that $[A, B] = 0$, in view of the integrability of the connection $\nabla$ corresponding to (2.3)). We must prove existence and uniqueness of a solution of the system (2.3) of the form $\varphi(u, v) = h^{AB} h^{AB}$, where $\varphi(u, v)$ is analytic in a neighborhood of $(0, 0)$, and $\varphi(0, 0) = 1$. In other words, we must prove existence and uniqueness of an analytic function $\varphi(u, v)$ such that $\varphi(0, 0) = 1$, $\varphi \cdot \nabla_u \varphi = \partial \varphi/\partial u - h A u^{-1}$, and $\varphi^{-1} \cdot \nabla_v \varphi = \partial \varphi/\partial v - h B v^{-1}$, where $\nabla_u = \partial/\partial u - h A u^{-1} + R(u, v)u$ and $\nabla_v = \partial/\partial v - h B v^{-1} + S(u, v)$. This can be done by the method of successive approximations.

It is easily seen that $W_1, \ldots, W_5$ have analytic continuations into the whole
region \( z_1 < z_2 < z_3 < z_4 \). Formula (1.2) follows from the equalities
\[
W'_1 = W'_2 = (\Phi_{\text{KZ}} \otimes 1), \quad W'_2 = W'_3 = (\text{id} \otimes \Delta \otimes \text{id})(\Phi_{\text{KZ}}), \quad W'_4 = (1 \otimes \Phi_{\text{KZ}}), \quad W'_5 = (\Delta \otimes \text{id} \otimes \text{id})(\Phi_{\text{KZ}}), \quad W'_6 = (\text{id} \otimes \text{id} \otimes \Delta)(\Phi_{\text{KZ}}).
\]
We show how to prove the first two of these.

Putting \( V'_1 = W'_1 \cdot (z_4 - z_1)^{-\lambda r'_{11} - \lambda r'_{12} - \lambda r'_{13}} \) and
\[
V'_2 = W'_2 \cdot (\Phi_{\text{KZ}} \otimes 1) \cdot (z_4 - z_1)^{-\lambda r'_{11} - \lambda r'_{12} - \lambda r'_{13}},
\]

we will prove that \( V'_1 = V'_2 \). It is easily verified that \( V'_1 \) and \( V'_2 \) are analytic for \( z_1 < z_2 < z_3 < z_4 \), \( z_4 \in \mathbb{R}^2 \setminus \{z_1, z_3\} \) (\( z_4 \) can also equal \( \infty \)). Furthermore, \( V'_1 \) and \( V'_2 \) both satisfy the equations
\[
\frac{\partial V}{\partial z_i} = h \sum_{j \neq i} \frac{t^{ij}}{z_i - z_j} \cdot V, \quad i = 2, 3, \tag{2.4}
\]
\[
\frac{\partial V}{\partial z_1} = h \sum_{j \neq 1} \frac{t^{1j}}{z_1 - z_j} \cdot V - h V \cdot \frac{t^{14} + t^{24} + t^{34}}{z_1 - z_4}, \tag{2.5}
\]
\[
\frac{\partial V}{\partial z_4} = h \sum_{j \neq 4} \frac{t^{14}}{z_4 - z_j} \cdot V. \tag{2.6}
\]

From (2.4), (2.5), and the asymptotics of \( V'_1 \) and \( V'_2 \), it follows that \( V'_1 \) and \( V'_2 \) coincide for \( z_4 = \infty \). This and (2.6) imply \( V'_1 = V'_2 \).

Now put \( U'_1 = W'_2 \cdot (z_3 - z_2)^{-\lambda r'_{32}} \) and
\[
U'_2 = W'_3 \cdot (\text{id} \otimes \Delta \otimes \text{id})(\Phi_{\text{KZ}}) \cdot (z_3 - z_2)^{-\lambda r'_{32}},
\]

we show that \( U'_1 = U'_2 \). It is easily verified that \( U'_1 \) and \( U'_2 \) are analytic in the region \( z_1 < z_2 < z_4 \), \( z_1 < z_3 < z_4 \) (\( z_2 \) can equal \( z_1 \) and \( z_3 \)). Furthermore, \( U'_1 \) and \( U'_2 \) satisfy the equations
\[
\frac{\partial U}{\partial z_i} = h \sum_{j \neq i} \frac{t^{ij}}{z_i - z_j} \cdot U, \quad i = 1, 4, \tag{2.7}
\]
\[
\frac{\partial U}{\partial z_2} = h \sum_{j \neq 2, 3} \frac{t^{2j}}{z_2 - z_j} \cdot U + h \frac{t^{23}}{z_2 - z_3} \cdot U, \tag{2.8}
\]
\[
\frac{\partial U}{\partial z_3} = h \sum_{j \neq 2, 3} \frac{t^{3j}}{z_3 - z_j} \cdot U - h \frac{t^{32}}{z_3 - z_2} \cdot U. \tag{2.9}
\]

It is easily seen that \( U'_1 \) and \( U'_2 \) coincide for \( z_2 = z_3 \). From this and (2.8) it follows that \( U'_1 = U'_2 \).

Thus, (1.2) is proved. Replacing \( x \) by \( 1 - x \) in (2.1) shows that \( \Phi_{\text{KZ}} \) satisfies the equality
\[
\Phi^{121} = \Phi^{-1}. \tag{2.10}
\]

Therefore (1.6b) follows from (1.6a): it suffices to apply to both sides of (1.6a) the operator that interchanges the first tensor factor with the third, and to employ the equalities \( R^{21} = R \) and \( \Delta' = \Delta \). The proof of (1.6a) is contained in
§3 of [1]. It uses six solutions of the system (2.2) for \( n - 3 \) in the complex domain that have the standard asymptotic behavior in the corresponding zones; they correspond to the “vertices” of the hexagon (1.9a).

Now replace (2.1) by the equation

\[
G'(z) = \frac{1}{2\pi i} \left( \frac{A}{x} + \frac{B}{x - 1} \right) G(x),
\]

(2.11)

where \( A \) and \( B \) are noncommuting symbols, and \( G \) is a formal series in \( A \) and \( B \) with coefficients that are analytic functions of \( x \). Consider, as above, solutions \( G_1 \) and \( G_2 \) with the standard asymptotics for \( x = 0 \) and \( x = 1 \). Put \( \phi_{KZ}(A, B) = G^{-1}_2 G_1 \). The algebra \( C\langle\langle A, B \rangle\rangle \) of noncommutative formal series is a topological Hopf algebra with the comultiplication \( \Delta(A) = A \otimes 1 + 1 \otimes A \), \( \Delta(B) = B \otimes 1 + 1 \otimes B \). Clearly, \( \Delta(\phi_{KZ}) = \phi_{KZ} \otimes \phi_{KZ} \). Therefore \( \ln \phi_{KZ}(A, B) \) is a Lie formal series, i.e., an element of the complete free Lie algebra over \( C \) with generators \( A, B \) (see [16], Chapter II, §3, Corollary 2, Theorem 1). In the same way as for (2.10) one proves that \( \phi_{KZ} \) satisfies the equality

\[
\phi(B, A) = \phi(A, B)^{-1}.
\]

(2.12)

To obtain analogues of (1.2) and (1.6) for \( \phi_{KZ} \), observe that as in [7], the integrability of the connection corresponding to (2.2) follows from the relations \( t^{ij} = t^{ij} \) and \( [t^{ij}, t^{kl}] = 0 \) for \( i \neq j \neq k \neq l \), and \( [t^{ij} + t^{ji}, t^{ik} + t^{ki}] = 0 \) for \( i \neq j \neq k \). We now introduce, as in [17], the Lie algebra \( a_n^C \) as the quotient of the complete free Lie algebra over \( C \) with generators \( X^{ij}, 1 \leq i \leq n, 1 \leq j \leq n, i \neq j \), modulo the ideal topologically generated by the elements of the following three types: 1) \( \tilde{X}^{ij} - \tilde{X}^{ji} \); 2) \( [\tilde{X}^{ij}, X^{kl}], i \neq j \neq k \neq l \); 3) \( [\tilde{X}^{ij} + \tilde{X}^{ik}, \tilde{X}^{jk}], i \neq j \neq k \). The image of \( \tilde{X}^{ij} \) in \( a_n^C \) we denote by \( X^{ij} \).

Replacing now \( h^{ij} \) in (2.2) by \( X^{ij} \), we find that the same arguments that prove (1.2) and (1.6) for \( \Phi = \Phi_{KZ} \) also prove that \( \phi_{KZ} \) satisfies the relations

\[
\varphi(X^{12}, X^{23} + X^{24}) \cdot \varphi(X^{13} + X^{23}, X^{34}) = \varphi(X^{23}, X^{34}) \cdot \varphi(X^{12} + X^{13}, X^{24} + X^{34}) \cdot \varphi(X^{12}, X^{23}),
\]

(2.13)

\[
\exp((X^{13} + X^{23})/2) = \varphi(X^{13}, X^{12}) \cdot \exp((X^{13}/2) \cdot \varphi(X^{13}, X^{23})^{-1} \cdot \exp(X^{23}/2) \cdot \varphi(X^{12}, X^{23}),
\]

(2.14a)

\[
\exp((X^{12} + X^{13})/2) = \varphi(X^{23}, X^{13})^{-1} \cdot \exp(X^{13}/2) \cdot \varphi(X^{12}, X^{13}) \cdot \exp(X^{12}/2) \cdot \varphi(X^{12}, X^{23})^{-1},
\]

(2.14b)

where both sides of (2.13) belong to \( \exp a_n^C \) while both sides of (2.14a) and (2.14b) belong to \( \exp a_n^C \). Here \( \exp a_n^C = \{e^x \mid x \in a_n^C \} \), where \( e^x \) is regarded as an element of the complete universal enveloping algebra \( Ua_n^C \). In other words, \( \exp a_n^C \) is the Lie group corresponding to \( a_n^C \).

If we assume for the moment that \( [A, B] = 0 \), then (2.11) has the solution \( A^{x}, B^{x}/(1 - x)^{2x} \) with the standard asymptotics both at \( x = 0 \) and at \( x = 1 \). Therefore \( \ln \phi_{KZ} \in p \), where \( p \) is the commutant of the complete free Lie algebra with generators \( A, B \). Let us find the image of \( \ln \phi_{KZ} \in p / [p, p] \). Since \( p \) is a topologically free Lie algebra with generators \( U_{kl} = (\text{ad} B)^l (\text{ad} A)^k [A, B] \).
(see, e.g., §2.4.2 of [18]), the images of the \( U_{kl} \) in \( p/[p, p] \) (which we denote by \( \overline{U}_{kl} \)) form a topological basis in \( p/[p, p] \). Observe that \( \overline{U}_{kl} \) is also the image of \((\text{ad} A)^k(\text{ad} B)^l[A, B] \) in \( p/[p, p] \). The coefficients of the expansion of the image of \( \ln \varphi_{KZ} \) in \( p/[p, p] \), with respect to the basis \( \overline{U}_{kl} \), we denote by \( c_{kl} \).

We show that

\[
1 + \sum_{k, l} c_{kl} u^{k+1} v^{l+1} = \exp \sum_{n=2}^{\infty} \frac{\zeta(n)}{n \cdot (2\pi i)^n} (u^n + v^n - (u + v)^n).
\]

(2.15)

Write the standard solutions \( G_i \) and \( G_j \) of equation (2.11) in the form \( G_j(x) = \overline{A}^{x-1} \overline{V}_j(x) \), where \( \overline{A} = A/2\pi i \) and \( \overline{B} = B/2\pi i \). The functions \( V_j \) have continuous extensions to \([0, 1]\) and satisfy the equation

\[
V'_{(x)} = Q(x) V_j(x),
\]

(2.16)

\[
Q(x) \overset{\text{def}}{=} e^{-\ln(1-x) \cdot \text{ad} \overline{A}/x - 1} \overline{B} \in p.
\]

Furthermore, \( V_j(0) = 1 \) and \( V_j(1) = 1 \). Therefore \( \varphi_{KZ} = \overline{V}_2^{-1} V_2 V_j(1) V(j) \), where \( \varphi \) is any solution of (2.16). This means that the image of \( \ln \varphi_{KZ} \) in \( p/[p, p] \) is equal to \( \int_0^1 Q(x) \, dx \), where \( Q(x) \) is the image of \( Q(x) \) in \( p/[p, p] \). Hence,

\[
c_{kl} = \frac{1}{(2\pi i)^{k+1} \Gamma(k+1)!} \int_0^1 \left( \ln \frac{1}{1-x} \right)^l \frac{dx}{x-1}.
\]

(2.17)

Assuming for the moment that \( u, v \in \mathbb{C}, \text{Im} u < 0, \text{Im} u < 2\pi \), we find that the left-hand side of (2.15) is equal to

\[
1 + \overline{u} \int_0^1 (1-x^{-\overline{u}})(1-x)^{-\overline{v}-1} \, dx = -\overline{u} \int_0^1 x^{-\overline{u}}(1-x)^{-\overline{v}-1} \, dx
\]

\[
= \Gamma(1-\overline{u})\Gamma(1-\overline{v})/\Gamma(1-\overline{u} - \overline{v}),
\]

where \( \overline{u} = u/2\pi i \) and \( \overline{v} = v/2\pi i \). Using the formula \( \ln \Gamma(1-z) = \gamma z + \sum_{n=2}^{\infty} (\zeta(n)/n) \cdot z^n \), which follows from the expansion of the \( \Gamma \)-function as an infinite product ([19], Chapter 12), we obtain (2.15).

From (2.15) it follows in particular that

\[
c_{k,0} = c_{0,k} = -\zeta(k+2)/(2\pi i)^{k+2}.
\]

(2.18)

One can also give a somewhat different proof of (2.18): \( c_{k,0} \) can be computed by means of (2.17), the formula \( (1-x)^{-1} = 1+x+x^2+\ldots \) and the substitution \( x = e^{-y} \), and \( c_{0,k} \) by the formula \( c_{lk} = c_{kl} \), which is a consequence of (2.12).

**Remark.** According to the Introduction in [11], similar computations have previously been made by Z. Wojtkowiak; indeed, they served as a stimulus to Deligne.

§3. Proofs of Theorems A, A', and B

In this section we examine the quasitriangular quasi-Hopf QUE-algebras over \( k[[h]] \), where \( k \) is a field of characteristic 0. Let us recall (see Proposition 3.5 of [1]) that a) any such algebra can be brought by an appropriate twist into symmetric form (i.e., we can make \( R^2 = R \); 2) twisting via \( F \) preserves
symmetric form if and only if $F^{21} = F$; 3) if $R^{21} = R$, then $\Delta' = \Delta$ and (2.10) holds. We recall also (see §2) that if $R^{21} = R$, then (1.6b) follows from (1.6a) and (2.10).

Let $g$ be a Lie algebra over $k$, and $t \in g \otimes g$ be symmetric and $g$-invariant. Putting $A = (Ug)[[h]]$ we define in the usual fashion $\Delta: A \to A \otimes A$ and $c: A \otimes k[[h]]$. We look for $g$-invariant elements $R \in A \otimes A$ and $\Phi \in A \otimes A \otimes A$ such that $R^{21} = R$, $R \equiv 1 + h/t/2 \bmod h^2$, $\Phi \equiv 1 \bmod h$ and equations (1.2), (1.4), (1.6a), and (2.10) are satisfied (we do not require $R = e^{ht/2}$).

