COUNTING POINTS OF HOMOGENEOUS VARIETIES OVER FINITE FIELDS

by

Michel Brion and Emmanuel Peyre

Abstract. — Let X be an algebraic variety over a finite field $\mathbf{F}_q$, homogeneous under a linear algebraic group. We show that there exists an integer N such that for any positive integer n in a fixed residue class mod N, the number of rational points of X over $\mathbf{F}_{q^n}$ is a polynomial function of q^n with integer coefficients. Moreover, the shifted polynomials, where q^n is formally replaced with $q^n + 1$, have non-negative coefficients.

Résumé. — Soit X une variété algébrique sur un corps fini $\mathbf{F}_q$ homogène sous un groupe algébrique linéaire. Nous démontrons que le nombre de points rationnels de X sur $\mathbf{F}_{q^n}$ est une fonction périodiquement polynomiale en q^n avec des coefficients entiers. De plus, les polynômes obtenus en remplaçant formellement q^n par $q^n + 1$ sont à coefficients positifs.

1. Introduction and statement of the results

Given an algebraic variety X over a finite field $k = \mathbf{F}_q$, one may consider the points of X which are rational over an arbitrary finite field extension $\mathbf{F}_{q^n}$. The number of these points is given by Grothendieck's trace formula,

$$|X(\mathbf{F}_{q^n})| = \sum_{i \geqslant 0} (-1)^i \operatorname{Tr}\left(F^n, H_c^i(X)\right), \tag{1.1}$$

where F denotes the Frobenius endomorphism of $X_{\bar{k}}$ and $H_c^i(X)$ stands for the ith ℓ-adic cohomology group of $X_{\bar{k}}$ with proper supports, ℓ being a prime not dividing q (see e.g. [**De77**, Thm. 3.2,p. 86]). Moreover, by celebrated results of Deligne (see [**De74, De80**]), each eigenvalue α of F acting on $H_c^i(X)$ is an algebraic number, and all the complex conjugates of α have absolute value $q^{\frac{w}{2}}$

for some non-negative integer $w \leqslant i$, with equality if X is smooth and complete. This implies the general properties of the counting function $n \mapsto |X(\mathbf{F}_{q^n})|$ predicted by the Weil conjectures.

We shall obtain more specific properties of that function under the assumption that X is *homogeneous*, i.e., admits an action of an algebraic group G over k such that $X(\bar{k})$ is a unique orbit of $G(\bar{k})$; then X is of course smooth, but possibly non-complete. We begin with a structure result for these varieties:

Theorem 1.1. — *Let X be a homogeneous variety over a finite field k. Then*

$$X \cong (A \times Y)/\Gamma, \tag{1.2}$$

where A is an abelian k-variety, Y is a homogeneous k-variety under a connected linear algebraic k-group H, and Γ is a finite commutative k-group scheme which acts faithfully on A by translations, and acts faithfully on Y by automorphisms commuting with the action of H.

Moreover, A, Y and Γ are unique up to compatible isomorphisms, Y/Γ is a homogeneous k-variety under H, and there is a canonical isomorphism

$$H_c^*(X) \cong H^*(A) \otimes H_c^*(Y/\Gamma). \tag{1.3}$$

In particular,

$$|X(\mathbf{F}_{q^n})| = |A(\mathbf{F}_{q^n})| \ |(Y/\Gamma)(\mathbf{F}_{q^n})|. \tag{1.4}$$

Theorem 1.1 is deduced in Section 2 from a structure result for algebraic groups over finite fields, due to Arima (see [**Ar60**]).

In view of (1.4) and the known results on the counting function of abelian varieties, we may concentrate on homogeneous varieties under linear algebraic groups. For these, we obtain:

Theorem 1.2. — *Let X be a variety over $\mathbf{F}_q$, homogeneous under a linear algebraic group. Then $|X(\mathbf{F}_{q^n})|$ is a periodic polynomial fonction of q^n with integer coefficients.*

By this, we mean that there exist a positive integer N and polynomials $P_0(t), \ldots, P_{N-1}(t)$ in $\mathbf{Z}[t]$ such that

$$|X(\mathbf{F}_{q^n})| = P_r(q^n) \quad \text{whenever} \quad n \equiv r \pmod{N}. \tag{1.5}$$

We then say that N is a *period* of the function $q^n \mapsto |X(\mathbf{F}_{q^n})|$.

Notice that $|X(\mathbf{F}_{q^n})|$ is generally not a polynomial function of q^n. For example, if $\mathrm{char}(k) \neq 2$, then the affine conic $X \subset \mathbf{A}^2_k$ with equation $x^2 - ay^2 = b$ is homogeneous under the corresponding orthogonal group and satisfies $|X(\mathbf{F}_{q^n})| = q^n - \varepsilon$, where $\varepsilon = 1$ if a is a square in $\mathbf{F}_{q^n}$, and $\varepsilon = -1$ otherwise.

Theorem 1.2 is proved in Section 3, by showing that each eigenvalue of F acting on $H^*_c(X)$ is the product of a non-negative integer power of q with a root of unity (Proposition 3.1). As a consequence, there exists a unique polynomial $P_X(t) \in \mathbf{Z}[t]$ such that

$$P_X(q^n) = |X(\mathbf{F}_{q^n})| \tag{1.6}$$

for any sufficiently divisible, positive integer n. Our third result yields a factorization of that polynomial:

Theorem 1.3. — *Let X be a variety over $\mathbf{F}_q$, homogeneous under a linear algebraic group, and let $P_X(t)$ be the polynomial satisfying (1.6). Then there exists a non-negative integer r such that*

$$P_X(t) = (t-1)^r Q_X(t), \tag{1.7}$$

where $Q_X(t)$ is a polynomial with non-negative integer coefficients.

This result follows from [**BP02**, Thm. 1] when X is obtained from a complex homogeneous variety by reduction modulo a large prime. However, certain homogeneous varieties over finite fields do not admit any lift to varieties in characteristic zero (see [**LR97**] for specific examples). Also, the approach of [**BP02**] relies on the existence of Levi subgroups, which fails in our setting, and on arguments of equivariant cohomology which would require non-trivial modifications.

We present a proof of Theorem 1.3 in Section 4; it combines the reduction steps of Section 3 with a result adapted from [**BP02**] in a simplified form (Lemma 4.1, the only ingredient which relies on methods of ℓ-adic cohomology).

In Section 5, we show how to replace this ingredient with arguments of invariant theory, along the lines of classical results of Steinberg (see [**St68**, §14]). This yields elementary proofs of Theorems 1.2 and 1.3, and also of our most surprising result:

Theorem 1.4. — *Let X be a variety over $\mathbf{F}_q$, homogeneous under a linear algebraic group, and let $P_0(t), \ldots, P_{N-1}(t)$ be the polynomials satisfying (1.5). Then the shifted polynomials $P_0(t+1), \ldots, P_{N-1}(t+1)$ have non-negative coefficients.*

A similar positivity result has been conjectured by Mozgovoy and Reineke in the setting of quiver moduli (see [**MR07**, Rem. 6.5] and also [**Re08**, Conj. 8.5]).

They also observed that the existence of a decomposition of the considered moduli spaces into locally closed tori would yield a geometric explanation for their positivity property. Note that such a decomposition generally does not exist in the setting of homogenenous varieties under linear algebraic groups, since some of these varieties are not rational over $\bar{k}$ (this follows from results of Saltman, see [**Sa84a, Sa84b**]). This raises the question of finding a (geometric or combinatorial) interpretation of the coefficients of our shifted polynomials.

