Bibliography

1. H. Levi, *On the structure of differential polynomials and on their theory of ideals*, Trans. Amer. Math. Soc. vol. 51 (1942) pp. 532–568.
2. D. G. Mead, *Differential ideals*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 420–432.
3. J. F. Ritt, *Differential algebra*, Amer. Math. Soc. Colloquium Publications, vol. 33, 1950.

University of Washington

FORMS OF ALGEBRAIC GROUPS

DAVID HERTZIG

In [4] A. Weil solves the following problem: if V is a variety defined over an overfield K of a groundfield k, among the varieties birationally equivalent to V over K find one which is defined over k. The solution is essentially given by the 1-dimensional Galois cohomology. It was observed by J.-P. Serre that in the case V itself is defined over k the 1-cocycles can be regarded as putting a "twist" into V. In the particular case of simple algebraic groups over finite fields this gives rise to some new finite simple groups.

Let G be an algebraic group defined over a field k and K a Galois extension of k. An algebraic group G' defined over k will be called a k-form of G split by K if there is a rational isomorphism ϕ defined over K between G' and G. Denote by $\mathfrak{g}$ the Galois group of K over k. For $\sigma \in \mathfrak{g}$, $f_\sigma = \phi^\sigma \phi^{-1}$ is an automorphism of G defined over K and for all $\tau, \sigma \in \mathfrak{g}$ we have $f_{\tau\sigma} = f_\sigma^\tau f_\tau$, i.e. f is a 1-cocycle from $\mathfrak{g}$ to $\mathrm{Aut}_K G$, the group of automorphisms of G defined over K.

THEOREM 1. *Let G be a connected algebraic group defined over a field k and K a Galois extension of k with Galois group $\mathfrak{g}$. The distinct k-forms of G (up to k-isomorphism) are in one-to-one correspondence with the elements of $H^1(\mathfrak{g}, \mathrm{Aut}_K G)$.*

PROOF. Let f be a 1-cocycle from $\mathfrak{g}$ to $\mathrm{Aut}_K G$. By Weil's theorem [4, Theorem 1] there exists a variety G' defined over k together

Presented to the Society, August 28, 1957 under the title *On simple algebraic groups. Preliminary report*; received by the editors August 22, 1960.

with a birational map $\phi: G' \to G$ defined over K such that $f_\sigma = \phi^\sigma \phi^{-1}$ for all $\sigma \in \mathfrak{g}$. Let x and y be independent generic points of G' over k and define $F: G' \times G' \to G'$ by $F(x, y) = \phi^{-1}(\phi(x)\phi(y))$. Let T be the graph of F. For $\sigma \in \mathfrak{g}$, T^σ is the graph of $F^\sigma: G' \times G' \to G'$ given by $F^\sigma(x, y) = \phi^{-\sigma}(\phi^\sigma(x)\phi^\sigma(y))$. We have $F^\sigma(x,y) = \phi^{-\sigma}(f_\sigma(\phi(x))f_\sigma(\phi(y))) = \phi^{-\sigma} f_\sigma(\phi(x)\phi(y)) = \phi^{-1}(\phi(x)\phi(y)) = F(x, y)$ so that $T = T^\sigma$ and F is defined over k. Clearly F defines a group law on G' over k such that ϕ is an isomorphism from G' to G.

Let g be a 1-cocycle from $\mathfrak{g}$ to $\mathrm{Aut}_K G$ cohomologous to f, $g_\sigma = a^\sigma f_\sigma a^{-1}$. Let G'' be the k-form determined by g as above, say $g_\sigma = \psi^\sigma \psi^{-1}$. Then $\theta = \psi^{-1} a \phi$ is an isomorphism between G' and G'' and for each $\sigma \in \mathfrak{g}$, $\theta^\sigma = \psi^{-\sigma} a^\sigma \phi^\sigma = \psi^{-\sigma} a^\sigma f_\sigma \phi = \psi^{-\sigma} g_\sigma a \phi = \psi^{-1} a \phi = \theta$, so θ is defined over k. Therefore cohomologous cocycles give rise to equivalent k-forms.

