alg-geom/9607008

CONJUGACY CLASSES IN LOOP GROUPS AND G-BUNDLES ON ELLIPTIC CURVES

VLADIMIR BARANOVSKY AND VICTOR GINZBURG

1. Introduction

Let $\mathbb{C}[[z]]$ be the ring of formal power series and $\mathbb{C}((z))$ the field of formal Laurent power series, the field of fractions of $\mathbb{C}[[z]]$. Given an algebraic group G over $\mathbb{Z}$, we will write $G((z))$ for the group of $\mathbb{C}((z))$-rational points of G, thought of as a formal "loop group", and $a(z)$ for an element of $G((z))$. Let q be a fixed non-zero complex number. Define a "gauge-action" of $G((z))$ on itself by the formula

$$g(z) : a(z) \mapsto {}^g a = g(q \cdot z)^{-1} \cdot a(z) \cdot g(z) \tag{1.1}$$

We are concerned with the problem of classifying the orbits of the gauge-action on $G((z))$. If $q = 1$ the gauge action becomes the conjugation action and the problem reduces to the classification of conjugacy classes in $G((z))$.

In this paper we will be interested in the case $|q| < 1$. Let $G[[z]] \subset G((z))$ be the subgroup of $\mathbb{C}[[z]]$-points of G. Call an element of $G((z))$ *integral* if it is conjugate to an element of $G[[z]]$ under the gauge-action.

Introduce the elleptic curve $\mathcal{E} = \mathbb{C}^*/q^{\mathbb{Z}}$. Our main result is the following

THEOREM 1.2. *Let G be a connected split semisimple group over $\mathbb{Z}$. Then there is a natural bijection between the set of the gauge-conjugacy classes in $G((z))$ consisting of integral elements and the set of isomorphism classes of semi-stable holomorphic principal G-bundles on $\mathcal{E}$.*

We also have an analogous result for $G = GL_n$, although it is not a semisimple group:

THEOREM 1.2′. *There is a natural bijection between the set of the gauge-conjugacy classes in $GL_n((z))$ consisting of integral elements and the set of isomorphism classes of degree zero semi-stable holomorphic rank n vector bundles on $\mathcal{E}$.*

The main reason we are interested in the above results is that gauge-conjugacy classes in $G((z))$ may be interpreted as ordinary conjugacy classes

in a larger group. Specifically, the group $\mathbb{C}^*$ acts on $\mathbb{C}((z))$ by field automorphisms rescaling the variable z, i.e., $t \in \mathbb{C}^*$ acts by $a(z) \mapsto a(t \cdot z)$. This gives a $\mathbb{C}^*$-action on the group $G((z))$ called "*rotation of the loop*". Write $\mathbb{C}^* \ltimes G((z))$ for the corresponding semidirect product. It is easy to see that, for any $q \in \mathbb{C}^*$, conjugating an element $(q, a(z)) \in \mathbb{C}^* \ltimes G((z))$ does not affect the first coordinate q. Furthermore, for a fixed q, the second projection $(q, a(z)) \mapsto a(z)$ gives a bijection between ordinary conjugacy classes in $\mathbb{C}^* \ltimes G((z))$ with first coordinate q and gauge-conjugacy classes in $G((z))$. We note further that the group $\mathbb{C}^* \ltimes G((z))$ is the quotient of an affine Kac-Moody group modulo its center (since we do *not* take central extension of $G((z))$). Thus, gauge-conjugacy classes in $G((z))$ is essentially the same thing as ordinary conjugacy classes in a Kac-Moody group.

We arrived at theorem 1.2 while trying to find an algebraic version of the following unpublished analytic result due to Looijenga (cf. [EFK]). Let G be a complex Lie group, $G(\mathbb{C}^*)_{hol}$ the group of all holomorphic maps $a : \mathbb{C}^* \mapsto G$, and let q be a fixed non-zero complex number such that $|q| < 1$. Then Looijenga showed that

PROPOSITION 1.3. *There is a natural bijection between the set of all gauge-congugacy classes in $G(\mathbb{C}^*)_{hol}$ and the set of isomorphism classes of arbitrary holomorphic G-bundles on $\mathcal{E}$.*

PROOF. Observe that the pull-back via the projection $\pi : \mathbb{C}^* \to \mathbb{C}^*/q^{\mathbb{Z}} = \mathcal{E}$ establishes an equivalence between the category of G-bundles on $\mathcal{E}$ and the category of $q^{\mathbb{Z}}$-equivariant holomorphic G-bundles on $\mathbb{C}^*$. We associate to $a \in G(\mathbb{C}^*)_{hol}$ the trivial holomorphic G-bundle $\mathbb{C}^* \times G \to \mathbb{C}^*$ on $\mathbb{C}^*$ with $q^{\mathbb{Z}}$-equivariant structure given by the action $q : (z, g) \mapsto (q \cdot z, a(z) \cdot g)$. The corresponding G-bundle on $\mathcal{E}$ will be referred to as the G-bundle with multiplier a. It is easy to see that two G-bundles on $\mathcal{E}$ associated to two different multipliers are isomorphic if and only if the multipliers are gauge-conjugate. Conversely, it is known that any holomorphic G-bundle on $\mathbb{C}^*$ is trivial. The action of the element q on such a trivial bundle has to be of the form $q : (z, g) \mapsto (q \cdot z, a(z) \cdot g)$, where $a : \mathbb{C}^* \to G$ is a holomorphic map (changing trivialization has the effect of replacing a by a gauge-conjugate map). Hence, every $q^{\mathbb{Z}}$-equivariant holomorphic G-bundle on $\mathbb{C}^*$ can be obtained via the above construction. $\square$

Although motivation for theorem 1.2 came from loop groups, the result itself is most adequately understood in the framework of q-difference equations. To explain this assume, for simplicity, that $G = GL_n$, see theorem

1.2′. Given $q \in \mathbb{C}^*$ and $a(z) \in GL_n((z))$, we consider a difference equations

$$x(q \cdot z) = a(z) \cdot x(z)\,, \tag{1.4}$$

where $x(z) \in \mathbb{C}^n((z))$ is the unknown $\mathbb{C}^n$-valued formal power series. It is clear that if $x(z)$ is a solution to (1.4) and $g(z) \in GL_n((z))$, then $\tilde{x}(z) := g(z)x(z) \in \mathbb{C}^n((z))$ is a solution to a similar equation with $a(z)$ being replaced by $\tilde{a}(z) = g(q \cdot z) \cdot a(z) \cdot g(z)^{-1}$, a gauge-conjugate loop. Therefore classification of equations (1.4) modulo transformations $x(z) \mapsto \tilde{x}(z)$ reduces to the classification of the gauge-cojugacy classes in $GL_n((z))$.

