COUNTING CONJUGACY CLASSES IN SYLOW $p$-SUBGROUPS OF CHEVALLEY GROUPS

SIMON M. GOODWIN

Abstract. Let $p$ be a prime and let $q$ be a power of $p$. Let $U(q)$ be a Sylow $p$-subgroup of a finite Chevalley group $G(q)$ and let $B(q)$ be the normalizer of $U(q)$ in $G(q)$. In this paper we prove rationality of the zeta functions associated to: the number of conjugacy classes of $U(q)$; the number of $B(q)$-conjugacy classes in $U(q)$; and the number of conjugacy classes of $B(q)$. Our proof is constructive and provides a parametrization of the conjugacy classes; it also leads to a method to calculate the zeta functions.

1. Introduction

Let $p$ be a prime and $q_0$ a fixed power of $p$. Let $K = \mathbb{F}_{q_0}$ be the field of $q_0$ elements and let $k$ be the algebraic closure of $K$. Let $G$ be a connected split reductive linear algebraic $K$-group; we identify $G$ with its group of $k$-rational points $G(k)$. For a power $q = q_0^s$ of $q_0$, we write $G(q)$ for the finite Chevalley group consisting of $\mathbb{F}_q$-rational points of $G$; likewise for a closed $K$-subgroup of $G$.

Let $B$ be a Borel subgroup of $G$ that is defined over $K$ and write $U$ for the unipotent radical of $B$. We note that $U$ is defined over $K$ and $U(q)$ is a Sylow $p$-subgroup of $G(q)$.

Given closed $K$-subgroups $M$ and $N$ of $G$ with $N$ normalized by $M$, we write $k_{M,N}(q)$ for the number of $M(q)$-conjugacy classes in $N(q)$; we write $k_M(q)$ for $k_{M,M}(q)$. We may form the zeta function

$$\zeta_{M,N}(z) = \exp\left( \sum_{s=1}^{\infty} \frac{k_{M,N}(q_0^s)}{s} z^s \right)$$

in $\mathbb{C}[[z]]$; we write $\zeta_M(z)$ for $\zeta_{M,M}(z)$.

The principal result of this paper is

**Theorem 1.1.** The zeta functions $\zeta_U(z)$, $\zeta_{B,U}(z)$ and $\zeta_B(z)$ are rational functions in $z$, whose numerators and denominators may be assumed to be elements of $1 + z\mathbb{Z}[z]$.

**Remark 1.2.** Let $V \subseteq U$ be a normal subgroup of $B$, $S \subseteq B$ a torus and $C = SV$. We note that our proof of Theorem 1.1 can be easily adapted to prove rationality of the zeta functions $\zeta_V(z)$, $\zeta_{C,V}(z)$ and $\zeta_C(z)$. We chose not to work in this generality in order to simplify the notation.

In the case $G = \text{GL}_n$ (with the standard definition over $K$), we may take $B$ to be the group of upper triangular matrices in $G$. Then $U = U_n = \{(x_{ij}) \in G : x_{ij} = 0 \text{ for } i > j \text{ and } x_{ii} = 1\}$ is the group of upper unitriangular $n \times n$ matrices.

*Date: July 13, 2005.*

2000 Mathematics Subject Classification. 14G10, 20G40.
In [16] G. R. Robinson proved that for an algebra subgroup (see [12]) \( M \) of \( U_n \), the zeta function \( \zeta_M(z) \) is a rational function in \( z \) whose numerator and denominator may be assumed to be elements of \( 1 + z\mathbb{Z}[z] \). Theorem 1.1 generalizes Robinson’s result.

There has been recent interest from M. P. F. Du Sautoy in Poincaré series and zeta functions for the number of conjugacy classes in algebraic groups, see [18]. The main result in loc. cit. implies that the Poincaré series associated to the number of conjugacy classes of any algebraic \( K \)-group \( R \) is a rational function. The rationality of these Poincaré series implies the number of conjugacy classes \( k_R(q^s_0) \) satisfies a linear recurrence relation, [18, Cor. 1.3].

The rationality of the zeta functions \( \zeta_{M,N}(z) \) given in Theorem 1.1 also implies the existence of linear recurrence relations for the values of \( k_{M,N}(q) \). The condition that the numerator and denominator are elements of \( 1 + z\mathbb{Z}[z] \) means that this recurrence relation is monic.

We now prove a general result (Theorem 1.5), which is related to, and in fact implies part of, Theorem 1.1. The proof is included in the introduction, because it is short and it naturally leads on to a description of our proof of Theorem 1.1. Before stating and proving Theorem 1.5 we need to give some more notation; we also recall two theorems that are key to its proof.

Let \( V \) be a \( K \)-variety. We write \( F_0 \) for the Frobenius morphism corresponding to the \( K \)-structure on \( V \). Then \( F = F_q^s \) is the Frobenius morphism corresponding to the \( \mathbb{F}_q \)-structure on \( V \) (we recall that \( q = q^s_0 \)). The \( \mathbb{F}_q \)-rational points of \( V \) are denoted by \( V(q) \).

We now state a theorem of B. Dwork, which is key to our proofs of both Theorem 1.1 and Theorem 1.5. Dwork’s theorem implies the first of the Weil conjectures, see [23]; it was proved in [6].

**Theorem 1.3** (B. Dwork (1960)). The zeta function

\[
\zeta(V; z) = \exp \left( \sum_{s=1}^{\infty} \frac{|V(q^s_0)|}{s} z^s \right)
\]

is a rational function in \( z \).

Let \( R \) be an algebraic \( K \)-group. Suppose \( R \) acts on \( V \) and this action is defined over \( K \). We recall that a quotient of \( V \) by \( R \) over \( K \) is, by definition, a quotient morphism \( \pi : V \to X \) (see [2, 6.1]) such that the fibres of \( \pi \) are the orbits of \( R \) in \( V \) (cf. [2, 6.3]). In particular, if such \( \pi \) exists, then the points of \( X(q) \) correspond to the \( F \)-stable \( R \)-orbits in \( V \).

Below we state a version of Rosenlicht’s theorem for our situation; the more general version is in [17].

**Theorem 1.4** (M. Rosenlicht (1963)). There exists a dense open \( R \)-stable \( K \)-subvariety \( W \) of \( V \) such that there exists a quotient \( \pi : W \to X \) of \( W \) by \( R \) over \( K \).

We write \( k^{g}_{R,V}(q) \) for the number of \( F \)-stable \( R \)-orbits on \( V \) and we form the zeta function

\[
\zeta^{g}_{R,V}(z) = \exp \left( \sum_{s=1}^{\infty} \frac{k^{g}_{R,V}(q^s_0)}{s} z^s \right).
\]

The superscript \( g \) is chosen, because the \( F \)-stable \( R \)-orbits in \( V \) are sometimes called the geometric orbits of \( R \) in \( V(q) \).
We are now in a position to state and prove Theorem 1.5. The construction of the varieties $X_i$ in the proof is well-known, see for example [13, §1.9].

**Theorem 1.5.** The zeta function $\zeta_{g,R,V}(z)$ is a rational function in $z$, whose numerator and denominator may be assumed to be elements of $1 + z\mathbb{Z}[z]$.

**Proof.** Set $V_1 = V$. By Rosenlicht’s theorem there exists an open dense $R$-stable $K$-subvariety $W_1$ and a quotient $\pi : W_1 \to X_1$ of $W_1$ by $R$ over $K$. Now set $V_2 = V_1 \setminus W_1$, this is a closed $K$-subvariety of $V_1$. Since $W_1$ is dense in $V_1$, we have that $\dim V_2 < \dim V_1$. Therefore, we may inductively construct a finite family of $K$-varieties $X_1, \ldots, X_m$ such that the $R$-orbits in $V$ correspond to the points of the $X_i$ ($i = 1, \ldots, m$). Further, the points of the $X_i(q)$ correspond to the $F$-stable orbits of $R$ in $V$.

Now we can apply Dwork’s theorem (Theorem 1.3) to each $X_i$ to deduce that $\zeta_{X_i; z}$ is a rational function for each $i$. By construction $\zeta_{g,R,V}(z) = \prod_{i=1}^m \zeta_{X_i; z}$, so that $\zeta_{g,R,V}(z)$ is a rational function.

We do not prove the assumption on the numerator and denominator here, this is covered in §2.8. □

One can try to use an argument based on Rosenlicht’s theorem to show that the zeta function

$$\zeta_{R,V}(z) = \exp \left( \sum_{s=1}^{\infty} \frac{k_{R,V}(q^s)}{s} z^s \right)$$

is rational, where $k_{R,V}(q)$ denotes the number of $R(q)$-orbits in $V(q)$. As the proof of Rosenlicht’s theorem in [17] does not construct the open dense $K$-subvariety $W$ (in its statement), one has no grasp of the varieties $X_i$ in the proof of Theorem 1.5. In particular, it is not possible to say anything uniform about how the $F$-stable $R$-orbits corresponding to points in a certain $X_i(q)$ split up into $R(q)$-orbits.

Our proofs of rationality of $\zeta_U(z)$ and $\zeta_{B,U}(z)$ for Theorem 1.1, which are outlined below, are based on the proof of Theorem 1.5. We explicitly construct varieties, that play the role of the $X_i$ in the proof of Theorem 1.5. These varieties are constructed in a “nice” way so that we avoid the problem, discussed in the previous paragraph, about orbits splitting. Further, it is possible to “calculate” the varieties that we use to parameterize the $U$-conjugacy classes and the $F$-stable $B$-conjugacy classes in $U$. This gives rise to a method that could be used to calculate the zeta functions in Theorem 1.1 explicitly.