Conversely as we have seen any k-form G' of G split by K defines a 1-cocycle from $\mathfrak{g}$ to $\mathrm{Aut}_K G$ given by $f_\sigma = \phi^\sigma \phi^{-1}$ where ϕ is the isomorphism defined over K between G' and G. Let G'' be another k-form of G split by K and defining the 1-cocycle g with $g_\sigma = \psi^\sigma \psi^{-1}$. Suppose that there is an isomorphism θ between G' and G'' defined over k. Then $a = \psi \theta \phi^{-1} \in \mathrm{Aut}_K G$ and $a^\sigma f_\sigma a^{-1} = (\psi^\sigma \theta \phi^{-\sigma})(\phi^\sigma \phi^{-1})(\phi \theta^{-1} \psi^{-1}) = \psi^\sigma \psi^{-1} = g_\sigma$ so that k-isomorphic k-forms define cohomologous cocycles. q.e.d.

For an algebraic group G defined over a field k we denote by G_k the group of points of G rational over k.

Theorem 2. *Let G be a connected algebraic group defined over a field k, K a Galois extension of k with Galois group $\mathfrak{g}$, G' a k-form of G split by K and f the 1-cocycle from $\mathfrak{g}$ to $\mathrm{Aut}_K G$ defined by G'. Let $G^* = \{x \in G_K,\ x^\sigma = f_\sigma(x) \text{ for all } \sigma \in \mathfrak{g}\}$. Then G^* is a group isomorphic to G'_k.*

Proof. Clearly G^* is a group. Let ϕ be the isomorphism between G' and G so that $f_\sigma = \phi^\sigma \phi^{-1}$. Then for $x \in G'_k$, $(\phi(x))^\sigma = \phi^\sigma(x^\sigma) = \phi^\sigma(x) = f_\sigma(\phi(x))$ and so $\phi(x) \in G^*$. Conversely, if $x \in G^*$ then $(\phi^{-1}(x))^\sigma = \phi^{-\sigma}(x^\sigma) = \phi^{-\sigma} f_\sigma(x) = \phi^{-1}(x)$ and so $\phi^{-1}(x) \in G'_k$. q.e.d.

If G is a simple algebraic group, the group of automorphisms A of G is a semi-direct product $A = H \cdot A_0$ where A_0 is the connected component of A (inner automorphisms) and H is a finite group rational over the prime field. In the case G is of type B_n, C_n, E_7, E_8, F_4, G_2 we have $H = \{e\}$ and if G is of type A_n, $D_n (n \neq 4)$, E_6 then H is cyclic of order 2 while G of type D_4 implies H is the symmetric group on three letters.

Lemma. *Let $A = H \cdot A_0$ and let $\mathfrak{g}$ be a group of operators on A which* *operates trivially on H. Let f be a* 1*-cocycle from* $\mathfrak{g}$ *to* A *and define* $\mathfrak{g}_0=\{\sigma\in\mathfrak{g},\ f_\sigma\in A_0\}$. *Then* $\mathfrak{g}_0$ *is a normal subgroup of* $\mathfrak{g}$ *and* $\mathfrak{g}/\mathfrak{g}_0$ *is isomorphic to a subgroup of* H.

PROOF. We write for each $\sigma\in\mathfrak{g}$, $f_\sigma=h_\sigma g_\sigma$ uniquely with $g_\sigma\in A_0$ and $h_\sigma\in H$. Since $f_{\tau\sigma}=f_\sigma^\tau f_\tau=h_\sigma g_\sigma^\tau h_\tau g_\tau=h_\sigma h_\tau h_\tau^{-1}g_\sigma^\tau h_\tau g_\tau$ we have $h_{\tau\sigma}=h_\sigma h_\tau$ and the map $\rho\colon\mathfrak{g}\to H$ defined by $\rho\colon\sigma\to h_\sigma^{-1}$ is a homomorphism. The kernel of ρ is just $\mathfrak{g}_0$ and the assertion of the lemma follows immediately.