Equation (1.4) should be regarded as a q-analogue of the first order differential equation

$$z\frac{dx}{dz} = a(z) \cdot x(z)\,, \tag{1.5}$$

and gauge-conjugation (1.1) should be regarded as a q-analogue of the gauge transformation: $a(z) \mapsto g(z) \cdot a(z) \cdot g(z)^{-1} + z\frac{dg}{dz}g(z)^{-1}$. It is well-known that the classification of gauge equivalence classes of equations like (1.5) depends in an essential way on the type of functions a and g one is considering. If one puts himself into analytic framework, then a and g are taken to be elements of $\mathfrak{gl}_n(\mathbb{C}^*)_{hol}$ and $GL_n(\mathbb{C}^*)_{hol}$, respectively. It is well-known and easy to prove that in this case the differential equation is completely determined (up to equivalence) by the monodromy of its fundamental solution. Thus, there is a natural bijection between the set of equivalence classes of differential equations of type (1.5) and the set of conjugacy classes in G. This is a differential equation analogue of proposition 1.3.

The situation changes drastically if $\mathfrak{gl}_n(\mathbb{C}^*)_{hol}$ and $GL_n(\mathbb{C}^*)_{hol}$ are replaced by formal loops $\mathfrak{gl}_n((z))$ and $GL_n((z))$, respectively. The classical theory says that for the equation to be determined by its monodromy it should have *regular singularity* at $z = 0$. This is a differential analogue of the "integrality" condition in theorem 1.2′. Thus, the G-bundle in theorems 1.2 should be thought of as a q-analogue of the monodromy of a differential equation.

ACKNOWLEDGEMENTS. We are greatful to R. Bezrukavnikov for helpful discussions.

2. From loop groups to G-bundles on $\mathcal{E}$.

The ring homomorphism $\mathbb{C}[[z]] \to \mathbb{C}$, $f \mapsto f(0)$ induces, for any algebraic group H, a natural group homomorphism $H[[z]] \to H$. Let $H_1[[z]]$

denote the kernel of this homomorphism, a "congruence subgroup". We use the notation $H[z]$ and $H[z, z^{-1}]$ for the groups of $\mathbb{C}[z]$- and $\mathbb{C}[z, z^{-1}]$-points of H, respectively. Thus, $H[z] \subset H[[z]]$ and $H[z, z^{-1}] \subset H((z))$. Elements of $H[z, z^{-1}]$ will be referred to as *polynomial* loops.

From now on we fix a split connected semisimple group G over $\mathbb{Z}$ and $q \in \mathbb{C}^*$ such that $|q| < 1$. Abusing the notation, we write G for the corresponding complex group, and let $\mathfrak{g}$ denote its Lie algebra.

Our proof of theorem 1.2 consists of several steps. We first assign a G-bundle on $\mathcal{E}$ to an integral element $a \in G((z))$. The naive idea of using a as a multiplier (cf. proof of proposition 1.3) can not be applied here directly, for a is only a *formal* looop, hence, does not give a holomorphic map in general. To overcome this difficulty, we prove the following result.

PROPOSITION 2.1. *For any integral $a \in G((z))$, there exists a Borel subgroup $B \subset G$ with unipotent radical U, such that a is gauge-conjugate to a polynomial loop of the form $a_0 \cdot a_1(z)$ where $a_0 \in B$ and $a_1 \in U[z]$.*

To prove the proposition we need some preparations. Recall that for a semisimple element $s \in G$, the adjoint action of s on $\mathfrak{g}$ has a weight space decomposition $\mathfrak{g} = \bigoplus_\lambda \mathfrak{g}_\lambda$ where $\mathfrak{g}_\lambda$ is the eigenspace corresponding to an eigenvalue $\lambda \in \mathbb{C}^*$.

Let $a(z) = a_0 \cdot a_1(z) \in G[[z]]$, where $a_0 \in G$ is a constant loop and $a_1(z) \in G_1[[z]]$. Write $a_0^{ss} \in G$ for the the semisimple part in the Jordan decomposition of a_0, and let $\mathfrak{g} = \bigoplus_\lambda \mathfrak{g}_\lambda$ be the weight space decomposition with respect to the adjoint action of a_0^{ss}.

DEFINITION. The element $a(z) = a_0 \cdot a_1(z)$ is called *aligned* if it can be written as a product $a_0 \exp(x_1 z) \exp(x_2 z^2) \cdot \dots$, where $x_i \in \mathfrak{g}_{q^i}$.

Note that the product above is finite and gives an element of $G[z]$. Hence any aligned element is a polynomial loop.

LEMMA 2.2. *For any $a \in G[[z]]$, one can find $g \in G_1[[z]]$ such that ${}^g a$ is aligned.*

PROOF. Following [BV,pp.31, 68], we will construct a sequence of elements $x_i \in \mathfrak{g}$ and $y_i \in \mathfrak{g}_{q^i}$ as follows. Note that the exponential map gives a bijection $z \cdot \mathfrak{g}[[z]] \xrightarrow{\sim} G_1[[z]]$. Therefore we can write a in the form $a = a_0 \exp(a_1 z) \exp(a' z^2)$ where $a_1 \in \mathfrak{g}$ and $a' \in \mathfrak{g}[[z]]$.

Since the operator $(q \cdot Ad_{a_0^{-1}} - \mathrm{Id})$ is invertible on $\bigoplus_{\lambda \neq q} \mathfrak{g}_\lambda$, there are uniquely defined elements $x_1 \in \bigoplus_{\lambda \neq q} \mathfrak{g}_\lambda$ and $y_1 \in \mathfrak{g}_q$ such that

$$(q \cdot Ad_{a_0^{-1}} - \mathrm{Id})(x_1) + a_1 = y_1 \,.$$

We next find y_2. To that end, set $g_1 = \exp(x_1 z)$. Then the above equation implies that ${}^{g_1}a = a_0 \exp(y_1 z) \exp(a_2 z^2) \exp(a' z^3)$, where $a_2 \in \mathfrak{g}$ and $a' \in \mathfrak{g}[[z]]$. Hence there exist uniquely determined elements $x_2 \in \bigoplus_{\lambda \neq q^2} \mathfrak{g}_\lambda$ and $y_2 \in \mathfrak{g}_{q^2}$ such that