We note that [8, Prop. 6.2] and Theorem 1.5 imply that $\zeta_U(z)$ is a rational function. However, we choose to include our proof as it is required for our proof of rationality of the zeta function $\zeta_{B,U}(z)$, which in turn gives rise to our proof that $\zeta_{B,U}(z)$ is a rational function. Also as mentioned above our proof leads to a method to calculate $\zeta_U(z)$.

We note that there are many interesting actions of $R$ on $V$ for which the $F$-stable orbits coincide with the $R(q)$-orbits in $V(q)$, so that Theorem 1.5 implies rationality of $\zeta_{R,V}(z)$. For example, one could take $R = P$ to be a parabolic subgroup of $\text{GL}_n$ and $V$ to be any normal subgroup of $P$. Another well-known example of the above situation is given by the representation theory of quivers with relations. One can use Theorem 1.5 to deduce
rationality of zeta functions whose coefficients are defined by the number of (indecomposable) representations of a quiver with relations; for related stronger results see [13] and [15] and the references therein.

We now give an outline of our proof of Theorem 1.1. First we note that Springer isomorphisms (see §2.2) allow us to consider the adjoint action of $B$ on $u$ rather than the conjugation action of $B$ on $U$. This is more convenient for our purposes.

Our proof of the rationality of $\zeta_U(z)$ and $\zeta_{B,U}^g(z)$ is based on Dwork’s theorem (Theorem 1.3). As implied above, we construct a finite family of subvarieties $\{u^\text{min}_{c,I}: c \in C\}$ (where $C$ is some indexing set) of $u$ such that the orbits of $U$ in $u$ correspond to the points of the $u^\text{min}_{c,I}$. To prove the rationality of $\zeta_{B,U}^g(z)$ we require a more complicated construction: we give a family of subvarieties $\{u^\text{min}_{c,I}: c \in C, I \subseteq R_c\}$ of $u$ such that the $B$-orbits in $u$ correspond to the points in quotients of the $u^\text{min}_{c,I}$ by certain finite groups. Proving that these constructions are correct relies heavily on the author’s results in [8] and [9]; the relevant results are reviewed in §2.3. We prove rationality of $\zeta_U(z)$ in Section 3 and we prove $\zeta_{B,U}^g(z)$ is a rational function in §4.1.

In §4.2 we prove rationality of $\zeta_{B,U}(z)$. To do this we require a result giving some uniformity in $q$ in the Galois cohomology sets of $C_B(X)$ for $X \in u^\text{min}_{c,I}$. We show that the cohomology set $H^1(F,C_B(X))$ does not depend on the choice of $X \in u^\text{min}_{c,I}$ and that it depends on $q$ only up to certain congruences. The proof of this uniformity result is given in §2.5. Our proofs of the rationality of $\zeta_{B,U}^g(z)$ and $\zeta_{B,U}(z)$ are fairly technical, so we include two examples to illustrate the proofs at the end of §4.2.

Finally in Section 5, we use Jordan decompositions to deduce the rationality of $\zeta_B(z)$ from the rationality of $\zeta_{B,L,U_L}(z)$ for pseudo-Levi subgroups $L$ of $G$ ($B_L = B \cap L$, $U_L = U \cap L$). We show that the conjugacy classes of $B$ are given by pairs $(t, \bar{u})$ where $t \in T$ (where $T \subseteq B$ a maximal torus) and $\bar{u}$ is a unipotent conjugacy class of $B \cap C_G(t)^0$. We require a result about the number of elements of $T$ giving rise to each pseudo-Levi subgroup, which we prove in §2.6.

As a general reference for the theory of algebraic groups we refer the reader to the books of Borel [2] and Springer [20]. For information about algebraic groups defined over finite fields we refer the reader to Chapter 3 of Digne and Michel’s book [5] and to Chapters 11–17 of Springer’s book [20].

ACKNOWLEDGMENTS

I am grateful to G. R. Robinson for conversations about this work. I also thank G. Röhrle for many useful comments about previous versions. Finally, I thank LIEGRITS and CAALT for financial support while this paper was written.

2. Preliminaries

2.1. Notation. We fix the notation to be used for our proof of Theorem 1.5. Let $p$ be a prime and $q_0$ a fixed power of $p$. Let $K = \mathbb{F}_{q_0}$ be the field having $q_0$ elements and let $k$ be the algebraic closure of $K$. We denote by $q = q_0^s$ a power of $q_0$, which we allow to vary in the sequel. By an algebraic $K$-group $R$ we mean an algebraic group defined over $K$ and we identify such $R$ with its group of $k$-rational points $R(k)$; likewise for $K$-subgroups, $K$-varieties etc. Given a $K$-variety $V$ we denote by $\bar{V}(q)$ the set of $\mathbb{F}_q$-rational points of $V$. 4
Let \( R \) be an algebraic \( K \)-group and let \( V \) be a \( K \)-variety on which \( R \) acts \( K \)-morphically. For \( r \in R \) and \( v \in V \), we write \( r \cdot v \) for the image of \( v \) under \( r \), \( R \cdot v = \{ r \cdot v : r \in R \} \) for the \( R \)-orbit of \( v \) in \( V \), and \( C_R(v) = \{ r \in R : r \cdot v = v \} \) for the stabilizer of \( v \) in \( R \). If \( v \in V(q) \), then \( R \cdot v \) and \( C_R(v) \) are defined over \( \mathbb{F}_q \), see [20, Prop. 12.1.2].

Let \( G \) be a connected split reductive algebraic \( K \)-group. The Lie algebra of \( G \) is denoted by \( \mathfrak{g} = \text{Lie} G \); likewise for closed subgroups of \( G \). Let \( F_0 \) be the Frobenius morphism associated to the \( K \)-structure on \( G \); we also write \( F_0 \) for the map that \( F_0 \) induces on \( \mathfrak{g} \). Let \( F = F_0^* \), so \( F \) is the Frobenius morphism associated to the \( \mathbb{F}_q \)-structure on \( G \). For a closed \( K \)-subgroup \( H \) of \( G \), we recall that \( H(q) = H^F = \{ x \in H : F(x) = x \} \) (cf. [5, Prop. 3.3]); similarly, we have \( \mathfrak{h}(q) = \mathfrak{h}^F \).

Fix a \( K \)-split maximal torus \( T \) of \( G \) and let \( \Psi \) be the root system of \( G \) with respect to \( T \). Since \( T \) is split, for each \( \alpha \in \Psi \), we may choose a parametrization \( u_\alpha : k \to U_\alpha \) of the root subgroup \( U_\alpha \) so that the action of \( F_0 \) is given by \( F_0(u_\alpha(t)) = u_\alpha(t^{p_0}) \). Then \( e_\alpha = du_\alpha(1) \) is a generator for the corresponding root subspace \( \mathfrak{g}_\alpha \) of \( \mathfrak{g} \) and the action of \( F_0 \) on \( \mathfrak{g}_\alpha \) is given by \( F_0(ae_\alpha) = a^{p_0}e_\alpha \).

Let \( B \supseteq T \) be a Borel subgroup of \( G \) that is defined over \( K \) (such \( B \) exists, see [5, 3.15]) and let \( U \) be the unipotent radical of \( B \). We note that \( U \) is defined over \( K \) and \( U(q) \) is a Sylow \( p \)-subgroup of \( G(q) \), see [5, Prop. 3.19]. Let \( \Psi^+ \) be the system of positive roots of \( \Psi \) determined by \( B \); we write \( \Pi \) for the corresponding set of simple roots. The number of positive roots is denoted by \( N = |\Psi^+| = \dim U \), we write \( r = \dim T \) for the rank of \( G \).

We recall the standard (strict) partial order \( \prec \) on \( \Psi^+ \) is defined by: \( \alpha \prec \beta \) if \( \beta - \alpha \) is a sum of positive roots.

For \( \beta \in \Psi^+ \) write \( \beta = \sum_{\alpha \in \Pi} c_{\alpha \beta} \alpha \) with \( c_{\alpha \beta} \in \mathbb{Z}_{\geq 0} \). We recall that \( p \) is said to be bad for \( G \) if it divides \( c_{\alpha \beta} \) for some \( \alpha \) and \( \beta \), else it is called good for \( G \). We assume throughout this paper that \( p \) is good for \( G \). We may list the bad primes: \( p = 2 \) is bad unless all simple components of \( G \) are of type \( A_i \); \( p = 3 \) is bad if \( G \) has a simple component of type \( E_6 \), \( E_7 \), \( E_8 \), \( F_4 \) or \( G_2 \); and \( p = 5 \) is bad if \( G \) has a simple component of type \( E_8 \).

We write \( X^*(T) \) for the group of characters of \( T \) and \( X_*(T) \) for the group of cocharacters of \( T \). We recall that there is a perfect pairing between \( X^*(T) \) and \( X_*(T) \), defined by \( \langle \chi, \psi \rangle = n \), where \( \chi(\psi(t)) = t^n \). Further, given a \( \mathbb{Z} \)-basis \( \{ \psi_1, \ldots, \psi_r \} \) of \( X_*(T) \), the elements of \( T \) are of the form \( t = \psi_1(t_1) \cdots \psi_r(t_r) \), where \( t_i \in k^* \) and the action of \( F \) on \( T \) is given by \( F(t) = \psi_1(t_1^q) \cdots \psi_r(t_r^q) \).

### 2.2. Springer isomorphisms

Let \( \mathcal{U} \) denote the unipotent variety of \( G \) and \( \mathcal{N} \) the nilpotent variety of \( \mathfrak{g} \). In [19] T.A. Springer proved that if the derived subgroup of \( G \) is simply connected, then there exists a \( G \)-equivariant morphism of varieties \( \mathcal{U} \to \mathcal{N} \) which is a homeomorphism on the underlying topological spaces. This result has subsequently been strengthened (see [1, Cor. 9.3.4]) to give

**Theorem 2.1.** Assume the derived subgroup of \( G \) is simply connected. Then there exists a \( G \)-equivariant isomorphism \( \phi : \mathcal{U} \to \mathcal{N} \) defined over \( K \).