**Proposition 3.1.** Such $R$ and $\Phi$ exist.

**Proof.** Suppose we have already constructed $g$-invariant elements $R_n \in (Ug \otimes Ug)[[h]]$ and $\Phi_n \in (Ug \otimes Ug \otimes Ug)[[h]]$ such that $R_n^{21} = R_n$, $R_n \equiv 1 + h/t/2 \bmod h^2$, $\Phi_n \equiv 1 \bmod h$, and $R_n$, $\Phi_n$ satisfy modulo $h^n$ equations (1.2), (1.4), (1.6a), and (2.10) (for $n = 2$ we can put $R_1 = 1 + h/t/2$, $\Phi_2 = 1$). From the proof of Proposition 3.10 of [1] it follows that there exists a $g$-invariant $\Phi_n \in (Ug \otimes Ug \otimes Ug)[[h]]$ satisfying (1.2), (1.4), and (2.10) modulo $h^{n+1}$ and such that $\Phi_n = \Phi_n \bmod h^n$. Since $R_n$ and $\Phi_n$ satisfy (1.6a) modulo $h^n$, we have

$$
(\Delta \otimes \text{id})(R_n) \equiv \Phi_n^{312} R_n^{13} (\Phi_n^{13})^{-1} R_n^{23} \Phi_n + h^n \psi \bmod h^{n+1},
$$

(3.1a)

where $\psi \in Ug \otimes Ug \otimes Ug$ is $g$-invariant. Applying to both sides of (3.1a) the operator that interchanges first and third tensor factors, we obtain:

$$
(\text{id} \otimes \Delta)(R_n) \equiv (\Phi_n^{213})^{-1} R_n^{13} \Phi_n R_n^{213} \Phi_n^{-1} + h^n \psi^{321} \bmod h^{n+1}.
$$

(3.1b)

We now look for $R_{n+1}$ and $\Phi_{n+1}$ in the form $R_{n+1} = R_n + h^n r$ and $\Phi_{n+1} = \Phi_n + h^n \varphi$, where $r \in Ug \otimes Ug$ and $\varphi \in A^3 g \subset Ug \otimes Ug \otimes Ug$. The elements $r$ and $\varphi$ must be $g$-invariant and satisfy the equations

$$
r^{21} = R,
$$

(3.2)

$$
r^{13} + r^{23} = (\Delta \otimes \text{id})(r) + 3 \varphi = \psi.
$$

(3.3)

For such $r$ and $\varphi$ to exist, it is necessary that

$$
\psi^{214} - (\Delta \otimes \text{id} \otimes \text{id})(\psi) + (\text{id} \otimes \Delta \otimes \text{id})(\psi) - \psi^{124} = 0,
$$

(3.4)

$$
(\text{id} \otimes \text{id} \otimes \Delta)(\psi) - \psi^{123} - \psi^{124} = (\Delta \otimes \text{id} \otimes \text{id})(\psi^{321}) - \psi^{431} - \psi^{432},
$$

(3.5)

$$
r^{321} = - \alpha,
$$

(3.6)

where $\alpha = \psi - \psi^{214}$. We claim that (3.4)–(3.6) are also sufficient for existence of $r$ and $\varphi$. Indeed, (3.4) says that $\psi$ is a 2-cocycle in the complex $C^*(g) \otimes Ug$, where

$$
C^n(g) = (Ug)^{\otimes n},
$$

$$
d(a_1 \otimes \cdots \otimes a_n) = \otimes a_1 \otimes \cdots \otimes a_n
$$

$$
+ \sum_{t=1}^n (-1)^t a_1 \otimes \cdots \otimes a_{t-1} \otimes (a_t) \otimes a_{t+1} \otimes \cdots \otimes a_n
$$

$$
+ (-1)^{n+1} a_1 \otimes \cdots \otimes a_n \otimes 1.
$$

(3.7)
It follows therefore from Proposition 2.2 of [1] that $\alpha \in \Lambda^2 g \otimes U g$, while

$$\psi - \alpha/2 = t^{13} + t^{23} - (\Delta \otimes \text{id})(\bar{r}).$$

(3.8)

Here $\bar{r}$ can be chosen to be $g$-invariant; it suffices that under the usual identification of $U g$ with $\text{Sym}^* g$ (see [16], Chapter II, §1, Proposition 9), $\bar{r}$ goes into an element of $\text{Sym}^* g \otimes \text{Sym}^* g$ whose image in $g \otimes \text{Sym}^* g$ is 0. Since $\alpha \in \Lambda^2 g \otimes U g$, it follows from (3.6) that $\alpha \in \Lambda^3 g$. Put $\varphi = \alpha/6$. Then (3.2) and (3.3) become the following conditions on $s = r - \bar{r}$:

$$s - s^{21} = \bar{r} - \bar{r}, \quad s \in g \otimes U g.$$

(3.9)

For the existence of an $s$ satisfying (3.9) it is necessary and sufficient that $\bar{r}^{21} - \bar{r} \in (g \otimes U g) \otimes (U g \otimes g)$, i.e.,

$$(f \otimes f)(\bar{r}^{21} - \bar{r}) = 0,$$

(3.10)

where $f: U g \to U g \otimes U g$, $f(a) = a \otimes 1 + 1 \otimes a - \Delta(a)$. If (3.10) is satisfied, then $s$ can be chosen to be $g$-invariant; it suffices that the image of $s + \bar{r}$ in $\text{Sym}^* g \otimes \text{Sym}^* g$ have no component in $g \otimes g$. It remains to observe that (3.10) follows from (3.5), (3.8), and the fact that $\alpha \in \Lambda^3 g$.

We now prove (3.4)–(3.6). Transforming by means of (3.1a) both sides of the equality

$$\Phi_n^{123} \cdot (\Delta \otimes \text{id} \otimes \text{id})(\Delta \otimes \text{id})(R_n) = (\text{id} \otimes \Delta \otimes \text{id})(\Delta \otimes \text{id})(R_n) \cdot \Phi_n^{123}$$

and using (1.2) and (1.5), we obtain (3.4). Now express $(\Delta \otimes \Delta)(R_n)$ in terms of $R_n^1$, $R_n^4$, $R_n^{23}$, $R_n^{24}$ in two ways (we can apply first (3.1a) and then (3.1b), or first (3.1b) and then (3.1a)). Comparing the two expressions for $(\Delta \otimes \Delta)(R_n)$ and using (1.2) and (1.5), we obtain (3.5). In the same way as for the proof of formula (3.12) of [1], which generalized the Yang-Baxter relation, we can derive from (3.1a) the congruence

$$R_n^{12} \Phi_n^{312} R_n^{13} (\Phi_n^{132})^{-1} R_n^{23} \Phi_n^{321} + h^n \alpha \equiv \Phi_n^{321} R_n^{23} (\Phi_n^{132})^{-1} R_n^{13} \Phi_n^{231} R_n^{12} \mod h^{n+1}$$

(3.11)

Applying to both sides of (3.11) the operator that interchanges the first tensor factor with the third, and using the relations $R_n^{21} = R_n$ and $\Phi_n^{123} \equiv \Phi_n^{-1} \mod h^{n+1}$, we obtain (3.6).

The proof of Proposition 3.1 determines certain completely specific elements $\Phi$ and $R$, expressed in terms of $\tau = h t$ by means of $Q$-universal formulas $\Phi = \mathcal{M}(\tau)$ and $R = \mathcal{N}(\tau)$. Concerning these formulas it suffices for our purposes to know only that $\mathcal{M}(\tau) = 1 + O(\tau)$ and $\mathcal{N}(\tau) = 1 + \tau/2 - O(\tau)$, where $O(\tau)$ (resp. $O(\tau)$) denotes terms in $\tau$ of degree higher than 1 (resp. higher than or equal to 1).

**Proposition 3.2.** Let $g$ be a Lie algebra over $k$, and suppose that $R \in (U g \otimes U g)[[h]]$ and $\Phi \in (U g \otimes U g \otimes U g)[[h]]$ are invertible, $g$-invariant, and satisfy (1.2), (1.4), and (1.6). Then by twisting via some $g$-invariant $F \in (U g \otimes U g)[[h]]$ the elements $\Phi$ and $R$ can be turned into $\mathcal{M}(\theta h)$ and $\mathcal{N}(\theta h)$, where $\theta$ is a $g$-invariant element of $(\text{Sym}^* g)[[h]]$. Furthermore, $\theta$ is uniquely determined, while $F$ is determined up to multiplication by an element of the form...
\((u^{-1} \otimes u^{-1}) \Delta(u)\), where \(u\) belongs to the center of \((Ug)[[h]]\) and \(u \equiv 1 \mod h\), \(e(u) = 1\).

**Proof.** \((A, \Delta, e, \Phi, R)\) can be brought into symmetric form by twisting via some \(g\)-invariant element of \((Ug \otimes Ug)[[h]]\) (see the proof of Proposition 3.5 in [1]). We can therefore assume that \(R_{21} = R\) (in which case \(\Phi_{321} = \Phi^{-1}\) while \(F\) must be symmetric). Then everything reduces to the following lemma.

**Lemma.** Suppose \((\Phi_1, R_1)\) and \((\Phi_2, R_2)\) satisfy the conditions of the proposition, with \(R_{21} = R_1\), \(R_{21} = R_2\), \(\Phi_1 \equiv \Phi_2 \mod h^n\), and \(R_1 \equiv R_2 \mod h^n\). Let \(\varphi\) and \(r\) be the reductions mod \(h\) of the elements \(h^{-n}(\Phi_1 - \Phi_2)\) and \(h^{-n}(R_1 - R_2)\), respectively. Then \(r\) is a \(g\)-invariant element of \(\text{Sym}^2 g\), while \(\varphi\) can be written in the form

\[
\varphi = f^{23} - (\Delta \otimes \text{id})(f) + (\text{id} \otimes \Delta)(f) - f^{12},
\]

where \(f\) is a symmetric \(g\)-invariant element of \(Ug \otimes Ug\) such that \((e \otimes \text{id})(f) = 0 = (\text{id} \otimes e)(f)\). Furthermore, \(f\) is uniquely determined up to replacement by

\[
\tilde{f} = f + \Delta(v) - v \otimes 1 - 1 \otimes v,
\]

where \(v\) belongs to the center of \(Ug\) and \(e(v) = 0\).

**Proof.** Since \(R_1, R_2\) satisfy (1.6a), while \(\Phi_1, \Phi_2\) satisfy (2.10), we have \((\Delta \otimes \text{id})(r) = r^{11} - r^{21} = \text{Alt} \varphi/2\). The left-hand side of this equality is symmetric in the first two tensor factors, and the right-hand side skew-symmetric. Therefore both sides are 0; i.e., \(\text{Alt} \varphi = 0\) and \(r \in g \otimes Ug\). Since \(r \in g \otimes Ug\) and \(r^{21} = r\), we have \(r \in \text{Sym}^2 g\). Since \(\Phi_1, \Phi_2\) satisfy (1.2), (1.4), and (2.10), we have

\[
\varphi^{21} = (\Delta \otimes \text{id} \otimes \text{id})(\varphi) + (\text{id} \otimes \Delta \otimes \text{id})(\varphi) + (\text{id} \otimes \text{id} \otimes \Delta)(\varphi) - \varphi^{12} = 0,
\]

\[
(e \otimes e \otimes \text{id})(\varphi) = 0,
\]

\[
\varphi^{321} = -\varphi.
\]

Applying to (3.14) the mappings \(e \otimes e \otimes \text{id} \otimes \text{id}\) and \(\text{id} \otimes \text{id} \otimes e \otimes e\), and using (3.15), we obtain:

\[
(e \otimes e \otimes \text{id})(\varphi) = 0 = (\text{id} \otimes \text{id} \otimes e)(\varphi).
\]

(3.14) says that \(\varphi\) is a 3-cocycle in the complex (3.7). By Proposition 3.11 of [1], if such a cocycle is \(g\)-invariant and satisfies (3.15)-(3.17) and the condition \(\text{Alt} \varphi = 0\), it can be represented in the form (3.12), and the representation is unique up to the replacement (3.13).

Let \(\mathcal{M}\) and \(\mathcal{M}'\) be as above. In the same way as for Proposition 3.2 one proves the following.

**Proposition 3.3.** Let \((\mathcal{M}(x), \mathcal{M}'(x))\) be an arbitrary \(k\)-universal solution of equations (1.2), (1.4), and (1.6) such that \(\mathcal{M}'(x)\) is symmetric, \(\mathcal{M}(x) = 1 + x/2 + o(x)\). Then by twisting via a symmetric \(k\)-universal \(F(x)\) one can turn \((\mathcal{M}(x), \mathcal{M}'(x))\) into \((\mathcal{M}(x), \mathcal{M}'(x))\), where \(\mathcal{M}\) is expressed in terms of \(x\) by a \(k\)-universal formula of the form \(\mathcal{M} = x + O(x)\). Furthermore, \(\mathcal{M}\) is determined
by \((\mathcal{A}, \mathcal{N}')\) uniquely, and \(F(\tau)\) up to multiplication by \((u^{-1} \otimes u^{-1}) \cdot \Delta(u)\), where \(u\) is expressed in terms of \(\tau\) by a \(k\)-universal formula of the form \(u = 1 + O(\tau)\).

**Proposition 3.4.** Let \((\mathcal{A}(\tau), \mathcal{N}(\tau))\) be as in Proposition 3.3. Then \(\mathcal{N}(\tau) = e^{\tau/2}\), where \(\tau\) is expressed in terms of \(\tau\) by means of a \(k\)-universal formula of the form \(\tilde{\tau} = \tau + o(\tau)\).

**Proof.** If \(R = e^{ht}\), where \(t \in \mathfrak{g} \otimes \mathfrak{g}\) is symmetric and \(g\)-invariant, and \(F \in (U\mathfrak{g} \otimes U\mathfrak{g})[[h]]\) is likewise symmetric and \(g\)-invariant, then in formula (1.12) \(R = R\), since \([t, F] = 0\) (it suffices to use the formula \(t = (\Delta(C) - C \otimes 1 - 1 \otimes C)/2\), where \(C \in U\mathfrak{g}\) is the Casimir element corresponding to \(t\)). The \(k\)-universal version of this assertion is also true: \(F(\tau) e^{\tau/2} F(\tau)^{-1} = e^{\tau/2}\) for any \(k\)-universal \(F(\tau)\). Therefore, applying Proposition 3.3 to the case that \(\mathcal{N}(\tau) = e^{\tau/2}\) and \(\mathcal{A}(\tau)\) is defined by means of the KZ system (see \(\S\) 2), we find that \(\mathcal{N}(\tilde{\tau}) = e^{\tilde{\tau}/2}\) for some \(\tilde{\tau}\) of the form \(\tau + o(\tau)\). It remains now to apply Proposition 3.3 to an arbitrary pair \((\mathcal{A}(\tau), \mathcal{N}(\tau))\).

**Proof of Theorem A'.** In the process of proving Proposition 3.1 we constructed \(Q\)-universal elements \(\Phi = \mathcal{A}(\tau)\) and \(R = \mathcal{N}(\tau)\) satisfying (1.1)–(1.6) and the condition \(R^{21} = R\), with \(\mathcal{N}(\tau) = 1 + \tau/2 + o(\tau)\) and \(\mathcal{A}(\tau) = 1 + O(\tau)\). By Proposition 3.4, there exists a \(Q\)-universal \(\tilde{\tau}\) of the form \(\tau + o(\tau)\) such that \(\mathcal{N}(\tilde{\tau}) = e^{\tilde{\tau}/2}\). Then \(\Phi = \mathcal{A}(\tilde{\tau})\) and \(R = e^{\tilde{\tau}/2}\) satisfy (1.1)–(1.6). Uniqueness in Theorem A' follows from Proposition 3.3.