$$(q^2 \cdot Ad_{a_0^{-1}} - \mathrm{Id})(x_2) + a_2 = y_2 \,.$$

Set $g_2 = \exp(x_2 z^2) \exp(x_1 z)$. Then the above equation insures that ${}^{g_2}a = a_0 \exp(y_1 z) \exp(y_2 z^2) \exp(a_3 z^3) \exp(a'' z^4)$, where $a_3 \in \mathfrak{g}$ and $a'' \in \mathfrak{g}[[z]]$. Iterating this process we construct the sequence $\{x_i \in \mathfrak{g}\,,\ i = 1, 2, \ldots\}$, such that setting $g_k := \exp(x_k z^k) \exp(x_{k-1} z^{k-1}) \ldots \exp(x_1 z)$ we get

$$ {}^{g_k}a = a_0 \cdot \exp(y_1 z) \exp(y_2 z^2) \ldots \exp(y_k z^k) \exp(y z^{k+1}) \tag{2.3}$$

where $y_i \in \mathfrak{g}_{q^i}$ and $y \in \mathfrak{g}[[z]]$. Then the product $g := \lim g_k = \ldots \exp(x_k z^k) \cdot \exp(x_{k-1} z^{k-1}) \cdot \ldots \cdot \exp(x_1 z)$ stabilizes since $\mathfrak{g}_{q^k} = 0$ for all $k >> 0$. Equation (2.3) shows that ${}^{g}a$ is aligned. $\square$

Proof of proposition 2.1. Choose a maximal torus $T \subset G$ containing a_0^{ss}. Let $R \subset Hom(T, \mathbb{C}^*)$ be the set of roots of (G, T). The subset consisting of the roots $\gamma \in R$ such that $|\gamma(a_0^{ss})| \leq 1$ defines a parabolic $P \subset G$. Then, for any $i > 0$, the subspace $\mathfrak{g}_{q^i}$ is contained in the nilradical of Lie$P$, for $|q| < 1$.

Further, we may choose a Borel subgroup $B \subset P$ that contains the unipotent part of a_0. Let U denote the unipotent radical of B. Then the element $\exp(y_1 z) \exp(y_2 z^2) \ldots \exp(y_k z^k)$ constructed in the proof of lemma 2.2 belongs to $U[z]$, and the proposition follows. $\square$

Lemma 2.5. *Let B and $\widetilde{B}$ be two Borel subgroups with unipotent radicals U, $\widetilde{U}$. Let $a = a_0 \cdot a_1$, $(a_0 \in B\,,\ a_1 \in U_1[z])$, and $\tilde{a} = \tilde{a}_0 \cdot \tilde{a}_1$, $(\tilde{a}_0 \in B\,,\ \tilde{a}_1 \in U_1[z])$, be two polynomial loops. Then any element $g \in G((z))$ such that ${}^{g}a = \tilde{a}$ is a Laurent polynomial loop, i.e., $g \in G[z, z^{-1}]$.*

Proof. Multiplying g by an element of G we may assume that $B = \widetilde{B}$.

Further, we find a faithful rational representation $\rho : G \to SL_n(\mathbb{C})$ such that B is the inverse image of the subgroup of upper triangular matrices

in $SL_n(\mathbb{C})$. Thus, applying ρ, we are reduced to proving the lemma in the case $G = SL_n(\mathbb{C})$ and $B =$ upper triangular matrices. Thus, from now on, a and $\tilde{a}$ are are assumed to be upper triangular polynomial matrices. Set $M = max(\deg a, \deg \tilde{a})$, the maximum of the degrees of the corresponding matrix-valued polynomials. Note that, by assumption, the diagonal entries a_{ii} and $\tilde{a}_{ii}$ of the matrices a and $\tilde{a}$ are independent of z.

Let ${}^g a = \tilde{a}$. We can write $g(z) = \sum_{k \geq k_0} g(k) z^k$, where $g(k)$ are complex $n \times n$-matrices. Computing the bottom left corner matrix entry of each side of the equation $g(qz)a(z) = \tilde{a}(z)g(z)$ yields:

$$g(k)_{n,1} \cdot (q^k a_{1,1} - \tilde{a}_{n,n}) = 0 \, .$$

It follows, since the diagonal entries of $a, \tilde{a}$ are nonzero, that there exists $N >> 0$ such that for all $k \geq N$, we have $g(k)_{n,1} = 0$. Using this, we now compute the two matrix entries standing on $(n-1) \times 1$ and $n \times 2$ places of each side of the equation $g(qz)a(z) = \tilde{a}(z)g(z)$. We find that, for any $k \geq N + M$:

$$g(k)_{n-1,1} \cdot (q^k a_{1,1} - \tilde{a}_{n-1,n-1}) = 0 \quad , \quad g(k)_{n,2} \cdot (q^k a_{2,2} - \tilde{a}_{n,n}) = 0 \, .$$

We deduce, as before, that there exists $N_2 >> 0$ such that for all $k \geq N_2$, we have $g(k)_{n-1,1} = g(k)_{n,2} = 0$.

Continuing the process of computing the entries of each side of the equation $g(qz)a(z) = \tilde{a}(z)g(z)$ along the diagonals (moving from bottom left corner to top right corner) we prove by descending induction on $(i-j)$ that $g(k)_{i,j} = 0$, for all $k \gg 0$. $\square$

We define a map from integral gauge-conjugacy classes in $G((z))$ to G-bundles on the elliptic curve $\mathcal{E} = \mathbb{C}^*/q^{\mathbb{Z}}$ as follows. Given an integral element $a \in G((z))$, we find (proposition 2.1) an aligned element $f \in G((z))$ which is gauge-conjugate to a. The loop$f$ being polynomial, it gives a well-defined holomorphic map $f : \mathbb{C}^* \to G$. Hence, we can associate to f the holomorphic G-bundle on $\mathcal{E}$ with multiplier f, see proof of proposition 1.3. If f' is another aligned element which is gauge-conjugate to a, then by lemma 2.5, f and f' are gauge-conjugate to each other via a Laurent polynomial, hence via a holomorphic, loop. It follows that the G-bundles with multipliers f and f' are isomorphic. Thus, we have associated to a a well-defined isomorphism class of G-bundles on $\mathcal{E}$.

3. Going to a finite covering.

Recall that for any positive integer m the field imbedding $\mathbb{C}((z)) \hookrightarrow \mathbb{C}((w))$, $z \mapsto w^m$, makes $\mathbb{C}((w))$ a Galois extension of $\mathbb{C}((z))$ with the Galois group $\mathbb{Z}/m\mathbb{Z}$. From now on we will write $z^{1/m}$ instead of w, so that $(z^{1/m})^m = z$, and the generator of the Galois group acts as $\omega : z^{1/m} \mapsto e^{2\pi i/m} z^{1/m}$. Let $G((z^{1/m}))$ denote the group of $\mathbb{C}((z))$-rational points of G. We view $G((z))$ as the subgroup of ω-fixed points in $G((z^{1/m}))$. We will sometimes write $a = a(z^{1/m})$ for an element of $G((z^{1/m}))$.