Such an isomorphism \( \phi : \mathcal{U} \to \mathcal{N} \) is called a Springer isomorphism. One can show that a Springer isomorphism \( \phi \) maps \( U \) onto \( \mathfrak{u} \) so we can deduce Corollary 2.2 (see for example [8, Cor. 2.2]). We can remove the assumption that the derived subgroup of \( G \) is simply connected, because a covering map \( \sigma : \hat{G} \to G \) induces an isomorphism from \( \hat{U} \) to \( U \).
Corollary 2.2. There exists a $B$-equivariant isomorphism $\phi : U \to u$ defined over $K$.

In many parts of this paper it is more convenient to work with the adjoint action of $B$ on $u$, rather than the conjugation action of $B$ on $U$; the corollary above allows this convenience.

2.3. Recollection from [8] and [9]. Our proof of Theorem 1.1, requires results about the adjoint orbits of $U$ in $u$, given in [8], and their generalizations due to [9, Thm. 1.1]. In the following paragraphs we recall the relevant results from [8] and [9]; some of these results are generalizations, from the case $G=GL_n$ to arbitrary $G$, of results due to A. Véra-Lopez and J. M. Arregi in [22].

Fix an enumeration $\beta_1, \ldots, \beta_N$ of $\Psi^+$ such that $\beta_j \not\prec \beta_i$ for $i < j$ and define $B$-submodules $m_i$ of $u$ by

$$m_i = \bigoplus_{j=i+1}^N g_{\beta_j}$$

for $i = 0, \ldots, N$, then define $u_i = u/m_i$. We study the orbits of $U$ in $u$ by considering the action of $U$ on successive $u_i$.

Suppose $X \in u$ and consider the set

$$X + ke_{\beta_i} + m_i = \{X + \lambda e_{\beta_i} + m_i : \lambda \in k\} \subseteq u_i.$$  

The generalization of [8, Lem. 5.1] due to [9, Thm. 1.1] says that for $X \in u$ either:

(I) all elements of $X + ke_{\beta_i} + m_i$ are $U$-conjugate; or

(R) no two elements of $X + ke_{\beta_i} + m_i$ are $U$-conjugate.

This dichotomy allows to make the following definition.

Definition 2.3. Let $X \in u$ and $i \in \{1, \ldots, N\}$.

(i) $i$ is called an inert point of $X$ if (I) holds.

(ii) $i$ is called a ramification point of $X$ if (R) holds.

The first part of the following lemma follows easily from the results in [8, §5].

Lemma 2.4.

(i) Let $X \in u$ and $i \in \{1, \ldots, N\}$. Then $i$ is an inert point of $X$ if and only if

$$\dim C_U(X + m_i) = \dim C_U(X + m_{i-1}) - 1.$$  

Therefore, $\dim U \cdot (X + m_i)$ is the number of inert points of $X$ not greater than $i$.

(ii) Let $V$ be a $K$-subvariety of $u_i$ and suppose there is $m \in \mathbb{Z}_{\geq 0}$ such that if $X + m_i \in V$, then $\dim C_U(X + m_{i-1}) = m$. Then the elements of $V$ for which $i$ is a ramification point form a closed $K$-subvariety of $V$. Therefore, the elements of $V$ for which $i$ is an inert point form an open $K$-subvariety of $V$.

Proof. As remarked before the statement, we only need to prove part (ii). Let $C(U,V) = \{(u, X + m_i) \in U \times V : u \cdot (X + m_i) = X + m_i\}$. Applying [2, Cor. AG.10.3] to the projection onto the second factor $C(U,V) \to V$ shows that the elements of $V$ for which $i$ is a ramification point form a closed subvariety of $V$. The fact that this variety is defined over $K$ follows from [2, Thm. AG.14.4].
A partial order \( \leq_i \) on \( u_i \) is defined in [8, Defn. 5.3]; we write \( \leq \) for \( \leq_N \). In the following lemma we recall, from [8, Prop. 5.4 and Lem. 5.5], the properties of this partial order that we require.

**Lemma 2.5.**

(i) Each \( U \)-orbit in \( u_{i} \) contains a unique \( \leq_i \)-minimal representative.

(ii) \( X = \sum_{j=1}^{i} a_{j} e_{\beta_{j}} + m_{i} \) is the \( \leq_i \)-minimal representative of its \( U \)-orbit in \( u_{i} \), if and only if \( a_{j} = 0 \) whenever \( j \) is an inert point of \( X \).

We note that the partial order \( \leq_i \) and the \( \leq_i \)-minimal representatives depend on the chosen enumeration of \( \Psi^{+} \).

We conclude this subsection by recalling some results from [8, §6 and §7] regarding the adjoint orbits of \( U(q) \) and \( B(q) \) in \( u(q) \). We recall that by Corollary 2.2 the adjoint orbits of \( U(q) \) in \( u(q) \) correspond to the conjugacy classes of \( U(q) \), and the adjoint orbits of \( B(q) \) in \( u(q) \) correspond to the \( B(q) \)-conjugacy classes of \( U(q) \).

First we recall the following lemma; it is a consequence of [8, Prop. 6.2 and Lem. 6.3].

**Lemma 2.6.** The \( U(q) \)-orbits in \( u(q) \) correspond to the \( F \)-stable adjoint orbits of \( U \) in \( u \). Moreover, if \( X = \sum_{i=1}^{N} a_{i} e_{\beta_{i}} \) is the \( \leq \)-minimal representative of its \( U \)-orbit, then \( U \cdot X \) is \( F \)-stable if and only if \( a_{i} \in \mathbb{F}_{q} \) for each \( i \).

Finally we recall the following lemma, which is given by [8, Cor. 7.8].

**Lemma 2.7.** Suppose \( X \in u(q) \) is the \( \leq \)-minimal element in its \( U \)-orbit. Then the \( B(q) \)-orbits in \( (B \cdot X)(q) \) are in correspondence with the elements of the Galois cohomology set \( H^{1}(F,C_{T}(X)/C_{T}(X)^{0}) \).

In [8, §7] further results about the \( B \)-orbits in \( u \) are given. The approach we use in this paper is slightly different and we choose to postpone a discussion of the \( B \)-orbits until it is required in §4.1.

2.4. **Roots of unity in finite fields.** We require the following lemma about the number of roots of unity in finite fields. The result is well-known; we provide a proof for the reader’s convenience.

**Lemma 2.8.** Let \( d \in \mathbb{Z}_{\geq 1} \) and suppose \( p \) does not divide \( d \). Let \( \mathbb{F}_{q_{0}^{d}} \) be the splitting field of the polynomial \( x^{d} - 1 \) over \( K \). Let \( 1 = n_{1} < \cdots < n_{m} = n \) be all divisors of \( n \). For each \( i \) denote by \( d_{i} \) the number of \( d \)th roots of unity in \( \mathbb{F}_{q_{0}^{d_{i}}} \).

(i) Suppose the highest common factor of \( s \) and \( n \) is \( n_{i} \). Then the number of \( d \)th roots of unity in \( \mathbb{F}_{q_{0}^{d_{i}}} \) is \( d_{i} \).

(ii) Let \( a_{i} \) be the number of \( d \)th roots of unity in \( \mathbb{F}_{q_{0}^{d_{i}}} \) that are not in any proper subfield of \( \mathbb{F}_{q_{0}^{d_{i}}} \) that contains \( K \). Then \( n_{i} \) divides \( a_{i} \).

**Proof.** We note that \( d_{i} \) is the highest factor of \( d \) dividing \( q_{0}^{n_{i}} - 1 \) (or equivalently such that \( q_{0}^{n_{i}} - 1 \) (mod \( d_{i} \))); from which it is easy to see that if the highest common factor of \( s \) and \( n \) is \( n_{i} \), then the number of \( d \)th roots of unity in \( \mathbb{F}_{q_{0}^{d_{i}}} \) is \( d_{i} \). This proves (i).

If \( c \) is a divisor of \( d \) such that \( \mathbb{F}_{q_{0}^{n_{i}}} \) is the splitting field of \( x^{c} - 1 \) over \( \mathbb{F}_{q_{0}} \), then \( n_{i} \) is the order of \( q_{0} \) in the group of units \( \mu_{c} \) of the ring \( \mathbb{Z}/c\mathbb{Z} \) so \( n_{i} \) divides \( |\mu_{c}| \). It is easy to see that \( a_{i} \) is the sum of \( |\mu_{c}| \) over all \( c \) dividing \( d \) such that \( \mathbb{F}_{q_{0}^{n_{i}}} \) is the splitting field of \( x^{c} - 1 \) over \( \mathbb{F}_{q_{0}} \). Part (ii) follows. □
2.5. **Centralizers in \( T \) of sums of root vectors.** Let \( X = \sum_{\alpha \in \Gamma} e_\alpha \) be a sum of root vectors (\( \Gamma \subseteq \Psi^+ \)). In Lemma 2.9 we give the structure of the component group \( Z(X) = C_T(X)/C_T(X)^0 \) of the centralizer of \( X \) in \( T \). Then in Lemma 2.12 we describe the Galois cohomology set \( H^1(F, Z(X)) \).

Let \( \Gamma \subseteq \Psi^+ \) and write \( A = Z\Gamma \) for the lattice in \( X^*(T) \) generated by \( \Gamma \). The theory of finitely generated abelian groups says that we can choose a basis \( \chi_1, \ldots, \chi_r \) for \( X^*(T) \) such that \( d_1\chi_1, \ldots, d_l\chi_l \) is a basis for \( A \), where \( l \leq r \) and \( d_i \) divides \( d_{i+1} \) for each \( i = 1, \ldots, l - 1 \). For \( d \in \mathbb{Z}_{\geq 1} \), we denote by \( Z_d \) the multiplicative algebraic \( K \)-group consisting of \( d \)th roots of unity. We remark that if \( p \) divides \( d \) and \( d' \) is the \( p' \) part of \( d \), then \( Z_d = Z_{d'} \) (under our identification of \( Z_d \) with its group of \( k \)-rational points).

