J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

On rational points of homogeneous spaces over finite fields

Dedicated to Professor S. Iyanaga on his 60th birthday

By Makoto ISHIDA

(Received June 28, 1967)

Let G be a connected algebraic group and V a homogeneous space for G, which are defined over a finite field k. We denote by G_k the subgroup of G consisting of all the rational points over k and also by V_k the subset of V consisting of all the rational points over k. Then the operation of G to V induces an operation of G_k to V_k and so V_k is considered as a transformation space for G_k in the abstract sense.

The purpose of this paper is to calculate the number of the G_k-orbits in V_k and the number of points in each G_k-orbit, under an assumption on k, which will be referred to by $(*)$[1]. The main results are as follows (under the assumption $(*)$):

1) Let P_0 be a point in V_k and H the isotropy group of P_0 in G. Let s be the number of conjugate classes of the finite group H/H_0[2]. Then V_k is decomposed into the disjoint union of s G_k-orbits (Theorem 1). This fact is a consequence of 'Galois cohomology theory' (cf. [7]), but we shall give here an elementary proof of it. On the other hand, we can give an example, which shows that the number of points of each G_k-orbit is not necessarily same to each other.

2) We restrict ourselves to the case where V is complete. Then it is proved that H/H_0 is commutative and the normalizer $N(H)$ of H in G is connected (Proposition 1). From these facts, we can show that the number of G_k-orbits in V_k is equal to the index $(H:H_0)$ and the numbers of points in any G_k-orbits are all same (Theorem 2). Moreover, if G operates effectively on V, it is also proved that H is connected (Proposition 2). Hence, in this case, we see that V_k is a homogeneous space for G_k in the abstract sense (Theorem 2′).

3) Let $\mathfrak{g}$ be a finite subgroup of G_k. Then, we shall prove that the num-

1) Cf. the beginning of the section 2.

2) For an algebraic group H, we denote by H_0 the connected component containing the identity element.

ber of points in $(V/\mathfrak{g})_k$[3] is equal to the number of points in V_k (Theorem 3).

1. In this section, we prove two propositions on algebraic groups without any assumption on the ground fields.

Let G be a connected algebraic group; let L be the maximal connected linear normal algebraic subgroup of G and D the smallest normal algebraic subgroup of G giving rise to a linear factor group (cf. [5]).

PROPOSITION 1. *Let H be an algebraic subgroup of G, which contains a Borel subgroup B of L. Then* (i) *H/H_0 is commutative and* (ii) *the normalizer $N(H)$ of H in G is connected and coincides with $D\cdot(H\cap L)$.*

PROOF. In the case where $G=L$, it is known that such an algebraic subgroup H (i.e. a parabolic subgroup of L) is connected and coincides with its normalizer. In fact, we have $N(H)\supset H\supset H_0\supset B$ and so, for any element y in $N(H)$, $H_0=yH_0y^{-1}\supset yBy^{-1}$. Then there exists an element h_0 in H_0 such that $h_0Bh_0^{-1}=yBy^{-1}$, which implies that $h_0^{-1}y\in B$ i.e. $y\in H$ and so we have $N(H)=H$ (cf. [2]). Applying this fact to the parabolic subgroup H_0 of L, we have $H_0=N(H_0)\supset H$ and so $H=H_0$. In this case, we have $D=\{e\}$ and so all the assertions of Proposition are proved. We return to the general case. Then $H\cap L$ is a parabolic subgroup of L and so $H\cap L$ is connected and coincides with its normalizer $N_L(H\cap L)$ in L. Moreover, as $H\supset H\cap L$, we have $H_0\supset(H\cap L)_0=H\cap L\supset H_0\cap L$ and so $H_0\cap L=H\cap L$. Since L contains the commutator of any two elements of G, we see that $H\cap L=H_0\cap L$ contains the commutator subgroup of H, which proves the commutativity of H/H_0. Now it is also known that D is a central subgroup of G and we have $G=D\cdot L$ (cf. [5]). Then, for any element g of $N(H)$, we have $g=dl$ with $d\in D$ and $l\in L$. From $dlHl^{-1}d^{-1}=H$, it follows that $lHl^{-1}=H$ and so $l(H\cap L)l^{-1}=H\cap L$, which implies that $l\in N_L(H\cap L)=H\cap L$. Hence we have $N(H)\subset D\cdot(H\cap L)$. While it is clear that, as D is a central subgroup, we have $N(H)\supset D\cdot(H\cap L)$. So we have $N(H)=D\cdot(H\cap L)$ and, as D and $H\cap L$ are connected, $N(H)$ is also connected.