Further, we fix τ in the upper half-plane, $\mathrm{Im}\tau > 0$, such that $q = e^{2\pi i\tau}$. The automorphism $f(z) \mapsto f(q \cdot z)$ of the field $\mathbb{C}((z))$ can be extended to an automorphism of $\mathbb{C}((z^{1/m}))$ via the assignment $z^{1/m} \mapsto e^{2\pi i \cdot \tau/m} z^{1/m}$. This gives rise to a gauge-action $g : a \mapsto {}^g a$ on $G((z^{1/m}))$ that extends the one on $G((z))$.

Definition. An element $s \in G$ is said to be *reduced* if, for any finite dimensional rational representation $\rho : G \to GL(V)$, and any eigenvalue λ of the operator $\rho(s)$ we have $\lambda^k = q^l$, (for some $k, l \in \mathbb{Z} \setminus \{0\}$) $\implies \lambda = 1$.

View G as the subgroup of "constant loops" in $G((z^{1/m}))$.

Theorem 3.1. *Let $a(z) \in G[[z]]$ be an aligned element. Then one can find a positive integer m and $g \in G((z^{1/m}))$ such that ${}^g a$ is a constant loop and moreover the element ${}^g a \in G$ is reduced.*

Remark 3.2. One can show that the element $a(z) \in SL_2((z))$ given by the matrix $\begin{pmatrix} q^{1/2} & z \\ 0 & q^{-1/2} \end{pmatrix}$ is not gauge-conjugate to a constant loop within the group $SL_2((z))$. This explains the significance of taking g to be in $G(z^{1/m})$ in the theorem above. $\square$

To prove the theorem, we fix a maximal torus $T \subset G$, and let $X^*(T) = Hom_{alg}(T, \mathbb{C}^*)$ and $X_*(T) = Hom_{alg}(\mathbb{C}^*, T)$ denote the weight and coweight lattices, respectively. We first prove

Lemma 3.2. *For any $s \in T$ there exists $\phi \in X_*(T)$ and an integer $m \neq 0$ such that the following holds:*

(i) $s = \phi(e^{2\pi i \cdot \tau/m}) \cdot s_{red}$ where s_{red} is reduced;

(ii) Let $\alpha \in X^*(T)$. If $\alpha(s) = q^l$ for some $l \in \mathbb{Z}$, then $\alpha(\phi)/m = l$ and $\alpha(s_{red}) = 1$.

Proof of Lemma. In $\mathbb{C}^*$ consider the subgroup

$$\Gamma = \{z \in \mathbb{C}^* \mid \exists\ k, l \in \mathbb{Z} \text{ such that } z^k = q^l\}.$$

Let L be the subgroup of the weights $\alpha \in X^*(T)$ such that $\alpha(s) \in \Gamma$. Clearly, if $\alpha \in X^*(T)$ and $m \cdot \alpha \in \Gamma$ for some integer $m \neq 0$, then $\alpha \in \Gamma$. Hence, by the well known structure theorem about subgroups in $\mathbb{Z}^n$ we deduce that L splits off as a direct summand in $X^*(T)$. Therefore, there is another lattice $L_{red} \subset X^*(T)$ such that $X^*(T) = L \oplus L_{red}$. This direct sum decomposition of lattices must be induced by a direct product decomposition $T = T_1 \times T_{red}$, where T_1 and T_{red} are subtori in T such that $X^*(T_1) = L$ and $X^*(T_{red}) = L_{red}$. Thus, we have $s = s_1 \cdot s'_{red}$, where $s_1 \in T_1$ and $s'_{red} \in T_{red}$.

For any $\alpha \in X^*(T)$, we have by construction $\alpha(s_1) \in \Gamma$. Furthermore, $\alpha(s) \in \Gamma$ implies $\alpha \in L$, hence $\alpha(T_{red}) = 1$. Therefore, for $\alpha \in X^*(T)$ such that $\alpha(s'_{red}) \in \Gamma$ we have $\alpha(s_1 \cdot s'_{red}) \in \Gamma$, hence $\alpha \in L$, hence $\alpha(s'_{red}) = 1$. Thus, s'_{red} is reduced.

View the groups $X^*(T_1)$ and $X_*(T_1)$ as lattices in $\mathrm{Lie}(T_1)^*$ and $\mathrm{Lie}(T_1)$, respectively, so that $X_*(T_1)$ is the kernel of the exponential map.

Write $s_1 = \exp(h)$, where $h \in \mathrm{Lie}\ (T_1)$. Since $\alpha(s_1) \in \Gamma$ for any $\alpha \in X^*(T)$ and elements of Γ have the form $z = e^{2\pi i(\tau \cdot r + r')}$, $r, r' \in \mathbb{Q}$, it follows that $\alpha(h) \in \mathbb{Q} \cdot \tau + \mathbb{Q}$. Hence, $h \in \tau \cdot \mathbb{Q} \otimes_{\mathbb{Z}} X_*(T_1) + \mathbb{Q} \otimes_{\mathbb{Z}} X_*(T_1)$. Therefore, there exist $\phi, \psi \in X_*(T_1)$ and an integer m such that $h = \frac{\tau}{m}\phi + \frac{1}{m}\psi$. Thus, $s_1 = exp(h) = \epsilon \cdot \phi(e^{2\pi i \cdot \tau/m})$, where $\epsilon = \psi(e^{2\pi i/m})$ is an element of order m. We put $s_{red} = \epsilon \cdot s'_{red}$. Clearly, s_{red} is reduced, and $s = s_1 \cdot s'_{red} = \phi(e^{2\pi i \cdot \tau/m}) \cdot s_{red}$.

To prove part (ii), let $\alpha \in X^*(T)$ be such that $\alpha(s) = q^l$ for some $l \in \mathbb{Z}$. Then $\alpha \in L$, hence $\alpha(s'_{red}) = 1$. Furthermore, the equation

$$e^{2\pi i \cdot \tau \cdot l} = q^l = \alpha(s) = e^{2\pi i \cdot \tau \cdot \alpha(\phi)/m + 2\pi i \cdot \alpha(\psi)/m}$$

yields $\tau \cdot (l - \alpha(\phi)/m) + \alpha(\psi)/m \in \mathbb{Z}$. It follows, since $\alpha(\phi)$ and $\alpha(\psi)$ are integers, that $l = \alpha(\phi)/m$ and $\alpha(\psi)/m \in \mathbb{Z}$. Hence $\alpha(\epsilon) = \alpha(\psi(e^{2\pi i/m}) = 1$. Thus, $\alpha(s_{red}) = \alpha(\epsilon) \cdot \alpha(s'_{red}) = 1$, and (ii) follows. $\square$

Proof of theorem 3.1. We choose the Borel subgroup $B = T \cdot U$ as constructed in the proof of proposition 2.1. Put $\mathfrak{b} = \mathrm{Lie}B$. Thus we have $a(z) = a_0 \exp(x_1 z) \exp(x_2 z^2) \cdot \ldots \cdot exp(x_k z^k)$, where $a_0^{ss} \in T$ and $x_i \in \mathfrak{g}_{q^i} \subset \mathfrak{b}$, where $\mathfrak{g}_{q^i}$ stands for the q^i-eigenspace of Ad a_0^{ss}.