**Lemma 2.9.** Let \( X = \sum_{\alpha \in \Gamma} e_\alpha \) and \( Z(X) = C_T(X)/C_T(X)^0 \). Then \( Z(X) \cong Z_{d_1} \times \cdots \times Z_{d_l} \) and the action of \( F \) on \( Z(X) \) is given by \( F(x_1, \ldots, x_l) = (x_1^{q_1}, \ldots, x_l^{q_l}) \).

**Proof.** Let \( \psi_1, \ldots, \psi_r \) be the basis of \( X_*(T) \) dual to \( \chi_1, \ldots, \chi_r \). The elements of \( T \) are of the form \( t = \psi_1(t_1) \cdots \psi_r(t_r) \), where \( t_i \in k^\times \) and we have that \( t \in C_T(X) \) if and only if \( t_i^{d_i} = 1 \) (\( i = 1, \ldots, l \)). We can see that \( C_T(X)^0 = \{ \psi_{i_1}(t_{i_1}) \cdots \psi_{i_r}(t_r) : t_{i_1}, \ldots, t_r \in k^\times \} \) and the result follows. \( \Box \)

The next lemma follows easily from [21, 4.3]; it can be used to simplify parts of our proof of Theorem 1.1, for particular \( G \). For instance, simplifications are possible in case \( G \) is semisimple and of adjoint type. In the statement \( \mathbb{Z}\Psi \) denotes the root lattice of \( \Psi \).

**Lemma 2.10.** Let \( A \) and \( d_i \) be as above. Then the prime factorization of \( d_i \) contains only bad primes for \( G \) and primes dividing the order of the torsion part of \( X^*(T) \)/\( \mathbb{Z}\Psi \).

The following definition is required for the statement of Lemma 2.12. We recall that \( A = Z\Gamma \).

**Definition 2.11.** We define the **splitting number** \( n_A \) of \( A \) (with respect to \( q_0 \)) to be the degree of the splitting field of the polynomial \( x^{d_i} - 1 \) over \( K \) (where \( d_i \) is as above).

The next lemma shows there is some degree of uniformity (as \( q \) varies) in the Galois cohomology set \( H^1(F, Z(X)) \). For the statement we recall that \( q = q_0^s \) and \( F = F_0^s \).

**Lemma 2.12.** Let \( X = \sum_{\alpha \in \Gamma} e_\alpha \). Let \( n \) be the splitting number of \( \mathbb{Z}\Gamma \) and let \( 1 = n_1 < \cdots < n_m = n \) be all divisors of \( n \).

(i) There exist positive integers \( u_1, \ldots, u_m \) such that \( |H^1(F, Z(X))| = u_i \) if the highest common factor of \( s \) and \( n \) is \( n_i \).

(ii) Define \( v_i \) inductively by \( v_i = \sum_{j \in D_i} v_j \), where \( D_i = \{ j : n_j \text{ divides } n_i \} \). Then \( v_i \) is divisible by \( n_i \) for all \( i \).

**Proof.** We recall that \( Z(X) = Z_{d_1} \times \cdots \times Z_{d_l} \) and the action of \( F \) on \( Z(X) \) is the natural one. It follows that \( H^1(F, Z(X)) = H^1(F, Z_{d_1}) \times \cdots \times H^1(F, Z_{d_l}) \) and we easily see that we can reduce to the case \( Z(X) = Z_d \) for some \( d \in \mathbb{Z}_{\geq 1} \). Let \( d' \) be the \( p' \) part of \( d \). Under our identification of \( Z_d \) with its group of \( k \)-rational points we have \( Z_{d'} \) and \( Z_d \) are equal; therefore, we may assume that \( p \) does not divide \( d \).

Let \( c \) be the number of \( d \)th roots of unity in \( \mathbb{F}_q \). Let \( \xi \in k \) be a primitive \( d \)th root of unity.

Then the action of \( Z_d \) on itself by \( F \)-conjugation is given by \( \xi^a \cdot \xi^b = \xi^a \cdot \xi^b \cdot F(\xi^a)^{-1} = \xi^{a(1 - q) + b} \).
So $\xi^a : \xi^b = \xi^b$ if and only if $a(1 - q) = 0 \pmod{d}$; this occurs if and only if $d/c$ divides $a$. Therefore, the number of $F$-conjugacy classes in $Z_d$ is $c$.

Part (i) now follows from Lemma 2.8(i) by taking $u_i$ to be the number of $d$th roots of unity in $\mathbb{F}_{q^d}$. Then part (ii) follows directly from Lemma 2.8(ii), because “$v_i = a_i$” (in the notation of Lemma 2.8).

2.6. Pseudo-Levi subgroups. In this section we discuss pseudo-Levi subgroups of $G$. A pseudo-Levi subgroup of $G$ is, by definition, the connected centralizer of a semisimple element of $G$. We refer the reader to [14, §6] for information on pseudo-Levi subgroups. We consider pseudo-Levi subgroups of the form $L = Z_G(t)^0$ where $t \in T$. In particular, Lemma 2.16 regards the number of $t \in T(q)$ giving rise to a particular pseudo-Levi subgroup.

Consider the set $\Delta$ of all lattices $\mathbb{Z}\Gamma \subseteq X^*(T)$, where $\Gamma \subseteq \Psi^+$. For $t \in T$ there is a unique maximal $A(t) \in \Delta$ which kills $t$, i.e. $\lambda(t) = 1$ for all $\lambda \in A(t)$. We define

$$\Delta = \{ A \in \Delta : A = A(t) \text{ for some } t \in T \}.$$ 

For $A \in \Delta$ we define $L(A)$ to be the $K$-subgroup of $G$ generated by $T$ along with the root subgroups $U_\alpha$ such that $\alpha \in A \cap \Psi$. It follows from [14, Lem. 14] that $L(A(t)) = Z_G(t)^0$ is a pseudo-Levi $K$-subgroup of $G$ (see also [21, II §4.1]).

Remark 2.13. A result of D. I. Deriziotis, which is stated in [11, 2.15] implies that, in the case $G$ is simple, if $A \in \Delta$ then $A$ is conjugate by the Weyl group of $\Psi$ to some lattice of the form $\mathbb{Z}\Gamma$, where $\Gamma \subseteq \Pi \cup \{ \rho \}$ and $\rho$ denotes the highest root in $\Psi^+$. A general statement can be made when $G$ is only assumed to be reductive.

Let $A \in \Delta$. As in §2.5, we may choose a basis $\chi_1, \ldots, \chi_r$ for $X^*(T)$ such that $d_1 \chi_1, \ldots, d_l \chi_l$ is a basis for $A$, where $l \leq r$, and $d_i$ divides $d_{i+1}$ for each $i$. We define $d_A = d_l$. Let $\psi_1, \ldots, \psi_r$ be the basis of $X_*(T)$ that is dual to $\chi_1, \ldots, \chi_r$. Then we see that $t$ is killed by $A$ if and only if $t$ is of the form $t_1 \psi_1(t) \cdots \psi_r(t)$ with $t_i^{d_i} = 1$ for $i = 1, \ldots, l$.

The following definition is needed for Lemma 2.16; we recall that the splitting number of $A \in \Delta$ is introduced in Definition 2.11.

Definition 2.14. Let $d$ be the least common multiple of all $d_A$ for $A \in \Delta$. The splitting number $n_\Delta$ of $\Delta$ (with respect to $q_0$) is defined to be the degree of the splitting field of the polynomial $x^d - 1$ over $K$.

We note that we could have equivalently defined $n_\Delta$ to be the least common multiple of all $n_A$ for $A \in \Delta$, where $n_A$ is as introduced in Definition 2.11. The next lemma follows from Lemma 2.10.

Lemma 2.15. Let $d$ be as in Definition 2.14. Then $d$ is a product of bad primes for $G$ along with primes dividing the order of the torsion part of $X^*(T)/\mathbb{Z}\Psi$.

We note that in the case $G$ is simple and of adjoint type, Lemma 2.15 can be deduced from [14, Lem. 33].

The proof of the first part of the following lemma uses arguments in the proof of Lemma 2.12; therefore, we choose to omit the proof. The second part of the lemma can be proved using the first part and a straightforward inclusion-exclusion argument. We recall that $q = q_0$. 

9
Lemma 2.16. Let \( n \) be the splitting number of \( \Delta \), let \( 1 = n_1 < \cdots < n_m = n \) be all divisors of \( n \) and let \( A \in \Delta \). For each \( i \), define \( D_i = \{ j : n_j \text{ divides } n_i \} \).

(i) There exists a positive integer \( b_A \) and positive integers \( c_{A,i} (i = 1, \ldots, m) \) such that if the highest common factor of \( s \) and \( n \) is \( n_i \), then the number of \( t \in T(q) \) killed by \( A \) is equal to \( c_{A,i}(q - 1)^{b_A} \). Moreover, if \( d_{A,i} \) is defined inductively by \( c_{A,i} = \sum_{j \in D_i} d_{A,j} \), then \( d_{A,i} \) is divisible by \( n_i \).

(ii) Given a sequence of integers \( a_s \in \mathbb{Z}_{\geq 1} \), we write

\[
\zeta_a(z) = \exp \left( \sum_{s=1}^{\infty} \frac{a_s}{s} z^s \right).
\]

Lemma 2.17.