Acknowledgements. We thank J.-P. Serre and D. Timashev for their interest in our results, and for useful suggestions. Also, we thank the referee for his careful reading and valuable comments.

Notation and conventions. Throughout this article, we fix a finite field k of characteristic p, with q elements. Also, we fix an algebraic closure $\bar{k}$ of k. For any positive integer n, we denote by $\mathbf{F}_{q^n}$ the unique subfield of $\bar{k}$ with q^n elements; in particular, $k = \mathbf{F}_q$.

By a *variety*, we mean a geometrically integral, separated scheme of finite type over k; morphisms (resp. products) of varieties are understood to be over k. An *algebraic group* G is a smooth group scheme of finite type over k; then each connected component of G is a variety. The identity element of G is denoted by e_G. Notice that every algebraic subgroup of G is "defined over k" with our conventions.

For any variety X, we set

$$X_{\mathbf{F}_{q^n}} := X \times_k \mathbf{F}_{q^n}, \quad X_{\bar{k}} := X \times_k \bar{k},$$

and we denote by F the Frobenius endomorphism of $X_{\bar{k}}$.

Given a prime number $\ell \neq p$, we set for simplicity

$$H^i(X) := H^i(X_{\bar{k}}; \mathbf{Q}_\ell),$$

the ith ℓ-adic cohomology group of $X_{\bar{k}}$. Our notation for cohomology with proper supports is

$$H^i_c(X) := H^i_c(X_{\bar{k}}; \mathbf{Q}_\ell).$$

We shall use [**DG70, Sp98**] as general references for algebraic groups, and [**De77, Mi80**] for étale cohomology.

2. Proof of Theorem 1.1

We may choose a connected algebraic group G such that X is homogeneous under G. By [**Ar60**, Thm. 1] (see also [**Ro61**, Thm. 4]), we have $G = AH$,

where A is the largest abelian subvariety of G, and H is the largest connected linear algebraic subgroup of G; moreover, A and H centralize each other. So $G \cong (A \times H)/(A \cap H)$, and we may assume that

$$G = A \times H.$$

Replacing A and H with quotient groups, we may also assume that they both act faithfully on X.

Let G_X denote the kernel of the G-action on X. Then G_X is isomorphic to a subgroup of A (via the first projection) and also to a subgroup of H. Since A is complete and H is affine, it follows that G_X is finite.

Also, X contains a k-rational point x by Lang's theorem (see [**La56**, Thm. 2]). Denote by G_x its isotropy subgroup-scheme; then G_x is linear by the finiteness of G_X together with [**Ma63**, Lem. p. 154]. In particular, the reduced neutral component K of G_x (a closed normal subgroup of G_x) is contained in H. Let $\Gamma := G_x/K$; then Γ is a finite group scheme acting on G/K on the right via the action of G_x on G by right multiplication, and

$$X \cong G/G_x \cong (G/K)/\Gamma \cong (A \times Y)/\Gamma,$$

where $Y := H/K$. Denoting by $N_G(K)$ the normalizer of K in G, we have

$$\Gamma \subset N_G(K)/K = A \times N_H(K)/K.$$

Let Γ' denote the kernel of the projection of Γ to A. Then Γ' (resp. Γ/Γ') is isomorphic to a subgroup scheme of $N_H(K)/K$ (resp. of A), and

$$X \cong \Big(A \times (Y/\Gamma')\Big)/(\Gamma/\Gamma').$$

Thus, we may assume that Γ acts faithfully on A by translations. On the other hand, Γ acts H-equivariantly on Y via the action of $N_H(K)/K$ on H/K on the right, and the kernel of this action is isomorphic to a subgroup scheme of A which acts trivially on X. Thus, Γ acts faithfully on Y. This completes the proof of (1.2).

To show the uniqueness of (A, Y, Γ), we begin with a general observation:

Lemma 2.1. — *Let X be a variety over an arbitrary field. Then there exists an abelian variety A_X acting faithfully on X, such that any action of an abelian variety A on X arises from a unique homomorphism $A \to A_X$. Moreover, A_X centralizes any connected algebraic group of automorphisms of X.*

Proof. — Consider an abelian variety A and a connected algebraic group G, both acting faithfully on X. Then the morphism

$$f : A \times G \times X \longrightarrow X, \quad (a, g, x) \longmapsto aga^{-1}g^{-1}x$$

satisfies $f(a, e_G, x) = x$. By the rigidity lemma of [**Mu70**, p. 43], it follows that f factors through the projection $p_{23} : A \times G \times X \to G \times X$. But $f(e_A, g, x) = x$, so that f factors through the projection $p_3 : A \times G \times X \to X$. In other words, A centralizes G.

On the other hand, A stabilizes the smooth locus U of X. By a theorem of Nishi and Matsumura, the induced action of A on the Albanese variety of U has a finite kernel (see [**Ma63**], or [**Br07**, Thm. 2] for a more modern version). In particular, $\dim(A) \leqslant \dim(U) = \dim(X)$.

Combining these two steps yields our statement. □

Remark 2.2. — For a variety X, there may exist an infinite sequence $G_1 \subset G_2 \subset \cdots G_n \subset \cdots$ of closed connected algebraic groups, all acting faithfully and transitively on X. This happens e.g. for the variety $X = (\mathbf{A}^1 - \{0\}) \times \mathbf{A}^1$ and the group G_n consisting of automorphisms

$$x \longmapsto ax, \quad y \longmapsto y + P(x),$$

where $a \in \mathbf{G}_m$ and P is a polynomial of degree $\leqslant n$.

Returning to the situation of (1.2), we claim that $A_X = A$. To see this, consider the action of A on X via its action on itself by translations. The projection $p_2 : A \times Y \to Y$ induces a morphism

$$p : X \to Y/\Gamma \tag{2.1}$$

which is an A-torsor for the fppf topology (since the quotient morphism $Y \to Y/\Gamma$ is a Γ-torsor, and hence the square

$$\begin{array}{ccc} A \times Y & \xrightarrow{p_2} & Y \\ {\scriptstyle /\Gamma}\downarrow & & \downarrow{\scriptstyle /\Gamma} \\ X & \xrightarrow{p} & Y/\Gamma \end{array}$$

is cartesian). Also, note that the quotient variety

$$Y/\Gamma = X/A = G/G_x A$$

exists and is homogeneous under $H = G/A$. Thus, A is contained in A_X, and the quotient A_X/A acts on Y/Γ. Since any morphism from the connected linear algebraic group H to an abelian variety is constant, the Albanese variety of Y/Γ is

trivial. By the Nishi-Matsumura theorem again, it follows that the action of the abelian variety A_X/A on Y/Γ is trivial as well. In particular, each $A_X(\bar{k})$-orbit in $X(\bar{k})$ is an $A(\bar{k})$-orbit. This implies $\dim(A_X) = \dim(A)$, which proves our claim.

As a consequence, A (and Y/Γ) depend only on X. On the other hand, the natural map

$$q : X = (A \times Y)/\Gamma \longrightarrow A/\Gamma$$

is a morphism to an abelian variety, with fibers isomorphic to the homogeneous variety Y under H. It follows that q is the Albanese morphism of X. In particular, the subgroup scheme Γ of A, and the Γ-variety Y, depend only on X. This shows the desired uniqueness.