Applying lemma 3.2 to $s = a_0^{ss}$, we find an integer m and an algebraic group homomorphism $\phi : \mathbb{C}^* \to T$ such that $a_0^{ss} = \phi(e^{2\pi i \cdot \tau/m}) \cdot s_{red}$.

For any integer $i \geq 1$ we can write $x_i = \sum_\alpha x_\alpha$, where α is a positive root of (G, T) such that $\alpha(a_0^{ss}) = q^i$ and x_α is a non-zero root vector corresponding to α. For such an α part (ii) of lemma 3.2 yields $\alpha(\phi(z^{1/m})) =$

$z^{\alpha(\phi)/m)} = z^i$. We set $g = \phi(z^{1/m})$, a well-defined element of the group $G((z^{1/m}))$. Then, we obtain

$$(\text{Ad } g)(x_\alpha) = \alpha(\phi(z^{1/m})) \cdot x_\alpha = z^i \cdot x_\alpha \,.$$

It follows that a similar equation holds for x_i instead of x_α. From this we deduce

$$g^{-1} \cdot \exp(x_i z^i) \cdot g = \exp(x_i) \,. \tag{3.2.1}$$

Further, let u be the unipotent part of the Jordan decomposition of a_0. Write $u = \exp(y)$ and $y = \sum_\alpha y_\alpha$, where y_α are root vectors. Since a_0^{ss} commutes with y, we deduce similarly, using lemma 3.2(ii), that $\alpha(\phi) = 0$ for any root α such that $y_\alpha \neq 0$. It follows that $g^{-1} \cdot u \cdot g = u$. From this and (3.2.1) we obtain

$$^g a = \phi(e^{2\pi i \cdot \tau/m} z^{1/m})^{-1} \cdot a_0^{ss} \cdot u \cdot \exp(x_1 z) \exp(x_2 z^2) \cdot \ldots \cdot exp(x_k z^k) \cdot \phi(z^{1/m})$$

$$= \phi(e^{2\pi i \cdot \tau/m})^{-1} \cdot a_0^{ss} \cdot u \cdot \exp(x_1) \cdot \exp(x_2) \ldots \exp(x_k) \,.$$

Using lemma 3.2(i) we see that $\phi(e^{2\pi i \cdot \tau/m})^{-1} \cdot a_0^{ss} \cdot u = s_{red} \cdot u$. This element is reduced, and the theorem follows. $\square$

LEMMA 3.3. *Let $s \in G$ be reduced. Then any element $g \in G((z))$ such that $^g s = s$ is a constant loop.*

PROOF. Consider the adjoint representation $\rho : G \to GL(\mathfrak{g})$. We choose a basis in $\mathfrak{g}$ such that $\rho(s)$ is an upper-triangular matrix. Given g such that $^g s = s$, we write $\rho(g) = \sum_{k \geq k_0} g(k) z^k$, where $g(k)$ are complex $n \times n$-matrices. The same proccess as in the proof of lemma 2.5 gives equations of the type

$$g(k)_{m,n} \cdot (q^k s_{n,n} - s_{m,m}) = 0 \quad , \quad k \in \mathbb{Z} \,.$$

Since s is reduced, this implies $g(k)_{m,n} = 0$ for all $k \neq 0$. Hence the image of g in $GL(\mathfrak{g})(z)$ is constant. It follows that g is itself constant, for the kernel of the adjoint representation $G \to GL(\mathfrak{g})$ is finite. $\square$

COROLLARY 3.4. *Let $a \in G[[z]]$ be aligned and $s \in G$ be reduced. Assume $g \in G((z^{1/m}))$ is such that $^g a = s$. Then $g \in G[z^{1/m}, z^{-1/m}]$ is a Laurant polynomial loop in $z^{1/m}$. Furthermore, $\theta = g(e^{2\pi i \cdot \tau/m} z^{1/m}) g(z^{1/m})^{-1}$ is a constant loop, and $\theta^m = 1$.*

PROOF. The first claim follows from lemmas 2.2 and 2.5. To prove the second claim, recall the Galois automorphism $\omega : f(z^{1/m}) \mapsto f(e^{2\pi i \cdot \tau/m} z^{1/m})$ on $\mathbb{C}((z^{1/m}))$. We apply the induced automorphism of $G((z^{1/m}))$ to the

equation ${}^{g}a = s$. The RHS being independent of z, and a being fixed by ω, we get ${}^{\omega g}a = s$. This equation together with the original one, ${}^{g}a = s$, yield ${}^{\theta}s = s$ where $\theta = g(e^{2\pi i\cdot\tau/m}z^{1/m})g(z^{1/m})^{-1}$. Hence, θ is a constant loop, by lemma 3.3. Further, applying the automorphism ω to the first equation below we get a sequence of equations

$$\theta = (\omega g)\cdot g^{-1}\ \ ,\ \ \theta = (\omega^2 g)\cdot(\omega g)^{-1}\ ,\ldots,\ \theta = (\omega^m g)\cdot(\omega^{m-1}g)^{-1}\ .$$

Since $\omega^m = \mathrm{Id}$, taking the product of all these equations yields $\theta^m = 1$. □

We fix two generators, an "a-cycle" and a "b-cycle", of the fundamental group $\pi_1(\mathcal{E})$ as follows. a-cycle is defined to be the image of a generator of $\pi_1(\mathbb{C}^*) = \mathbb{Z}$ under the imbedding $\pi_1(\mathbb{C}^*) \hookrightarrow \pi_1(\mathcal{E})$ induced by the projection $\mathbb{C}^* \to \mathbb{C}^*/q^{\mathbb{Z}} = \mathcal{E}$. The b-cycle is the image of the segment $[1, q] \subset \mathbb{C}^*$ under the projection.

