Vol. 32, 1979 Fasc. 5

Torsion in linear algebraic groups over large algebraic fields

By

Moshe Jarden

Introduction. Let K be a finitely generated field (over its prime field). Let $\mathscr{G}(K_s/K)$ be the absolute Galois group of K. Every element $\sigma \in \mathscr{G}(K_s/K)$ is extended in the obvious way to an automorphism of the algebraic closure $\tilde{K}$ of K. If

$$(\sigma_1, \ldots, \sigma_e) \in \mathscr{G}(K_s/K)^e,$$

then $\tilde{K}(\sigma)$ denotes the fixed field of $\sigma_1, \ldots, \sigma_e$ in $\tilde{K}$. The following result was proved in [4] for $e = 1$.

A. *For almost all $\sigma \in \mathscr{G}(K_s/K)$, the field $\tilde{K}(\sigma)$ contains infinitely many roots of unity of prime order.* Here "almost all" is used in the sense of the normalized Haar measure defined on the compact group $\mathscr{G}(K_s/K)$.

Note that roots of unity are the points of finite order of the multiplicative group G_m of the field. For $e \geqq 2$ the following more comprehensive result was proved.

B. *For almost all $(\sigma) \in \mathscr{G}(K_s/K)^e$ and for every linear algebraic group G defined over $\tilde{K}(\sigma)$ the order of the torsion of $G(\tilde{K}(\sigma))$ is bounded.* Here $G(\tilde{K}(\sigma))$ denotes group of the $\tilde{K}(\sigma)$-rational points of G.

In particular, if G has only finitely many points of order m, for every m, then the torsion part $G_{tor}(\tilde{K}(\sigma))$ of $G(\tilde{K}(\sigma))$ is finite.

Note that the last condition is satisfied in the case where $G = T$ is a torus. Indeed, recall that an algebraic group T defined over a field L is said to be a torus, if it is isomorphic over $\tilde{L}$ to D_n, where $n = \dim T \geqq 1$. Here D_n (which is sometimes denoted by G_m^n) is the group of all n-tuples $(x_1, \ldots, x_n)$ of non-zero elements of the field, and the product is defined component-wise. Then the subgroup T_m of all m division points of T is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^n$, provided m is not divisible by the characteristic of p of L. In the latter case T_m is even smaller.

The aim of this note is first to complete the above results for tori by proving

Theorem C. *For almost all $\sigma \in \mathscr{G}(K_s/K)$ and for every torus T defined over $\tilde{K}(\sigma)$, there exist infinitely many primes l such that $T_l(\tilde{K}(\sigma)) \neq 1$.*

Note that C has been proved in [3] for elliptic curves E rather than for tori T. Indeed, the proof of C for tori uses methods developed both in [4] and in [3]. We

first prove a stronger theorem for D_n that involves the action of σ on the points of finite order D_n. Then we deduce C for arbitrary tori from the stronger theorem for D_n.

Finally we use structure theorems for linear algebraic groups and apply C to prove

Theorem D. *For almost all $\sigma \in \mathcal{G}(K_s/K)$ and for all connected linear algebraic groups G defined over $\tilde{K}(\sigma)$, the group $G(\tilde{K}(\sigma))$ contains infinitely many points of finite order, provided $G(\tilde{K})$ does.*

Another variant of Theorem D is

Theorem E. *Almost all $\sigma \in \mathcal{G}(K_s/K)$ have the following property: If G is a linear algebraic group defined over $\tilde{K}(\sigma)$ and if the order of the torsion of $G(\tilde{K})$ is not bounded, then there exists infinitely many primes l such that $G_l(\tilde{K}(\sigma)) \neq 1$.*

Acknowledgement. The author is indebted to Wulf-Dieter Geyer and to Gerhard Frey for discussions that led to the inclusion of Theorems D and E in the paper.

1. Fields of characteristic zero. We start with a description of the group $\mathrm{Aut}(D_n)$ of all (algebraic) automorphisms of D_n.