PROPOSITION 2. *Let V be a complete homogeneous space for G. We suppose that G operates effectively on V. Then, the isotropy group H of a point on V in G is connected and linear.*

PROOF. If G operates effectively on V, we have $H\cap D=\{e\}$ and so there exists a bijective rational homomorphism of H to an algebraic subgroup HD/D of the linear group G/D. Hence H is linear and $H_0\subset L$. Since V is complete, H and H_0 contain a Borel subgroup of L (cf. [1]). Then we have $N_L(H_0)\supset H\cap L\supset H_0$ and so $H\cap L=H_0$, which implies that $N(H)=D\cdot(H\cap L)$

3) For an algebraic set X defined over a field k, we denote by X_k the subset of X consisting of all the rational points over k.

$=DH_0 \supset H$ by Proposition 1. Hence any element h of H can be written in the form $h=dh_0$ with $d \in D$ and $h_0 \in H_0$. However $h=dh_0$ means that we have $d=hh_0^{-1}$ is in $D \cap H$. On the other hand, the effectiveness of the operation of G on V implies that we have $D \cap H=\{e\}$. So $h=h_0$ is in H_0 and we have $H=H_0$.

2. In this and the following sections of this paper, we suppose that the ground fields are finite fields.

Let V be a homogeneous space for a connected algebraic group G, defined over a finite field k with q elements. We denote by V_k and G_k the sets of all the rational points of V and G over k respectively. Then G_k is a subgroup of G and it is known that V_k is not empty (cf. [4]).

The operation of G to V induces naturally an operation of G_k to V_k. Since V_k is a finite set, V_k is decomposed into a disjoint union of a finite number of G_k-orbits and each G_k-orbit consists of a finite number of points.

For a point P_0 in V_k, let $H(P_0)$ be the isotropy group of P_0 in G. Then $H(P_0)$ and $H(P_0)_0$ are algebraic subgroups, defined over k, of G. By replacing k by its finite extension if necessary, we assume that the ground field k satisfies the following condition:

(*) There exists a point P_0 in V_k such that $H(P_0)$ has a representative system modulo $H(P_0)_0$ consisting of k-rational elements, i. e. we have $H(P_0) = \bigcup_{i=1}^{n} H(P_0)_0 h_i$ (disjoint) with $h_i \in H_k$ $(i=1, \cdots, n)$.

It is clear that if k satisfies (*) then any finite extension of k also satisfies the condition (*).

In the following, *we always suppose that k satisfies the condition* (*). Let P_0 be a point in V_k and $H=H(P_0)$ the isotropy group of P_0 in G such that we have

$$H=\bigcup_{i=1}^{n} H_0 h_i \qquad \text{(disjoint)} \qquad \text{with } h_1, \cdots, h_n \in H_k\,.$$

We fix P_0 and $h_1, \cdots, h_n$ once for all.

LEMMA 1. *We fix an index i $(1 \leqq i \leqq n)$. Then, for any element h_0' in H_0, there exists an element h_0 in H_0 such that we have $h_0'=h_0^{-1}h_i h_0^{(q)} h_i^{-1}$*[4].