Given an integer $m \neq 0$, set ${}^{m}\mathcal{E} = \mathbb{C}^*/q^{\frac{\mathbb{Z}}{m}}$, and let ${}^{m}\pi :{}^{m}\mathcal{E} \to \mathcal{E}$, $z \mapsto z^m$ be the natural projection. Thus ${}^{m}\mathcal{E}$ is an elliptic curve and the map ${}^{m}\pi$ is an m-sheeted Galois covering with the Galois group $\mathbb{Z}/m\mathbb{Z}$ acting as monodromy around the a-cycle.

Proposition 3.5. *Let $a \in G[z]$ be an aligned element and P the principal G-bundle on $\mathcal{E}$ with multiplier a. Then*

(i) The bundle ${}^{m}\pi^*P$ is isomorphic to the holomorphic G-bundle on ${}^{m}\mathcal{E}$ with a reduced constant multiplier $s \in G$;

(ii) Let $\tilde{\nabla}$ be the holomorphic connection on ${}^{m}\pi^*P$ transported via the isomorphism (i) from the trivial connection d on the trivial bundle. Then $\tilde{\nabla}$ descends to a well-defined holomorphic connection ∇ on P. The latter has finite monodromy around a-cycle and a reduced monodromy around b-cycle.

Proof. By theorem 3.1 there exists an element $g \in G(z^{1/m})$ such that ${}^{g}a = s$ is a constant loop where $s \in G$ is reduced. By corollary 3.4, $g = g(z^{1/m})$ is a Laurent polynomial in $z^{1/m}$. Hence, g may be viewed as a well-defined G-valued regular function on the m-fold covering of $\mathbb{C}^*$. Let P be the G-bundle on $\mathcal{E}$ with multiplier a. It follows that the pull-back, ${}^{m}\pi^*P$, has a multiplier which is gauge-conjugate to s. This proves part (i).

To prove (ii), recall that any G-bundle with a constant multiplier s has a natural flat holomorphic connection which is given (in the trivialization on $\mathbb{C}^*$ corresponding to s) by the deRham differential d. We transport this connection to ${}^{m}\pi^*P$ via the isomorphism given by the loop g. The connection $\tilde{\nabla} = g^{-1}\circ d\circ g$ thus obtained descends to to a connection on P if and only

if it is invariant under the Galois action of $\mathbb{Z}/m\mathbb{Z}$. But by corollary 3.4 we have $\omega g = \theta \cdot g$, hence we get

$$\omega(\tilde{\nabla}) = (\theta \cdot g)^{-1} \circ d \circ (\theta \cdot g) = g^{-1} \cdot (\theta^{-1} \circ d \circ \theta) \cdot g = g^{-1} \circ d \circ g = \tilde{\nabla}\,,$$

since θ commutes with d.

To compute the monodromy, note that g^{-1} is a flat section of the connection $\tilde{\nabla}$. Hence the monodromy of $\tilde{\nabla}$ around b-cycle equals $g(e^{2\pi i\cdot\tau/m} z^{1/m}) g(z^{1/m})^{-1}$ $= \theta$. Since the covering ${}^m\pi :^{(m)} \mathcal{E} \to \mathcal{E}$ has no monodromy around b-cycle and has finite monodromy around a-cycle, it follows that ∇ also has monodromy θ around b-cycle and has finite monodromy around a-cycle. $\square$

Given a finite dimensional rational G-module V, write $V_{_P}$ for the associated vector bundle on $\mathcal{E}$ corresponding to a principal G-bundle P.

LEMMA 3.6. *Let P be the G-bundle with an aligned multiplier, and ∇ the connection on P constructed in proposition 3.5. Then, for any rational representation $\phi : G \to GL(V)$, every holomorphic section of the associated vector bundle $V_{_P}$ is flat with respect to the induced connection on $V_{_P}$.*

PROOF. Since ∇ was obtained from a connection $\tilde{\nabla}$ on ${}^m\pi^* P$, the claim is equivalent to a similar claim for the vector bundle ${}^m\pi^* V_{_P}$. This vector bundle is isomorphic to the vector bundle $\mathcal{V}$ on ${}^m\mathcal{E}$ with multiplier $\phi(s)$, so that the connection $\tilde{\nabla}$ is isomorphic to the trivial connection d. Thus, proving the claim amounts to showing that any holomorphic section of the vector bundle $\mathcal{V}$ with multiplier $\phi(s)$ is constant.

To that end, write the matrix $\phi(s)$ in Jordan form $\phi(s) = \bigoplus_i J(\lambda_i, n_i)$, where $J(\lambda_i, n_i)$ is the $(n_i \times n_i)$ Jordan block with eigenvalue λ_i. This gives the corresponding vector bundle decomposition $\mathcal{V} = \bigoplus_i \mathcal{V}_i$ where $\mathcal{V}_i$ is the vector bundle with multiplier $J(\lambda_i, n_i)$. If L_i denotes the line bundle with multiplier λ_i, then there is a canonical vector bundle imbedding $L_i \hookrightarrow \mathcal{V}_i$. Furthermore, one can prove (using, e.g., the Fourier-Mukai transform) that the imbedding induces an isomorphism $\Gamma({}^m\mathcal{E},\, L_i) \;\tilde{\to}\; \Gamma({}^m\mathcal{E},\, \mathcal{V}_i)$ of the spaces of global sections. Hence, any holomorphic section of $\mathcal{V}_i$ comes from a holomorphic section of L_i. But L_i is a degree zero line bundle, hence has a non-zero section only if it is the trivial bundle, i.e if $\lambda_i = q^m$. Observe now that λ_i is an eigen-value of the matrix $\phi(s)$. Since $s \in G$ is reduced, equation $\lambda_i = q^m$ implies $\lambda_i = 1$. But then the only holomorphic section of L_i is a constant section. The latter is annihilated by the deRham differential d, and the lemma is proved. $\square$

PROPOSITION 3.7. *Let $a, a_1 \in G((z))$ be two aligned elements. If the G-bundle on $\mathcal{E}$ with multiplier a is isomorphic to the G-bundle on $\mathcal{E}$ with multiplier a_1, then a is gauge-conjugate to a_1 via a polynomial loop.*

PROOF. By theorem 3.1, there exist an integer $m \geq 1$ and elements $g, g_1 \in G((z^{1/m}))$ such that

$$ {}^{g}a = s \quad , \quad {}^{g_1}a_1 = s_1 \quad \text{where } s, s_1 \in G \text{ are reduced.} \tag{3.7.1} $$

Let ∇, ∇_1 be the holomorphic connections on the G-bundles on $\mathcal{E}$ with multipliers a and a_1, respectively, constructed in proposition 3.5. The monodromies of the connections around a-cycle, are equal to s and s_1, respectively, and the monodromies around b-cycle are are equal to θ and θ_1, respectively. By proposition 3.5 we have $\theta^m = \theta_1^m = 1$. If the G-bundles with multipliers a and a_1 are isomorphic, then we may view ∇_1 as another holomorphic connection on the G-bundle P with multiplier a.

