



Algebraic Groups Over Finite Fields

Serge Lang

American Journal of Mathematics, Volume 78, Issue 3 (Jul., 1956), 555-563.

Stable URL:

<http://links.jstor.org/sici?sici=0002-9327%28195607%2978%3A3%3C555%3AAGOFF%3E2.0.CO%3B2-M>

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/about/terms.html>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

American Journal of Mathematics is published by The Johns Hopkins University Press. Please contact the publisher for further permissions regarding the use of this work. Publisher contact information may be obtained at <http://www.jstor.org/journals/jhup.html>.

American Journal of Mathematics

©1956 The Johns Hopkins University Press

JSTOR and the JSTOR logo are trademarks of JSTOR, and are Registered in the U.S. Patent and Trademark Office. For more information on JSTOR contact jstor-info@umich.edu.

©2002 JSTOR

ALGEBRAIC GROUPS OVER FINITE FIELDS.*

By SERGE LANG.

1. Introduction. Let k be a finite field with q elements. Let G be an algebraic group defined over k . (For the foundations of the theory of algebraic groups and homogeneous spaces, see Weil [8], [9].) If x is a point of G , we denote by $x^{(q)}$ the point obtained by raising all coordinates of x to the q -th power, i.e. by applying to x the Frobenius automorphism of the universal domain leaving k fixed. The mapping $f(x) = x^{-1}x^{(q)}$ is a rational map of G into itself. It will be shown that it is in fact surjective, and that it gives a Galois, in general non abelian unramified covering of G over itself, the Galois group being that of the left rational translations. This sort of covering is of course impossible in characteristic 0.

More generally, it will be shown that G acts on itself as a homogeneous space, under the operation $F(x, y) = x \cdot y = x^{(q)}yx^{-1}$. Using this fact we shall show that every homogeneous space H of G defined over k has a rational point. If it is principal homogeneous, then it must be biregularly equivalent to G over k , and in case G is commutative, this means that the Weil group is trivial. We also use this result to give a new proof of a result due to Chatelet [4], that if a variety V/k becomes biregularly equivalent to projective space over the algebraic closure of k , then it is already so over k itself.

Finally we consider the class field theory for our covering defined by the map $z \rightarrow z^{-1}z^{(q)}$, get a partial non abelian reciprocity law, and prove that the Artin L -series are trivial. This is used to prove the following result: Let g be a subgroup of the rational points of G over k . Let H be the homogeneous space of cosets of $G \bmod g$. Then G and H have the same number of rational points.

In case the group G is commutative, then one can get a complete reciprocity law, and one can use it to derive the class field theory over a variety V having a rational map into G by means of which the abelian coverings of G by commutative groups can be pulled back in a one-one manner.

* Received March 9, 1956.

This abelian class field theory is carried out in detail elsewhere, and in this paper, we have concentrated exclusively on the non abelian aspects of the covering $z^{-1}z^{(q)}$.

2. The map $f(z) = z^{-1}z^{(q)}$. The map $f(z)$ being as above we contend that if z is a generic point of G/k then $f(z)$ is also a generic point of G/k , and in fact the extension $k(z)$ over $k(f(z))$ is separable algebraic. Namely, putting $x = f(z)$ we have $k(z) = k(x, z) = k(x, z^{(q)})$. Our contention now follows from the following elementary and well known result of field theory:

PROPOSITION 1. *Let F be a field and E/F a finitely generated extension. We assume the characteristic p is $\neq 0$. If E/F is separable algebraic, then $E^{p^\mu}F = E$ for all powers p^μ , and conversely, if $E^{p^\mu}F = E$ for some power p^μ , then E/F is separably algebraic.*

(By E^{p^μ} we denote the field obtained by raising all elements of E to the p^μ -th power.)

We have trivially for z, w in G :

$$(1) \quad (zw)^{(q)} = z^{(q)}w^{(q)}, \quad (z^{-1})^{(q)} = (z^{(q)})^{-1}.$$

Furthermore our rational map satisfies the following formalism:

$$(2) \quad f(zw) = f(z)wf(w)$$

where y^w is defined to be $w^{-1}yw$.