To prove the isomorphism (1.3), we first consider the case where the group scheme Γ is reduced. Then we have canonical isomorphisms

$$H_c^*(X) \cong H_c^*(A \times Y)^\Gamma \cong \Big(H^*(A) \otimes H_c^*(Y)\Big)^\Gamma$$

$$\cong H^*(A) \otimes H_c^*(Y)^\Gamma \cong H^*(A) \otimes H_c^*(Y/\Gamma),$$

where the first and last isomorphism follow from Lemma 2.3 (i) below, the second one from the Künneth isomorphism and the properness of A, and the third one holds since the action of Γ on $H^*(A)$ is trivial (indeed, Γ acts on A by translations).

In the general case, the reduced subscheme Γ_{red} is a finite subgroup of Γ, and the natural map

$$(A \times Y)/\Gamma_{\mathrm{red}} \to (A \times Y)/\Gamma = X$$

is finite and bijective on $\bar{k}$-rational points. By Lemma 2.3 (ii) below, it follows that

$$H_c^*(X) \cong H_c^*\Big((A \times Y)/\Gamma_{\mathrm{red}}\Big).$$

Together with the preceding step and Lemma 2.3 (ii) again, this yields the isomorphism (1.3).

Finally, (1.4) follows by combining (1.1) and (1.3) or, more directly, by considering the morphism (2.1): for any $z \in (Y/\Gamma)(\mathbf{F}_{q^n})$, the fiber X_z (a variety over $\mathbf{F}_{q^n}$) is a torsor under $A_{\mathbf{F}_{q^n}}$. By Lang's theorem, it follows that X_z contains $\mathbf{F}_{q^n}$-rational points, and these form a unique orbit of $A(\mathbf{F}_{q^n})$.

Lemma 2.3. — (i) *Let Γ be a finite group acting on a variety X such that the quotient morphism $f : X \to Y$ exists, where Y is a variety (this assumption is satisfied*

if X is quasi-projective, see [**Mu70**, p. 69]*. Then Γ acts on $H_c^*(X)$, and we have a canonical isomorphism*

$$H_c^*(Y) \cong H_c^*(X)^\Gamma.$$

(ii) *Let $f : X \to Y$ be a finite morphism of varieties, bijective on $\bar{k}$-rational points. Then we have a canonical isomorphism*

$$H_c^*(Y) \cong H_c^*(X).$$

Proof. — (i) Note that $f_!\mathbf{Q}_\ell = f_*\mathbf{Q}_\ell$ and $R^i f_!\mathbf{Q}_\ell = 0$ for all $i \geqslant 1$, since f is finite. This yields a canonical isomorphism

$$H_c^*(X) \cong H_c^*(Y_{\bar{k}}; f_*\mathbf{Q}_\ell). \tag{2.2}$$

Moreover, Γ acts on $f_*\mathbf{Q}_\ell$ and hence on $H_c^*(X)$. Thus, (2.2) restricts to an isomorphism

$$H_c^*(X)^\Gamma \cong H_c^*(Y_{\bar{k}}; (f_*\mathbf{Q}_\ell)^\Gamma).$$

To complete the proof, it suffices to show that the natural map from the constant sheaf $\mathbf{Q}_\ell$ to $f_*\mathbf{Q}_\ell$ induces an isomorphism $\mathbf{Q}_\ell \cong (f_*\mathbf{Q}_\ell)^\Gamma$. In turn, it suffices to prove that

$$H^0(X_{\bar{y}}; \mathbf{Q}_\ell)^\Gamma \cong \mathbf{Q}_\ell, \tag{2.3}$$

where $X_{\bar{y}}$ denotes the geometric fiber of f at an arbitrary point $y \in Y$. But $X_{\bar{y}}$ is a finite scheme over the field $\overline{\kappa(y)}$, equipped with an action of Γ which induces a transitive action on its set of connected components; this implies (2.3).

(ii) is checked similarly; here the map $\mathbf{Q}_\ell \to f_*\mathbf{Q}_\ell$ is an isomorphism. □

Remarks 2.4. — (i) Lemma 2.3 is certainly well-known, but we could not locate a specific reference. The first assertion is exactly [**Sr79**, (5.10)]; however, the proof given there is only valid for Γ-torsors.

(ii) If X in Theorem 1.1 is complete, then Γ is trivial in view of a result of Sancho de Salas (see [**SS03**]). Moreover, we have $Y \cong H/Q$, where Q is a subgroup scheme of H such that the reduced subscheme Q_{red} is a parabolic subgroup. It follows easily that $|Y(\mathbf{F}_{q^n})|$ is a polynomial function of q^n (for details, see Steps 1 and 3 in Section 4).

For an arbitrary homogeneous variety X, the subgroup scheme Γ is generally non-trivial. Indeed, consider an abelian variety A having a k-rational point p of order 2. Let also $Y := \mathrm{SL}(2)/T$, where $T \subset \mathrm{SL}(2)$ denotes the diagonal torus. The group Γ of order 2 acts on A via translation by p, and on Y via

right multiplication by the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which normalizes T; the variety $X := (A \times Y)/\Gamma$ is the desired example. One easily checks that

$$|(Y/\Gamma)(\mathbf{F}_{q^n})| = q^{2n}, \quad \text{whereas} \quad |Y(\mathbf{F}_{q^n})| = q^n(q^n + 1).$$

Thus, Y/Γ cannot be replaced with Y in the equality (1.4).

(iii) The isomorphism (1.2) only holds for homogeneous varieties defined over finite fields. Consider indeed a field k which is not algebraic over a finite subfield. By [**ST76**], there exists an elliptic curve C over k, having a k-rational point x of infinite order. Let L be the line bundle on C associated with the divisor $(x)-(0)$. Denote by G the complement of the zero section in the total space of L, and by $q : G \to C$ the projection; then q is a torsor under the multiplicative group $\mathbf{G}_m$. In fact, G has a structure of an algebraic group over k, extension of C by $\mathbf{G}_m$; in particular, q is the Albanese map. If the isomorphism (1.2) holds for G, then $C \cong A/\Gamma$ and $Y \cong \mathbf{G}_m$. Thus, G has non-constant regular functions, namely, the non-constant regular functions on the quotient $Y/\Gamma \cong \mathbf{G}_m$. In other words, there exists an integer $n \neq 0$ such that the power L^n has a non-zero section; but this is impossible, since L^n is a non-trivial line bundle of degree 0.

The above group G is an example of an anti-affine algebraic group in the sense of [**Br09**]. That article contains a classification of these groups, and further examples in characteristic zero.

3. Proof of Theorem 1.2

First, it suffices to show that $|X(\mathbf{F}_{q^n})|$ is a *periodic Laurent polynomial function of q^n with algebraic integer coefficients*, i.e., there exist a positive integer N and $P_0(t), \ldots, P_{N-1}(t) \in \bar{\mathbf{Z}}[t, t^{-1}]$ satisfying (1.5), where $\bar{\mathbf{Z}}$ denotes the ring of algebraic integers. Indeed, if $P(t) \in \bar{\mathbf{Z}}[t, t^{-1}]$ and $P(q^n)$ is an integer for infinitely many positive integers n, then $P(t) \in \mathbf{Z}[t]$.

Next, it suffices to show the following:

Proposition 3.1. — *Let X be a homogeneous variety under a linear algebraic group. Then each eigenvalue α of F acting on $H_c^*(X)$ is of the form ζq^j, where $\zeta = \zeta(\alpha)$ is a root of unity, and $j = j(\alpha)$ is an integer.*

Indeed, in view of Grothendieck's trace formula (1.1), that proposition implies readily that $|X(\mathbf{F}_{q^n})|$ is a periodic Laurent polynomial function of q^n, with coefficients being sums of roots of unity.