Since the cotagent bundle on $\mathcal{E}$ is trivial the difference $X = \nabla_1 - \nabla$ may be viewed as a holomorphic section of the adjoint bundle $\mathfrak{g}_P$. Since s is reduced the section X is flat with respect to ∇, by lemma 3.6. Let $p : \tilde{\mathcal{E}} \to \mathcal{E}$ be a universal cover of $\mathcal{E}$. The bundle p^*P on $\tilde{\mathcal{E}}$ has a horisontal holomorphic section. This section gives a trivialization of p^*P such that, in the induced trivialization of $p^*\mathfrak{g}_P$, the pull-back p^*X is a constant element $x \in \mathfrak{g}$. Observe that in general, any element $y \in \mathfrak{g}$ gives rise in this way to a flat multivalued section of $\mathfrak{g}_P$, and the monodromy of this section around a- and b-cycles is equal to $\mathrm{Ad}\theta(y)$ and $\mathrm{Ad}s(y)$, respectively. It follows, since X is a single-valued flat section of $\mathfrak{g}_P$ without monodromy, that x commutes with both θ and s. Hence, equation $\nabla_1 = \nabla + X$ shows that the monodromy of the connection ∇_1 is given by the formulas

$$ \theta_1 = \exp(x) \cdot \theta \quad , \quad s_1 = \exp(\tau x) \cdot s \, . \tag{3.7.2} $$

From these formulas and the equations $\theta_1^m = \theta^m = 1$ we deduce $\exp(m \cdot x) = 1$. Thus, we may find a maximal torus T containing θ, θ_1 and $\phi \in X_*(T)$, such that $x = \phi/m$ (cf. proof of lemma 3.2).

Clearly, $\phi(z^{1/m})$ is a well defined element of $G((z^{1/m}))$, and from the first formula in (7.3.2) we deduce $\phi(e^{2\pi i \cdot \tau/m} z^{1/m}) \cdot s \cdot \phi(z^{-1/m}) = s_1$. Recall the notation of (7.3.1), and put $f(z^{1/m}) = g_1(z^{1/m})^{-1} \cdot \phi(z^{1/m}) \cdot g(z^{1/m}) \in G((z^{1/m}))$. We claim that $f \in G((z))$. To prove this, it suffices to show that

$f(e^{2\pi i\cdot\tau/m}z^{1/m}) = f(z^{1/m})$. The latter follows from the chain of equalities:

$$f(e^{2\pi i\cdot\tau/m}z^{1/m}) = g_1^{-1}(e^{2\pi i\cdot\tau/m}z^{1/m})\cdot\phi(e^{2\pi i\cdot\tau/m}z^{1/m})\cdot g(e^{2\pi i\cdot\tau/m}z^{1/m}) =$$
$$g_1^{-1}(z^{1/m})\cdot\theta_1^{-1}\cdot\exp(x)\cdot\phi(z^{1/m})\cdot\theta\cdot g(z^{1/m}) =$$
$$g_1^{-1}(z^{1/m})\cdot\theta_1^{-1}\cdot\exp(x)\cdot\theta\cdot\phi(z^{1/m})\cdot g(z^{1/m}) =$$
$$g_1^{-1}(z^{1/m})\cdot\phi(z^{1/m})\cdot g(z^{1/m}) = f(z^{1/m})\,.$$

Finally, using (7.3.1) we calculate

$$^f a \;=\; {}^{g_1^{-1}\cdot\phi\cdot g}a \;=\; {}^{g_1^{-1}\cdot\phi}s \;=\; {}^{g_1^{-1}}s_1 \;=\; a_1\,.$$

Thus, a and a_1 are gauge-conjugate by an element of $G((z))$. Lemma 2.5 completes the proof. $\square$

4. Semistable G-bundles and holomorphic connections.

Recall that G is a complex connected semisimple group. For the definition and properties of semistable holomorphic G-bundles on an elliptic curve we refer to [R] and [RR].

PROPOSITION 4.1. *A holomorphic principal G-bundle over an elliptic curve is semistable if and only if it has a holomorphic connection (necessarily flat).*

PROOF. The "if" part is a corollary of the main result of [B]. The "only if" part follows from theorem 4.2 below. $\square$

THEOREM 4.2. *For any semistable G-bundle P on $\mathcal{E}$, there exists a holomorphic connection on P with finite order monodromy around a-cycle such that, for any rational G-module V, every holomorphic section of the associated vector bundle V_P is flat with respect to the induced connection on V_P.*

PROOF. We choose and fix a faithful rational representation $G \to GL(V)$. By a theorem of Ramanan and Ramanathan [RR], semistability of P implies semistability of V_P. By the classification of semistable vector bundles on $\mathcal{E}$, due to Atiyah [A], any semistable vector bundle is isomorphic to the vector bundle with a constant multiplier. Hence, the bundle V_P has constant multiplier $a \in GL(V)$. View a as an element of the semisimple group $PGL = PGL(V)$, and let P_a be the principal PGL-bundle with the constant multiplier a. By construction, the $PGL(V)$-bundle P_a is induced from the G-bundle P via the composition $G \to GL(V) \to PGL(V)$.

We may regard the element $a \in PGL$ as a constant aligned loop in $PGL((z))$. Applying proposition 3.5, we see that there is an integer $m \neq 1$ and a reduced element $s \in PGL$ such that the bundle ${}^m\pi^*P$ on ${}^m\mathcal{E}$ is isomorphic to the PGL-bundle on ${}^m\mathcal{E}$ with multiplier $s \in PGL$. Let ∇ be the connection on P_a constructed in proposition 3.5.

We claim that the connection ∇ on P_a arises from a holomorphic connection on the G-bundle P via the composite homomorphism $\rho : G \to GL(V) \to PGL(V)$. Note that this composition has finite kernel, so that the induced canonical map $i : P \to P_a$ is an immersion. Let TP_a be the tangent bundle on P_a. Our claim is equivalent to saying that the distribution in TP_a formed by the horisontal subspaces of the connection ∇ is tangent to the immersed submanifold $i(P) \subset P_a$. Observe that the canonical map $i : P \to P_a$ gives rise to a holomorphic section $\nu : \mathcal{E} = P/G \to P_a/\rho(G)$. The horisontal distribution is tangent to $i(P)$ if and only if ν is a horisontal section.