Theorem A' implies the existence part of Theorem A. Uniqueness is a consequence of the following proposition.

**Proposition 3.5.** Let \(\mathfrak{g}\) be a deformation algebra over \(k[[h]]\) (see \(\S\) 1), and \(R \in U\mathfrak{g} \otimes U\mathfrak{g}\) and \(\Phi \in U\mathfrak{g} \otimes U\mathfrak{g} \otimes U\mathfrak{g}\) invertible \(g\)-invariant elements satisfying (1.2), (1.4), and (1.6). Then by twisting via some \(g\)-invariant \(F \in U\mathfrak{g} \otimes U\mathfrak{g}\) we can turn \(\Phi\) and \(R\) into \(\mathcal{A}(h\theta)\) and \(e^{h\theta/2}\), where \(\theta\) is a \(g\)-invariant element of \(\text{Sym}^2 \mathfrak{g}\). Furthermore, \(F\) is uniquely determined up to multiplication by an element of the form \((u^{-1} \otimes u^{-1}) \times \Delta(u)\), where \(u\) belongs to the center of \(U\mathfrak{g}\) and \(u \equiv 1 \mod h\), \(e(u) = 1\).

**Proof.** The proof is basically like the one given above (see Proposition 3.2) in the case \(\mathfrak{g} = \mathfrak{g}_0[[h]]\), where \(\mathfrak{g}_0\) is a Lie algebra over \(k\). It differs in the following respect. Suppose \(R^{21} = R\), \(\Phi = \mathcal{A}(h\theta_\tau)\mod h^n\), and \(R = \exp(h\theta_\tau/2) \mod h^n\) for some \(g\)-invariant \(\theta_\tau \in \text{Sym}^2 \mathfrak{g}\). Let \(r\) and \(\varphi\) be the residue classes \(\mod h\) of the elements \(h^{-n}(R - \exp(h\theta_\tau/2))\) and \(h^{-n}(\Phi - \mathcal{A}(h\theta_\tau))\), respectively. As in the proof of Proposition 3.2, one shows that \(r\) is an invariant element of \(\text{Sym}^2 \mathfrak{g}_0\), where \(\mathfrak{g}_0 = \mathfrak{g}/\mathfrak{g}\), while \(\varphi\) can be represented in the form (3.12), where \(f\) is a symmetric invariant element of \(U\mathfrak{g}_0 \otimes U\mathfrak{g}_0\) such that \((\varepsilon \otimes \text{id})(f) = (\text{id} \otimes \varepsilon)(f) = 0\). But to construct \(g\)-invariant symmetric elements \(F_n \in U\mathfrak{g} \otimes U\mathfrak{g}\) and \(\theta_{n+1} \in \mathfrak{g} \otimes \mathfrak{g}\) such that \(\Phi = \mathcal{A}(h\theta_{n+1}) \mod h^{n+1}\) and \(R = \exp(h\theta_{n+1}/2) \mod h^{n+1}\), where \(\tilde{\Phi}\) and \(\tilde{R}\) are obtained by twisting \(\Phi\) and \(R\) via \(F_n\), we must still prove that \(r \in \text{Sym}^2 \mathfrak{g}_0\) lifts to an invariant element \(\xi \in \text{Sym}^2 \mathfrak{g}\), while \(f \in \text{Sym}^2(U\mathfrak{g}_0)\) can be chosen so as to lift to an invariant element \(\bar{f} \in \text{Sym}^2(U\mathfrak{g})\). For \(\xi\) we can take \(\pi(h^{n}(\ln R - \theta_2/2))\).
where $\pi: Ug \otimes Ug \to g \otimes g$ is the projection defined by identification of $Ug$ with $\text{Sym}^*g$ (we are forced to use $\pi$, since it has not yet been proved that $\ln R \in g \otimes g$). We claim that $f$ exists if $f$ is constructed as in the proof of Proposition 3.11 of [1]. Indeed, if we identify $Ug_0$ with $\text{Sym}^*g_0$ in the usual fashion, then $Ug_0 \otimes Ug_0$ is identified with $\text{Sym}^*(g_0 \otimes g_0) = \bigoplus_m a_m \otimes S_m(Q^2)^{\otimes m}$, $(Ug_0)^{\otimes 3}$ with $\bigoplus_m a_m^{\otimes 3} \otimes S_m(Q^3)^{\otimes m}$ and the $f$ constructed in [1] is equal to $L_0(\varphi)$, where $L_0: (Ug_0)^{\otimes 3} \to (Ug_0)^{\otimes 2}$ is defined by means of certain $S_m$-equivariant operators $\delta_m: (Q^3)^{\otimes m} \to (Q^2)^{\otimes m}$. We can therefore put $f = L(\varphi)$, where $\varphi = h^{-n}(\Phi - A(h\theta))$, and $L: (Ug)^{\otimes 3} \to (Ug)^{\otimes 2}$ is defined by means of the same $\delta_m$.

A similar problem arises in proving the uniqueness of $F$ up to multiplication by $(u^{-1} \otimes u^{-1})\Delta(u)$, and it is dealt with in the same way.

**COROLLARY.** In the situation of Proposition 3.5, $R^{21}R = e^{h\theta}$, where $\theta$ is a $g$-invariant element of $\text{Sym}^2g$. In particular, if $R^{21} = R$, then $R = e^{h\theta/2}$.

**REMARKS.** 1. The corollary shows that if $A$ is a universal enveloping algebra with the usual $\Delta$ and $\varepsilon$, then (1.1)–(1.6) imply the equality $(\Delta \otimes \text{id})(\ln(R^{21}R)) = \ln(R^{21}R^{13}) + \ln(R^{22}R^{23})$. The author has not been able to derive this equality directly from (1.1)–(1.6).

2. A proof similar to that of Proposition 3.5 can be made for an analogous proposition concerning coboundary quasi-Hopf QUE-algebras in the sense of §3 of [1].

**PROOF OF THEOREM B.** Let $(A, \Delta, \varepsilon, \Phi, R)$ be a quasisymmetric quasi-Hopf QUE-algebra over $k[[h]]$. Put $R = R \cdot (R^{21}R)^{-1/2}$. By Proposition 3.3 of [1], $(A, \Delta, \varepsilon, \Phi, R)$ is a coboundary quasi-Hopf QUE-algebra. Therefore, by Proposition 3.13 of [1], a suitable twist turns $(A, \Delta, \varepsilon)$ into $Ug$ with the usual comultiplication and counit, where $g$ is a deformation Lie algebra. Now apply Proposition 3.5.

**REMARKS.** 1. Theorem B can be proved without the use of Proposition 3.5 by arguing as in the proof of Proposition 3.13 of [1].


4. The Grothendieck–Teichmüller group

Suppose given a quasisymmetric category (see §1), i.e., a category $C$, a functor $\otimes$, commutativity and associativity isomorphisms, as well as an identity object $k$ and isomorphisms $V \cong k \cong V$ and $k \otimes V \cong V$ for all objects $V$ in $C$ (with diagrams (1.7)–(1.9) commutative). We try to change the commutativity and associativity isomorphisms without changing the rest of the structure appearing in the definition of quasisymmetric category. Changing the associativity isomorphism $(V_1 \otimes V_2) \otimes V_3 \cong V_1 \otimes (V_2 \otimes V_3)$ amounts to multiplying it by an automorphism of $(V_1 \otimes V_2) \otimes V_3$. Observe that on $(V \otimes V) \otimes V$, where $V$ is an object in $C$, there is an action of the braid group $B_3$: the generator $\sigma_1 \in B_3$ determines the isomorphism $c \otimes \text{id}$, where $c$ is the commutativity isomorphism $V \otimes V \cong V \otimes V$, and the generator $\sigma_2 \in B_3$ determines the isomorphism $a^{-1}(\text{id} \otimes c)a$. Where $a$ is the associativity isomorphism
\((V \otimes V) \otimes V \cong V \otimes (V \otimes V)\). In the same way, every \(\alpha \in B_3\) determines an isomorphism \((V_i \otimes V_j) \otimes V_k \cong (V_i \otimes V_k) \otimes V_j\), where \((i_1, i_2, i_3)\) is the permutation corresponding to \(\alpha^{-1}\). We have therefore on \((V_i \otimes V_j) \otimes V_k\) an action of the colored-braid group \(K_3 = \text{Ker}(B_3 \rightarrow S_3)\). Thus, a choice of \(\varphi \in K_3\) determines a new associativity isomorphism. Similarly, a choice of \(\psi \in K_3\) determines a new commutativity isomorphism. Any \(\psi \in K_3\) is of the form \(\psi = \sigma^m\), where \(\sigma\) is the generator of \(B_2\) and \(m \in \mathbb{Z}\). Therefore changing the commutativity isomorphism amounts to raising it to the power \(\lambda = 2m + 1\). Any \(\varphi \in K_3\) is of the form \(\varphi = \sigma_{i_1}^2 \sigma_{i_2}^2 \cdots \sigma_{i_n}^2\), where \(n \in \mathbb{Z}\) and \(f(X, Y)\) is an element of the free group with generators \(X, Y\) (we note that \((\sigma_3 \sigma_2)^3 = (\sigma_2 \sigma_1)^3\) generates the center of \(B_3\)). For new commutativity and associativity isomorphisms the diagrams of the form (1.8) remain commutative as before, but the requirement of commutativity for (1.7) and (1.9) imposes conditions on \(f, \lambda\), and \(n\).

Commutativity of (1.9a) imposes the condition \(n = 0\) and the relation

\[
f(X_1, X_2)X_1^m f(X_3, X_1)X_3^m f(X_2, X_1)^{-1} X_2^m = 1
\]

for \(X_1X_2X_3 = 1\), \(m = (\lambda - 1)/2\). \(\text{(4.1)}\)

Commutativity of (1.9b) imposes the condition \(n = 0\) and the relation

\[
f(X_2, X_1)^{-1} X_1^m f(X_3, X_1)X_3^m f(X_2, X_1)^{-1} X_2^m = 1
\]

for \(X_1X_2X_3 = 1\), \(m = (\lambda - 1)/2\). \(\text{(4.2)}\)

(4.1) and (4.2) are equivalent to the relations

\[
f(Y, X) = f(X, Y)^{-1},
\]

\[
f(X_3, X_1)X_3^m f(X_2, X_3)X_2^m f(X_1, X_2)X_1^m = 1
\]

for \(X_1X_2X_3 = 1\), \(m = (\lambda - 1)/2\). \(\text{(4.3)}\)

Finally, commutativity of (1.7) imposes the following condition on \(\varphi \in K_3\):

\[
\partial_3(\varphi) \cdot \partial_i(\varphi) = \partial_3(\varphi) \cdot \partial_2(\varphi) \cdot \partial_i(\varphi).
\]

Here \(\partial_3(\varphi)\) (resp. \(\partial_i(\varphi)\)) is obtained from the braid \(\varphi\) by adding one more string on the left (resp. right) to the existent three, while \(\partial_i(\varphi)\) for \(1 \leq i \leq 3\) is obtained from \(\varphi\) by replacing the \(i\)th string of the braid \(\varphi\) by two strings, one just to the left of the other (note that the \(K_n\) form a cosimplicial group, where the boundary homomorphisms are the \(\partial_i: K_n \rightarrow K_{n+1}\), while the degeneracy homomorphisms \(K_{n+1} \rightarrow K_n\) are obtained by deleting one of the \(n+1\) strings). It is known [20] that \(K_n\) is generated by the elements \(x_{ij}\), \(1 \leq i < j \leq n\), where

\[
x_{ij} = (\sigma_{j-2} \cdots \sigma_i)^{-1} \sigma_{j-2}^2 (\sigma_{j-2} \cdots \sigma_i) = (\sigma_{j-1} \cdots \sigma_i) \sigma_{j-1}^2 (\sigma_{j-1} \cdots \sigma_i)^{-1}.
\]

(4.6)

and the defining relations among the \(x_{ij}\) are of the form

\[
(a_{ijk} \cdot x_{ij}) = (a_{ijk} \cdot x_{ik}) = (a_{ijk} \cdot x_{jk}) = 1,
\]

where \(i < j < k\), \(a_{ik} = x_{ii} x_{ik} x_{ki}\). \(\text{(4.7)}\)

\[
(x_{ij} \cdot x_{kl}) = (x_{il} \cdot x_{jk}) = 1 \quad \text{for} \quad i < j < k < l,
\]

\[
(x_{ik} \cdot x_{ij}) = (x_{jk} \cdot x_{il}) = 1 \quad \text{for} \quad i < j < k < l.
\]

(4.8)
Here $(u, v)$ means $uvw^{-1}v^{-1}$. In terms of the $x_{ij}$, (4.5) says that

$$f(x_{12} x_{23} x_{24} x_{34})f(x_{13} x_{23} x_{34}) = f(x_{23} x_{34})f(x_{12} x_{13} x_{24} x_{34})f(x_{12} x_{23}).$$

(4.10)

Thus, every pair $(\lambda, f)$, $\lambda \in 1 + 2\mathbb{Z}$, satisfying (4.3), (4.4), and (4.10) determines a "natural" way of constructing for any quasitensored category $C$ a new quasitensored category $C'$, where the only change is in the commutativity and associativity isomorphisms ("natural" means that if $F : C_1 \to C_2$ is a tensor functor in the sense of Definition 1.8 of [6], then $F$ is a tensor functor from $C'_1$ to $C'_2$). It is easily shown that the correspondence is bijective. The interpretation of the pairs $(\lambda, f)$ satisfying (4.3), (4.4), and (4.10) as ways of changing the commutativity and associativity isomorphisms allows us to define on the set of all such pairs a semigroup structure $(\lambda_1, f_1) \cdot (\lambda_2, f_2) = (\lambda, f)$, where

$$\lambda = \lambda_1 \lambda_2,$$

$$f(X, Y) = f_1(f_2(X, Y)X^{\lambda_2} f_2(X, Y)^{-1}, Y^{\lambda_2}) \cdot f_2(X, Y).$$

(4.11)

Now suppose $(A, \Delta, e, \Phi, R)$ satisfies (1.1)–(1.6). Then the $A$-modules form a quasitensored category (see §1). If we change the commutativity and associativity isomorphisms by means of a pair $(\lambda, f)$ satisfying (4.3), (4.4), and (4.10), where

$$R = R \cdot (R^{21} \cdot R)^{m} - (R \cdot R^{21})^{m} \cdot R, \quad m = (\lambda - 1)/2,$$

(4.12a)

$$\Phi = \Phi \cdot f(R^{21} R^{12}, \Phi^{-1} R^{32} R^{23} \Phi)$$

$$= f(\Phi R^{21} R^{12} \Phi^{-1}, R^{32} R^{23}).$$

(4.12b)

The formulas (4.12) define an action of the semigroup of all pairs $(\lambda, f)$ satisfying (4.3), (4.4), and (4.10) on the collection of sets $(A, \Delta, e, \Phi, R)$ satisfying (1.1)–(1.6). Unfortunately, this semigroup consists only of the identity element $(\lambda = 1, f = 1)$ and the involution $(\lambda = -1, f = 1)$ taking $(A, \Delta, e, \Phi, R)$ into $(A, \Delta, e, \Phi, R^{-1})$. This is a consequence of the following proposition, since by (4.10) $f(X, Y)$ belongs to the commutant of the free group with generators $X, Y$.