The subgroup of G consisting of the elements rational over the field k_d (unique extension of k of degree d) will be denoted by G_d .

$$(3) \quad \text{An element } a \text{ of } G \text{ is in } G_1 \text{ if and only if } f(a) = 0. \text{ More generally, } f(z) = f(w) \text{ if and only if } z = aw \text{ for some } a \text{ in } G_1.$$

The first part of the statement is obvious. If $z = aw$, it is also obvious that $f(z) = f(w)$. Suppose $f(z) = f(w)$. Then $z^{-1}z^{(q)} = w^{-1}w^{(q)}$, whence $(zw^{-1}) = (zw^{-1})^{(q)}$. This means that zw^{-1} is rational over k , as desired.

We now see that if z is a generic point of G/k , then the extension $k(z)/k(f(z))$ is Galois, the distinct conjugates of z over $k(f(z))$ being az , with a rational over k .

The mapping $g(z) = z^{(q)}z^{-1}$ has analogous properties with respect to right translations, and we shall use them freely whenever needed.

PROPOSITION 2. *Let y be an arbitrary point of G and x a generic point over $k(y)$. Then $x^{(q)}yx^{-1}$ is a generic point of G over $k(y)$.*

Proof. Let $w = x^{(q)}yx^{-1}$. Put $K = k(y)$. Then $K(w, x) = K(w, x^{(q)})$. This implies that $K(x)$ is separable algebraic over $K(w)$, and that w has the same dimension as x over K . Hence it is a generic point of G/K .

Given two arbitrary points x and y of G , we denote by $x \cdot y$ the point $x^{(q)}yx^{-1}$. We obviously have for x, y, z arbitrary,

$$(4) \quad (xy) \cdot z = x \cdot (y \cdot z) \quad \text{and} \quad e \cdot x = x$$

To prove that G is a homogeneous space over itself with the above defined external law of composition, we need only prove the following statement:

THEOREM 1. *Given two points y and w in G , there exists a point x such that $x \cdot y = w$.*

Proof. In fact, using the associativity, it suffices to prove: Given y in G , there exists x such that $x \cdot y = e$. Let t be a generic point of G over $K = k(y)$. Then $t \cdot y$ is a generic point of G/K by Proposition 2. There is an isomorphism σ which is identity on K and maps $t^{(q)}t^{-1}$ on $t \cdot y = t^{(q)}yt^{-1}$. We can extend σ to the field $K(t)$. Let $u = t^\sigma$. Then

$$g(u) = g(t^\sigma) = g(t)^\sigma = t^{(q)}yt^{-1}.$$

If we put $x = u^{-1}t$, we have what we want.

COROLLARY. *The map $z \rightarrow z^{-1}z^{(q)}$ is surjective, i.e. given any y in G , there exists z such that $y = z^{-1}z^{(q)}$.*

Proof. According to the theorem, there exists z in G such that $z^{(q)}y^{-1}z^{-1} = e$. This element z does what is required.

From this corollary we see that we have indeed an unramified covering of G over itself. Given any point Q in G , there exists n points P such that $Q = P^{-1}P^{(q)}$, where n is the order of G_1 . Given any one of them, all the others are simply the left rational translations of this one.

As another application of Theorem 1, we prove

THEOREM 2. *Let H/k be a homogeneous space over G . Then H has a rational point.*

Proof. We must show that there is some point u in H such that $u^{(q)} = u$. Let v be any point of H . Since H is defined over k , then $v^{(q)}$ is also in H . Since H is a homogeneous space, there exists an element x in G such that $xv^{(q)} = v$. By the corollary to Theorem 1, we can write $x = y^{-1}y^{(q)}$. From

this we see that $(yv)^{(a)} = (yv)$ and hence $u = yv$ is the element we are looking for.

We would like to point out here that Theorem 3 of [6] is a special case of the preceding result. Indeed, if a variety V/k becomes biregularly equivalent to an abelian variety over the algebraic closure of k , then V can be viewed as a principal homogeneous space over its Albanese variety A , which is known (by Chow's work) to be defined over k . (See Weil [9], Prop. 4.) However, because of the completeness of the group, we could give a direct proof, without using the Albanese variety. The proof can in fact be further simplified as follows:

We wish to prove that if a variety V over a finite field k becomes biregularly equivalent to a complete group variety over the algebraic closure of k , and hence over a finite extension k' of k , then V has a rational point over k . Over k' we can put a law of composition on V which makes it into a complete group variety (we don't even need to know it is abelian). There is a unit element e , rational over k' , but not necessarily over k . Let z be a generic point of V over k . With respect to the composition law over k' , we consider the point $f(z) = z^{-1}z^{(a)}$. It is a generic point of V over k' (by Proposition 1). Since V is complete, we can extend a specialization of $f(z)$ on e to a specialization of z to a point ξ on V , and then $\xi^{-1}\xi^{(a)} = e$. This point ξ satisfies $\xi = \xi^{(a)}$, and is therefore a rational point.