Before proving the proposition, we introduce two notions which will also be used in the proof of Theorem 1.3.

Definition 3.2. — We say that a variety X is *weakly pure*, if it satisfies the assertion of Proposition 3.1.

Also, X is *strongly pure* if $H_c^i(X) = 0$ for any odd i, and for any even i, each eigenvalue of F acting on $H_c^i(X)$ is of the form $\zeta q^{\frac{i}{2}}$, where ζ is a root of unity.

Clearly, any strongly pure variety X is weakly pure; it is also pure in the (usual) sense that all the complex conjugates of eigenvalues of F acting on $H_c^i(X)$ have absolute value $q^{\frac{i}{2}}$, for all i. Yet some weakly pure varieties are not pure, e.g., tori.

Weak and strong purity are preserved under base change by any finite extension; specifically, a variety X is weakly (resp. strongly) pure if and only if so is $X_{\mathbf{F}_{q^n}}$ for some (or for any) positive integer n. Further easy properties of these notions are gathered in the following:

Lemma 3.3. — (i) *Let Γ be a finite group acting on a variety X, such that the quotient variety $Y = X/\Gamma$ exists. If X is weakly (resp. strongly) pure, then so is Y.*
(ii) *Let $f : X \to Y$ be a finite morphism of varieties, bijective on $\bar{k}$-rational points. Then X is weakly (resp. strongly) pure if and only if so is Y.*
(iii) *Let Y be a closed subvariety of a variety X, with complement U. If both Y and U are weakly (resp. strongly) pure, then so is X.*

Proof. — (i) and (ii) follow from Lemma 2.3, and (iii) from the exact sequence $H_c^i(U) \longrightarrow H_c^i(X) \longrightarrow H_c^i(Y)$. □

Next, we obtain a result of independent interest, which is the main ingredient of the proof of Proposition 3.1:

Proposition 3.4. — *Let G be a connected linear algebraic group, and $\pi : X \to Y$ a G-torsor, where X and Y are varieties. Then X is weakly (resp. strongly) pure if and only if so is Y.*

Proof. — (i) We may choose a Borel subgroup B of G and a maximal torus T of B. Then π is the composite morphism

$$X \xrightarrow{\pi_T} X/T \xrightarrow{\varphi} X/B \xrightarrow{\psi} X/G = Y,$$

where π_T is a T-torsor, φ is smooth with fiber B/T isomorphic to the unipotent radical of B, and ψ is projective and smooth with fiber G/B, the flag variety of G.

We claim that X/T is weakly (resp. strongly) pure if and only if so it X/B. Indeed, B/T is isomorphic to an affine space $\mathbf{A}^d$, and hence $R^i\varphi_!\mathbf{Q}_\ell = 0$ for all $i \neq 2d$, while $R^{2d}\varphi_!\mathbf{Q}_\ell \cong \mathbf{Q}_\ell(-d)$ via the trace map. This yields a canonical isomorphism

$$H_c^i(X/B) \cong H_c^{i+2d}(X/T)(d).$$

Thus, the eigenvalues of F in $H_c^i(X/B)$ are exactly the products βq^{-d}, where β is an eigenvalue of F in $H_c^{i+2d}(X/T)$. This implies our claim.

Next, we claim that X/B is weakly (resp. strongly) pure if and only if so is X/G. Indeed, the Leray spectral sequence associated with the flag bundle ψ degenerates (since the cohomology ring of the fiber G/B is generated by Chern classes of line bundles associated with characters of B, and all such line bundles extend to X/B); moreover, the sheaves $R^j\psi_!\mathbf{Q}_\ell = R^j\psi_*\mathbf{Q}_\ell$ are constant. This yields an isomorphism of graded $\mathbf{Q}_\ell$-vector spaces with F-action

$$H_c^*(X/B) \cong H_c^*(X/G) \otimes H^*(G/B).$$

In particular, $H_c^*(X/G)$ may be identified with a F-stable subspace of $H_c^*(X/B)$. Thus, if X/B is weakly (resp. strongly) pure, then so is X/G. The converse holds since G/B is strongly pure (as follows from the Bruhat decomposition, see Step 3 in Section 4 for details).

By combining both claims, we may assume that $G = T$. Replacing k with a finite extension, we may further assume that T is split. Thus, we are reduced to the case where $G = T = \mathbf{G}_m$. Then we have the Gysin long exact sequence

$$\cdots H_c^i(X) \longrightarrow H_c^{i-2}(Y)(2) \xrightarrow{c_1(L)} H_c^i(Y) \longrightarrow H_c^{i+1}(X) \cdots,$$

where $c_1(L)$ denotes the multiplication by the first Chern class of the invertible sheaf L associated with the $\mathbf{G}_m$-torsor $\pi : X \to Y$. Thus, if Y is weakly (resp. strongly) pure, then so is X. The converse is obtained by decreasing induction on i, since $H_c^i(Y) = 0$ for each $i > 2\dim(Y)$, and F acts on $H_c^{2\dim(Y)}(Y)$ via multiplication by $q^{\dim(Y)}$. □

We may now prove Proposition 3.1. We have $X \cong G/H$, where G is a linear algebraic group, and H a closed subgroup scheme. Since X is a variety, we may assume that G is connected. Moreover, since the reduced subscheme H_{red} is a closed algebraic subgroup, and the natural map $G/H_{\mathrm{red}} \to G/H$ is finite and bijective on $\bar{k}$-rational points, we may assume that H is an algebraic group in view of Lemma 2.3(ii).

Applying Proposition 3.4 to the torsors $G \to \mathrm{Spec}(k)$ and $G \to G/H^0$ (where H^0 denotes the neutral component of H), we see that G and G/H^0 are weakly pure. Thus, so is $G/H \cong (G/H^0)/(H/H^0)$, by Lemma 3.3(i).

4. Proof of Theorem 1.3

As above, we consider a homogeneous variety $X = G/H$, where G is a connected linear algebraic group, and H is a closed subgroup scheme. We first reduce to the case where G is reductive, and H is a closed subgroup such that H^0 is a torus. For this, we carry out a sequence of four reduction steps, where we use elementary counting arguments rather than ℓ-adic cohomology and the Grothendieck trace formula, to prepare the way for the completely elementary proofs of Section 5.

Step 1. Since the natural map $(G/H_{\mathrm{red}})(\bar{k}) \to (G/H)(\bar{k})$ is bijective, we have $|(G/H)(\mathbf{F}_{q^n})| = |(G/H_{\mathrm{red}})(\mathbf{F}_{q^n})|$ for any positive integer n, and hence

$$P_{G/H}(t) = P_{G/H_{\mathrm{red}}}(t).$$

Replacing (G, H) with (G, H_{red}), we may thus assume that H *is an algebraic group*.

Step 2. The unipotent radical $R_u(G)$ acts on X, with quotient morphism the natural map $f : G/H \to G/R_u(G)H$. The fiber of f at any coset $gR_u(G)H$ equals

$$gR_u(G)H/H \cong R_u(G)/\Big(R_u(G) \cap gHg^{-1}\Big) \cong R_u(G)/g\Big(R_u(G) \cap H\Big)g^{-1}.$$

The induced map $(G/H)(\mathbf{F}_{q^n}) \to \Big(G/R_u(G)H\Big)(\mathbf{F}_{q^n})\Big)$ is surjective by Lang's theorem. Moreover, since $R_u(G)$ is connected and unipotent, each fiber has q^{nd} elements, where $d := \dim R_u(G)/\Big(R_u(G) \cap H\Big)$. Hence

$$P_{G/H}(t) = t^d P_{G/R_u(G)H}(t).$$

Replacing G with the quotient $G/R_u(G)$ and H with its image in that quotient, we may assume in addition that G *is reductive*.