**PROPOSITION 4.1.** Equations (4.3) and (4.4), where $f(X, Y)$ belongs to the free group with generators $X$ and $Y$, are satisfied only by $\lambda = \pm 1$, $f(X, Y) = Y^l X^{-l}$.

**PROOF.** If $(\lambda, f)$ satisfies equations (4.3) and (4.4), then these are also satisfied by $(\lambda, f)$, where $f(X, Y) = Y^{-l} f(X, Y) X^l$. From (4.3) it follows that for a suitable $s$ either $\tilde{f} = 1$ or the noncancellable representation of $\tilde{f}(X, Y)$ is of the form $X^{l_s} \cdots Y^{-l_s}$, $l \neq 0$. Since $\tilde{f}$ satisfies (4.4), the second case is impossible, and in the first case $\lambda = \pm 1$.

Observe now that if $k$ is a field of characteristic 0, then formulas (4.3), (4.4), (4.10), and (4.11) are meaningful even if we suppose that $\lambda \in k$, while $f(X, Y)$ belongs to the $k$-pro-unipotent completion of the free group with generators $X, Y$, i.e., $f(X, Y)$ is a formal expression of the form $\exp F(\ln X, \ln Y)$, where $F$ is a Lie formal series over $k$. Then both sides of (4.10) belong to the $k$-pro-unipotent completion of $K_4$, i.e., are of the form $e^v$, where $v$
belongs to the quotient algebra of Lie formal series in the variables $\xi_{ij}, 1 \leq i < j \leq 4$ modulo the ideal corresponding to the relations (4.7)–(4.9) for $x_{ij} = \exp \xi_{ij}$.

We denote by $\text{GT}(k)$ the semigroup of pairs $(\lambda, f)$ satisfying (4.3), (4.4), and (4.10), where $\lambda \in k$ and $f$ belongs to the $k$-pro-unipotent completion of the free group. The group of invertible elements of $\text{GT}(k)$ will be denoted by $\text{GT}(k)^*$; we call it the $k$-pro-unipotent version of the Grothendieck-Teichmüller group. It is easily seen that $\text{GT}(k) = \{(\lambda, f) \in k \mid \lambda \neq 0\}$. It turns out (see §5, 6) that the group $\text{GT}(k)$ is rather large: it is infinite-dimensional, and the homomorphism $\text{GT}(k) \to k^*$ taking $(\lambda, f)$ to $\lambda$ is surjective.

If $(\lambda, f) \in \text{GT}(k)$ and $(A, \Delta, \varepsilon, \Phi, R)$ is a quasitriangular quasi-Hopf QUE-algebra over $k[[h]]$, then the formulas (4.12) are meaningful. Thus, $\text{GT}(k)$ acts on the set of quasitriangular quasi-Hopf QUE-algebras. A twist (see (1.10)–(1.12)) commutes with the action of $\text{GT}(k)$. Suppose now that $A$ is $Ug$ with the usual comultiplication, $R = e^{ih/2}$ and $\Phi = \exp P(h^{1/2}, h^{23})$, where $g$ is a deformation Lie algebra over $k[[h]], t \in g \geq g$ is symmetric and $g$-invariant, and $P$ is a Lie formal series over $k$. Then the $R$ and $\Phi$ defined by formulas (4.12) are of the form $R = e^{ih/2}$ and $\Phi = \exp P(h^{1/2}, h^{23})$, where $P$ is a Lie formal series over $k$.

We can interpret the elements of $\text{GT}(k)$ as endomorphisms of a certain completion $B_n(k)$ of the group $B_n$. Suppose $\lambda, f$ satisfy (4.3), (4.4), and (4.10), with $\lambda \in 1 + 2\mathbb{Z}$ and $f(\lambda, Y)$ belonging to the free group on the generators $X, Y$ (forget that there are only two such pairs $(\lambda, f)$). Let $V$ be an object in a quasitensored category $C$, $V^{\otimes 2} = V \otimes V$, $V^{\otimes 3} = V^{\otimes 2} \otimes V$, etc. On $V^{\otimes k}$ there is an action of $B_n$. Changing the commutativity and associativity isomorphisms in $C$ by means of $(\lambda, f)$ gives rise to a new action of $B_n$ on $V^{\otimes n}$. It is obtained from the old by composition with the endomorphism of $B_n$ given by $\sigma_i \mapsto \sigma_i, \sigma_i \mapsto f(y_i, \sigma_i^2)^{-1} \sigma_i^2 f(y_i, \sigma_i^2)$ for $i > 1$, where $y_i = \sigma_{i-1} \cdots \sigma_1 \sigma_i \cdots \sigma_{i-1}$ (in the notation of (4.6), $y_i = x_{i-1}x_{i+1} \cdots x_{i-1}$). Now let $K_n(k)$ be the $k$-pro-unipotent completion of $K_n$, and $B_n(k)$ the quotient of the semidirect product of $B_n$ and $K_n(k)$ (the automorphisms $A \in \text{Aut} B_n(k)$ that extend to $K_n(k)$) modulo the subgroup of elements of the form $x \cdot x^{-1}$, where $x$ is regarded as an element of $B_n$, and $x^{-1}$ as an element of $K_n(k)$. The formulas

$$\sigma_1 \mapsto \sigma_1^{(k)}, \quad \sigma_i \mapsto f(y_i, \sigma_i^2)^{-1} \sigma_i^2 f(y_i, \sigma_i^2), \quad 1 \leq i \leq n, \quad (4.13)$$

where $\sigma_i^{(k)} = \sigma_i \cdot (\sigma_i^2)^{(\lambda-1)/2}$, $y_i = \sigma_{i-1} \cdots \sigma_1 \sigma_i \cdots \sigma_{i-1}$, define a right action of $\text{GT}(k)$ on $B_n(k)$, which is faithful for $n \geq 3$. The endomorphisms (4.13) are compatible with the imbeddings $B_n(k) \to B_{n+1}(k)$ that take $\sigma_i$ onto $\sigma_i$ and they induce the identity automorphisms on the groups $S_n = B_n(k)/K_n(k)$. The author does not know whether any set of automorphisms $\gamma_n \in \text{Aut} B_n(k)$ that has these properties results from an element of $\text{GT}(k)$ (perhaps the methods of [15] can elucidate this). In any case, the endomorphisms of $B_n(k)$ that take $\sigma_i$ onto $\sigma_i^{(k)}$ and induce the identity automorphism on $S_n$ do have the form (4.13) or, what is equivalent, the form

$$\sigma_1 \mapsto \sigma_1^{(k)}, \quad \sigma_1 \sigma_2 \sigma_1 \mapsto \sigma_1 \sigma_2 \sigma_1 \cdot [(\sigma_1 \sigma_2)^3]^{(\lambda-1)/2} f(\sigma_1^2, \sigma_2^2), \quad (4.14)$$
where $f$ satisfies (4.3) and (4.4). Conversely, (4.3) and (4.4) imply that (4.14) defines an endomorphism of $B_3(k)$.

We describe now, following [2], how to construct a canonical homomorphism $\text{Gal}(\overline{Q}/Q) \to \text{GT}(Q)$, where $\overline{Q}$ is the algebraic closure of $Q$ in $C$ (although this construction will not be used in the sequel). Let us denote by $\hat{\text{GT}}$ (resp. $\text{GT}_l$) the semigroup of all pairs $((\lambda, f)$ satisfying (4.3), (4.4), and (4.10), where $f$ belongs to the pro-finite completion (resp. pro-$l$-completion) of the free group, and $\lambda \in 1 + 2\hat{\mathbb{Z}}$ (resp. $\lambda \in 1 + 2\mathbb{Z}_l$). Here $\hat{\mathbb{Z}} = \lim_{\leftarrow n} \mathbb{Z}/n\mathbb{Z}$. The groups of invertible elements in $\hat{\text{GT}}$ and $\text{GT}_l$, we denote by $\hat{\text{GT}}$ and $\text{GT}_l$. There exist natural homomorphisms $\hat{\text{GT}} \to \text{GT}_l$ and $\text{GT}_l \to \text{GT}(Q)$. What remains is to construct a homomorphism $\text{Gal}(\overline{Q}/Q) \to \hat{\text{GT}}$. Let us first recall the construction, due to Belyi [21], of a homomorphism $\text{Gal}(\overline{Q}/Q) \to \text{Aut} \hat{\Gamma}$, where $\Gamma$ is the quotient of $B_3$ by its center, and $\hat{\Gamma}$ is the pro-finite completion of $\Gamma$. There exists a canonical isomorphism $\hat{\Gamma} \cong \pi_1(M, x)$, where $M$ is the stack which is the quotient of $\mathbb{C}P^1 \setminus \{0, 1, \infty\}$ by the group $S_3$ of projective transformations permuting $0, 1, \infty$, and $x$ is the image of a point in $\mathbb{C}P^1$ that lies on the real axis near $0$. Therefore $\hat{\Gamma} = \text{Gal}(F/E)$ where $E$ is the subfield of $S_3$-invariants in $Q(z)$ ($S_3$ acts on $z$ as indicated above), and $F$ is the maximal algebraic extension of $Q(z)$ in $L = \bigcup_n Q((z^{1/n}))$ that is unramified outside $0, 1, \infty$. The group $\text{Gal}(\overline{Q}/Q)$ acts on $L$, leaving $E$ and $F$ invariant. Therefore $\text{Gal}(\overline{Q}/Q)$ acts on $\text{Gal}(F/E) = \hat{\Gamma}$. The subgroup $H \subseteq \hat{\Gamma}$ that is topologically generated by the image of $\sigma_1 \in B_3$ is invariant with respect to $\text{Gal}(\overline{Q}/Q)$, and the action of $\text{Gal}(\overline{Q}/Q)$ on the quotient group $S_3$ of $\hat{\Gamma}$ is the identity. The semigroup of endomorphisms $\varphi: \hat{\Gamma} \to \hat{\Gamma}$ such that $\varphi(H) \subset H$ and the action of $\varphi$ on $S_3$ is the identity is anti-isomorphic to the semigroup of pairs $((\lambda, f)$ satisfying (4.3) and (4.4), where $\lambda \in 1 + 2\hat{\mathbb{Z}}$ and $f$ belongs to the pro-finite completion of the free group: the pair $((\lambda, f)$ corresponds (see (4.14)) to the endomorphism $\varphi: \hat{\Gamma} \to \hat{\Gamma}$ such that $\varphi(\sigma_1) = \sigma_1^{-1}$, $\varphi(\sigma_2 \sigma_3) = \sigma_i \sigma_j \sigma_k / (\sigma_i \sigma_j \sigma_k)$, where $\sigma_i$ is the image of $\sigma_i$ in $\hat{\Gamma}$. To obtain an isomorphism between the groups of invertible elements of the two semigroups, combine the antihomomorphism with the mapping $\nu \mapsto \nu^{-1}$.

It remains to show that the pairs $((\lambda, f)$ corresponding to elements of $\text{Gal}(\overline{Q}/Q)$ satisfy (4.10). This can be inferred from §2 of Grothendieck [2]. It is proposed in [2] to consider, for any $g$ and $\nu$, the “Teichmüller groupoid” $I_{g, \nu}$, i.e., the fundamental groupoid of the module stack $M_{g, \nu}$ of compact Riemann surfaces $X$ of genus $g$ with $\nu$ distinguished points $x_1, \ldots, x_\nu$. The fundamental groupoid differs from the fundamental group in that we choose not one, but several distinguished points. In the present case it is convenient to choose the distinguished points “at infinity” (see §15 of [11]) in accordance with the methods of “maximal degeneration” of the set $(X, x_1, \ldots, x_\nu)$. Since degeneration of the set $(X, x_1, \ldots, x_\nu)$ results in decreasing $g$ and $\nu$, the groupoids $I_{g, \nu}$, for different $g$ and $\nu$ are connected by certain homomorphisms. The collection of all $I_{g, \nu}$ and all such homomorphisms is called in [2] the Teichmüller tower. It is observed in [2] that there exists a natural homomorphism $\text{Gal}(\overline{Q}/Q) \to G$, where $G$ is the group of automorphisms of the
pro-finite analogue of the Teichmüller tower (in which $T_{g, \nu}$ is replaced by its pro-finite completion $\tilde{T}_{g, \nu}$). It is also stated in [2], as a plausible conjecture, that $\tilde{T}_{0,4}$ and $\tilde{T}_{1,1}$ in a definite sense generate the whole tower $\{\tilde{T}_{g, \nu}\}$ and that all relations between generators of the tower come from $\tilde{T}_{0,4}, \tilde{T}_{1,1}, \tilde{T}_{0,5}$, and $\tilde{T}_{1,2}$. This conjecture has been proved, apparently, in Appendix B of the physics paper [22]. In any case, it is easily seen that $\tilde{T}_{0,4}$ generates the subtower $\{\tilde{T}_{0, \nu}\}$, and that all relations in $\{\tilde{T}_{0, \nu}\}$ come from $\tilde{T}_{0,4}$ and $\tilde{T}_{0,5}$.

It can be shown that $\tilde{G}T$ is the automorphism group of the tower $\{\tilde{T}_{0, \nu}\}$. Indeed, an automorphism of this tower is uniquely determined by its action on $\tilde{T}_{0,4}$, i.e., on $\tilde{G}$. This action is described by a pair $(\lambda, f)$ satisfying (4.3) and (4.4), and (4.10) is necessary and sufficient for the automorphism of $\tilde{T}_{0,4}$ to extend to one of $\tilde{T}_{0,5}$. Grothendieck’s conjecture implies that the group of automorphisms of the tower $\{\tilde{T}_{g, \nu}\}$ that are compatible with the natural homomorphism $\tilde{T}_{0,4} \to \tilde{T}_{1,1}$ (to a quadruple of points on $P^1$ is assigned the double covering of $P^1$ ramified at these points) is also equal to $\tilde{G}T$: if an automorphism of $\tilde{T}_{0,4}$ extends to one of $\tilde{T}_{0,5}$, then it also extends to one of $\tilde{T}_{1,2}$, since, as noted in [2], $M_{1,2}$ is almost the same as $M_{0,5}$.

The homomorphism $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \tilde{G}T$ is, by Belyi’s theorem [21], injective. The study of the kernel and image of the homomorphism $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \tilde{G}T$ has been dealt with by a number of papers (see [11]–[14] and the literature cited there).

§5. Proof of Theorem A''

Let $k$ be a field of characteristic 0, $Fr_k(A, B)$ the algebra of Lie formal series over $k$ in the variables $A$ and $B$ (Fr is short for “free”). $Fr_k(A, B) = \exp Fr_k(A, B)$ and $M_f(k)$ the set of $\varphi \in Fr_k(A, B)$ satisfying (2.13) and (2.14), where

$$X^{ij} = X^{ji}, \quad [X^{ij}, X^{rl}] = 0 \quad \text{for} \quad i \neq j \neq r \neq l,$$

$$[X^{ij} + X^{ji}, X^{rl}] = 0 \quad \text{for} \quad i \neq j \neq r.$$

Let $a_n^k$ be the completion (with respect to the natural grading) of the Lie algebra over $k$ with generators $X^{ij}$, $1 \leq i \leq n$, $1 \leq j \leq n$, $i \neq j$, and defining relations (5.1). For $n \geq 3$ the algebras $a_n^k$ are not free, but they reduce to free ones: $a_n^k$ is the semidirect product of $a_{n-1}^k$ and the topologically free algebra generated by the $X_{in}$, $1 \leq i \leq n - 1$ (the latter is an ideal in $a_n^k$). For $n = 3$ there is a more convenient realization: $a_3^k$ is the direct sum of its center, generated by the element $X^{13} + X^{13} + X^{13}$, and the topologically free algebra generated by $X^{12}$ and $X^{23}$. Therefore (2.14a) is equivalent to two equalities, one of which is obtained by substituting $X^{12} = A$, $X^{23} = B$, $X^{13} = -A-B$ and the other by substituting $X^{12} = X^{23} = 0$. The second equality is a tautology, and the first is of the form

$$e^{A/2} \varphi(C, A)e^{C/2} \varphi(C, B)e^{-A/2} = 1,$$

where $A + B + C = 0$. (5.2a)
Similarly, (2.14b) is equivalent to the equality
\[ \varphi(B, A)^{-1} e^{A/2} \varphi(C, A) e^{C/2} \varphi(C, B)^{-1} e^{B/2} = 1, \]
(5.2b)
where \( A + B + C = 0 \),

obtained by substituting \( X^{12} = C \), \( X^{23} = B \), \( X^{13} = A \). (5.2a) and (5.2b) imply (2.12). On the other hand, if (2.12) holds, then (5.2a) and (5.2b) are equivalent to the equality
\[ e^{A/2} \varphi(C, A) e^{C/2} \varphi(B, C) e^{B/2} \varphi(A, B) = 1, \]
(5.3)
where \( A + B + C = 0 \).