PROOF (cf. [4] and [6]). For a generic point x of H_0 over $K=k(h_0')$, $\varphi(x) = x^{-1}h_i x^{(q)} h_i^{-1}$ and $\psi(x)=x^{-1}h_0' h_i x^{(q)} h_i^{-1}$ are generic points of H_0 over K; so φ and ψ are generically surjective and everywhere defined rational mapping of H_0 to H_0. Then the images $\varphi(H_0)$ and $\psi(H_0)$ contain open sets of H_0 respectively and so we have $\varphi(H_0) \cap \psi(H_0) \neq \phi$. Let t be an element of this inter-

4) (q) means the rational transformation induced by the automorphism of the universal domain: $\xi \rightarrow \xi^q$.

section. Then we have $u^{-1}h_i u^{(q)} h_i^{-1} = t = v^{-1}h'_0 h_i v^{(q)} h_i^{-1}$ with $u, v \in H_0$ and so we have $h'_0 = h_0^{-1} h_i h_0^{(q)} h_i^{-1}$ with $h_0 = uv^{-1}$.

Now we can find n elements $g_1, \cdots, g_n$ of G such that

$$h_i = g_i^{-1} g_i^{(q)} \tag{1}$$

(cf. [4]). Then, as $(g_i P_0)^{(q)} = g_i^{(q)} P_0 = g_i h_i P_0 = g_i P_0$, the point $g_i P_0$ is in V_k. On the other hand, let gP_0 with $g \in G$ be any point in V_k. Then, as $g^{(q)} P_0 = gP_0$, we have $g^{-1} g^{(q)} = h'_0 h_i$ with some $h'_0 \in H_0$ and $1 \leqq i \leqq n$. By Lemma 1 and (1), there exists an element h_0 in H_0 such that we have $g^{-1} g^{(q)} = h_0^{-1} h_i h_0^{(q)} h_i^{-1} h_i = h_0^{-1} g_i^{-1} g_i^{(q)} h_0^{(q)}$ and so $g h_0^{-1} g_i^{-1}$ is in G_k and the given point $gP_0 = (g h_0 g_i^{-1}) g_i P_0$ is in the G_k-orbit $G_k(g_i P_0)$ of $g_i P_0$. Hence we have

$$V_k = \bigcup_{i=1}^{n} G_k(g_i P_0),$$

which of course is not necessarily a disjoint union. Next, for $1 \leqq i, j \leqq n$, we suppose that $G_k(g_i P_0) \cap G_k(g_j P_0)$ is not empty i.e. $G_k(g_i P_0) = G_k(g_j P_0)$. Then $g_j P_0$ is in $G_k(g_i P_0)$ and so we have $g_j = g_0 g_i h$ with some $g_0 \in G_k$ and $h \in H$, which implies that we have $h_j = g_j^{-1} g_j^{(q)} = h^{-1} g_i^{-1} g_i^{(q)} h^{(q)} = h^{-1} h_i h^{(q)}$. Denoting by π the canonical homomorphism of H onto H/H_0 and writing $h = h_0 h_t$ with $h_0 \in H_0$ and $1 \leqq t \leqq n$, we have $h^{(q)} = h_0^{(q)} h_t$ and so we see that $\pi(h_j) = \pi(h_t)^{-1} \pi(h_i) \pi(h_t)$ is conjugate to $\pi(h_i)$ in H/H_0. Conversely, for $1 \leqq i, j \leqq n$, we suppose that $\pi(h_j)$ is conjugate to $\pi(h_i)$ in H/H_0. Then we can write $h'_0 h_j = h_t h_i h_t^{-1}$ with some $h'_0 \in H_0$ and $1 \leqq t \leqq n$. By Lemma 1, we have $h'_0 = h_0^{-1} h_j h_0^{(q)} h_j^{-1}$ with some $h_0 \in H_0$ and so $h_0^{-1} h_j h_0^{(q)} = h_t h_i h_t^{-1}$ i.e. $h_0^{-1} g_j^{-1} g_j^{(q)} h_0^{(q)} = h_t g_i^{-1} g_i^{(q)} h_t^{-1}$. So $g_j h_0 h_t g_i^{-1}$ is in G_k and $g_j P_0 = (g_j h_0 h_t g_i^{-1}) g_i P_0$ is in the orbit $G_k(g_i P_0)$.