(i) Suppose \( \zeta_a(z) \) and \( \zeta_b(z) \) are rational functions in \( z \). Then \( \zeta_{a+b}(z) \) is a rational function in \( z \).

(ii) Suppose \( \zeta_a(z) \) is a rational function in \( z \) and \( f(x) \in \mathbb{Z}[x] \). Let \( c \in \mathbb{Z} \), and define \( b_s = f(c^s) a_s, b = (b_s) \). Then \( \zeta_b(z) \) is a rational function in \( z \).

Proof. The first part is easy, because \( \zeta_{a+b}(z) = \zeta_a(z) \zeta_b(z) \). Then, using part (i), it is clear that part (ii) is easier to present. For each \( s \), define \( f(x) = x^n \) for \( n \in \mathbb{Z}_{\geq 0} \). Let \( c \) and \( b \) be as in the statement, then

\[
\zeta_b(z) = \exp \left( \sum_{s=1}^{\infty} \frac{c^s a_s}{s} z^s \right) = \exp \left( \sum_{s=1}^{\infty} \frac{a_s}{s} (c^n z)^s \right) = \zeta_a(c^n z).
\]

Therefore, \( \zeta_b(z) \) is a rational function in \( z \). \( \square \)

The next two lemmas are rather technical; we require them in §4.2 and §5. We now set up the notation for Lemma 2.18.

Let \( n \in \mathbb{Z}_{\geq 1} \) and write \( 1 = n_1 < \cdots < n_m = n \) for all factors of \( n \). For each \( i \), define \( D_i = \{ j : n_j \text{ divides } n_i \} \). Let \( a^i = (a_{ij}) (i = 1, \ldots, m) \) be sequences of integers and let \( v_1, \ldots, v_m \) be integers such that \( v_i \) is divisible by \( n_i \) for each \( i \). Define the sequence \( a = (a_s) \), as follows: if the highest common factor of \( s \) and \( n \) is \( n_i \), then

\[
a_s = \sum_{j \in D_i} v_j a^i_{s/n_j}.
\]

Lemma 2.18. Suppose that \( \zeta_{a^i}(z) \) is a rational function in \( z \), for all \( i \). Then \( \zeta_a(z) \) is a rational function in \( z \).
Proof. It is straightforward to check that
\[ \zeta_a(z) = \prod_{i=1}^{m} \zeta_{a_i}(z^{n_i})^{\nu_i}. \]

We continue to use the notation for Lemma 2.18. Now let \( f_i(x) \in \mathbb{Z}[x] (i = 1, \ldots, m) \) be such that all the coefficients in \( f_i(x) \) are divisible by \( n_i \). Let \( c \in \mathbb{Z} \) and define the sequence \( b = (b_s) \) as follows: if the highest common factor of \( s \) and \( n \) is \( n_i \), then
\[ b_s = \sum_{j \in D_i} f_j(c) a_j^{s/n_j}. \]
Combining the proofs of Lemmas 2.17 and 2.18 one can prove

**Lemma 2.19.** Suppose that \( \zeta_a(z) \) is a rational function in \( z \), for all \( i \). Then \( \zeta_b(z) \) is a rational function in \( z \).

2.8. **Numerator and denominator condition.** Let \( a = (a_s)_{s \in \mathbb{Z}_{\geq 1}} \) be a sequence of integers and define \( \zeta(z) = \zeta_a(z) \) as in §2.7. Suppose that \( \zeta(z) \) is a rational function in \( z \) and \( z = 0 \) is not a zero or pole of \( \zeta(z) \), so that in particular the series \( \sum_{s=1}^{\infty} a_s z^s \) has a positive radius of convergence about \( z = 0 \). We outline arguments showing that we may assume that the numerator and denominator of \( \zeta(z) \) are elements of \( 1 + z\mathbb{Z}[z] \). Therefore, in the remainder of this paper, we are just concerned with showing that certain zeta functions are rational functions.

We may write
\[ \zeta(z) = \frac{c \prod_{i=1}^{e}(1 - \lambda_i z)^{m_i}}{d \prod_{j=1}^{f}(1 - \mu_j z)^{n_j}}, \]
where \( c \) and \( d \) are non-zero complex numbers, the \( \lambda_i \) and \( \mu_j \) are uniquely determined, pairwise distinct, complex numbers, and the \( m_i \) and \( n_j \) are positive integers. Evaluating both sides of the above expression for \( \zeta(z) \) at \( z = 0 \) gives \( c = d \), so we may suppose that \( c = d = 1 \).

Now
\[ \frac{\zeta'(z)}{\zeta(z)} = \frac{d}{dt} \log \zeta(z) = \sum_{s=1}^{\infty} a_s z^{s-1}. \]
From which one can deduce that
\[ a_s = \sum_{i=1}^{e} -m_i \lambda_i^s + \sum_{j=1}^{f} n_j \mu_j^s, \]
for each integer \( s \geq 1 \).

We include a proof of the following lemma for the reader’s convenience; it was communicated to the author by G. R. Robinson.

**Lemma 2.20.** Let \( m_1, m_2, \ldots, m_n \) be non-zero integers, and let \( \alpha_1, \alpha_2, \ldots, \alpha_n \) be distinct non-zero complex numbers. Suppose that for each positive integer \( s \), we have
\[ \sum_{i=1}^{n} m_i \alpha_i^s \in \mathbb{Z}. \]
Then the $\alpha_i$s are all algebraic integers, and $m_i = m_{i'}$ whenever $\alpha_i$ and $\alpha_{i'}$ are algebraically conjugate.

Proof. We first prove that the $\alpha_i$s are algebraic numbers. Let $V$ be the Van der Monde matrix with $(i,j)$ entry $\alpha_j^{i-1}$. Let $D$ be the diagonal matrix with $i$th diagonal entry $\alpha_i$. Let $m_i$ be the $n$-long column vector with $i$th entry $m_i$. For $s \geq 0$, let $x_s$ be the vector $VD^s m$, which is integral by hypothesis.

Since the $m_i$s are non-zero (and the $\alpha_i$s are distinct), we see that $\{D^s m : 0 \leq s \leq n - 1\}$ is a basis for $\mathbb{C}^n$, hence so is $\{x_s : 0 \leq s \leq n - 1\}$. Since $x_n$ is integral, and each $x_s$ is integral, we see that $x_n$ is a $\mathbb{Q}$-combination of $\{x_s : 0 \leq s \leq n - 1\}$. Set $T = VDV^{-1}$. Then $\{x_s : 0 \leq s \leq n - 1\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}^n$ with respect to which (the linear transformation represented by) $T$ has a rational matrix. Its eigenvalues are therefore algebraic numbers. But the eigenvalues of $T$ are $\{\alpha_i : 1 \leq i \leq n\}$, so the $\alpha_i$ are algebraic numbers, and are closed under algebraic conjugation.

Now there is a least positive integer $h$ such that $h\alpha_i$ is an algebraic integer for each $i$. We note that $\sum_{i=1}^n m_i(h\alpha_i)^s$ is an integer multiple of $h^s$ for each integer $s$, so by a standard lemma about Dedekind domains, see for example [16, Lem. 2.2], we deduce that $h\alpha_i$ is an algebraic integer multiple of $h$ for each $i$. Hence, each $\alpha_i$ is already an algebraic integer.

The final claim follows by induction on the maximal value of $|m_i|$, since $\{\alpha_i\}$ is closed under algebraic conjugation. \hfill $\Box$

Lemma 2.20 implies that the $\lambda_i$ and $\mu_j$ in (2.8.1) are algebraic integers. Elementary Galois theory now implies that we may assume the numerator and denominator of $\zeta(z)$ are elements of $1 + z\mathbb{Z}[z]$.

3. Rationality of $\zeta_U(z)$

We present two proofs that $\zeta_U(z)$ is a rational function. The first of these arguments is given independently by M. P. F. Du Sautoy in [18, §2.1] as an alternative way to prove G. R. Robinson’s result from [16]. We note that this argument also applies when $G$ is not assumed to be split; although in this case the zeta functions that we obtain are perhaps a little strange, see Remark 3.1. The construction used in our second argument leads to our proof of rationality of $\zeta_{BU}(z)$ in §4.1. Also this construction gives a parametrization of the $U$-orbits in $\mathfrak{u}$, see Remark 3.6.

3.1. Argument 1. Consider the commuting variety of $U$

$$C(U) = \{ (x, y) \in U \times U : xy = yx \};$$

it is defined over $K$ and its $\mathbb{F}_q$-rational points are

$$C(U)(q) = \{ (x, y) \in U(q) \times U(q) : xy = yx \}.$$

We have

$$|C(U)(q)| = \sum_{x \in U(q)} |C_U(q)(x)|.$$

Also the Burnside formula gives

$$(3.1.1) \quad k_{U}(q) = \frac{1}{|U|} \left( \sum_{x \in U(q)} |C_{U(q)}(x)| \right).$$
Therefore, we have
\[ k_U(q) = \frac{|C(U)(q)|}{q^N}. \]

We can apply Dwork’s theorem (Theorem 1.3) to the variety \( C \) to get that
\[ \zeta(C(U); z) = \exp \left( \sum_{s=1}^{\infty} \frac{|C(U)(q_0^s)|}{s} z^s \right) \]
is a rational function in \( z \). We have
\[ \zeta_U(z) = \exp \left( \sum_{s=1}^{\infty} \frac{k_U(q_0^s)}{s} z^s \right) = \exp \left( \sum_{s=1}^{\infty} \frac{|C(U)(q_0^s)|}{s} \left( \frac{z}{q_0^N} \right)^s \right) = \zeta \left( C(U); \frac{z}{q_0^N} \right). \]

It follows immediately that \( \zeta_U(z) \) is a rational function in \( z \).