Thus, \( M_{\mu}(k) \) is the set of \( \varphi \in \text{Fr}_k(A, B) \) satisfying (2.12), (5.3), and (2.13). Let \( M_{\mu}(k) \) be the set of \( \varphi \in \text{Fr}_k(A, B) \) satisfying (2.12), (2.13), and the equation obtained from (5.3) by replacing \( e^{A/2}, e^{B/2}, e^{C/2} \) by \( e^{\mu A/2}, e^{\mu B/2}, e^{\mu C/2} \). Put \( M(k) = \{ (\mu, \varphi) | \mu \in k, \varphi \in M_{\mu}(k) \} \) and \( M(k) = \{ (\mu, \varphi) \in M(k) | \mu \neq 0 \} \). On \( M(k) \) there is an action of \( \text{GT}(k) \): an element \( (\lambda, f) \in \text{GT}(k) \) takes \( (\mu, \varphi) \in M(k) \) into \( (\lambda \mu, \varphi) \), where \( \varphi(A, B) = f(\varphi(A, B)) e^{\lambda} \varphi(A, B)^{-1}, e^{\lambda} \times \varphi(A, B) \) (cf. (4.12)).

**Proposition 5.1.** The action of \( \text{GT}(k) \) on \( M(k) \) is free and transitive.

**Proof.** If \( (\mu, \varphi) \in M(k) \) and \( (\mu, \psi) \in M(k) \), then there is exactly one \( f \) such that \( \varphi(A, B) = f(\varphi(A, B)) e^{\lambda} \varphi(A, B)^{-1}, e^{\lambda} \cdot \varphi(A, B) \). We need to show that \( (\lambda, f) \in \text{GT}(k) \), where \( \lambda = \mu / \mu \). We prove (4.10). Let \( G_n \) be the semidirect product of \( S_n \) and \( \exp \alpha_n \). Consider the homomorphism \( B_n \rightarrow G_n \) that takes \( \alpha_i \) into
\[ \varphi(X^{11} + \cdots + X^{1-i-1}, X^{1-i+1}) e^{\alpha_i + 1} e^{\mu X^{i-i+1}} / 2 \varphi(X^{11} + \cdots + X^{1-i-1}, X^{1-i+1}), \]
where \( \alpha_i \in S_n \) transposes \( i \) and \( j \). It induces a homomorphism \( K_n \rightarrow \exp \alpha_n \), and therefore a homomorphism \( \alpha_n : K_n(k) \rightarrow \exp \alpha_n \), where \( K_n(k) \) is the \( k \)-pro-unipotent completion of \( K_n \). It is easily shown that the left- and right-hand sides of (4.10) have the same images in \( \exp \alpha_n \). It remains to prove that \( \alpha_n \) is an isomorphism. The algebra \( K_n(k) \) is topologically generated by the elements \( \xi_{ij} \), \( 1 \leq i < j \leq n \), with defining relations obtained from (4.7)–(4.9) by substituting \( x_{ij} = e^{\xi_{ij}} \). The principal parts of these relations are the same as in (5.1), while \( (\alpha_n)_{ij} (\xi_{ij}) = \mu X^{ij} + \{ \text{lower terms} \} \), where \( (\alpha_n)_{ij} : \text{Lie } K_n(k) \rightarrow \alpha_n \) is induced by the homomorphism \( \alpha_n \). Therefore \( \alpha_n \) is an isomorphism, i.e., (4.10) is proved. (4.3) is obvious. To prove (4.4), we can interpret it in terms of \( K_n \) and argue as in the proof of (4.10), or, what is equivalent, make the substitution
\[ X_1 = e^A, \quad X_2 = e^{A/2} \varphi(B, A) e^B \varphi(B, A)^{-1} e^{A/2}, \]
\[ X_3 = \varphi(C, A) e^C \varphi(C, A)^{-1}, \]
(5.4)
where \( A + B + C = 0 \).

Identifying \( \mathfrak{M}_{\mu}(k) \) with the quotient of \( M(k) \) by the natural action of \( k^* \) acting \( (\mu, \varphi) \) into \( (c \mu, \varphi) \), where \( \varphi(A, B) = \varphi(cA, cB) \), we obtain an action of \( \text{GT}(k) \) on \( \mathfrak{M}_{\mu}(k) \). Proposition 5.1 says that the subgroup \( \mathfrak{G}_1(k) = \{ (\lambda, f), \lambda \in \text{GT}(k) | \lambda = 1 \} \) acts on \( \mathfrak{M}_{\mu}(k) \) freely and transitively; and
if \( M_1(k) \neq \emptyset \), then the sequence \( 1 \rightarrow \text{GT}_1(k) \rightarrow \text{GT}(k) \xrightarrow{\nu} k^* \rightarrow 1 \), where
\[
\nu(\lambda, f) = \lambda,
\]
is exact and to every \( \varphi \in M_1(k) \) corresponds a homomorphism \( \theta_\varphi : k^* \rightarrow \text{GT}(k) \) such that \( \nu \circ \theta_\varphi = \text{id} \), while \( \theta_\varphi(k^*) \) is the stabilizer of \( \varphi \) in \( \text{GT}(k) \).

Denote the Lie algebras of the pro-algebraic groups \( \text{GT}(k) \) and \( \text{GT}_1(k) \) by \( \text{gt}(k) \) and \( \text{gt}_1(k) \). Substituting \( f(X, Y) = \exp \epsilon \psi(\ln X, \ln Y) \) and \( \lambda = 1 + \epsilon \) into (4.3), (4.4), and (4.10), and linearizing with respect to \( \epsilon \), we find that \( \text{gt}(k) \) consists of the pairs \((s, \psi), s \in k, \psi \in \text{Fr}_k(\alpha, \beta)\), such that
\[
\psi(\alpha, \beta) = -\psi(\beta, \alpha),
\]
\[
\psi(\alpha, \beta; \gamma) + \psi(\beta, \gamma) + \psi(\gamma, \alpha) + \frac{s}{2}(\alpha + \beta + \gamma) = 0,
\]
where \( e^\alpha e^\beta e^{-1} = 1 \).
\[
\psi(\xi_{12}, \xi_{23} \ast \xi_{24}) + \psi(\xi_{13} \ast \xi_{23}, \xi_{34})
\]
\[
= \psi(\xi_{23}, \xi_{34}) + \psi(\xi_{12}, \xi_{13}, \xi_{24} \ast \xi_{34}) + \psi(\xi_{12}, \xi_{23}).
\] (5.7)

Here \( u \ast v = \ln(e^u e^v) \), and the \( \xi_{ij} \) satisfy the relations obtained from (4.7)-(4.9) by substituting \( x_{ij} = \exp \xi_{ij} \). A commutator in \( \text{gt}(k) \) has the form
\[(s_1, \psi_1), (s_2, \psi_2) = (0, \psi), \]
where \( \psi = [\psi_1, \psi_2] + s_1 D(\psi_1) - s_2 D(\psi_2) + D_{\psi_1}(\psi_2) - D_{\psi_2}(\psi_1) \), with \( D \) and \( D_{\psi} \) derivations of \( \text{Fr}_k(\alpha, \beta) \) such that \( D(\alpha) = \alpha, D(\beta) = \beta, D_{\psi_1}(\alpha) = [\psi_1, \alpha], \) and \( D_{\psi}(\beta) = 0 \).

If \( M_1(k) \neq \emptyset \), then the sequence
\[
0 \rightarrow \text{gt}_1(k) \rightarrow \text{gt}(k) \xrightarrow{\nu} k \rightarrow 0,
\]
is exact, and to every \( \varphi \in M_1(k) \) corresponds a splitting, defined by the Lie algebra of the stabilizer of \( \varphi \) in \( \text{GT}(k) \).

**Proposition 5.2.** The mapping \( M_1(k) \rightarrow \{ \text{splittings of the sequence (5.8)} \} \) is bijective. In particular, exactness of (5.8) implies that \( M_1(k) \neq \emptyset \).

**Proof.** The mapping takes \( \varphi \in M_1(k) \) into the splitting defined by the element \((1, \psi) \in \text{gt}(k)\), where \( \psi \) is found from the condition
\[
\varphi(A, B)^{-1} \frac{d}{dt} \varphi(tA, tB)|_{t=1} = \psi(A, \varphi(A, B)^{-1}B\varphi(A, B)).
\] (5.9)

Given \( \psi \), there exists exactly one \( \varphi \in \text{Fr}_k(A, B) \) satisfying (5.9). In view of (5.5), (5.9) remains valid if \( \varphi(A, B) \) is replaced by \( \varphi(B, A)^{-1} \). Therefore \( \varphi(A, B) = \varphi(B, A)^{-1} \). We prove (5.3). Denote the left-hand side of (5.3) by \( Q(A, B) \). Then
\[
Q(A, B)^{-1} \frac{d}{dt} Q(tA, tB)|_{t=1}
\]
\[
= \psi(A, B) + \psi(\overline{B}, C) + \psi(\overline{C}, A) + \frac{\overline{A} + B + C}{2},
\]
where
\[
\overline{A} = Q(A, B)^{-1}AQ(A, B), \quad \overline{B} = \varphi(A, B)^{-1}B\varphi(A, B),
\]
\[
\overline{C} = \varphi(A, B)^{-1} e^{-\frac{B}{2}} \varphi(B, C)^{-1} C\varphi(B, C) e^{\frac{B}{2}} \varphi(A, B).
\] (5.10)
Suppose we have already proved that $Q(A, B) \equiv 1 \mod \deg n$ (i.e., $Q(A, B) = 1 +$ terms of degree $n$ and higher). If $Q(A, B) \equiv 1 + q(A, B) \mod \deg(n + 1)$, where $q$ is homogeneous of degree $n$, then the left-hand side of (5.10) is congruent to $n \cdot q(A, B) \mod \deg(n + 1)$. Since $e^\theta e^C = e^{-\lambda/2}Q(A, C)e^{-\lambda/2}Q(A, B)$, we find, denoting by $\alpha$, $\beta$, and $\gamma$ the residue classes of $A$, $B - q(A, B)$, and $C - q(A, C) \mod \deg(n + 1)$, that $e^\alpha e^\beta e^\gamma = 1$. Therefore (5.6) holds, with $s = 1$. Hence the right-hand side of (5.10) is congruent to $q(A, B) + q(A, C) \mod \deg(n + 1)$. From the definition of $Q$ it follows that $q(A, C) = q(B, A)$. Thus, $q(B, A) = (n - 1) \cdot q(A, B)$. Therefore, $q = 0$ (for $n = 2$, this follows from the fact that $q(A, B)$ is a Lie polynomial and therefore proportional to $[A, B]$).

It remains to prove (2.13). Denote the left-hand side of (2.13) by $f$, and the right by $g$. Suppose we have already proved that $f \equiv g \mod \deg(n)$. To prove that $f \equiv g \mod \deg(n + 1)$, it suffices to show that

\[
\begin{align*}
f(X^{12}, X^{13}, \ldots)^{-1} \cdot \frac{d}{dt} f(tX^{12}, tX^{13}, \ldots)|_{t=1} &
\equiv g(X^{12}, X^{13}, \ldots)^{-1} \cdot \frac{d}{dt} g(tX^{12}, tX^{13}, \ldots)|_{t=1} \mod \deg(n + 1),
\end{align*}
\]

i.e., that

\[
\psi(\alpha, \beta) + \psi(\gamma, \delta) \equiv \psi(\lambda, \delta) + \psi(\mu, \nu) + \psi(\alpha, \lambda) \mod \deg(n + 1),
\]

where

\[
\begin{align*}
\alpha &= X^{12}, \\
\beta &= f^{-1} \cdot (X^{23} + X^{24}) \cdot f, \\
\gamma &= X^{13} + X^{23}, \\
\delta &= \phi(X^{13} + X^{23}, X^{14})^{-1} \cdot X^{23} \phi(X^{13} + X^{23}, X^{34}), \\
\lambda &= \phi(X^{12}, X^{23})^{-1} X^{23} \phi(X^{12}, X^{23}), \\
\mu &= \phi(X^{12}, X^{23})^{-1} (X^{12} + X^{13}) \phi(X^{12}, X^{23}), \\
\nu &= \phi(X^{12}, X^{23})^{-1} \phi(X^{12} + X^{13}, X^{24} + X^{34})^{-1} \\
&\times (X^{24} + X^{34}) \phi(X^{12} + X^{13}, X^{24} + X^{34}) \phi(X^{12}, X^{23}).
\end{align*}
\]

Using (2.12), (5.3), and the congruence $f \equiv g \mod \deg n$, we construct (see the proof of Proposition 5.1) a homomorphism $h: K_4(k) \to \exp(a_k^*)/I$, where $I = \{a \in a_k^* | a \equiv 0 \mod \deg(n + 1)\}$. Then in (5.7) putting $\xi_{ij} = \ln h(x_{ij})$, where the $x_{ij}$ are defined by (4.6), we obtain (5.11). 

**Proposition 5.3.** $M_i(k) \neq \emptyset$.

**Proof.** Since $M_i(C) \neq \emptyset$ (see §2), the sequence (5.8) is exact for $k = C$. This implies (5.8) is exact for $k = Q$. Therefore $M_i(Q) \neq \emptyset$ (see Proposition 5.2) and, so much the more, $M_i(k) \neq \emptyset$. Another version of the proof: since the composite of the homomorphism $\text{Gal}(\overline{Q}/Q) \to \text{GT}(Q_i)$ (see §4) and the homomorphism $\nu: \text{GT}(Q_i) \to Q$ is the homomorphism $f: \text{Gal}(\overline{Q}/Q) \to Z$, defined by the relation $\sigma^{-1}(\zeta) = \zeta^{\sigma(1)}$, where $\zeta^{i-1}, \sigma \in \text{Gal}(\overline{Q}/Q)$, it follows that the image of $\nu$ is infinite, the sequence (5.8) is exact for $k = Q_i$, etc. 

Thus, Theorem $A''$ (see §1) is proved.
PROPOSITION 5.4. The set \( M^*_1(k) = \{ \varphi \in M_1(k) \mid \varphi(A, -B) = \varphi(-A, B) \} \) is nonempty. It is acted on by the group \( \text{GT}^+(k) = \{ (\lambda, f) \in \text{GT}(k) \mid f(X^{-1}, Y^{-1}) = f(X, Y) \} \), and the action on \( M^*_1(k) \) by the subgroup \( \text{GT}^+(k) \cap \text{GT}_1(k) \) is free and transitive.