Lemma 1.1. $\mathrm{Aut}(D_n) \cong \mathrm{GL}(n, \mathbb{Z})$

Proof. Let $\varepsilon \in \mathrm{Aut}(D_n)$ and let ε_i be the projection of ε on the i-th coordinate. Then ε_i is an algebraic character of D_n and hence there exist $a_{i1}, \ldots, a_{in} \in \mathbb{Z}$ such that $\varepsilon_i(x_1, \ldots, x_n) = x_1^{a_{i1}}, \ldots, x_n^{a_{in}}$ for every non-zero elements $x_1, \ldots, x_n$ of the field over which D_n is defined (c.f. Borel [1, p. 208]). It follows that

$$\varepsilon(x_1, \ldots, x_n) = \left(\prod_{j=1}^{n} x^{a_{j1}}, \ldots, \prod_{j=1}^{n} x_j^{a_{nj}} \right) \tag{1}$$

and (a_{ij}) is a matrix in $\mathrm{GL}(n, \mathbb{Z})$. In particular $\det(a_{ij}) = \pm 1$. The Lemma follows.

Proposition 1.2. *Let K be a finitely generated field over $\mathbb{Q}$. Then for almost all $\sigma \in \mathcal{G}(\tilde{K}/K)$ and for every $\varepsilon \in \mathrm{Aut}(D_n)$ there exist infinitely many primes l for which there exists a point $P \in \tilde{K}^{x^n}$ of order l, such that $\varepsilon P = \sigma P$.*

Proof. The group $\mathrm{Aut}(D_n)$ is countable. Hence it suffices to prove that given an $\varepsilon \in \mathrm{Aut}(D_n)$, then for almost all $\sigma \in \mathcal{G}(\tilde{K}/K)$ there exist infinitely many primes l for which there exists a point $P \in \tilde{K}^{\times n}$ of order l such that $\sigma P = \varepsilon P$.

Indeed let (a_{ij}) be the matrix corresponding to ε by (1). Let $f(x)$ be the characteristic polynomial of (a_{ij}). By Čebotarev Density Theorem there exists a set Λ of primes having a positive density such that the congruence $f(x) \equiv 0 \bmod l$ is solvable for every $l \in \Lambda$. The assumption that K is finitely generated over $\mathbb{Q}$ implies that there exists a l_0 such that $\mathcal{G}(K(\zeta_l)/K) \cong (\mathbb{Z}/l\mathbb{Z})$ for every $l > l_0$, and that the set of fields $\{K(\zeta_l) \mid l > l_0\}$ is linearly disjoint over K. Here ζ_l denotes the root of unity of order l. Without loss of generality we can assume that $l > l_0$ for every $l \in \Lambda$.

Let $l \in \Lambda$ and choose a positive integer z such that $f(z) \equiv 0 \bmod l$. The integer z is a characteristic root of (a_{ij}) module l. Hence there exists integers $\alpha_1, \ldots, \alpha_n$, not all of them are divisable by l, such that $\sum_{j=1}^{n} a_{ij}\alpha_j \equiv z\alpha_i \bmod l$ for $i = 1, \ldots, n$. Let $\zeta = \zeta_l$. Then the order of $P = (\zeta^{\alpha_1}, \ldots, \zeta^{\alpha_n})$ is l and

$$\varepsilon(P) = (\zeta^{\sum a_{ij}\alpha_j}, \ldots, \zeta^{\sum a_{nj}\alpha_j}) = (\zeta^{z\alpha_1}, \ldots, \zeta^{z\alpha_n}). \tag{2}$$

The product of all the characteristic roots module l of (a_{ij}) is equal to $\pm \det(a_{ij}) = \pm 1$. Hence z is relatively prime to l. It follows that there exists an element $\sigma_l \in \mathscr{G}(K(\zeta)/K)$ such that $\sigma_l(\zeta) = \zeta^z$. This element satisfies $\sigma_l(P) = \varepsilon P$, by (2).