Remark 3.1. We note that the above argument holds without the assumption that \( G \) is split. However, the zeta functions we obtain seem, perhaps, a bit unnatural. For example, we could take \( G \) to be \( GL_n \) with definition over \( K \) such that \( G(q) \) is the unitary group \( \text{Unit}_n(q_0^2) \). Then for a power \( q = q_0^2 \) we have \( G(q) = \text{Unit}_n(q^2) \) if \( s \) is odd, and \( G(q) = \text{GL}_n(q) \) if \( s \) is even. It would be interesting to know if the zeta function associated to the number of conjugacy classes in a Sylow \( p \)-subgroup of \( \text{Unit}(q^2) \) is a rational function; and whether the analogous zeta functions are rational for other non-split groups.

3.2. Argument 2. We now show that \( \zeta_U(z) \) is a rational function by constructing a family of varieties \( \{ u_c : c \in C \} \) such that the adjoint orbits of \( U(q) \) in \( u(q) \) correspond to the points of these varieties. Then we apply Dwork’s theorem to each of the \( u_c \).

As in §2.3 we fix an enumeration \( \beta_1, \ldots, \beta_N \) of \( \Psi^+ \) such that \( \beta_j \neq \beta_i \) for \( i < j \) and define \( B \)-submodules of \( u \) by \( m_i = \bigoplus_{j=i+1}^{N} g_{\beta_j} \) for \( i = 0, \ldots, N \). Then we define \( u_c = u/m_i \).

Let \( X \in u \). We recall from Definition 2.3 that each \( i = 1, \ldots, N \) is either an inert point or a ramification point of \( X \). Further, we recall from Lemma 2.5 that each \( U \)-orbit in \( u \) contains a unique \( \leq \)-minimal representative.

We now define some subsets of \( u \), that we require to prove \( \zeta_U(z) \) is a rational function.

Definition 3.2. We write \( C = \{ \text{in, ram} \}^N \).

(i) For \( c \in C \), we define
\[ u_c = \{ X \in u : i \text{ is an inert point of } X \text{ if and only if } c_i = \text{in} \}. \]

(ii) For \( c \in C \), we define \( u_c^{\text{min}} \) to consist of the elements of \( u_c \) that are the \( \leq \)-minimal representatives of their \( U \)-orbits.

We note that for most values of \( c \), \( u_c \) is empty; however, the following lemma says it is always a variety.

Lemma 3.3. For \( c \in C \), \( u_c \) is a \( K \)-subvariety of \( u \).

Proof. Define \( u_{c,i} \) to be the image of \( u_c \) under the natural projection \( u \to u_i \). We prove by induction on \( i \) that \( u_{c,i} \) is a subvariety of \( u_i \) defined over \( K \).

The case \( i = 0 \) is trivial so assume inductively that \( u_{c,i-1} \) is a \( K \)-subvariety of \( u_{i-1} \). We may identify \( u_i \), as a variety, with \( \prod_{j=1}^{i} g_{\beta_j} \), which in turn we may identify with \( u_{i-1} \times g_{\beta_i} \). Then \( u_{c,i-1} \times g_{\beta_i} \) is a \( K \)-subvariety of \( u_i \) (because \( u_{c,i-1} \) is a \( K \)-subvariety of \( u_{i-1} \)). Now we may complete the induction using Lemma 2.4. \( \square \)
We recall from Lemma 2.5 that $X = \sum_{i=1}^{N} a_i e_{\beta_i} \in u$ is the $\leq$-minimal representative of its $U$-orbit if $a_i = 0$ whenever $i$ is an inert point of $X$. Therefore, we clearly have

**Proposition 3.4.** $u_c^{\min}$ is a closed $K$-subvariety of $u_c$.

**Remark 3.5.** It is not clear whether the map from $u_c$ to $u_c^{\min}$ sending $X$ to the $\leq$-minimal representative of its $U$-orbit is a morphism of varieties. It is easy to check that if this map is a morphism, then $u_c^{\min}$ is a quotient for the action of $U$ on $u_c$.

We recall from Corollary 2.2 and Lemma 2.6 that the conjugacy classes of $U(q)$ correspond to the $F$-stable $\leq$-minimal representatives of $U$-orbits in $u$. Therefore, by construction, we have

$$k_U(q) = \sum_{c \in C} |u_c^{\min}(q)|.$$  

Hence,

$$\zeta_U(z) = \prod_{c \in C} \zeta(u_c^{\min}; z)$$

is a rational function in $z$ by Dwork's theorem (Theorem 1.3) and Proposition 3.4.

**Remark 3.6.** The varieties $u_c^{\min}$ give a parametrization of the $U$-orbits in $u$. However, this parametrization depends on the chosen enumeration of $\Psi^+$. Further, the parametrization is perhaps not too helpful, as it seems difficult to get a grasp of the structure of the $u_c^{\min}$ in general.

### 4. Rationality of $\zeta_{B,U}(z)$

#### 4.1. $\zeta_{B,U}^g(z)$

We extend the methods of §3.2 to the adjoint action of $B$ on $u$ to show that $\zeta_{B,U}^g(z)$ is a rational function in $z$. As before we fix an enumeration $\beta_1, \ldots, \beta_N$ of $\Psi^+$ such that $\beta_j \neq \beta_i$ for $i < j$. We define $m_i = \bigoplus_{j=i+1}^{N} g_{\beta_j}$ and $u_i = u/m_i$, for $i = 0, \ldots, N$.

We recall the definition of the set $C$ and, for $c \in C$, the $K$-varieties $u_c$ and $u_c^{\min}$ from Definition 3.2. It follows from the results in [8, §7], that each $u_c^{\min}$ is stable under the adjoint action of $T$ and the $B$-orbits in $u_c$ correspond to the $T$-orbits in the $u_c^{\min}$. Further, the $F$-stable $B$-orbits in $u_c$ correspond to the $F$-stable $T$-orbits in the $u_c^{\min}$: an $F$-stable $B$-orbit contains some $X \in u_c(q)$ and therefore the $\leq$-minimal representative $Y$ of the $U$-orbit of $X$ in $u_c$, and we have $Y \in u_c^{\min}(q)$ for some $c \in C$.

We now define some objects that we need to prove rationality of $\zeta_{B,U}^g(z)$.

**Definition 4.1.** For $c \in C$, we define $R_c = \{ i : c_i = \text{ram} \}$.

(i) Let $c \in C$ and $I \subseteq R_c$ and define $u_{c,I} \subseteq u_c^{\min}$ to consist of those $X = \sum_{i=1}^{N} a_i e_{\beta_i}$ such that $a_i \neq 0$ if and only if $i \in I$.

(ii) Let $c \in C$ and $I \subseteq R_c$. We define the set

$$\text{li}(I) = \{ i \in I \mid \beta_i \text{ is linearly independent of } \{ \beta_j \mid j \in I, j < i \} \}.$$  

Then $u_{c,I}^{\min} \subseteq u_{c,I}$ is defined to consist of those $X = \sum_{i=1}^{N} a_i e_{\beta_i}$ such that $a_i = 1$ if $i \in \text{li}(I)$.  

14
Lemma 4.2. Let \( c \in C \). Then:

(i) \( u_{c,I} \) is a \( T \)-stable \( K \)-subvariety of \( u^\text{min}_c \) for all \( I \subseteq R_c \), and we have

\[
u^\text{min}_c = \bigcup_{I \subseteq R_c} u_{c,I}
\]
as a disjoint union; and

(ii) \( u^\text{min}_{c,I} \) is a closed \( K \)-subvariety of \( u_{c,I} \), for each \( I \subseteq R_c \).

Proof. For part (i), we first note that \( u_{c,I} \) is a locally closed \( K \)-subvariety of \( u^\text{min}_c \). It is clear that \( u_{c,I} \) is \( T \)-stable and that the union (4.1.1) is disjoint.

Part (ii) is obvious. \( \Box \)

In general, the \( T \)-orbits in \( u_{c,I} \) do not correspond to the points of the \( u^\text{min}_{c,I} \), see [8, Prop. 7.3]; so we have to continue our construction.

For \( c \in C \) and \( I \in R_c \), we define \( X_{c,I} = \sum_{i \in \mu(I)} e_{c_i} \) and \( X_c = \sum_{i \in I} e_{c_i} \). According to [8, Prop. 7.3], the quotient group \( A_{c,I} = C_T(X_{c,I})/C_T(X_c) \) is finite and the \( T \)-orbits in \( u_{c,I} \) correspond to the \( A_{c,I} \)-orbits in \( u^\text{min}_{c,I} \).

The next proposition allows us to complete our proof that \( \zeta^g_{B,U}(z) \) is a rational function.

Proposition 4.3. There exists a quotient \( \pi_{c,I} : u^\text{min}_{c,I} \to \bar{u}^\text{min}_{c,I} \) of \( u^\text{min}_{c,I} \) by \( A_{c,I} \) over \( K \). Further, the points of \( \bar{u}^\text{min}_{c,I} \) correspond to the \( T \)-orbits in \( u_{c,I} \) and the \( \mathbb{F}_q \)-rational points of \( \bar{u}^\text{min}_{c,I} \) correspond to the \( \mathbb{F}_q \)-stable \( A_{c,I} \)-orbits in \( u^\text{min}_{c,I} \).

Proof. Thanks to [2, Prop. 6.15], there exists a quotient of \( u^\text{min}_{c,I} \) by \( A_{c,I} \) over \( K \) as in the statement. The \( \mathbb{F}_q \)-rational points of \( \bar{u}^\text{min}_{c,I} \) correspond to the \( \mathbb{F}_q \)-stable \( A_{c,I} \)-orbits in \( u^\text{min}_{c,I} \).