PROOF. \( M^*_1(k) \) is the set of \( \sigma \)-invariant elements of \( M_1(k) \), where \( \sigma \in \text{GT}(k) \) is the involution corresponding to \( \lambda = -1, f = 1 \). Since (5.8) has a \( \sigma \)-invariant splitting, we have \( M^*_1(k) \neq \emptyset \). The rest is obvious.

REMARK. \( \varphi_{kZ}(-A, -B) \neq \varphi_{kZ}(A, B) \) (see (2.15), (2.17), or (2.18)).

The above proof of Proposition 5.3 is nonconstructive. Our next objective is to prove Proposition 5.8, which will show that constructing elements of \( M_1(k) \) by successive approximations presents no problems. For this we introduce the following modification \( \text{GRT}(k) \) of the group \( \text{GT}(k) \). We denote by \( \text{GRT}_1(k) \) the set of all \( g \in \mathfrak{r}_k(A, B) \) such that

\[
g(B, A) = g(A, B)^{-1},
\]

\[
g(C, A)g(B, C)g(A, B) = 1 \quad \text{for } A + B + C = 0.
\]

\[
A + g(A, B)^{-1}Bg(A, B) + g(A, C)^{-1}Cg(A, C) = 0
\]

for \( A + B + C = 0 \),

\[
g(X^{12}, X^{23} + X^{24})g(X^{13} + X^{23}, X^{24})
\]

\[
= g(X^{23}, X^{24})g(x^{12} + x^{13}, x^{24} + x^{24})g(X^{12}, X^{23}),
\]

where the \( X^{ij} \) satisfy (5.1). \( \text{GRT}_1(k) \) is a group with the operation

\[
(g_1 \circ g_2)(A, B) = g_1(g_2(A, B)Ag_2(A, B)^{-1}, B) \cdot g_2(A, B).
\]

On \( \text{GRT}_1(k) \) there is an action of \( k^* \), given by \( e(A, B) = g(c^{-1}A, c^{-1}B) \), \( c \in k^* \). The semidirect product of \( k^* \) and \( \text{GRT}_1(k) \) we denote by \( \text{GRT}(k) \). The Lie algebra \( \mathfrak{gr}_1(k) \) of the group \( \text{GRT}_1(k) \) consists of the series \( \psi \in \mathfrak{r}_k(A, B) \) such that

\[
\psi(B, A) = -\psi(A, B),
\]

\[
\psi(C, A) + \psi(B, C) + \psi(A, B) = 0 \quad \text{for } A + B + C = 0,
\]

\[
\psi(B, \psi(A, B)) + [C, \psi(A, C)] = 0 \quad \text{for } A + B + C = 0,
\]

\[
\psi(X^{12}, X^{23} + X^{24}) + \psi(X^{13} + X^{23}, X^{24})
\]

\[
= \psi(X^{23}, X^{24}) + \psi(x^{12} + x^{13}, x^{24} + x^{24}) + \psi(x^{12}, x^{23}).
\]

where the \( X^{ij} \) satisfy (5.1). A commutator \( \langle , , \rangle \) in \( \mathfrak{gr}_1(k) \) is of the form

\[
\langle \psi_1, \psi_2 \rangle = [\psi_1, \psi_2] + D_{\psi_1}(\psi_2) - D_{\psi_2}(\psi_1).
\]

where \( [\psi_1, \psi_2] \) is the commutator in \( \mathfrak{r}_k(A, B) \) and \( D_{\psi} \) is the derivation of \( \mathfrak{r}_k(A, B) \) given by \( D_{\psi}(A) = [\psi, A], D_{\psi}(B) = 0 \). The algebra \( \mathfrak{gr}_1(k) \) is graded, and the Lie algebra \( \mathfrak{gr}(k) \) of the group \( \text{GRT}(k) \) is the semidirect sum of the 1-dimensional algebra \( k \) and \( \mathfrak{gr}_1(k) \), where \( k \) acts on \( \mathfrak{gr}_1(k) \) as follows: \( 1 \in k \) takes a homogeneous element \( \psi \in \mathfrak{gr}_1(k) \) of degree \( n \) into \( -n\psi \).
Remarks. 1) \(g_t(k)\) has the filtration whose \(n\)th term is \(\{(0, \psi) \in g_t(k) | \psi \equiv 0 \mod\ deg n\}\). We can use it to construct a complete graded Lie algebra \(\hat{g}_t(k)\). It will be shown (see Proposition 5.6) that \(\hat{g}_t(k) = g_t(k)\). This is the reason for the notations \(g_t, GRT\). It is not hard to prove the inclusion \(\hat{g}_t(k) \subset g_t(k)\): (5.19) follows from the fact that \(\psi(\alpha, \beta) - e^{-\beta} \psi(\alpha, \beta) e^{\beta} + e^{\alpha} \psi(\alpha, \gamma) e^{-\gamma} - \psi(\alpha, \gamma) = 0\). where \((0, \psi) \in g_t(k), e^{\alpha} e^{\beta} e^{\gamma} = 1\). This in turn follows from the analogues fact about \(GT_t(k)\): if \((1, f) \in GT_t(k)\), then

\[
X_1 \cdot f(X_1, X_2)^{-1} X_2 f(X_1, X_2) \cdot f(X_1, X_3)^{-1} X_3 f(X_1, X_3) = \frac{X_1 f(X_2, X_1) X_2 f(X_3, X_2) X_3 f(X_1, X_3)}{f(\bar{X}, X_1) f(X_3, \bar{X}) f(X_1, X_3)} = 1
\]

for \(X_1 X_2 X_3 = 1\), where \(\bar{X} = X_1 X_2 X_3^{-1} = X_3^{-1} X_1 X_2\). However it is not necessary for (5.19) to be verified (see Proposition 5.7).

2) The connection between \(GT_t(k)\) and \(GRT_t(k)\) can also be explained in the following way: if \(\{g_\varepsilon\}\) is a family of elements of \(Fr_k(A, B)\) such that \((1, f_\varepsilon) \in GT_t(k)\) for \(\varepsilon \neq 0\), where \(f_\varepsilon(X, Y) = g_\varepsilon \varepsilon^{1/2} \ln X, \varepsilon^{1/2} \ln Y\), then \(g_\varepsilon \in GRT_t(k)\).

3) \(GRT_t(k)\), as well as \(GRT(k)\), has a categorical interpretation. Let \(C\) be a tensored category, and suppose given automorphisms \(\tau_{V, W} \in \text{Aut}(V \otimes W)\), functorial in \(V, W \in C\), with \(c_{V, W} \tau_{V, W} = \tau_{V, W} c_{V, W}\) and

\[
\ln \tau_{U \otimes V, W} = \text{id}_U \otimes \ln \tau_{V, W} + (c_{U, V}^{-1} \otimes \text{id}_W)(\text{id}_V \otimes \ln \tau_{U, W})(c_{U, V} \otimes \text{id}_W),
\]

where \(c\) is the commutativity isomorphism (of course, one must first have formulated conditions on \(C\) and \(\tau\) sufficient for the latter equality to be meaningful; typical example: \(C\) is the category of \(h\)-adically complete \(U\)-modules, and \(\tau_{V, W}\) is the operator in \(V \otimes W\) corresponding to \(e^{ht} \in U g \otimes U g\), where \(g\) and \(t\) are as in §1). Suppose meaningful all expressions of the form

\[
g(\ln \tau_{U, V} \otimes \text{id}_W, \text{id}_U \otimes \ln \tau_{U, V}, w),
\]

where \(g(A, B) \in Fr_k(A, B)\). Then if \(g \in GRT_t(k)\) and we take \(g(\ln \tau_{U, V} \otimes \text{id}_W, \text{id}_U \otimes \ln \tau_{U, V}, w)\) as a new associativity isomorphism \((U \otimes V) \otimes W \simeq U \otimes (V \otimes W)\) without changing \(c\) and \(\tau\), we obtain a structure of the same type as the original.

The formula \(\bar{\varphi}(A, B) = \varphi(g(A, B) A g(A, B)^{-1}, B) \cdot g(A, B)\), where \(\varphi \in M_t(k)\) and \(g \in GRT_t(k)\), defines a right action of \(GRT_t(k)\) on \(M_t(k)\). This gives \(GRT_t(k)\) a right action on \(M(k) = \{(\mu, \varphi) | \varphi \in M_t(k)\}\). The formulas \(\bar{\varphi}(A, B) = \varphi(c^{-1} A, c^{-1} B) \) and \(\bar{\mu} = c^{-1} \mu\), where \(c \in k^\ast\), define an action of \(k^\ast\) on \(M(k)\). As a result, we obtain a right action of \(GRT(k)\) on \(M(k)\). It commutes with the left action of \(GT(k)\).

Proposition 5.5. The action of \(GRT(k)\) on \(M(k)\) is free and transitive. The same is true for the action of \(GRT_t(k)\) on \(M_t(k)\).

Proof. It suffices to prove the second statement. If \(\varphi, \bar{\varphi} \in M_t(k)\) then there exists exactly one \(g \in Fr_k(A, B)\) such that \(\bar{\varphi}(A, B) = \varphi(g(A, B) A g(A, B)^{-1}, B) \cdot g(A, B)\), namely,

\[
g(A, B) = \chi(\bar{\psi}(A, B) A \bar{\psi}(A, B)^{-1}, B) \cdot \bar{\psi}(A, B),
\]

(5.22) where \(\chi \in Fr_k(A, B)\) is inverse to \(\varphi\) with respect to the operation (5.16), i.e. \(\chi(\psi(A, B) A \psi(A, B)^{-1}, B) \cdot \psi(A, B) = 1\). Arguing as in the proof of
Proposition 5.1, we find that \((0, f) \in G_{II}'(k)\), where \(f(X, Y) = \chi(\ln X, \ln Y)\). Equation (5.22) says that \(g\) is the result of the action of \((0, f)\) on \(\Phi\), and therefore \(g \in M_{0}(k)\), i.e., \(g\) satisfies (5.12), (5.13), and (5.15). We now use the equality
\[
\ln X_{1} + X_{1}^{1/2} f(X_{1}, X_{2})^{-1} \ln X_{2} \cdot f(X_{1}, X_{2}) X_{1}^{-1/2}
+ f(X_{1}, X_{2})^{-1} \ln X_{2} \cdot f(X_{1}, X_{2}) = 0,
\]
where \(X_{1} X_{2} X_{3} = 1\), proved by the substitution (5.4). Finally, making a substitution like (5.4) in (5.23) with \(\phi\) replaced by \(\Phi\), and using (5.22), we obtain (5.14). * 

From Propositions 5.1 and 5.5 follows

PROPOSITION 5.6. Every \(\phi \in M(k)\) determines an isomorphism \(s_{\phi}: \text{GRT}(k) \cong \text{GT}(k)\), which is characterized by the fact that say \(\gamma \in \text{GRT}(k)\) acts on \(\phi\) on the right the same way \(s_{\phi}(\gamma)\) acts on the left. The diagram

\[
\begin{array}{c}
\text{GRT}(k) \\
\downarrow \\
\text{GT}(k)
\end{array}
\]

is commutative, so that \(s_{\phi}(\text{GRT}_{1}(k)) = \text{GT}_{1}(k)\). The splitting of the sequence (5.8) that corresponds to \(\phi \in M_{1}(k)\) is defined by the homomorphism \(s_{\phi} \circ i: k^{*} \rightarrow \text{GT}(k)\), where \(i\) is the canonical embedding \(k^{*} \rightarrow \text{GRT}(k)\). Finally, \(\text{GRT}_{1}(k) = \text{gt}_{1}(k)\), and if \(\phi \in M_{1}(k)\), then \(s_{\phi}\) induces the identity mapping \(\text{gt}_{1}(k) \rightarrow \text{gt}_{1}(k)\).

PROPOSITION 5.7. (5.17), (5.18), and (5.20) imply (5.19).

PROOF. Denote the left-hand side of (5.19) by \(s(B, C)\). Then \(s(B, C) = s(C, B)\). Furthermore,
\[
s(Y_{1}, Y_{2}) = s(Y_{1}, Y_{2} + Y_{3}) + s(Y_{1} + Y_{2}, Y_{3}) - s(Y_{2}, Y_{3}) = 0,
\]
where the \(Y\) are generators of the free Lie algebra. Indeed, denote the left-hand side of (5.24) by \(u(Y_{1}, Y_{2}, Y_{3})\). Then it follows from (5.17) and (5.18) that

\[
u(X^{14}, X^{24}, X^{34}) = [X^{14} + X^{24} + X^{34}, \mu^{1234} - [X^{14} + X^{24}, \mu^{1243}] + [X^{14}, \mu^{1423}]]
\]

where \(\mu^{1234} = \text{left-hand side of (5.20)} - \text{right-hand side of (5.20)}\). Therefore (5.17), (5.18), and (5.20) imply (5.24). It remains to prove that if a symmetric Lie polynomial \(s(B, C)\) satisfies (5.24), then \(s = 0\). It is well known that if \(s(x, y)\) is an ordinary (commutative) polynomial in two sets of variables \(x = (x^{(1)}, \ldots, x^{(n)})\) and \(y = (y^{(1)}, \ldots, y^{(n)})\) such that \(s(y, x) = s(x, y)\) and (5.24) holds, then \(s\) is of the form \(f(x+y) - f(x) - f(y)\). This can be seen (see the proof of Proposition 2.2 of [1]) by representing the space of homogeneous polynomials \(s(x, y)\) of degree \(n\) in the form \(V_{m} \otimes S_{n} W_{m}\), where \(V_{m}\) is the space of polynomials in \(x_{1} = (x_{1}^{(1)}, \ldots, x_{1}^{(n)})\), \(\ldots, x_{m} = (x_{m}^{(1)}, \ldots, x_{m}^{(n)})\), linear in each \(x_{i}\), and \(W_{m}\) is an appropriate \(S_{m}\)-module. The same argument goes through in the Lie case (for \(V_{m}\) we must take the space of all Lie polynomials in \(m\) variables, linear in each variable); but now \(f(x)\) is a Lie polynomial in \(x\), i.e., \(f(x) = cx, c \in k\). Therefore \(s = 0\). *
Put \( \mathfrak{fr}_r(A, B) = \mathfrak{fr}_r(A, B)/I_r \), where \( I_r = \{ u \in \mathfrak{fr}_r(A, B) \mid u \equiv 0 \text{ mod } \deg r \} \). Let \( \mathfrak{Fr}_r(A, B) = \exp \mathfrak{fr}_r(A, B) \), and \( M_r(k) \) be the set of all \( \varphi \in \mathfrak{Fr}_r(A, B) \) satisfying (2.12), (5.3), and (2.13) mod \( \deg r \).

**Proposition 5.8.** The mapping \( M^{(r+1)}_1(k) \to M^{(r)}_1(k) \) is surjective.

**Proof.** Similarly to GRT, we consider the group \( GRT_1^{(r)}(k) \), consisting of all elements \( g \in \mathfrak{Fr}_k(A, B) \) satisfying (5.12)–(5.15) mod \( \deg n \). Similarly to Proposition 5.5 we can prove that \( GRT_1^{(r)}(k) \) acts on \( M^{(r)}_1(k) \) freely and transitively. It remains to prove that the homomorphism \( GRT_1^{(r+1)}(k) \to GRT_1^{(r)}(k) \) is surjective. Since both groups are unipotent and therefore connected, it suffices to prove surjectivity for the homomorphism \( \mathfrak{gr}_1^{(r+1)}(k) \to \mathfrak{gr}_1^{(r)}(k) \). And in fact, from Proposition 5.7 it follows that \( \mathfrak{gr}_1^{(r)}(k) \) is the sum of the homogeneous components of \( \mathfrak{gr}_1(k) \) of degree less than \( r \).