The statement made in our above mentioned paper that there is a rational place is a consequence of the following well known fact: *Let k be any field, and V/k any variety (say affine). Let Q be a simple point of V , rational over k . Let v be a generic point of V/k . Then there exists a place ϕ of $k(v)$ over k such that $\phi(v) = Q$ and such that ϕ is rational over k (i. e. k -valued).* One often says that Q is at the center of ϕ . Here of course, we have the additional property that the place can be chosen in such a way that the residue class field is canonically isomorphic to k itself: No irrationalities are needed in extending the specialization $v \rightarrow Q$ to a place of the function field. There exist many proofs of the above fact, and one of them runs along the following lines. The completion of the local ring of Q in $k(v)$ is isomorphic to a power series ring in r variables ($r = \dim V$) with coefficients in k , because Q is simple. There is therefore a canonical isomorphism of $k(v)$ in the quotient field of this power series ring. This quotient field itself can be embedded in the repeated power series field, which has obviously a k -valued place mapping all the variables on 0, one after the other. The restriction of this place to $k(v)$ is the one we are looking for.

We now return to the arbitrary algebraic group G over the finite field k .

Let $\sigma, \tau, \dots$ range over the group of automorphisms of the extension k_d of k . This group (which is cyclic) operates on G_d in an obvious fashion. Referring to this operation, we show that the 1-cocycles split:

PROPOSITION 3. *Let $\{x_\sigma\}$ be a set of elements of G_d such that $x_\tau \sigma x_\sigma = x_{\sigma\tau}$. Then there exists y in G_d such that $x_\sigma = y^\sigma y^{-1}$.*

Proof. We can change our indices from σ to integers mod d . According to the corollary of Theorem 2, we can write $x_1 = y^{(a)} y^{-1}$ for some y in G (we do not know yet whether it is in G_d). Then by the cocycle property, we get $x_i = y^{(a^i)} y^{-1}$. Finally, taking $i = d$ we must have

$$e = x_0 = x_d = y^{(a^d)} y^{-1}.$$

This shows that y is rational over k , because $y^{(a^d)} = y$.

As an application, we prove Chatelet's theorem:

THEOREM 3. *Let V be an abstract variety defined over k , which becomes biregularly equivalent to projective space S over the algebraic closure of k . Then V is biregularly equivalent to S over k .*

Proof. Let $T: V \rightarrow S$ be the correspondence, defined over some k_d . With Chatelet ([3], [4]) we take $x_\sigma = T^\sigma T^{-1}$, which is a birational biregular correspondence between S and itself. It is therefore projective, and is an element of the projective group G , rational over k_d . It satisfies the condition of Proposition 3, and if we let y be the projective transformation as in Proposition 3, we consider $T_1 = y^{-1} T$. Then T_1 is obviously fixed under every automorphism σ of k_d over k , and hence T_1 is defined over k .

For a proof that the only biregular correspondences of S with itself are projective, see Chow [5]. In that paper, other varieties are proved to have that property, and our theorem applies to them as well.

3. Class field theory. We shall now investigate the covering $f(x) = x^{-1} x^{(a)}$ from the point of view of class field theory. By a cycle, we shall always mean a cycle of dimension 0. Let $\mathfrak{p}$ be a prime rational cycle of G over k , and let Q be any point in it. Let P be any point such that $f(P) = Q$. All other points are of type aP , where a is rational over k . If $\mathfrak{p}$ is of degree d , then $f(P^{(a^d)}) = f(P)^{(a^d)} = Q$. Hence $P^{(a^d)}$ also lies in the inverse image of Q under f , and hence there exists a rational point a in G_1 such that $aP = P^{(a^d)}$.

We define $\pi_a(Q)$ to be the product $QQ^{(a)} \cdots Q^{(a^{d-1})}$. Then we have

$$(6) \quad aP = P^{(a)} = P\pi_a(Q).$$

It is clear that the point a in G_1 is completely well defined by the prime $\mathfrak{p}$, up to conjugacy in G_1 . Furthermore we have

PROPOSITION 4. *Given two points Q_1 and Q_2 in G_1 , let a_1 and a_2 in G_1 be any points determined by the condition*

$$a_1P_1 = P_1^{(a)} = P_1Q_1, \quad a_2P_2 = P_2^{(a)} = P_2Q_2.$$

Then a_1 is conjugate to a_2 in G_1 if and only if Q_1 is conjugate to Q_2 in G_1 .