Step 3. If H is not reductive, then it is contained in some proper parabolic subgroup P of G (see [**BT71**]). We may further assume that H is not contained in a proper parabolic subgroup of P; then the image of H in the reductive group $P/R_u(P)$ is reductive as well.

Choose a Borel subgroup B of P and a maximal torus T of B; denote by U the unipotent radical of B, and by $N_G(T)$ the normalizer of T in G. Then

$W := N_G(T)/T$ is the Weyl group of (G, T); it contains the Weyl group W_P of (P, T). Choose a set W^P of representatives in W of the quotient W/W_P. Also, for any $w \in W^P$, choose a representative $n_w \in N_G(T)$. Then, by the Bruhat decomposition, we have

$$G = \bigcup_{w \in W^P} Bn_w P, \tag{4.1}$$

where the $Bn_w P$ are disjoint locally closed subvarieties. Moreover, for any $w \in W^P$, there exists a closed subgroup U^w of U, normalized by T, such that the map

$$U^w \times P \longrightarrow Bn_w P, \quad (x, y) \longmapsto xn_w y \tag{4.2}$$

is an isomorphism; each U^w is isomorphic to an affine space. Thus, G/H is the disjoint union of the locally closed subvarieties

$$Bn_w P/H \cong U^w \times P/H.$$

It follows that

$$|(G/H)(\mathbf{F}_{q^n})| = |(G/P)(\mathbf{F}_{q^n})|\,|(P/H)(\mathbf{F}_{q^n})|,$$

and $|(G/P)(\mathbf{F}_{q^n})|$ is a polynomial function of q^n with non-negative integer coefficients. This yields the factorization

$$P_{G/H}(t) = P_{G/P}(t)\, P_{P/H}(t).$$

Thus, we may replace (G, H) with (P, H). By Step 2, we may further replace (P, H) with $\Big(P/R_u(P), R_u(P)H/R_u(P)\Big)$. So we may assume that *G and H are both reductive*.

Step 4. We now choose a maximal torus T_H of H, and denote by N_H its normalizer in H. We claim that the natural map

$$p : G/N_H \to G/H$$

induces a surjective map $(G/N_H)(\mathbf{F}_{q^n}) \to (G/H)(\mathbf{F}_{q^n})$ such that each fiber has $q^{n \dim(H/N_H)}$ elements.

Indeed, consider $g \in G(\bar{k})$ such that the coset $gH_{\bar{k}}$ lies in $(G/H)(\mathbf{F}_{q^n})$. Then the subgroup $(gHg^{-1})_{\bar{k}}$ of $G_{\bar{k}}$ is defined over $\mathbf{F}_{q^n}$. Moreover, the fiber of p at $gH_{\bar{k}}$ is isomorphic to the variety of maximal tori of $(gHg^{-1})_{\bar{k}}$; hence its number

of $\mathbf{F}_{q^n}$-rational points equals $q^{n\dim(H/N_H)}$, by a theorem of Steinberg (see [**St68**, Cor. 14.16]). This implies our claim and, in turn, the equality

$$P_{G/H}(t) = t^{-\dim(H/N_H)}\, P_{G/N_H}(t).$$

Replacing (G,H) with (G,N_H), we may thus assume that H^0 *is a torus*.

We may also freely replace k with any finite extension, since this does not affect the definition of P_X, nor the statement of Theorem 1.3.

By Lemma 4.1 below (a version of [**BP02**, Lem. 1, Lem. 2]), there exists a torus $S \subset G$ acting on G/H^0 with finite isotropy subgroup schemes, such that the quotient $S\backslash G/H^0$ is strongly pure. Then S also acts on $X = G/H$ with finite isotropy subgroup schemes, and the quotient

$$S\backslash X = (S\backslash G/H^0)/(H/H^0)$$

is also strongly pure by Lemma 3.3(i).

We now claim that there exists a decomposition of X into finitely many locally closed S-stable subvarieties

$$X_i \cong (S/\Gamma_i) \times Y_i,$$

where Γ_i is a finite subgroup scheme of S. Indeed, by a theorem of Chevalley, X is G-equivariantly isomorphic to an orbit in the projectivization $\mathbf{P}(V)$ of a finite-dimensional G-module V. Choosing a basis of S-eigenvectors in the dual module V^* yields homogeneous coordinates on $\mathbf{P}(V)$, and hence a decomposition of $\mathbf{P}(V)$ into locally closed S-stable tori S_i (where some prescribed homogenous coordinates are non-zero, and all others are zero). Clearly, S acts on each S_i via a homomorphism $f_i : S \to S_i$. Denote by Γ_i the kernel of f_i. Then we may identify S/Γ_i with a subtorus of S_i, and hence there exists a "complementary" subtorus $S_i' \subset S_i$ such that the multiplication map $(S/\Gamma_i) \times S_i' \to S_i$ is an isomorphism. If S_i meets X, then Γ_i is finite, and the natural map $(S/\Gamma_i) \times (X \cap S_i') \to X \cap S_i$ is an isomorphism. Thus, our claim holds for the subvarieties $X_i := X \cap S_i$ and $Y_i := X \cap S_i'$.

That claim yields a similar decomposition of $S\backslash X$ into the subvarieties Y_i. Note that each S/Γ_i is a torus of dimension

$$r := \dim(S) = \dim(T) - \dim(H).$$

Thus, we have for any sufficiently divisible n:

$$|X(\mathbf{F}_{q^n})| = \sum_i |X_i(\mathbf{F}_{q^n})| = \sum_i |(S/\Gamma_i)(\mathbf{F}_{q^n})|\,|Y_i(\mathbf{F}_{q^n})|$$
$$= (q^n-1)^r \sum_i |Y_i(\mathbf{F}_{q^n})| = (q^n-1)^r\,|(S\backslash X)(\mathbf{F}_{q^n})|.$$

In other words, $P_X(t) = (t-1)^r P_{S\backslash X}(t)$. By strong purity, the coefficients of the polynomial $P_{S\backslash X}(t)$ are non-negative; this yields the desired factorization.

Lemma 4.1. — *Let G be a connected reductive group, and $H \subset G$ a torus. Choose a maximal torus T of G containing H and denote by W the Weyl group of (G,T).*

Then, possibly after base change by a finite extension $\mathbf{F}_{q^N}$, there exist subtori S of T such that $T = S\,w(H)$ and $S \cap w(H)$ is finite for all $w \in W$.

Any such torus S acts on G/H with finite isotropy subgroup schemes, and the quotient $S\backslash G/H$ is a strongly pure, affine variety.

Proof. — We may assume that T is split. Let Λ be its character group; this is a lattice equipped with an action of W, and containing the lattice Λ^H of characters of T/H. We may find a subgroup Λ' of Λ such that Λ/Λ' is a lattice, $\Lambda' \cap w(\Lambda^H) = \{0\}$ and $\Lambda' + w(\Lambda^H)$ has finite index in Λ for any $w \in W$ (indeed, the subspaces $w(\Lambda^H)_{\mathbf{Q}}$ of the rational vector space $\Lambda_{\mathbf{Q}}$ have a common complement). Then $\Lambda' = \Lambda^S$ for a subtorus S of T which satisfies the first assertion.