**Remarks.**

1) Any \( \varphi \in M^{(r)}_1(k) \) such that \( \varphi(-A, -B) = \varphi(A, B) \) can be lifted to a \( \tilde{\varphi} \in M^{(r+1)}_1(k) \) such that \( \tilde{\varphi}(-A, -B) = \tilde{\varphi}(A, B) \): it suffices to put \( \tilde{\varphi}(A, B) = (\varphi(A, B) + \tilde{\varphi}(-A, -B))/2 \), where \( \tilde{\varphi} \) is any inverse image of \( \varphi \) in \( M^{(r+1)}_1(k) \).

2) The proof of Proposition 5.8 uses Proposition 5.3. Without using Proposition 5.3, one can show, by standard methods of deformation theory, that the obstruction to the existence, for a given \( \varphi \in M^{(r)}_1(k) \), of an inverse image in \( M^{(r+1)}_1(k) \) belongs to the \( r \)-th component of the 4-th cohomology group of the following complex \( L^* \). Consider first a complex \( L^* \), where \( L^n \) is the algebraic direct sum of the homogeneous components of \( a_n^\varphi \), and the differential in \( L^* \) is such that for any Lie \( k \)-algebra \( g \) and any symmetric invariant \( t \in g \otimes g \) the homomorphisms \( a_n^\varphi \rightarrow (U_g)^{\otimes n} \) taking \( \chi^{ij} \) into \( t^{ij} \) define a morphism from \( L^* \) to the complex \( C^*(g) \) (see (3.7)). \( C^*(g) \) contains the Harrison-Barr subcomplex \( C^*(g) \otimes (\odot_n C^*(g)) \) is the free Lie superalgebra generated by the vector space \( U_g \), whose elements are regarded as odd, while \( \odot_n C^*(g) \) is a free associative algebra. In [23] a projection \( e_n \in \mathbb{Q}[S_n] \) is constructed such that \( L^*(g) = e_n \cdot C^*(g) \); namely, \( e_n = (n!)^{-1} \sum \varepsilon(\sigma) c_{\sigma} \cdot \sigma \), where \( \sigma \in S_n \), \( \varepsilon(\sigma) \) is the sign of \( \sigma \), and \( c_{\sigma} = (-1)^{\sigma_1 n(n-1)-a} \), \( a = \text{Card}\{ k \mid \sigma^{-1}(k) > \sigma^{-1}(k+1) \} \). The desired complex \( L^* \) is defined by the formula \( L^* = e_n \cdot L^n \). The author does not know whether its \( 4 \)-th cohomology group \( H^4 \) is equal to 0. It is easily seen that \( H^2 = L^2 = 0 \) for \( n < 2 \), \( \dim H^2 = \dim L^2 = 1 \), and \( H^3 \) is the algebraic direct sum of the homogeneous components of \( \mathfrak{gr}_1(k) \).

**Proposition 5.9.** (5.12), (5.13), and (5.15) imply (5.14). In other words, \( \text{GRT}_1(k) = M_0(k) \).

**Proof.** It suffices to show that if \( \varphi \in M_0(k) \), \( \varphi \equiv 1 \text{ mod } \deg n \), then the result of acting on \( \varphi \) by some \( g \in \text{GRT}_1(k) \), where \( g \equiv 1 \text{ mod } \deg n \), is congruent to \( 1 \text{ mod } \deg (n+1) \). Indeed, let \( \psi \) be the component of degree \( n \) of the series of \( \varphi \in \text{fr}_k(A, B) \). Then \( \psi \) satisfies (5.17), (5.18), and (5.20), and therefore also (5.19). I.e., \( \psi \in \mathfrak{gr}_1(k) \). We can therefore put \( g = \text{Exp}(-\psi) \), where \( \text{Exp} \) is the exponential mapping \( \mathfrak{gr}_1(k) \to \text{GRT}_1(k) \) corresponding to the operation (5.16).
REMARKS 1) With the aid of Proposition 5.9 or its method of proof, it is easy to obtain a proof of Proposition 5.5 simpler than the one above, but using Proposition 5.7.

2) Here is an outline of another proof of Proposition 5.2. Denote by $\text{Spl}(k)$ the set of homomorphisms $k \to \mathfrak{gl}(k)$ that split (5.8). Put $\text{GT}_0(k) = \{ (\lambda, f) \in \mathfrak{gl}(k) : \lambda = 0 \}$ and $\text{GT}'_0(k) = \{ (0, f) \in \text{GT}_0(k) \mid f \text{ satisfies (5.23)} \}$. In the process of proving Proposition 5.5 we constructed a mapping $M^*(k) \to \text{GT}'_0(k)$. It is easily shown to be bijective. On the other hand, an element of $\text{Spl}(k)$, or, what is the same, an element of $\mathfrak{gl}(k)$ of the form $(1, \psi)$, determines a 1-parameter subgroup $\gamma: k^* \to \text{GT}(k)$. A priori, $\gamma$ is a formal mapping (i.e., $\gamma(\lambda)$ is expressed in terms of formal series in $\lambda - 1$), but in fact $\gamma$ is regular and, furthermore, extends to a regular (i.e., polynomial) mapping $\gamma: k^* \to \text{GT}(k)$. This follows from the fact that $\gamma(\lambda) = (\lambda, f_\lambda)$, where

$$\lambda \frac{d}{d\lambda} f_\lambda(X, Y) = \psi(\lambda f_\lambda(X, Y) \cdot \ln X \cdot f_\lambda(X, Y)^{-1}, \lambda \ln Y) \cdot f_\lambda(X, Y).$$

Put $f = f_0$. Then $(0, f) \in \text{GT}'_0(k)$. Indeed, since $(\lambda, f_\lambda) \in \text{GT}(k)$ and $(-1, 1) \in \text{GT}(k)$, we have $(-\lambda, f_\lambda) = (-1, 1) \cdot (\lambda, f_\lambda) \in \mathfrak{gl}(k)$, and to prove (5.23) it suffices to subtract from equality (4.4) for $(\lambda, f_\lambda)$ equality (4.4) for $(-\lambda, f_\lambda)$, divide by $\lambda$ and let $\lambda$ approach 0. The composite mapping $\text{Spl}(k) \to \text{GT}'_0(k) \to M^*_1(k)$ is inverse to the mapping $M^*_1(k) \to \text{Spl}(k)$ involved in Proposition 5.2.

3) In fact, $\text{GT}'_0(k) = \text{GT}'_0(k)$. Indeed, choose $\varphi \in M^*_1(k)$, and let $g$ be the result of acting by $(0, f) \in \text{GT}'_0(k)$ on $\varphi$. Then $g \in M^*_0(k)$. Therefore $g \in \text{GRT}_1(k)$ (see Proposition 5.9). If $\widehat{\varphi}$ is the result of the right action of $g^{-1}$ on $\varphi$, then the result of the left action of $(0, f)$ on $\widehat{\varphi}$ is 1, i.e., $(0, f)$ is the image of $\varphi$ under the canonical mapping $M^*_1(k) \to \text{GT}'_0(k)$.

4) Here is another proof of Theorem B. Take a fixed $\varphi \in M^*_1(k)$, and let $(0, f)$ be the corresponding element in $\text{GT}'_0(k)$. Let $(A, \Delta, \varepsilon, \Phi, R)$ be a quasitriangular quasi-Hopf QUE-algebra over $k[[h]]$. Operating by the element $(0, f) \in \text{GT}'_0(k)$ on $(A, \Delta, \varepsilon, \Phi, R)$ (see (4.12)), we obtain a triangular quasi-Hopf QUE-algebra $(A, \Delta, \varepsilon, \Phi, \overline{R})$ (triangularity is quasitriangularity plus the equality $R^{21} = R^{-1}$). By Propositions 3.6 and 3.7 of [1], a suitably chosen twist makes $\overline{R} = 1$ and $\Phi = 1$, and then $(A, \Delta, \varepsilon)$ is the universal envelope of some deformation Lie algebra $g$ over $k[[h]]$. In this situation we put $t = 2h^{-1}$. In $R$ and show that $t$ is a symmetric $g$-invariant element of $g \otimes g$, while $\Phi = \varphi(ht^{12}, ht^{23})$. Since $\overline{R} = 1$, we have $R^{21} = R$, i.e., $t^{21} = 1$. From (1.5) we have that $t$ is $g$-invariant. Substituting $X_1 = (\Delta \otimes \text{id})(R^{21} R)^{-1}$, $X_2 = (R^{21})^{-1} (\Phi^{213})^{-1} R^{21} R^{13} \Phi^{21} R^{12}$, and $X_3 = \Phi^{-1} R^{23} \Phi^{213} R^{12}$ into (5.23), and using the fact that $X_1^{-1} \cdot R^{21} R^{12}$ commutes with $X_1, X_2, X_3$, we find that

$$(\Delta \otimes \text{id})(\ln(R^{21} R)) = \Phi^{-1} \cdot \ln(R^{12} R^{23}) \cdot \Phi + (R^{21})^{-1} (\Phi^{213})^{-1} \cdot \ln(R^{21} R^{13}) \cdot \Phi^{213} R^{12},$$

i.e., $(\Delta \otimes \text{id})(t) = t^{13} + t^{23}$. Therefore, $t \in g \otimes g$. Finally, we have $\varphi(\chi(A, B) A \chi(A, B)^{-1}, B) \cdot \chi(A, B) = 1$, where $\chi(A, B) = f(e^4, e^8)$ (see the proof of Proposition 5.5). Putting $A = h \cdot \Phi t^{12} \Phi^{-1}$ and $B = ht^{23}$, we obtain $\varphi(h \cdot \Phi t^{12} \Phi^{-1}, ht^{23}) \cdot \Phi t^{12} \Phi^{-1} = 1$, i.e., $\Phi = \varphi(ht^{12}, ht^{23})$. 

§6. On the algebra $\text{grt}_1(k)$

We recall that by $\text{fr}_k(A, B)$ is meant the set of Lie formal series $\psi(A, B)$ with coefficients in $k$, and by $\text{grt}_1(k)$ the set of all $\psi \in \text{fr}_k(A, B)$ that satisfy (5.17)-(5.20). By Proposition 5.7, equalities (5.17), (5.18), and (5.20) imply (5.19). Furthermore, (5.17) and (5.19) imply (5.18): indeed, from (5.17) and (5.19) one easily derives that the left-hand side of (5.18) commutes with $A$ and $B$. Now, $\text{grt}_1(k)$ is a Lie algebra with commutator (5.21). The set of all $\psi \in \text{fr}_k(A, B)$ that satisfy (5.17), (5.19), and therefore (5.18) also forms a Lie algebra with commutator (5.21). This algebra we name $\text{Il}_1(k)$, in honor of Ihara. Both algebras $\text{grt}_1(k)$ and $\text{Il}_1(k)$ are graded: $\text{grt}_1(k) = \bigoplus_n \text{grt}_1^n(k)$ and $\text{Il}_1(k) = \bigoplus_n \text{Il}_1^n(k)$, where $\bigoplus$ means complete direct sum. Since $\text{Il}_1^1(k)$ is generated by the central element $A - B$, the study of $\text{Il}_1(k)$ reduces to the study of the subalgebra $\text{Il}_1^1(k) = \bigoplus_{n \geq 1} \text{Il}_1^n(k)$. We note that $\text{grt}_1(k) \subset \text{Il}_1(k)$ (it suffices to substitute $X^{12} = A$ and $X^{13} = X^{14} = X^{23} = X^{34} = 0$ into (5.20)).

In [13] and [14], Ihara uses the following realization of $\text{Il}_1(k)$. He calls a continuous derivation $\partial: \text{fr}_k(A, B) \to \text{fr}_k(A, B)$ special if $\partial(A) = [R, A]$, $\partial(B) = [R, B]$, and $\partial(C) = [R, C]$ for some $R_1, R_2, R_3 \in \text{fr}_k(A, B)$, where $C = -A - B$. The special derivations form a Lie algebra $S\text{Der} \text{fr}_k(A, B)$. Consider $\text{fr}_k(A, B)$, the action of the group $S_3$ that permutes $A, B, C$. It induces an action of $S_3$ on $S\text{Der} \text{fr}_k(A, B)$ and on the set of inner derivations $\text{Int} \text{fr}_k(A, B)$. It can be shown that the subalgebra of $S_3$-invariants of the algebra $S\text{Der} \text{fr}_k(A, B)/\text{Int} \text{fr}_k(A, B)$ is canonically isomorphic to $\text{Il}_1(k)$: an element $\psi \in \text{Il}_1(k)$ corresponds to the class of the derivation $\partial_\psi: \text{fr}_k(A, B) \to \text{fr}_k(A, B)$ given by $\partial_\psi(A) = 0$ and $\partial_\psi(B) = [\psi, B]$. Indeed, we can identify $S\text{Der} \text{fr}_k(A, B)/\text{Int} \text{fr}_k(A, B)$ with the algebra of derivations $\partial: \text{fr}_k(A, B) \to \text{fr}_k(A, B)$ such that $\partial(A) = 0$, $\partial(B) = [\psi, B]$, and $\partial(C) = [\chi, C]$ for some $\psi, \chi \in \text{fr}_k(A, B)$ and $\partial(B) \equiv 0 \mod 3$. Such a $\partial$ is determined by specifying $\psi, \chi \in \text{fr}_k(A, B)$ such that $[\psi(A, B), B] + [\chi(A, B), C] = 0$, $\psi \equiv 0 \mod 2$, $\chi \equiv 0 \mod 2$. Invariance of $\partial$ with respect to permutation of $B$ and $C$ means that $C(A, B) = \psi(A, C)$. Invariance of $\partial$ modulo $\text{Int} \text{fr}_k(A, B)$ with respect to permutation of $A$ and $B$ means that $\psi(B, A) = -\psi(A, B)$. Finally, $\partial_\psi(\psi_1, \psi_2) = [\partial_\psi, [\psi_1, \psi_2]]$: indeed, in (5.21) $D_\psi = \text{ad} \psi - \partial_\psi$, and therefore $\partial_\psi(\psi_1, \psi_2) = \partial_\psi(\psi_2) - \partial_\psi(\psi_1) - [\psi_1, \psi_2]$.

Remark. If from the right action (4.13) of the group $\text{G}_1(k)$ on the complete free group with generators $\sigma^2_1$ and $\sigma^2_2$ we construct in the usual fashion a left action, and then pass from groups to Lie algebras and from filtered algebras to graded, we obtain the action of $\text{grt}_1(k)$ on $\text{fr}_k(A, B)$ given by the formula $\psi \cdot \varphi = [\varphi, \psi]$.

We pass now to a “hamiltonian” interpretation of $\text{Il}_1(k)$. For any Lie algebra $\mathfrak{g}$ we denote by $\mathcal{F}(\mathfrak{g})$ the quotient of $\mathfrak{g} \times \mathfrak{g}$ by the subspace generated by elements of the form $[x, y] \times x$ and $[x, y] \times z - x \times [y, z]$, where $x, y, z \in \mathfrak{g}$. The image of $x \times y$ in $\mathcal{F}(\mathfrak{g})$ we denote by $(x, y)$. The equalities $\langle x, y \rangle = [x, y]$ and $[x, y] = x \times y - y \times x$ allow us to regard $(x, y)$ as an invariant scalar product with values in $\mathcal{F}(\mathfrak{g})$ (any $k$-valued invariant scalar product in $\mathfrak{g}$ is obtained from this by composition with some linear functional $\mathcal{F}(\mathfrak{g}) \to k$).