Denote by S the set of all $\sigma \in \mathscr{G}(\tilde{K}/K)$ for which there exist infinitely many $l \in \Lambda$ such that $\sigma | K(\zeta_l) = \sigma_l$. We know that $\sum_{l \in \Lambda} l^{-1} = \infty$. Hence, by the Borel-Cantelli lemma (c.f. [4, Lemma 1.4]) and by construction, S has measure 1. Moreover, for every $\sigma \in S$ there exist infinitely many primes l for which there exists a point $P \in \tilde{K}^{\times n}$ of order l such that $\varepsilon P = \sigma P$. ∎

Let K be a field and let L be a normal extension of K of degree d. Let G and G' be algebraic groups defined over K and L respectively. Suppose that there exists an isomorphism $\varphi: G \to G'$, of algebraic groups, defined over L. Let σ be an element of $\mathscr{G}(K_s/K)$. Then $\varepsilon_\sigma = (\sigma\varphi) \circ \varphi^{-1}$ belongs to $\mathrm{Aut}(G')$ and it is defined over L. Here $\sigma\varphi$ is the isomorphism of G onto G' obtained from φ by applying σ on the coefficients of φ. If $\sigma | L = 1$, then ε_σ is the identity map of G'. If τ is an additional element of $\mathscr{G}(K_s/K)$, then $\varepsilon_{\tau\sigma} = \tau\varepsilon_\sigma \circ \varepsilon_\tau$. Using induction we obtain

$$\varepsilon_{\sigma^k} = \sigma^{k-1}\varepsilon_\sigma \circ \sigma^{k-2}\varepsilon_\sigma \circ \cdots \circ \sigma\varepsilon_\sigma \circ \varepsilon_\sigma$$

for every positive integer k. If ε_σ is already defined over K, then $\sigma\varepsilon_\sigma = \varepsilon_\sigma$ and hence $\varepsilon_\sigma^d = 1$.

The possibility of reducing Theorem C to Proposition 1.2 is based on the following observation:

Let P be a point in $G(\tilde{K})$, let $P' = \varphi P$ and let $\sigma \in \mathscr{G}(K_s/K)$. Then

$$\sigma P = P \Leftrightarrow \sigma P' = \varepsilon_\sigma P'. \tag{3}$$

Lemma 1.3. *Let K be a finitely generated field over $\mathbb{Q}$ and let T be a torus which is defined over K. Then for almost all $\sigma \in \mathscr{G}(\tilde{K}/K)$ there exist infinitely many primes l such that $T_l(K(\sigma)) \neq 1$.*

Proof. There exists a finite normal extension L of K and there exists an isomorphism $\varphi: T \to D_n$ which is defined over L, where $n = \dim T$.

Let σ be an element of $\mathscr{G}(\tilde{K}/K)$ that satisfies the conclusion of Proposition 1.2. Then $\varepsilon_\sigma = \sigma\varphi \circ \varphi^{-1}$ is an automorphism of D_n. Using the observation (3) we conclude that there exist infinitely many primes l for which there exists a point $P \in T(\tilde{K}(\sigma))$ of order l. ∎

Remark. The above method of proof implies the stronger

Theorem. *Let K be a finitely generated field over $\mathbb{Q}$, let T be a torus defined over K and let $\delta \in \mathrm{Aut}(T)$. Then for almost all $\sigma \in G(\tilde{K}/K)$ there exists infinitely many primes l for which there exists a point $P \in T(\tilde{K})$ of order l such that $\sigma P = \delta P$.*

Indeed, one has only to define ε_σ in the last proof as $\sigma\varphi \cdot \delta \circ \varphi^{-1}$.

However, our methods fail to prove the analogous theorem in characteristic p. Therefore, for the sake of completeness, we have decided to prove the theorem only in the case of $\delta = 1$.

2. Fields of characteristic p.

Lemma 2.1. *Let $A \in \mathrm{GL}(n, \mathbb{Z})$ be a matrix of a finite order. Then for every l_0 there exists a q_0 such that if $q > q_0$ is a power of p, then there exists a prime $l > l_0$ such that q is a characteristic root of A module l.*

Proof. Let λ be a characteristic root of A. Then λ is a root of unity of order, say, m. Hence λ is on one side a root of the m-th cyclotomic polynomial $\Phi_m(X)$, which is irreducible and on the other side a root of the characteristic polynomial $f(X)$ of A. It follows that $\Phi_m(X)$ divides $f(X)$ in $\mathbb{Z}[X]$.