For the second assertion, we may choose a Borel subgroup B of G that contains T. As in (4.1, 4.2), consider the Bruhat decomposition $G = \bigcup_{w\in W} Bn_wB$ and the isomorphisms

$$U^w \times U \times T \longrightarrow Bn_wB, \quad (u,v,t) \longmapsto un_wvt.$$

The resulting projection

$$p : Bn_wB \longrightarrow T$$

is equivariant with respect to $T \times T$ acting on Bn_wB via left and right multiplication, and on T via

$$(x,y)\cdot z = w^{-1}(x)\,z\,y^{-1}.$$

The fiber of p at the identity element of T is isomorphic to the affine space $U^w \times U$. This yields a cartesian square

$$\begin{array}{ccc} Bn_wB & \xrightarrow{p} & T \\ {\scriptstyle /H}\downarrow & & {\scriptstyle /H}\downarrow \\ Bn_wB/H & \xrightarrow{f} & T/H, \end{array}$$

where f is T-equivariant. Moreover, T/H is homogeneous under S acting via $s \cdot tH = w^{-1}(s)tH$, and the corresponding isotropy subgroup scheme is $S \cap w^{-1}(H)$. Thus, Bn_wB/H is the quotient of $U^w \times U \times S$ by $S \cap w^{-1}(H)$ acting linearly on $U^w \times U$, and on S via multiplication.

By our assumption on S, it follows that all isotropy subgroup schemes for its action on G/H are finite; in particular, all orbits are closed. Since the variety G/H is affine, the quotient $S\backslash G/H$ exists and is affine as well. Moreover, this quotient is decomposed into the locally closed varieties

$$S\backslash Bn_wB/H \cong (U \times U^w)/\Big(S \cap w(H)\Big).$$

Thus, $S\backslash G/H$ is strongly pure in view of Lemma 3.3(i). □

5. Elementary proofs of Theorems 1.2, 1.3 and 1.4

As in Section 4, we may assume that $X = G/H$, where G is a connected reductive group and H is a closed subgroup such that H^0 is a torus. We first obtain a formula for the number of $\mathbf{F}_{q^n}$-rational points of X, by standard arguments of Galois descent.

Denote by Γ the finite group H/H^0. For any $\gamma \in \Gamma$, choose a representative $h_\gamma \in H(\bar{k})$. By Lang's theorem, we may choose $g_\gamma \in G(\bar{k})$ such that $h_\gamma = g_\gamma^{-1} F(g_\gamma)$.

Consider a point $x \in (G/H)(\bar{k})$ with representative $g \in G(\bar{k})$. Then $x \in (G/H)(\mathbf{F}_q) = (G/H)^F$ if and only if $g^{-1}F(g) \in H(\bar{k})$, that is, $g^{-1}F(g) \in h_\gamma H^0(\bar{k})$ for a unique $\gamma \in \Gamma$. Equivalently, we have $g = zg_\gamma$, where $z \in G(\bar{k})$ satisfies

$$z^{-1}F(z) \in F(g_\gamma)H^0(\bar{k})F(g_\gamma^{-1}).$$

Moreover,

$$F(g_\gamma)H^0F(g_\gamma^{-1}) = F(g_\gamma H^0 g_\gamma^{-1}) = g_\gamma h_\gamma H^0 h_\gamma^{-1} g_\gamma^{-1} = g_\gamma H^0 g_\gamma^{-1}.$$

Thus, each $g_\gamma H^0 g_\gamma^{-1}$ is defined over k, and

$$z^{-1}F(z) \in g_\gamma H^0(\bar{k}) g_\gamma^{-1}.$$

Applying Lang's theorem again, we see that

$$z \in G(\mathbf{F}_q) g_\gamma H^0(\bar{k}) g_\gamma^{-1}.$$

Thus, the preimage of $(G/H)(\mathbf{F}_q)$ in $(G/H^0)(\bar{k})$ is the disjoint union of the orbits $G(\mathbf{F}_q)g_\gamma H^0$, where $\gamma \in \Gamma$. This yields the equality

$$|(G/H)(\mathbf{F}_q)| = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \frac{|G(\mathbf{F}_q)|}{|(g_\gamma H^0 g_\gamma^{-1})(\mathbf{F}_q)|}. \tag{5.1}$$

But $G(\mathbf{F}_q) = G^F$ and $(g_\gamma H^0 g_\gamma^{-1})(\mathbf{F}_q) = (g_\gamma H^0 g_\gamma^{-1})^F \cong (H^0)^{\gamma^{-1}F}$, where γ acts on H^0 via conjugation by h_γ (this makes sense since H^0 is commutative). Thus, we may rewrite (5.1) as

$$|(G/H)(\mathbf{F}_q)| = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \frac{|G^F|}{|(H^0)^{\gamma F}|}. \tag{5.2}$$

This still holds when q is replaced with q^n, and F with F^n, where n is an arbitrary positive integer.

Next, we obtain a more combinatorial formula for $|(G/H)(\mathbf{F}_{q^n})|$. Denote by

$$\Lambda = \Lambda_{H^0} := \mathrm{Hom}(H^0, \mathbf{G}_m)$$

the character group of the torus H^0. Then Λ is a lattice, where Γ acts via its action on H^0 by conjugation. Moreover, F defines an endomorphism of Λ that we still denote by F, via $\Big(F(\lambda)\Big)(x) = \lambda\Big(F(x)\Big)$ for all points λ of Λ and x of H^0. Since H^0 splits over some finite extension $\mathbf{F}_{q^N}$, we have

$$F^N = q^N \,\mathrm{id}$$

as endomorphisms of Λ. Thus, we may write $F = qF_0$, where F_0 is an automorphism of finite order of the rational vector space $\Lambda_{\mathbf{Q}}$. Then F_0 normalizes Γ, and

$$|(H^0)^{\gamma F}| = |\Lambda/(\gamma F - \mathrm{id})\Lambda| = |\det_{\Lambda_{\mathbf{Q}}}(\gamma F - \mathrm{id})| = \det_{\Lambda_{\mathbf{Q}}}(q\,\mathrm{id} - F_0^{-1}\gamma^{-1})$$

by results of [**Ca85**, 3.2, 3.3]. As a consequence,

$$|(H^0)^{\gamma F}| = q^{\dim(H)} \det_{\Lambda_{\mathbf{Q}}}(\mathrm{id} - F^{-1}\gamma^{-1}).$$

Combined with (5.2), this yields

$$|(G/H)(\mathbf{F}_q)| = \frac{|G^F|}{q^{\dim(H)}} \frac{1}{|\Gamma|} \sum_{\gamma\in\Gamma} \frac{1}{\det_{\Lambda_{\mathbf{Q}}}(\mathrm{id} - F^{-1}\gamma)}. \tag{5.3}$$

Now consider the expansion

$$\frac{1}{\det_{\Lambda_{\mathbf{Q}}}(\mathrm{id} - F^{-1}\gamma)} = \sum_{n=0}^{\infty} \mathrm{Tr}_{S^n(\Lambda_{\mathbf{Q}})}(F^{-1}\gamma),$$

where S^n denotes the nth symmetric power. Since all eigenvalues of F in $\Lambda_{\mathbf{Q}}$ have absolute value q, the series in the right-hand side converges absolutely. Thus, we may write

$$|(G/H)(\mathbf{F}_q)| = \frac{|G^F|}{q^{\dim(H)}} \sum_{n=0}^{\infty} \mathrm{Tr}_{S^n(\Lambda_{\mathbf{Q}})} \Big(F^{-1} \frac{1}{|\Gamma|} \sum_{\gamma\in\Gamma} \gamma\Big). \tag{5.4}$$