The proof is trivial and formal, and we leave it to the reader.

We have a mapping from the primes to the conjugacy classes of G_1 defined by (6), and if the prime is of degree 1, then we obtain a 1-1 mapping of the conjugacy classes of G_1 (viewed as a set of primes of degree one) onto the conjugacy classes of G_1 (viewed as Galois group of left translations). The period of the point a is clearly equal to the period of $\pi_a(Q)$, and thus we can tell the period of the Frobenius class associated with a prime. Furthermore, we see that $\mathfrak{p}$ splits completely if and only if $\pi_a(Q) = e$.

I have not been able to determine whether the conjugacy class of a is always equal to that of Q (when Q is in G_1) and more generally to determine if a and $\pi_a(Q)$ are conjugate in G_a . In order to obtain the complete decomposition laws, we would need to know that any rational point b in G_1 , conjugate to $\pi_a(Q)$ in G_a is conjugate to a in G_1 . This would imply that the Frobenius class associated with $\mathfrak{p}$ in G_1 can be determined rationally. (This is the case for the full linear group.)

We now consider the L -series.

Let z be a generic points of G/k . Let

$$f_n(z) = z^{-1}z^{(a^n)} \quad \text{and} \quad \pi_n(z) = zz^{(a)} \cdots z^{(a^{n-1})}$$

Then $\pi_n(f_1(z)) = f_n(z)$.

Let $E = k(z)$, $F = k(f_1(z))$, and $K = k(f_n(z))$. We have inclusions $E \supset F \supset K$, and E/F is Galois (it is the extension discussed previously). Let E_n , F_n , and K_n be the constant field extensions by k_n . Then E_n/K_n becomes Galois, with group G_n . The group G is a model of each one of our function fields, but of course in a different way each time.

Referring to these models, we shall prove that the L -series are trivial for a character not containing the identity.

Let χ be a character of G_1 . Let $\mathfrak{p}$ be a prime cycle of G/k . Let $T_{\mathfrak{p}}$ be any one of the translations of G_1 in the Frobenius class associated with $\mathfrak{p}$ in G_1 . Then the L -series are defined by

$$t \frac{d}{dt} \text{Log } L(t, \chi, E/F) = \sum \chi(T_{\mathfrak{p}}^{\mu}) \deg(\mathfrak{p}) t^{\mu \deg(\mathfrak{p})}$$

the sum being taken over all primes and all $\mu \geq 1$.

If we look at the coefficient of t^n we see that we must prove that

$$\sum_{\deg(\mathfrak{p})|n} \chi(T_{\mathfrak{p}}^{n/\deg(\mathfrak{p})}) \deg(\mathfrak{p}) = 0.$$

This sum can be rewritten in terms of points in G_n as follows: To each point Q in G_n , we can associate a translation $T_Q^{(n)}$ (well defined up to conjugacy) in G_1 , such that for any P in $f_1^{-1}(Q)$ we have $T_Q^{(n)}(P) = P^{(Q^n)}$. It is then clear that the above sum is equal to

$$(7) \quad \sum_{Q \in G_n} \chi(T_Q^{(n)}).$$

For $n=1$ we know by Proposition 4 that each class will have a representative $T_Q^{(1)}$ for some Q in G_1 , and that this representative will occur in our sum as many times as there are element in that class. Consequently the value of our sum is the same as the value of the character taken over the sum of the conjugacy classes in the group ring of G_1 . If χ does not contain the identity character, then this sum must be 0.

For arbitrary n , we note that the coefficient of t^n in our L -series $L(t, \chi, E/F)$ is by definition and formula (7) the same as the coefficient of t in $L(t, \chi, E_n/F_n)$. We have thus reduced the computation of the n -th term to the computation of the first term of an L -series over a bigger constant field. By one of the main theorems on L -series, we know that

$$L(t, \chi, E_n/F_n) = L(t, \chi^*, E_n/K_n)$$

where χ^* is the induced character. If χ does not contain the identity, then neither does χ^* . The extension E_n/K_n is now of a type analogous to that considered above for $n=1$ (i.e. belonging to a rational map f_n). Hence the first coefficient of the L -series is equal to zero, as desired.