To show the latter, we apply Chevalley's theorem [S, Theorem 5.1.3] to the algebraic subgroup $\rho(G) \subset PGL$. The theorem says that we can find a rational representation $\phi : PGL \to GL(E)$ and a 1-dimensional subspace $\mathbf{l} \subset E$ such that $\rho(G) = \{g \in PGL \mid \ \phi(g)(\mathbf{l}) = \mathbf{l}\}$. Notice, that since G is semisimple, it stabilises a vector $l \in \mathbf{l}$. Hence, the assignment $g \mapsto g(l)$ gives rise to an imbedding $PGL/\rho(G) \hookrightarrow E$. Now let E_{P_a} be the associated vector bundle corresponding to E, equiped with the connectioned induced by ∇. The imbedding $PGL/\rho(G) \hookrightarrow E$ gives rise to an imbedding $P_a/\rho(G) \hookrightarrow E_{P_a}$ compatible with the connections. To show that ν is horisontal, it suffices to show that its image under the above imbedding is a flat section. But this image is a holomorphic section of E_{P_a}. By lemma 3.6, any holomorphic section of the vector bundle E_{P_a} is flat with respect to the connection on E_{P_a} induced by ∇. This proves that ν is horisontal, so that the horisontal distribution on TP_a is tangent to $i(P)$ and the connection ∇ comes from a holomorphic G-connection on P.

Observe further that the connection ∇ on P_a has finite monodromy around a-cycle. The map $i : P \to P_a$ being an immersion with finite fibers, it follows that the G-connection on P also has finite monodromy around a-cycle.

Finally, it remains to show that there exists a holomorphic connection on P with finite order monodromy around a-cycle such that, for any rational G-module V, every holomorphic section of the associated vector bundle V_P is flat with respect to the induced connection on V_P. We do not claim that

the connection we have constructed has this property. Instead we proceed as follows. We first use the connection that we have constructed above to prove that any semistable G-bundle on $\mathcal{E}$ is isomorphic to a G-bundle with an aligned multiplier. This will be done in the proof of theorem 4.3 below. We can then apply proposition 3.5(ii) and lemma 3.6 to get a connection on P with all the required properties. $\square$

THEOREM 4.3. *A G-bundle on $\mathcal{E}$ is semistable if and only if it is isomorphic to the G-bundle with an aligned multiplier $a \in G(z)$.*

PROOF. By proposition 3.5(ii), any G-bundle P with an aligned multiplier has a holomorphic connection. Then, the "if" part of proposition 4.1 (due to Biswas) implies that P is semistable.

Conversely, let P be a semistable G-bundle. By theorem 4.2, we can equip P with a holomorphic connection that has monodromies $\theta, b \in G$ around the a- and the b-cycle respectively, such that $\theta^m = 1$ for some integer $m \geq 1$. Observe that the elements θ and b commute, for $\pi_1(\mathcal{E})$ is an abelian group. Hence there is a maximal torus $T \subset G$ such that $\theta, b^{ss} \in T$. As in the proof of proposition 2.1, we choose a Borel subgroup $B \supset T$ such that $b \in B$ and $|\alpha(b^{ss})| \leq 1$ for any positive (with respect to B) root α.

Further, since $\theta^m = 1$ there exists $\phi \in X_*(T)$ such that $\theta = \phi(e^{2\pi i/m})$. Let $g = \phi(z^{1/m})^{-1}$, a well-defined polynomial loop in $G((z^{1/m}))$. We put $a =^g b \in G((z^{1/m}))$. We have $g(e^{2\pi i/m} z^{1/m}) = \theta^{-1} g(z^{1/m})$. Since θ commutes with b, we deduce that $a(e^{2\pi i/m} z^{1/m}) = a(z^{1/m})$. It follows that a is fixed by the Galois group, hence, $a \in G((z))$.

Let U be the unipotent radical of B. We have $b = b^{ss} \cdot u$ where $u \in U$. Hence, the condition $|\alpha(b^{ss})| \leq 1$ for any positive root α, insures that $a = {}^g b = b^{ss} \cdot a_1$ where $a_1 \in U_1[[z]]$. Moreover, since g is a polynomial loop we have $a_1 \in U_1[z]$. By proposition 1.3, the element a is gauge-conjugate in $G((z))$ to an aligned element a'. Using lemma 2.5 and the fact that $a \in B \cdot U[z]$, we see that a is gauge-conjugate to a' via a polynomial loop. Thus, there is an element $f \in G[z^{1/m}, z^{-1/m}]$ such that

$$ {}^f a' = b \quad , \quad f(e^{2\pi i/m} z^{1/m}) f(z^{1/m})^{-1} = \theta \,. $$

These equations show (see proof of proposition 3.5) that the G-bundle P' with multiplier a' has a holomorphic connection with the monodromies θ and $b \in G$ around a- and b-cycle, respectively. Thus P and P' are two G-bundles with connections that have the same monodromy. Since a holomorphic G-bundle with connection is determined, up to isomorphism, by

the monodromy representation, we deduce that $P \simeq P'$, and the theorem follows. $\square$

PROOF OF THEOREM 1.2. Proposition 3.5 shows that the G-bundle associated to any integral gauge-conjugacy class in $G((z))$ via the procedure described at the end of §2 has a holomorphic connection, hence is semistable, due to proposition 4.1. Theorem 4.3 insures that the map $\{$*integral gauge-conjugacy classes*$\} \longrightarrow \{$ *isomorphism classes of semistable* G*-bundles* $\}$ is surjective. Injectivity of the map follows from proposition 3.7. $\square$

References

[A] Atiyah M.F., *Vector bundles over an elliptic curve* Proc. London. Math. Soc. (3), 7, 1957, 414-452.

[B] Biswas I. *Principal bundles admitting a holomorphic connection.* preprint alg-geom/9601019.

[BV] Babbit D.G., V.S.Varadarajan *Formal reduction theory of meromorphic differential equations: a group theoretic view.* Pac.Jour.Math **109** (1983), no.1, 1-80.

[EFK] Etingof P., Frenkel I., Kirilllov A, Jr. *Spherical functions on affine Lie groups.* Duke Math. J., **80** (1995), 59-90.

[R] Ramanathan A. *Stable principal bundles on a compact Riemann surface.* Math.Ann. **213** (1975) 129-152.

[RR] Ramanan S., Ramanathan A. *Some remarks on the instability flag.* Tohôku Math.J. **36** (1984) 269-291.

[S] Springer T.A. *Linear algebraic groups.* Progress in Mathematics vol.9, Boston: Birkhäuser, 1981.

UNIVERSITY OF CHICAGO, DEPARTMENT OF MATHEMATICS, CHICAGO IL 60637.

barashek@math.uchicago.edu

ginzburg@math.uchicago.edu