Since the operator $\frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\gamma$ of any Γ-module M is the projection onto the subspace M^Γ of Γ-invariants, the series in the right-hand side of (5.4) equals

$$\sum_{n=0}^{\infty} \mathrm{Tr}_{S^n(\Lambda_{\mathbf{Q}})^\Gamma}(F^{-1}) = \mathrm{Tr}_{S^\Gamma}(F^{-1}),$$

where S denotes the symmetric algebra of $\Lambda_{\mathbf{Q}}$, and S^Γ the subalgebra of Γ-invariants; here F acts on S by algebra automorphisms, and preserves S^Γ. This yields the equality

$$|(G/H)(\mathbf{F}_q)| = \frac{|G^F|}{q^{\dim(H)}} \mathrm{Tr}_{S^\Gamma}(F^{-1}). \tag{5.5}$$

To obtain the desired combinatorial formula, it remains to compute $|G^F|$. For this, choose a maximal torus T of G containing H^0 (and defined over k), with normalizer $N_G(T)$ and Weyl group W; denote by Λ_T the character group of T, and by R its symmetric algebra over $\mathbf{Q}$. Applying (5.5) to $H = N_G(T)$ yields

$$|G^F| = \frac{q^{\dim(G)}}{\mathrm{Tr}_{R^W}(F^{-1})}$$

in view of Steinberg's theorem. Substituting in (5.5) and replacing F with F^n yields our combinatorial formula

$$|(G/H)(\mathbf{F}_{q^n})| = q^{n\dim(G/H)}\frac{\mathrm{Tr}_{S^\Gamma}(F^{-n})}{\mathrm{Tr}_{R^W}(F^{-n})}. \tag{5.6}$$

Here F acts on R^W and S^Γ by automorphisms of graded algebras which are diagonalizable over $\bar{\mathbf{Q}}$ with eigenvalues of the form ζq^j, where ζ is a root of unity and j is a non-negative integer.

We now obtain an invariant-theoretical interpretation of the right-hand side of (5.6). The restriction map $\Lambda_T \to \Lambda_{H^0}$ induces a surjective, F-equivariant homomorphism

$$\rho : R \longrightarrow S.$$

We claim that $\rho(R^W)$ is contained in S^Γ. To see this, consider $\gamma \in \Gamma$ and its representative $h_\gamma \in H(\bar{k}) \subset N_G(H^0)(\bar{k})$. Then T and $h_\gamma^{-1}Th_\gamma$ are maximal tori of the centralizer $C_G(H^0)$. It follows that h_γ is a $\bar{k}$-rational point of $N_G(T)C_G(H^0)$. Thus, the automorphism of S induced by γ lifts to an automorphism of R induced by some $w \in W$; this implies our claim.

By that claim, S^Γ is a graded R^W-module; that module is finitely generated, since the R^W-module R is finitely generated. Moreover, R^W is a graded polynomial algebra over $\mathbf{Q}$, and hence S^Γ admits a finite free resolution

$$0 \to R^W \otimes E_m \xrightarrow{\varphi_m} R^W \otimes E_{m-1} \xrightarrow{\varphi_{m-1}} \cdots \xrightarrow{\varphi_1} R^W \otimes E_0 \to S^\Gamma \to 0,$$

where $E_0, \ldots, E_m$ are finite-dimensional vector spaces equipped with an action of F, and $\varphi_1, \ldots, \varphi_m$ are F-equivariant homomorphisms of R^W-modules. Thus,

$$\mathrm{Tr}_{S^\Gamma}(F^{-n}) = \mathrm{Tr}_{R^W}(F^{-n}) \sum_{i=0}^{m}(-1)^i \ \mathrm{Tr}_{E_i}(F^{-n})$$

for all integers n. Together with (5.6), this yields

$$|(G/H)(\mathbf{F}_{q^n})| = q^{n\dim(G/H)}\sum_{i=0}^{m}(-1)^i \ \mathrm{Tr}_{E_i}(F^{-n}) \tag{5.7}$$

for any positive integer n.

We may further assume that our free resolution is minimal, i.e., each φ_i maps bijectively a basis of E_i to a minimal set of generators of the R^W-module $\mathrm{Im}(\varphi_i) = \mathrm{Ker}(\varphi_{i-1})$ (see [**Ei95**, Lem. 19.4]). In particular, $E_0 \cong \mathbf{Q}$, and each E_i is F-equivariantly isomorphic to a subspace of $R^W \otimes E_{i-1}$. Since the action

of F on R^W is diagonalizable over $\bar{\mathbf{Q}}$ with eigenvalues of the form ζq^j as above, it follows by induction on i that the same holds for the action of F on E_i, and hence on $R^W \otimes E_i$. Together with (5.7), this yields that $|(G/H)(\mathbf{F}_{q^n})|$ is a linear combination of powers $\zeta^{-n} q^{n(\dim(G/H)-j)}$ with integer coefficients. In other words, $|(G/H)(\mathbf{F}_{q^n})|$ is a periodic Laurent polynomial function of q^n with algebraic integer coefficients. As noted at the beginning of Section 3, this implies Theorem 1.2.

We now adapt these arguments to prove Theorem 1.3. Again, we may replace $\mathbf{F}_q$ with $\mathbf{F}_{q^N}$ and assume that the torus T is split, i.e., F acts on $(\Lambda_T)_{\mathbf{Q}}$ as $q\,\mathrm{id}$. Then the actions of F on the algebras $R, R^W, S, \ldots$ are determined by their gradings, and $\mathrm{Tr}_R(F^{-n}), \mathrm{Tr}_{R^W}(F^{-n}), \mathrm{Tr}_S(F^{-n}), \ldots$ are obtained from the Hilbert series $h_R(t), h_{R^W}(t), h_S(t), \ldots$ of the corresponding graded algebras by putting $t = q^{-n}$.

Consider the graded algebra

$$A := R \otimes_{R^W} S^\Gamma.$$

Since R is a free R^W-module of finite rank, the S^Γ-module A is also free, of finite rank; moreover,

$$h_A(t) = \frac{h_R(t)\, h_{S^\Gamma}(t)}{h_{R^W}(t)} = \frac{h_{S^\Gamma}(t)}{(1-t)^{\dim(T)}\, h_{R^W}(t)}. \tag{5.8}$$

The algebra of invariants S^Γ is Cohen-Macaulay of Krull dimension $\dim(H)$ (see e.g. [**Ei95**, Exercise 18.14]), and hence so is A. But A is a finitely generated module over the polynomial algebra R. By Noether normalization, it follows that A is a finitely generated module over a polynomial subalgebra $R' \subset R$ generated by elements $z_1, \ldots, z_{\dim(H)}$ of degree 1. In particular, $z_1, \ldots, z_{\dim(H)}$ generate an ideal of A of finite codimension; therefore, they form a regular sequence in A. It follows that A is a free module of finite rank over R' (see e.g. [**Ei95**, Cor. 18.17]); thus, the Hilbert series of A satisfies

$$h_A(t) = \frac{Q(t)}{(1-t)^{\dim(H)}},$$

where $Q(t)$ is a polynomial with non-negative integer coefficients. Combined with (5.8), this yields the equality

$$\frac{h_{S^\Gamma}(t)}{h_{R^W}(t)} = (1-t)^r\, Q(t),$$

where $r = \dim(T) - \dim(H)$. Evaluating at q^{-n} and using (5.6) yields the desired factorization,

$$|(G/H)(\mathbf{F}_{q^n})| = (q^n - 1)^r \, q^{n(\dim(G/H) - r)} \, Q(q^{-n})$$

(note that the function $(t-1)^r \, t^{\dim(G/H)-r} \, Q(t^{-1})$ is polynomial by Theorem 1.2, and hence so is the function $t^{\dim(G/H)-r} \, Q(t^{-1})$).