Therefore we have the following

THEOREM 1. *Let V be a homogeneous space for G defined over a finite field k with q elements and P_0 a point in V_k. Let H be the isotropy group of P_0 in G and let s be the number of conjugate classes of H/H_0. We suppose that $H_0 h_1, \cdots, H_0 h_s$ are the representatives of all the conjugate classes and $h_i \in H_k$ $(i = 1, \cdots, s)$. Then, writing $h_i = g_i^{-1} g_i^{(q)}$ with $g_i \in G$ $(i = 1, \cdots, s)$, we have*

$$V_k = \bigcup_{i=1}^{s} G_k(g_i P_0) \qquad \text{(disjoint union)}. \tag{2}$$

REMARK. The number s and the representatives $H_0 h_i$ $(i = 1, \cdots, s)$ are not dependent on the ground field but the elements g_i $(i = 1, \cdots, s)$ are dependent on the ground field i.e. on the number q of the elements of k.

In the rest of this section, we consider the case where H is a finite subgroup of G, i.e. H_0 consists of a single element e. As in Theorem 1, we suppose that H is contained in G_k. Let gP_0 be any point in V_k; so $g^{-1} g^{(q)} = h$ is in H. The isotropy group of gP_0 in G is clearly gHg^{-1}. Then an element

$gh'g^{-1}$ with $h' \in H = H_k$ belongs to $(gHg^{-1})_k$ if and only if $g^{(q)}h'g^{(q)-1} = gh'g^{-1}$ i.e. h' is in the normalizer $N_H(h)$ of h in H. Since the number of points in $G_k(gP_0)$ is equal to the index of $(gHg^{-1}) \cap G_k = (gHg^{-1})_k$ in G_k, we have

$$\sharp G_k(gP_0) = \sharp G_k / \sharp N_H(h)^{5)}, \tag{3}$$

where $h = g^{-1}g^{(q)}$. Then, by Theorem 1, we have

$$\begin{aligned}\sharp(G/H)_k = \sharp V_k &= \sum_{i=1}^{s} \sharp G_k / \sharp N_H(h_i) \\ &= (\sharp G_k / \sharp H) \cdot \sum_{i=1}^{s} (H : N_H(h_i)),\end{aligned}$$

where $h_1, \cdots, h_s$ are the representatives of all the conjugate classes of H. As $\sum_{i=1}^{s} (H : N_H(h_i)) = \sharp H = \sharp H_k$, we have

$$\sharp(G/H)_k = \sharp G_k, \tag{4}$$

which is a result of Lang (cf. [4]).

The formula (3) implies that the number of points in each G_k-orbit in V_k is not necessarily same (cf. Theorem 2). For example, let Ω be the universal domain containing k and $G = GL(3, \Omega)$, which is a connected algebraic group defined over k. Then there exists a subgroup H of G such that we have $H \cong S_3$ (the symmetric group of 3 letters) and $H \subset G_k$. In this case, by Theorem 1 and (3), we see that $(G/H)_k$ consists of three disjoint G_k-orbits G_kP_1, G_kP_2 and G_kP_3 such that $\sharp G_kP_1 = \sharp G_k/2$, $\sharp G_kP_2 = \sharp G_k/3$ and $\sharp G_kP_3 = \sharp G_k/6$. So the numbers of points in G_k-orbits in $(G/H)_k$ are distinct to each other. Moreover this example shows the following fact: even if G operates effectively on V, the operation of G_k on V_k is not necessarily transitive (cf. Theorem 2′). In fact, from the elementary properties of S_3, we see that, for any element $h \neq e$ in $H \cong S_3$, there exists an element h' of H such that $h'h \neq hh'$. Writing $h' = gg^{(q)-1}$ with $g \in G$, we see that $g^{(q)-1}hg^{(q)} \neq g^{-1}hg$ i.e. $g^{-1}hg$ is not rational over k. Hence $g^{-1}hg$ does not belong to $H = H_k$ i.e. $h \notin gHg^{-1}$, which implies that we have $\bigcap_{g \in G} gHg^{-1} = \{e\}$. So G operates effectively on G/H, but G_k does not operate transitively on $(G/H)_k$.