We note that [2, Prop. 6.15] only gives quotients for the action of a finite group on an affine variety; however, we can deduce the existence of the required quotient because \( u^\text{min}_{c,I} \) is obtained from the affine variety \( \{ \sum_{i \in I} a_i e_{c_i} : a_i \in k^\times \} \), by taking \( A_{c,I} \)-stable open and closed subvarieties. The proposition now follows from the discussion before its statement. \( \Box \)

We recall that the \( \mathbb{F}_q \)-stable \( B \)-orbits in \( u \) correspond to the \( \mathbb{F}_q \)-stable \( T \)-orbits in the \( u^\text{min}_c \)’s. Therefore, by (4.1.1) and Proposition 4.3, we have

\[ k^g_{B,U}(q) = \sum_{c \in C} \sum_{I \subseteq R_c} |\bar{u}^\text{min}_{c,I}(q)|. \]

Hence,

\[ \zeta^g_{B,U}(z) = \prod_{c \in C} \prod_{I \subseteq R_c} \zeta(\bar{u}^\text{min}_{c,I};z) \]
is a rational function in \( z \) by Dwork’s theorem (Theorem 1.3) and Proposition 4.3.

Remark 4.4. Thanks to [8, Rem. 7.4], in the case \( G \) is of type \( A_r \) we have that \( A_{c,I} \) is the trivial group for all \( c, I \). Therefore, we can just work with the varieties \( u^\text{min}_{c,I} \) (and we do not need to introduce \( \bar{u}^\text{min}_{c,I} \)).

Remark 4.5. The main result of [10], allows an alternative proof of the rationality of \( \zeta^g_{B,U}(z) \), where we do not need to take quotients. We now outline how this works.
Let \( I \subseteq R_c \) and define \( \Gamma = \{ \beta_i : i \in I \} \). Then the main result of [10] says there is a subset \( \Delta \) of \( \Gamma \) such that \( \Delta \) is a \( \mathbb{Z} \)-basis for the lattice \( \mathbb{Z} \Gamma \). Let \( J = \{ i \in I : \beta_i \in \Delta \} \) and define
\[
u_{c,I,J}^{\text{min}} = \left\{ X = \sum_{i=1}^{N} a_i e_{\beta_i} \in \nu_{c,I} : a_i = 1 \text{ if } i \in J \right\}.
\]
Then, one can check that each \( T \)-orbit in \( \nu_{c,I} \) has a unique representative in \( \nu_{c,I,J}^{\text{min}} \). Therefore, the \( B \)-orbits in \( \nu \) are in correspondence with the points of the \( \nu_{c,I,J}^{\text{min}} \).

The author has chosen not to use this argument as the proof in [10] involves case by case checking and computer calculations.

4.2. \( \zeta_{B,U}(z) \). We continue to use the notation of the previous subsection. In particular, we require the objects introduced in Definition 4.1 and the quotient \( \bar{\nu}_{c,I} \) from Proposition 4.3. Further, we require the following notation to distinguish between certain zeta functions: for a \( K \)-variety \( V \), we write
\[
\zeta(V, q^a_0; z) = \exp \left( \sum_{s=1}^{\infty} \frac{\left| V(q^n_0) \right|}{s} z^s \right).
\]

We show that \( \zeta_{B,U}(z) \) is a rational function in \( z \) using Lemma 2.12 and the rationality of \( \zeta(\bar{\nu}_{c,I}^{\text{min}}, q^a_0; z) \) for any \( n \in \mathbb{Z}_{\geq 1} \) (\( c \in C, I \subseteq R_c \)).

Fix \( c \in C \) and \( I \subseteq R_c \). Define \( \Gamma = \{ \beta_i : i \in I \} \) and \( X = \sum_{\beta \in \Gamma} e_{\beta} \). The next lemma, which follows from the definition of \( \nu_{c,I} \), is important for our proof that \( \zeta_{B,U}(z) \) is a rational function. Although it is not necessarily true that \( X \in \nu_{c,I} \), we do have

**Lemma 4.6.** If \( Y \in \nu_{c,I} \), then \( C_T(Y) = C_T(X) \).

As in §2.5 we write \( Z(X) \) for the component group \( C_T(X)/C_T(X)^0 \). We recall that information about the Galois cohomology set \( H^1(F, Z(X)) \) is given in Lemma 2.12. Let \( n \) be the splitting number of \( A = \mathbb{Z} \Gamma \) (see Definition 2.11) and let \( 1 = n_1 < \cdots < n_m = n \), be all the divisors of \( n \). Let \( u_1, \ldots, u_m \) be the positive integers such that \( |H^1(F, Z(X))| = u_i \) if the highest common factor of \( s \) and \( n \) is \( n_i \), see Lemma 2.12; and recall that if \( v_i \) is defined inductively by \( u_i = \sum_{j \in D_i} v_j \) (where \( D_i = \{ i : n_i \text{ divides } n_i \} \), then \( v_i \) is divisible by \( n_i \).

We define \( b_{c,I}(q) \) to be the number of \( B(q) \)-orbits in \( u(q) \) which intersect \( \nu_{c,I} \) nontrivially. Then, if the highest common factor of \( s \) and \( n \) is \( n_i \),
\[
b_{c,I}(q) = \sum_{j \in D_i} v_j |\bar{\nu}_{c,I}^{\text{min}}(q)|,
\]
by Lemma 2.7 and Proposition 4.3. Dwork’s theorem implies \( \zeta(\bar{\nu}_{c,I}^{\text{min}}, q^a_0; z) \) is a rational function, for each \( i \). It now follows from Lemma 2.18 that
\[
\eta_{c,I}(z) = \exp \left( \sum_{s=1}^{\infty} \frac{b_{c,I}(q^a_0)}{s} z^s \right)
\]
is a rational function in \( z \).

We have, by construction, that \( k_{B,U}(q) = \sum_{c \in C} \sum_{I \subseteq R_c} b_{c,I}(q) \), so that
\[
\zeta_{B,U}(z) = \prod_{c \in C} \prod_{I \subseteq R_c} \eta_{c,I}(z).
\]
Hence, $\zeta_{B,U}(z)$ is a rational function in $z$.

Remark 4.7. We note that in the case $G = \text{GL}_n$, the centralizer $C_T(X)$ is connected for any $X \in \mathfrak{u}$. Therefore, in this case $\zeta_{B,U}(z) = \zeta_{B,U}^g(z)$, so the proof of rationality of $\zeta_{B,U}(z)$ is simplified.

Further, one can check that the proof can be simplified if $G$ is a symplectic or special orthogonal group. In this case the component group $C_T(X)/C_T(X)^0$ has exponent 2, for all $\leq$-minimal representatives $X \in \mathfrak{u}$. Therefore, the Galois cohomology set $H^1(F, Z(X))$ does not depend on $q$ and the proof of rationality of $\zeta_{B,U}(z)$ is easier.

In the following two examples we illustrate the arguments in this section and those in §2.5.

Example 4.8. We consider the case when $G$ is simple of type $G_2$, in this case it is straightforward to calculate $\zeta_{B,U}(z)$. Since the root lattice and weight lattice coincide for $G$ of type $G_2$ we have that $G$ is both simply connected and adjoint. We take $q_0 = p$ and we assume that $p \neq 1 \pmod{3}$; the case $p = 1 \pmod{3}$ is easier. Recall that we are assuming that $p$ is good for $G$ so we also have $p \neq 2, 3$. The example shows that the number of $B(q)$-conjugacy classes in $U(q)$ is given by two polynomials depending on the value of $q \pmod{3}$.

We take the enumeration $\beta_1 = 10, \beta_2 = 01, \beta_3 = 11, \beta_4 = 21, \beta_5 = 31, \beta_6 = 32$ of $\Psi^+$, using the notation for the roots from [3, Planche IX]. Using the results in [8, §7] (see §2.3) and Lemmas 2.7, 2.9 and 2.12 it is easy to check that the contents of Table 1 below are correct; they can also be read from [4, Table 2: Case G2R], although the case corresponding to $j = 5$ in the table below is not explained fully in [4].

The first column of Table 1 gives a label $j$ to the row. In the second column of the table we give the values of $c_j$ and $I_j$ for which $u_{c_j, I_j}$ is nonempty; we give a 6-tuple $(d_1, d_2, d_3, d_4, d_5, d_6)$ where

$$d_i = \begin{cases} 
i & \text{if } c_i = \text{in} \\ n & \text{if } c_i = \text{ram} \text{ and } i \in I \\ z & \text{if } c_i = \text{ram} \text{ and } i \notin I. \end{cases}$$

In the third column the values of $|\tilde{u}_{c_j, I_j}(q)|$ are given. Then in the fourth column the structure of $Z(X_j)$ is given, where $X_j = \sum_{i \in I_j} e_{\beta_i}$. The last column gives the number $b_{c_j, I_j}(q)$ of $B(q)$-orbits which intersect $u_{c_j, I_j}$ non-trivially.

We note that the case $j = 5$ gives the only instance, when there is more than one $T$-orbit in $u_{c, I_j}$. Further, we note that in this case $u_{c,I}(q)$ has size $2q - 2$, and $A_{c, I}$, which has order 2, acts non-trivially, see [8, Exmp. 7.5]. The only case where the Galois cohomology set $H^1(F, Z(X_j))$ depends on $q$ is $j = 6$.