Finally, we prove Theorem 1.4. By (5.1), we may assume that H is connected, and hence that

$$|(G/H)(\mathbf{F}_{q^n})| = \frac{|G(\mathbf{F}_{q^n})|}{|H(\mathbf{F}_{q^n})|}.$$

By [**St68**] (see also [**Ca85**, 2.9]), the numerator and denominator of the right-hand side are products of terms $q^{nd} - \zeta^n$, where d is a positive integer, and ζ is either 0 or a root of unity. It follows that the non-zero roots of the polynomials $P_0(t), \ldots, P_{N-1}(t)$ of (1.5) are roots of unity. Since these polynomials have real coefficients, their roots are either 0, 1, -1, or come by pairs of complex conjugates $\zeta, \bar{\zeta}$, where ζ is a root of unity. Moreover, each polynomial $(t+1-\zeta)(t+1-\bar{\zeta})$ has non-negative real coefficients; thus, the same holds for each $P_r(t)$.

Remarks 5.1. — (i) The final step of the preceding proof does not extend to all homogeneous varieties under linear algebraic groups, as the polynomials $P_0(t), \ldots, P_N(t)$ may have roots of absolute value > 1.

For example, let Γ be a group of order 2, and H_r the semi-direct product of the split r-dimensional torus $\mathbf{G}_m^r$ with Γ, where the non-trivial element of Γ acts on $\mathbf{G}_m^n$ via $(t_1, \ldots, t_r) \mapsto (t_1^{-1}, \ldots, t_r^{-1})$. Then $H_r^0 = \mathbf{G}_m^r$ and $H_r \cong H_1 \times \cdots \times H_1$ (r copies); moreover, H_1 is the subgroup of SL(2) consisting of all diagonal or anti-diagonal matrices. Thus, H_r is isomorphic to a closed F-stable subgroup of GL($2r$), where F is the usual Frobenius endomorphism of GL($2r$) that raises all matrix coefficients to the power q. With the notation of the preceding proof, we have

$$|\operatorname{GL}(2r)^F| = q^{r(2r-1)} \prod_{i=1}^{2r-1} (q^i - 1)$$

and

$$\frac{1}{q^{\dim(H_r)}} \operatorname{Tr}_{S^\Gamma}(F^{-1}) = \frac{1}{2q^r}\Big(\frac{1}{(1-q^{-1})^r} + \frac{1}{(1+q^{-1})^r}\Big) = \frac{Q_r(q)}{(q^2-1)^r},$$

where

$$Q_r(t) := \frac{1}{2}\Big((q+1)^r + (q-1)^r\Big) = \sum_{i,\, 0 \leqslant 2i \leqslant r} \binom{r}{2i} t^{r-2i}.$$

By (5.5), it follows that the homogeneous variety $X_r := \mathrm{GL}(2r)/H_r$ satisfies

$$|X_r(\mathbf{F}_q)| = Q_r(q)\, q^{r(2r-1)} \prod_{i=1}^{r} (q^{2i-1} - 1) \prod_{j=1}^{r} \frac{q^{2j} - 1}{q^2 - 1}.$$

In particular, $|X_r(\mathbf{F}_q)|$ is a polynomial in q, and the maximal absolute value of its roots tends to infinity as $r \to \infty$.

(ii) By the reduction steps in Section 4 and the equation (5.3), we may take for the period N the least common multiple of the orders of all the Frobenius endomorphisms of tori with dimension $\leqslant \mathrm{rk}(G)$. As a consequence, we may take

$$N = \mathrm{lcm}\Big(n,\, \varphi(n) \leqslant \mathrm{rk}(G)\Big),$$

where φ denotes the Euler function.

References

[Ar60] S. Arima, *Commutative group varieties*, J. Math. Soc. Japan **12** (1960), 227–237.

[BT71] A. Borel and J. Tits, *Eléments unipotents et sous-groupes paraboliques de groupes réductifs I*, Inventiones math. **12** (1971), 95–104.

[BP02] M. Brion and E. Peyre, *The virtual Poincaré polynomials of homogeneous spaces*, Compositio Math. **134** (2002), 319–335.

[Br07] M. Brion, *Some basic results on actions of non-affine algebraic groups*, arXiv: math.AG/0702518, to appear in the proceedings of the conference "Symmetry and Spaces" (E. Campbell, ed).

[Br09] M. Brion, *Anti-affine algebraic groups*, J. Algebra **321** (2009), 934–952.

[Ca85] R. W. Carter, *Finite groups of Lie type. Conjugacy classes and complex characters*, John Wiley & Sons, Inc., New York, 1985.

[De74] P. Deligne, *La conjecture de Weil I*, Publ. Math. IHES **43** (1974), 273–307.

[De77] P. Deligne, *Cohomologie étale*, Séminaire de Géométrie Algébrique du Bois-Marie, avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier, Lect. Notes in Math. **569**, Springer-Verlag, Berlin-New York, 1977.

[De80] P. Deligne, *La conjecture de Weil II*, Publ. Math. IHES **52** (1980), 137–252.

[DG70] M. Demazure and P. Gabriel, *Groupes algébriques*, Masson, Paris, 1970.

[Ei95] D. Eisenbud, *Commutative Algebra with a View Towards Algebraic Geometry*, Springer, New York, 1995.

[La56] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

[LR97] N. Lauritzen and A. Rao, *Elementary counterexamples to Kodaira vanishing in prime characteristic*, Proc. Indian Acad. Sci. Math. Sci. **107** (1997), 21–25.

[Ma63] H. Matsumura, *On algebraic groups of birational transformations*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **34** (1963), 151–155.

[Mi80] J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, 1980.

[MR07] S. Mozgovoy and M. Reineke, *On the number of stable quiver representations over finite fields,* arXiv: 0708.1259.

[Mu70] D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford, 1970.

[Re08] M. Reineke, *Moduli of representations of quivers,* arXiv: 0802.2147.

[Ro61] M. Rosenlicht, *Toroidal algebraic groups*, Proc. Amer. Math. Soc. **12** (1961), 984–988.

[Sa84a] D. J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), 71–84.

[Sa84b] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984), 165–215.

[SS03] C. Sancho de Salas, *Complete homogeneous varieties: structure and classification,* Trans. Amer. Math. Soc. **355** (2003), 3651–3667.

[ST76] I. R. Shafarevich and J. Tate, *The rank of elliptic curves*, Sov. Math. Dokl. **8** (1967), 917–920.

[Sp98] T. A. Springer, *Linear algebraic groups. Second edition,* Progress in Math. **9**, Birkhäuser, Boston, 1998.

[Sr79] B. Srinivasan, *Representations of finite Chevalley groups*, Lect. Notes in Math. **764**, Springer-Verlag, Berlin-New York, 1979.

[St68] R. Steinberg, *Endomorphisms of linear algebraic groups*, Memoirs Amer. Math. Soc. **80**, AMS, Providence, 1968.

Michel Brion and Emmanuel Peyre, Université de Grenoble I, Département de Mathématiques, Institut Fourier, UMR 5582 du CNRS, 38402 Saint-Martin d'Hères Cedex, France • *E-mail :* Michel.Brion@ujf-grenoble.fr
E-mail : Emmanuel.Peyre@ujf-grenoble.fr