3. Now we consider the case where V is a complete homogeneous space for G (defined over k with the property $(*)$). Then, using the notations of Theorem 1, H contains a Borel subgroup of the maximal connected linear normal algebraic subgroup L of G (cf. [1]) and so, by Proposition 1, we see that H/H_0 is commutative and the normalizer $N(H)$ of H is connected. Hence,

5) For a finite set S, we denote by $\sharp S$ the number of elements in S.

in Theorem 1, we have $s=(H:H_0)$. Moreover, also using the notations of Theorem 1, the isotropy group $g_iHg_i^{-1}$ of g_iP_0 in G is defined over k. Then the set $g_iN(H)=\{g\in G \mid gHg^{-1}=g_iHg_i^{-1}\}$ is not empty and is a homogeneous space for a connected algebraic group $N(H)$, defined over k. So $g_iN(H)$ has a rational point $g_i^{(0)}$ over k (cf. [4]) and so $g_iHg_i^{-1}=g_i^{(0)}Hg_i^{(0)-1}$, which implies that we have $\#(g_iHg_i^{-1})_k=\#(g_i^{(0)}Hg_i^{(0)-1})_k=\#H_k$. Hence the number of points in the orbit $G_k(g_iP_0)$ is equal to $\#G_k/\#(g_iHg_i^{-1})_k=\#G_k/\#H_k$, which is independent of the index i.

Therefore we have the following

THEOREM 2. *Let V be a complete homogeneous space for G defined over a finite field k. Let H be the isotropy group of a point P_0 in V_k in G. Then the number of distinct G_k-orbits in V_k is equal to the index $(H:H_0)$ and each G_k-orbit consists of the same number $\#G_k/\#H_k$ of points.*

COROLLARY. *We have*

$$\#V_k=\#G_k/\#(H_0)_k\,.$$

PROOF. We have $H_k=\bigcup_{i=1}^{n}(H_0)_kh_i$ and so $\#H_k=(\#(H_0)_k)\cdot(H:H_0)$. Hence we have, by Theorem 2, $\#V_k=(H:H_0)\cdot(\#G_k/\#H_k)=\#G_k/\#(H_0)_k$.

THEOREM 2′. *In Theorem 2, we suppose that G operates effectively on V. Then we have*

$$V_k=G_kP_0\,, \tag{6}$$

i.e. G_k operates transitively on V_k.

PROOF. By Proposition 2, we have $(H:H_0)=1$. Then the assertion follows from Theorem 2.

COROLLARY 1. *In Theorem 2, let N be a normal algebraic subgroup of G defined over k. Then, for any points P_0 and P_0' in V_k, we have*

$$\#(NP_0)_k=\#(NP_0')_k\,. \tag{7}$$

PROOF. Let M be the intersection of the isotropy groups of all the points on V, which is a normal algebraic subgroup of G defined over k. Let f be the canonical homomorphism of G onto $G'=G/M$. Then G' operates transitively and effectively on V by $f(g)P=gP$ for $g\in G$ and $P\in V$. Clearly $f(N)=N'$ is a normal algebraic subgroup of G' and we have $N'P_0=NP_0$ and $N'P_0'=NP_0'$. By Theorem 2′, there exists an element g_0' in G_k' such that we have $g_0'P_0=P_0'$. Then the mapping of $N'P_0$ to $N'P_0'$ defined by $n'P_0\to g_0'n'P_0$ $(n'\in N')$ induces a bijective mapping of $(N'P_0)_k=(NP_0)_k$ onto $(N'P_0')_k=(NP_0')_k$.