THEOREM 3. *Let G be a simple algebraic group defined over the finite field k and G' a k-form of G. Then if G is of type B_n, C_n, E_7, E_8, F_4, G_2 we have G' is already split over k. If G is of type A_n, D_n $(n\neq 4)$, E_6 then G' is split over a quadratic extension of k while if G is of type D_4 then G' is split over a quadratic or a cubic extension of k.*

PROOF. Let G' be a k-form of G split by K determined by the 1-cocycle f from $\mathfrak{g}$ to $A=\operatorname{Aut} G=H\cdot A_0$ and let $\mathfrak{g}_0=\{\sigma\in\mathfrak{g},\ f_\sigma\in A_0\}$. By the lemma, $\mathfrak{g}_0$ is a normal subgroup of $\mathfrak{g}$; let K_0 be the fixed field of $\mathfrak{g}_0$ so that $\mathfrak{g}_0$ is the Galois group of K over K_0 and $\mathfrak{g}/\mathfrak{g}_0$ is the Galois group of K_0 over k. The restriction of f to $\mathfrak{g}_0$ is a 1-cocycle from $\mathfrak{g}_0$ to A_0 and by a theorem of S. Lang [1, Proposition 3] since A_0 is connected and k is finite, there exists $a\in A_0$ such that for all $\sigma\in\mathfrak{g}_0$, $f_\sigma=a^\sigma a^{-1}$. Let $g_\sigma=a^{-\sigma}f_\sigma a$; then g is a 1-cocycle from $\mathfrak{g}$ to A cohomologous to f and for all $\sigma\in\mathfrak{g}_0$, $g_\sigma=1$. Replacing f by g we see there is no loss of generality in assuming $f_\sigma=1$ for all $\sigma\in\mathfrak{g}_0$. Then if $f_\sigma=\phi^\sigma\phi^{-1}$ where ϕ is the isomorphism from G' to G defined over K, we have $\phi^\sigma=\phi$ for all $\sigma\in\mathfrak{g}_0$, i.e. ϕ is defined over K_0 and so G' is split over K_0.

Now $\mathfrak{g}/\mathfrak{g}_0$ is the Galois group of K_0 over k and by the lemma, $\mathfrak{g}/\mathfrak{g}_0$ is isomorphic to a subgroup of H. If G is of type B_n, C_n, E_7, E_8, F_4, G_2 then $H=\{e\}$ and $K_0=k$; if G is of type A_n, D_n $(n\neq 4)$, E_6 then H is cyclic of order 2 and either $K_0=k$ or K_0 is a quadratic extension of k; if G is of type D_4 then H is the symmetric group on three letters and so either $K_0=k$, K_0 is a quadratic extension of k, or K_0 is a cubic extension of k. q.e.d.

Applying Theorems 2 and 3 to the usual classical simple groups we obtain the rational points over finite fields. For example, for type A_n, if we take G to be $SL(n+1)$, k the field with q elements, K_0 the field with q^2 elements and denote by a bar the automorphism of G induced by the generator of the Galois group of K_0 over k, we have $G^*=\{x\in G_K,\ x^\sigma=f_\sigma(x)\}=\{x\in SL(n+1,\ K),\ \bar{x}={}^t x^{-1}\}$, i.e. G^* consists of unitary matrices. In this manner we obtain the usual finite simple groups and in addition, for E_6 with a quadratic extension and

D_4 with a cubic extension we obtain new ones (cf. R. Steinberg [2] and J. Tits [3]).

It is clear that analogous theorems may be proved for algebras. In this manner one can construct new simple Lie algebras as forms of E_6 and D_4. Also note the forms depend only on the automorphisms of the algebra. If we start with an involution on an associative algebra and consider either the Lie algebra of skew elements or the Jordan algebra of symmetric elements we consequently get an identical classification of forms.

Bibliography

1. S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. vol. 78 (1956) pp. 555–563.

2. R. Steinberg, *Variations on a theme of Chevalley*, Pacific J. Math. vol. 9 (1959) pp. 875–891.

3. J. Tits, *Sur la trialité et certains groupes qui s'en déduisent*, Inst. Hautes Études Sci. Publ. Math. no. 2 (1959) pp. 37–84.

4. A. Weil, *The field of definition of a variety*, Amer. J. Math. vol. 78 (1956) pp. 509–524.

Cornell University