We recall the standard identity:

$$\exp\left(\sum_{s=1}^{\infty} \frac{1}{s} z^s\right) = \frac{1}{1 - z}.$$

Then it is straightforward to check the contents of Table 2 using Lemmas 2.17 and 2.18, for which we recall that

$$\eta_{c_j, I_j}(z) = \exp\left(\sum_{s=1}^{\infty} \frac{b_{c_j, I_j}(q_0^s)}{s} z^s\right).$$
Therefore, we get
\[ \zeta_{B,U}(z) = \frac{1}{(1-z)^{18}(1-pz)(1-z^2)}. \]

**Example 4.9.** We consider the case \( G = SL_{18} \) and \( q_0 = p \), which we assume satisfies \( p \neq 2, 3 \) and \( p \neq \pm 1 \pmod{9} \); it is straightforward to adapt the methods below to other values of \( q_0 \). An enumeration \( \beta_1, \ldots, \beta_N \) of \( \Psi^+ \) is chosen so that \( \{\beta_1, \ldots, \beta_{17}\} = \Pi \). The \( B \)-orbit of a regular nilpotent element in \( u \) is \( u_{c,I} \), where \( c_i = \text{ram} \) for \( i = 1, \ldots, 17 \), \( c_i = \text{in} \) for \( i > 17 \), and \( I = \{1, \ldots, 17\} \). Below we calculate
\[ \eta_{c,I}(z) = \exp \left( \sum_{s=1}^{\infty} \frac{b_{c,I}(p^s)}{s} z^s \right). \]
Let \( \Gamma = \{ \beta_i : i \in I \} = \Pi \); then \( \mathbb{Z}\Gamma \) is the root lattice \( \mathbb{Z}\Psi \). We set \( X = \sum_{a \in \Pi} e_a \). Since \( \mathbb{Z}\Gamma = \mathbb{Z}\Psi \), we have that \( C_T(X) \) coincides with the centre of \( G \) which is isomorphic to \( \mathbb{Z}_{18} \). Hence we have \( Z(X) = C_T(X)/C_T(X)^9 = \mathbb{Z}_{18} \).

We have that \( |\eta_{c,I}^{|\mu^{\text{fin}}_{c,I}}| = 1 \). Therefore, \( b_{c,I}(q) = |H^1(F, \mathbb{Z}(X))| \), by Lemma 2.7. By the proof of Lemma 2.12, \( |H^1(F, \mathbb{Z}(X))| \) is the number of 18th roots of unity in \( \mathbb{F}_q \). Now \( \pm 1 \in \mathbb{K} \) are the square roots of 1, so the splitting field of \( x^9 - 1 \) over \( \mathbb{K} \) is the same as the splitting field of \( x^9 - 1 \). Further, the number of 18th roots of unity in \( \mathbb{F}_q \) is twice the number of 9th roots of unity in \( \mathbb{F}_q \).

The splitting field of \( x^9 - 1 \) over \( \mathbb{K} = \mathbb{F}_p^r \) (because 6 is the least positive integer \( n \) such that 9 divides \( p^n - 1 \)); so 6 is the splitting number of \( \mathbb{Z}\Gamma \). The divisors of 6 are \( n_1 = 1, n_2 = 2, n_3 = 3, n_4 = 6 \). It easy to check that the number of 9th roots of unity in \( \mathbb{F}_p^r \) is 1 if \( \text{hcf}(s, 6) \in \{1, 3\} \); 3 if \( \text{hcf}(s, 6) = 2 \); 9 if \( \text{hcf}(s, 6) = 6 \).

Therefore, we have
\[
b_{c,I}(q) = \begin{cases} 
2 & \text{if } \text{hcf}(s, 6) \in \{1, 3\} \\
6 & \text{if } \text{hcf}(s, 6) = 2 \\
18 & \text{if } \text{hcf}(s, 6) = 6 
\end{cases}
\]

and
\[
\sum_{s=1}^{\infty} \frac{b_{c,I}(p^s)}{s} z^s = \sum_{s=1}^{\infty} \frac{2}{s} z^s + \sum_{s=1}^{\infty} \frac{4}{2s} z^{2s} + \sum_{s=1}^{\infty} \frac{12}{6s} z^{6s}.
\]

Hence,
\[
\eta_{c,I}(z) = \exp \left( \sum_{s=1}^{\infty} \frac{b_{c,I}(p^s)}{s} z^s \right)
\]
\[
= \exp \left( \sum_{s=1}^{\infty} \frac{1}{s} z^s \right) \exp \left( \sum_{s=1}^{\infty} \frac{1}{s} z^{2s} \right) \exp \left( \sum_{s=1}^{\infty} \frac{1}{s} z^{6s} \right)^2
\]
\[
= \frac{1}{(1 - z)^2(1 - z^2)^2(1 - z^6)^2}.
\]

5. Rationality of \( \zeta_B(z) \)

We use Jordan decompositions to deduce the rationality of \( \zeta_B(z) \) from the rationality of \( \zeta_{B_L,U_L}(z) \) for certain pseudo-Levi \( K \)-subgroups \( L \) of \( \mathbb{G} \) \( (B_L = B \cap L \) and \( U_L = U \cap L) \). Our arguments are similar to those used for the Glauberman correspondence, cf. [7]. We include all arguments for the reader’s convenience.

Let \( x \in B(q) \). We have the Jordan decomposition \( x = su \), where \( s \in B \) is semisimple and \( u \in C_B(s) \), see [2, Thm. 4.4]. Moreover, the uniqueness of the Jordan decomposition implies that \( s \in B(q) \) and \( u \in C_B(s)(q) \). Up to conjugacy in \( B(q) \) we may assume that \( s \in T(q) \).

We require the description of the \( B(q) \)-conjugacy classes given in Proposition 5.2 below. The proposition is a consequence of the following lemma.

**Lemma 5.1.** Let \( s, s' \in T \) and \( u, u' \in U \). Suppose \( x = su \) and \( x' = s'u' \) are conjugate in \( B \). Then \( s = s' \).
Proof. Let $b \in B$ be such that $b_{\text{sub}}^{-1} = s'u'$. We may write $b$ (uniquely) as $vt$ with $v \in U$ and $t \in T$. Then

$$b_{\text{sub}}^{-1} = (vtst^{-1}v^{-1})(bub^{-1}) = (usv^{-1})\hat{u} = s(s^{-1}vs)v^{-1}\hat{u} = s\hat{u},$$

where $\hat{u} = bub^{-1}$, $\hat{u} = (s^{-1}vs)v^{-1}\hat{u} \in U$. Now the uniqueness of the decomposition $x' = s'u'$ with $s' \in T$ and $u' \in U$ implies $s = s'$ (and $u' = \hat{u}$).

Proposition 5.2. The conjugacy classes of $B(q)$ are given by pairs $(s, \hat{u})$, where $s \in T(q)$ and $\hat{u}$ is a $C_B(s)(q)$-conjugacy class in $C_U(s)(q)$.

We recall from §2.6 that for $t \in T$ the lattice $A(t) \subseteq X^*(T)$ is defined to be maximal subject to killing $t$; and $\Delta$ is defined to be the set of all sublattices $A$ of $X^*(T)$ such that $A = A(t)$ for some $t \in T$. For $A \in \Delta$ the pseudo-Levi subgroup $L(A)$ of $G$ is defined to be the subgroup of $G$ generated by $T$ along with the root subgroups $U_\alpha$ for $\alpha \in A \cap \Psi$. We recall from §2.6 that for $t \in T$ and $A \in \Delta$, we have $C_G(t)^0 = L(A)$ if and only if $A(t) = A$.

We note that $L(A)$ is $K$-split (because $T \subseteq L(A)$), reductive ([14, Lem. 14]) and $p$ is good for $L(A)$ ([14, Lem. 17]). One can see that $B_{L(A)} = B \cap L(A)$ is a Borel subgroup of $L(A)$ with unipotent radical $U_{L(A)} = U \cap L(A)$. Therefore, the zeta function $\zeta_{B_{L(A)}, U_{L(A)}}(z)$ is a rational function in $z$, by §4.2.

We recall the definition of the splitting number $n$ of $\Delta$ from Definition 2.14. Let $1 = n_1 < \cdots < n_m = n$ be all divisors of $n$. For $A \in \Delta$ let $f_{A,i}(x) \in \mathbb{Z}[x]$ $(i = 1, \ldots, m)$ be such that if the highest common factor of $s$ and $n$ is $n_i$, then the number of $t \in T(q)$ with $A(t) = A$ is equal to $f_{A,i}(q)$ (see Lemma 2.16(i)). We recall from Lemma 2.16(ii) that if $g_{A,i}(x)$ is defined inductively by $f_{A,i}(x) = \sum_{j \in D_i} g_{A,j}(x)$ (where $D_i = \{ j < i : n_j \text{ divides } n_i \}$), then all coefficients of $g_{A,i}(x)$ are divisible by $n_i$.

We define

$$h_A(q) = f_{A,i}(q) = \sum_{j \in D_i} g_{A,j}(q)$$

when the highest common factor of $s$ and $n$ is $n_i$. As remarked above each coefficient $g_{A,i}(x)$ is divisible by $n_i$. Also by §4.2

$$\zeta_{B_{L(A)}, U_{L(A)}}(q_0^n; z) = \exp \left( \sum_{s=1}^{\infty} \frac{k_{B_{L(A)}, U_{L(A)}}(q_0^n; s)}{s} z^s \right)$$

is rational, for each $i$. Therefore,

$$\theta_A(z) = \exp \left( \sum_{s=1}^{\infty} \frac{h_A(q_0^n; k_{B_{L(A)}, U_{L(A)}}(q_0^n; s))}{s} z^s \right)$$

is rational, by Lemma 2.19.

Using Proposition 5.2, we see that the number of conjugacy classes of $B(q)$ is

$$\sum_{A \in \Delta} h_A(q) k_{B_{L(A)}, U_{L(A)}}(q).$$

Therefore,

$$\zeta_B(z) = \prod_{A \in \Delta} \theta_A(z).$$

As each function in this product is rational, we deduce that $\zeta_B(z)$ is a rational function in $z$.\]
References


Institut for Matematiske Fag, Aarhus Universitet, DK-8000, Aarhus C, Denmark.
E-mail address: goodwin@imf.au.dk
URL: http://home.imf.au.dk/goodwin