COROLLARY 2. *In Theorem 2, let A be an Albanese variety of V, defined over k. Then, for any point P_0 in V_k, we have*

$$\#V_k=\#A_k\cdot\#(LP_0)_k\,. \tag{8}$$

PROOF (cf. [3]). It is clear that, denoting by α the canonical mapping of V into A, we have

$$\# V_k = \sum_{a \in A_k} \# \alpha^{-1}(a)_k ,$$

where the sum ranges over all $a \in A_k$. Moreover we have $\alpha^{-1}(a) = LP_0'$ with some $P_0' \in V_k$. Then the assertion follows from Corollary 1.

4. Finally, we prove a generalization of the result of Lang stated in the end of **2**, which asserts that, for a connected algebraic group G defined over a finite field k, if $\mathfrak{g}$ is a finite subgroup of G_k then we have $\#(G/\mathfrak{g})_k = \# G_k$ (cf. [4]).

LEMMA 2. *Let G be a connected algebraic group, which operates regularly on an irreducible variety V, all defined over a finite field k. Let $\mathfrak{g}$ be a finite subgroup of G_k such that the quotient variety $V/\mathfrak{g}$ exists. Then we have*

$$\#(V/\mathfrak{g})_k = \# V_k . \tag{9}$$

PROOF. Let q be the number of elements in k and n the order of $\mathfrak{g}:\mathfrak{g} = \{h_1, \cdots, h_n\}$. We put, for each $h_i \in \mathfrak{g}$, $F_i = \{P \in V \mid P^{(q)} = h_i P\}$. Then it is easily verified that we have

$$\#(V/\mathfrak{g})_k = (1/n) \cdot \sum_{i=1}^{n} \# F_i . \tag{10}$$

Since h_i is an element of a connected algebraic group G defined over k, there exists an element g_i of G such that $h_i = g_i^{(q)-1} g_i$ (cf. [4]). Then we have a bijective mapping φ_i of F_i to V_k by $\varphi_i(P) = g_i P$. In fact, $(g_i P)^{(q)} = g_i^{(q)} P^{(q)} = g_i h_i^{-1} P^{(q)} = g_i P$ i.e. $g_i P \in V_k$. The injectiveness of φ_i is trivial and, for any point P_0 in V_k, $(g_i^{-1} P_0)^{(q)} = g_i^{(q)-1} P_0 = h_i g_i^{-1} P_0$ i.e. $g_i^{-1} P_0 \in F_i$ and $\varphi_i(g_i^{-1} P_0) = P_0$. Hence, by (10), we have $\#(V/\mathfrak{g})_k = (1/n) \cdot \sum_{i=1}^{n} \# F_i = (1/n) \cdot \sum_{i=1}^{n} \# V_k = \# V_k$.

THEOREM 3. *Let V be a homogeneous space for G defined over a finite field k. If $\mathfrak{g}$ is a finite subgroup of G_k, then we have*

$$\#(V/\mathfrak{g})_k = \# V_k . \tag{11}$$

PROOF. By Lemma 2, we have only to show that there exists the quotient variety $V/\mathfrak{g}$. This is a consequence of the fact that V has a projective embedding (cf. [6]).

Tokyo Metropolitan University

References

[1] A. Borel, Groupes linéaires algébriques, Ann. of Math., **64** (1956), 20–82.
[2] C. Chevalley, Classification des groupes de Lie algébriques, Séminaire E. N. S. (1956–58).
[3] M. Ishida, On algebraic homogeneous spaces, Pacific J. Math., **15** (1965), 525–535.
[4] S. Lang, Algebraic groups over finite fields, Amer. J. Math., **78** (1956), 555–563.
[5] M. Rosenlicht, Some basic theorems on algebraic groups, Amer. J. Math., **78** (1956), 401–443.
[6] J.-P. Serre, Groupes algébriques et corps de classes, Paris, 1959.
[7] J.-P. Serre, Cohomologie galoisienne, Berlin, 1964.