Let $\lambda: G \rightarrow H$ be a homomorphism of an algebraic group G onto an algebraic group H , defined over k , and with finite kernel. Let z be a generic point of G/k . As usual, $f_G(z) = z^{-1}z^{(a)}$. We also have an f -mapping on H , denoted by f_H . Then obviously $f_H\lambda = \lambda f_G$. Taking the degree of both sides, we see that the degree of f_H must equal that of f_G , i.e. that G and H have

the same number of rational points (hence the same zeta function). If kernel of λ is contained in G_1 , and λ is separable, then G is Galois over H , and this again suggests that the L -series for the covering are trivial. This is indeed the case, and can be proved as follows: Put $y = \lambda(z)$. Then $E = k(z) \supset k(y) = M \supset k(z^{-1}z^{(q)}) = F$. If χ is a character for the Galois group of E/M , and does not contain the identity, then the induced character χ^* to the Galois group of E/F does not contain the identity either, and by what has been proved before, the L -series belonging to it must be trivial.

More generally, if the identity for E/M occurs with some multiplicity in χ , then the identity for E/F occurs with the same multiplicity in χ^* . (See for instance Brauer-Tate [2], where we put Θ = identity in formula (5).) From this remark we can deduce the following result.

Let H be the homogeneous space obtained from G by the cosets of a subgroup of G_1 . Then we have a rational map $\lambda: G \rightarrow H$ (not necessarily a homomorphism), and the same type of field inclusion as before: $k(z) \supset k(y) \supset k(x)$. The zeta function of H , denoted by $Z_H(t)$, can be written

$$Z_H(t) = L(t, 1, E/M) = L(t, 1^*, E/F)$$

where 1 stands for the identity character on the Galois group of E/M . The identity for E/F occurs exactly once in 1^* , and hence the above L -series is equal to $Z_G(t) \cdot L(t, \chi, E/F)$, where χ is some character for E/F , which does not contain the identity, and $Z_G(t)$ is the zeta function of G . This shows that the zeta function of G and H coincide, and hence that G and H have the same number of rational points.

Knowing that the L -series are trivial, we can of course apply the formal argument given by Artin (Satz 4 of [1]) to get the density of primes in a given arithmetic progression. Let χ_i be the simple characters of G_1 . Then we know that

$$(8) \quad \sum_{Q \in G_n} \chi_i(T_Q^{(n)}) = \begin{cases} 0 & i \neq 1 \\ q^{nr} + O(q^{n(r-1/2)}) & i = 1 \end{cases}$$

because for $i = 1$, we deal with the zeta function and can use the results of [7]. Let C_j be a fixed class in G_1 and T any element of C_j . Let h be the order of G_1 and h_j the number of elements in C_j . Multiplying (8) by $\chi_i(T^{-1})$ and summing, we use the orthogonality relations (see formula (3) of [1]) to get

$$\frac{h}{h_j} N(n, C_j) = q^{nr} + O(q^{n(r-1/2)}),$$

where $N(n, C_j)$ is the number of points in G_n having their $T_Q^{(n)}$ in the given class C_j . One sees trivially that to get an estimate for the number of primes, one has to divide by n .

COLUMBIA UNIVERSITY.

REFERENCES.

- [1] E. Artin, "Über eine neue Art von L -Reihen," *Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität*, vol. 3 (1923), pp. 89-108.
- [2] R. Brauer and J. Tate, "On the characters of finite groups," *Annals of Mathematics*, vol. 62 (1955), pp. 1-7.
- [3] F. Chatelet, "Variations sur un thème de Poincaré," *Annales de l'Ecole normale supérieure*, vol. 61 (1944), pp. 249-300.
- [4] ———, "Les courbes de genre 1 dans un champ de Galois," *Comptes rendus des seances de l'Academie des Sciences*, vol. 224 (1947), pp. 1616-1618.
- [5] W. L. Chow, "On the geometry of algebraic homogeneous spaces," *Annals of Mathematics*, vol. 50 (1949), pp. 32-67.
- [6] S. Lang, "Abelian varieties over finite fields," *Proceedings of the National Academy of Sciences*, vol. 41 (1955), pp. 174-176.
- [7] ——— and A. Weil, "Number of points of varieties in finite fields," *American Journal of Mathematics*, vol. 76 (1954), pp. 819-827.
- [8] A. Weil, "Algebraic groups of transformations," *American Journal of Mathematics*, vol. 77 (1955), pp. 355-391.
- [9] ———, "On algebraic groups and homogeneous spaces," *American Journal of Mathematics*, vol. 77 (July 1955), pp. 493-512.