If $\mathfrak{g}$ is a free Lie algebra with generators $Y_1, \ldots, Y_m$, then instead of $\mathcal{F}(\mathfrak{g})$ we shall write $\mathcal{F}(Y_1, \ldots, Y_m)$. An element $f \in \mathcal{F}(\mathfrak{g}, B)$ can be regarded as a formula defining for every metricized Lie algebra $\mathfrak{g}$ (i.e., finite-dimensional Lie
algebra with a nondegenerate invariant scalar product) a function $f_g: g \times g \to k$.

For example, $f = ([A, B], [A, B]) \in \mathcal{F}(A, B)$ defines the function $f_g(x, y) = ([x, y], [x, y])$. It is easily shown that if $f \neq 0$, then $f_g \neq 0$ for some metrized Lie algebra $g$ (for we can take $gl(n)$, where $n$ is sufficiently large). If $g$ is a metrized Lie algebra, then $g \cong g$ identifies with $g^* \times g^*$, and consequently the space of functions on $g \times g$ has a natural Poisson bracket (the “Kirillov bracket”). If $f, \varphi \in \mathcal{F}(A, B)$, then $(f_g, \varphi_g) = \psi_g$ for some $\psi \in \mathcal{F}(A, B)$ independent of $g$, which we denote by $\{f, \varphi\}$. Thus, $\mathcal{F}(A, B)$ is a Lie algebra with respect to this Poisson bracket. The action described above of $S_3$ on $\mathfrak{fr}_k(A, B)$ induces an action of $S_3$ on $\mathcal{F}(A, B)$.

**Proposition 6.1.** 1) The action of $S_3$ on $\mathcal{F}(A, B)$ preserves the Poisson bracket.

2) The subalgebra of $S_3$-invariants of the algebra $\mathcal{F}(A, B)$ is isomorphic to $\bigoplus_n \text{In}_n(k)$, where $\bigoplus$ is the algebraic direct sum.

**Proof.** 1) It suffices to show that for any Lie algebra $g$ the action of $S_3$ on the Poisson algebra of $g$-invariant functions on $g^* \times g^*$ obtained by identifying $g^* \times g^*$ with $\{\lambda_1, \lambda_2, \lambda_3\} \in g^* \times g^* \times g^* | \lambda_1 + \lambda_2 + \lambda_3 = 0\}$ via the projection $(\lambda_1, \lambda_2, \lambda_3) \mapsto (\lambda_1, \lambda_2)$ preserves the Poisson bracket. This follows from the fact that Poisson algebra in question can be represented as the quotient of the Poisson algebra of $g$-invariant functions on $g^* \times g^* \times g^*$ by the ideal of functions that equal 0 when $\lambda_1 + \lambda_2 + \lambda_3 = 0$ (that this is Poisson is known from hamiltonian reduction theory).

2) If $f \in \mathcal{F}(Y_1, \ldots, Y_m)$, we denote by $\partial f / \partial Y_i$ the Lie polynomial in $Y_1, \ldots, Y_m$ such that the part of $f(Y_1, \ldots, Y_{i-1}, Y_i + Z, Y_{i+1}, \ldots, Y_m)$ linear in $Z$ is equal to $\partial f / \partial Y_i, Z$. From the $g$-invariance of $f_g$ for any metrized Lie algebra $g$ it follows that $\sum_{i=1}^m [Y_i, \partial f / \partial Y_i] = 0$.

**Lemma.** If $\sum_{i=1}^m [Y_i, P_i] = 0$, where the $P_i$ are Lie polynomials in $Y_1, \ldots, Y_m$, then there exists exactly one $f \in \mathcal{F}(Y_1, \ldots, Y_m)$ such that $\partial f / \partial Y_i = P_i$ for all $i$.

**Proof.** The usual connection between polynomials and symmetric multilinear functions allows us to restrict ourselves to the case that $P_i$ does not contain $Y_i$, while $P_1, \ldots, P_m$ and $f$ are linear in $Y_1$. In this case, if $f$ exists, then $f = (Y_1, P_1)$. Conversely, if $f = (Y_1, P_1)$, then $\partial f / \partial Y_i = P_i$ for all $i$. Indeed, put $Q_i = P_i - \partial f / \partial Y_i$. Then $Q_i = 0$ and $\sum [Y_i, Q_i] = 0$. For $i > 1$ write $Q_i$ in the form $R_i (\text{ad} Y_2, \ldots, \text{ad} Y_m) Y_i$, where $R_i$ is an associative polynomial. Then $\sum_{i=2}^m u_i R_i (u_2, \ldots, u_m) = 0$, and therefore $R_2 = \ldots = R_m = 0$.

Suppose $\psi \in \bigoplus_n \text{In}_n(k)$. It follows from the lemma that there exists a unique $f \in \mathcal{F}(A, B)$ such that $\partial f / \partial A = \psi (A, -A-B)$ and $\partial f / \partial B = \psi (B, -A-B)$.

Clearly, $f(B, A) = f(A, B)$. Furthermore, $f(A, B) = f(-A - B, B)$ (both sides of this equality have the same partial derivatives). This implies that $f$ is $S_3$-invariant. Conversely, if $f \in \mathcal{F}(A, B)$ is invariant with respect to $S_3$, then, defining $\psi (A, B)$ from the relation $\psi (A, -A - B) = \partial f / \partial A$, we find that $\psi \in \text{In}(k)$.

To prove that the Poisson bracket in $\mathcal{F}(A, B)$ corresponds to the commutator in $\text{In}(k)$, we use the imbedding $\text{In}(k) \to \text{Der} \mathfrak{fr}_k(A, B)$ taking $\psi$ into
\[ \delta = \sigma \partial_{\psi} \sigma, \text{ where } \partial_{\psi} \in \text{Der} \mathfrak{fr}_k(A, B) \text{ is as before and } \sigma \text{ is the automorphism of } \mathfrak{fr}_k(A, B) \text{ given by } \sigma(A) = -A - B \text{ and } \sigma(B) = B. \text{ We have } \delta_{\psi}(A) = [\psi(-A - B, A), A] \text{ and } \delta_{\psi}(B) = [\psi(-A - B, B), B]. \text{ If } \psi \text{ corresponds to } f \in \mathcal{F}(A, B), \text{ then } \delta_{\psi}(A) = [A, \partial f/\partial A] \text{ and } \delta_{\psi}(B) = [B, \partial f/\partial B]. \text{ These formulas can be regarded as the Hamilton equation corresponding to } f. \text{ It remains to use the connection between the Poisson bracket of Hamiltonians and the commutator of the corresponding vector fields.} \]

**Remarks.** 1) The element \( f \in \mathcal{F}(A, B) \) that corresponds to \( \psi \in \mathfrak{gt}_1^n(k) \subset \text{Lh}(k) \) (see the proof of Proposition 6.1) can be given the following interpretation. Suppose \( \varphi \in M_1(k) \), and \( \tilde{\varphi} \) is obtained from \( \varphi \) by the action of \( \text{Exp}(\varphi) \), where \( \text{Exp} \) is the exponential mapping \( \mathfrak{gt}_1^n(k) \to \text{GRT}_1^n(k) \). If \( g \) is a metrized Lie algebra over \( k \), and \( \iota \in g \otimes g \) corresponds to the scalar product in \( g \), then \( \Phi = \varphi(h_{12}, h_{21}) \) and \( \tilde{\Phi} = \tilde{\varphi}(h_{12}, h_{21}) \) are connected by the transformation (1.11) for some \( F \in (U_k \otimes U_k)[[h]] \) (see Theorem A). It is easily shown that \( F \) can be chosen so that 1) \( F \equiv 1 \mod h^n \), 2) \( h^{-n}(F - 1) \mod h \in L_{n+1} \), where \( L_{n+1} \) is the set of elements of \( U_k \otimes U_k \) that are polynomials of degree no higher than \( n + 1 \) in elements of \( g \otimes 1 \) and \( 1 \otimes g \), and 3) the image of \( h^{-n}(F - 1) \mod h \) in \( L_{n+1}/L_n = \text{Sym}^{n+1}(g \otimes g) - \text{Sym}^{n+1}(g^* \otimes g^*) \), regarded as a function on \( g \times g \), is equal to \( -f \).

2) Deligne has noted that, arguing as in the proof of Proposition 6.1, one can obtain for any \( n \) an \( S_n \)-equivariant isomorphism between the quotient of the algebra of special derivations of \( \mathfrak{fr}_k(A_1, \ldots, A_n) \) by the ideal of inner derivations and the quotient of \( \mathcal{F}(A_1, \ldots, A_n) \) by the subspace generated by the elements \( (A_1, A_i), 1 \leq i \leq n + 1, \) where \( A_{n+1} = -A_1 - \cdots - A_n \). Namely, the element \( f \in \mathfrak{fr}_k(A_1, \ldots, A_n) \) corresponds to the derivation \( A_1 \to [A_1, \partial f/\partial A_i], 1 \leq i \leq n \).

**Proposition 6.2** (Deligne-Ihara [13]). \( \text{dim } \text{Lh}^n(k) = \alpha_n - \beta_{n+1}, \) where

\[
\alpha_n = (3n)^{-1} \left\{ \sum_{d \mid n} (1 - a(d/3)) \mu(d)2^{n/d} - e_n \right\},
\]

\[
\beta_n = (6n)^{-1} \left\{ \sum_{d \mid n} (1 + 3a(d/2) + 2a(d/3)) \mu(d)2^{n/d} + e_n \right\};
\]

\( \mu \) is the Mobius function, \( a(x) = 1 \) for \( x \in \mathbb{Z}, \ a(x) = 0 \) for \( x \notin \mathbb{Z}, \ e_n = -1 \) if \( n \) is of the form \( 3^m, \ e_n = 2 \) if \( n = 2 \cdot 3^m, \) and \( e_n = 0 \) otherwise.

**Proof.** Let \( V \) be a 2-dimensional vector space with basis \( A, B \). On \( V \) there is an action of \( S_3 \), permuting \( A, B, \) and \( C = -A - B \). Let \( L_n(V) \) be the homogeneous component of degree \( n \) of the free Lie algebra generated by \( V \), i.e., \( L_n(V) = \mathfrak{fr}_k^n(A, B) \). The formula \( \psi \to A \otimes \psi(-A - B, A) + B \otimes \psi(-A - B, B) \) defines an isomorphism \( \text{Lh}^n(k) \cong (V \otimes L_n(V))^S_3 \cap \ker f \), where \( f \) is the commutator mapping \( V \otimes L_n(V) \to L_{n+1}(V) \). Since \( f \) is surjective, we have \( \dim \text{Lh}^n(k) = \dim(V \otimes L_n(V))^S_3 = \dim(L_{n+1}(V))^S_3 \). Now use the formula for the character of the representation of \( \text{GRT}_n(V) \) in \( L_n(V) \) [16], Chapter II, §3, formula (16)].

Here are the values of the numbers \( \alpha_n = \dim \text{Lh}^n(k) \) for \( n \leq 13 \): \( a_1 = a_2 = a_4 = a_6 = 0, a_3 = a_5 = a_8 = 1, a_7 = a_{10} = 2, a_9 = 4, a_{11} = 9, a_{12} = 7, a_{13} = 21 \). A basis in \( \oplus_{n \leq 7} \text{Lh}^n(k) \) is formed by the elements of \( \text{Lh}(k) \).
corresponding (see Proposition 6.1) to the elements $f_1, f_2, f_3, f_4 \in \mathcal{T}(A, B)$, where
\[
f_1 = ([A, B], [A, B]), \tag{6.1}
\]
\[
f_2 = (x, x) + (x, y) + (y, y), \quad \text{where } x = [A, [A, B]], \quad y = [B, [A, B]], \tag{6.2}
\]
\[
f_3 = (z, z), \quad \text{where } z = [A, [A, [A, B]]] + [A, [B, [A, B]]] + [B, [B, [A, B]]], \tag{6.3}
\]
\[
f_4 = ([A, u], [B, u], u), \quad \text{where } u = [A, B]. \tag{6.4}
\]
In the process of proving Proposition 1 of [14], Ihara obtained the following result.

**Proposition 6.3.** For any odd $n \geq 3$ there exists a $\psi \in \text{gr}_1^n(k)$ such that
\[
\psi(A, B) \equiv \sum_{m=1}^{n-1} \binom{n}{m} (\text{ad } A)^{m-1}(\text{ad } B)^{n-m-1}[A, B] \mod [p_k, p_k],
\]
where $p_k$ is the commutant of $\tau_k(A, B)$.

Ihara's proof uses $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Here is another proof. We can assume that $k = \mathbb{C}$. Put $\varphi_{KZ}(A, B) = \varphi_{KZ}(-A, -B)$. By Proposition 5.5, $\varphi_{KZ}$ is obtained from $\varphi_{KZ}$ by the action of some $g \in \text{GRT}_1(\mathbb{C})$. Let $\tilde{\psi}$ be the homogeneous component of degree $n$ of the image of $g$ under the logarithmic mapping $\text{GRT}_1(\mathbb{C}) \to \text{gr}_1^n(\mathbb{C})$. From (2.15) it is easily found that $(n(2\pi i)^n/2\zeta(n)) \cdot \tilde{\psi}$ is the element desired. ⋄

It is not hard to show that if $\psi_1, \psi_2 \in p_k$, then the right-hand side of (5.21) belongs to $[p_k, p_k]$. It follows therefore from Proposition 6.3 that $\text{gr}_1^n(k)$ has at least one generator of degree $n$ for every odd $n \geq 3$.

**Questions.** Is it true that $\text{gr}_1^n(k)$ has exactly one generator of degree $n$ for every odd $n \geq 3$ and no generators of other degrees? Is the algebra $\bigoplus_n \text{gr}_1^n(k)$ free?

**Remarks.** 1) An affirmative answer to the first question is equivalent to the conjunction of Deligne's conjecture in the Introduction of [14] and the density conjecture for the Zariski image of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\text{GT}(\mathbb{Q})$.

2) For $n = 1, 2, 4, 6$ we have $\text{gr}_1^n(k) = \text{Ih}(k) = 0$. Since $\dim \text{Ih}^3(k) = \dim \text{Ih}^5(k) = 1$, it follows from Proposition 6.3 that $\text{gr}_1^n(k) = \text{Ih}^n(k)$ for $n = 3, 5$. Since $\dim \text{Ih}^5(k) = 1$, and $[\text{Ih}^3(k), \text{Ih}^5(k)] \neq 0$ (see [14]), we have $\text{gr}_1^8(k) = \text{Ih}^8(k) = \{\text{gr}_1^3(k), \text{gr}_1^5(k)\}$. It can be shown that $\dim \text{gr}_1^7(k) = 1 < \dim \text{Ih}^7(k)$ and $\text{gr}_1^7(k)$ is generated by the element corresponding to $8f_2 - f_4 \in \mathcal{T}(A, B)$, where $f_2$ and $f_4$ are determined by formulas (6.3) and (6.4).

**Bibliography**


Physico-Technical Institute of Low Temperatures, Academy of Sciences of the Ukrainian SSR

Khar’kov

Received 12/DEC/89

Translated by J. A. ZILBER