By a theorem of Carmichael [2, Thm. XXIII], there exists a k_0 such that for every $k > k_0$ the positive integer $p^{km} - 1$ has a primitive divisor, i.e. a prime l that divides $p^{km} - 1$ but does not divide $p^s - 1$ for every $s < km$. By taking k_0 large enough one can ensure that $l > \max(l_0, m)$. It follows for $q = p^k$ that $\mathrm{ord}_l q = m$, i.e. q is an m-th primitive of unity modulo l. Hence $\Phi_m(q) \equiv 0 \bmod l$, hence $f(q) \equiv 0 \bmod l$, i.e. q is a characteristic root of A module l. ∎

Consider now the group D_n in characteristic p and let ε be an automorphism of D_n given by a matrix $A = (a_{ij})$, as in Lemma 1.1. For every power q of p let π_q denote the Frobenius automorphism defined by $\pi_q(x) = x^q$.

Lemma 2.2. *If ε has a finite order, then for every l_0 there exists a q_0 such that for every p-power $q > q_0$ there exists a prime $l > l_0$ and a point $P \in D_n(\tilde{\mathbb{F}}_p)$ of order l such that $\varepsilon P = \pi_q P$.*

Proof. The matrix A corresponding to ε has a finite order. Let $l_0 > p$ be an integer and let q_0 be an integer as in Lemma 2.1. Consider a p-power $q > q_0$. Then there exists a prime $l > l_0$ such that q is a characteristic root of A module l. Let $(x_1, \ldots, x_n)$ be a characteristic vector of A module l that belongs to q, i.e.

$$\sum_{j=1}^{n} a_{ij} x_j \equiv q x_i \bmod l \quad \text{for} \quad i = 1, \ldots, n. \tag{1}$$

Let $\zeta = \zeta_l$. Then $(\zeta^{x_1}, \ldots, \zeta^{x_n})$ is a point of order l and

$$\varepsilon(\zeta^{x_1}, \ldots, \zeta^{x_n}) = \pi_q(\zeta^{x_1}, \ldots, \zeta^{x_n}), \quad \text{by (1)}. \quad ∎$$

Proposition 2.3. *For almost all $\sigma \in \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)$ and for every $\varepsilon \in \mathrm{Aut}(D_n)$ of a finite order, there exists infinitely many primes l for which there exists a point $P \in D_n(\tilde{\mathbb{F}}_p)$ of order l such that $\sigma P = \varepsilon P$.*

Proof. Let ε be an automorphism of D_n of order d. For every prime r denote by $\mathbb{F}_p^{(r)}$ the maximal r-extension of $\mathbb{F}_p$. It is an infinite Galois extension with

$$\mathcal{G}(\mathbb{F}_p^{(r)}/\mathbb{F}_p) \cong \mathbb{Z}_r .$$

In particular every infinite extension of $\mathbb{F}_p$ which is contained in $\mathbb{F}_p^{(r)}$ coincides with $\mathbb{F}_p^{(r)}$. Let σ be an element of $\mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)$ that does not belong to $\bigcup_{r|d} \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p^{(r)})$ and such that $M = \tilde{\mathbb{F}}_p(\sigma)$ is an infinite extension of $\mathbb{F}_p$. By [4, Lemma 2.1] almost all $\sigma \in \mathcal{G}(\tilde{\mathbb{F}}_p/\mathbb{F}_p)$ satisfy these conditions.

Suppose that we have already proved the existence of k primes $l_1 < \cdots < l_k$ for which there exist points $P_1, \ldots, P_k$ in $D_n(\tilde{\mathbb{F}}_p)$ of orders $l_1, \ldots, l_k$, respectively, such that $\sigma P_i = \varepsilon P_i$ for $i = 1, \ldots, k$. Our assumptions on σ imply that $M \cap \mathbb{F}_p^{(r)}$ is a finite field for every prime r that divides d. Hence by Lemma 2.2, there exists a p-power q such that

$$\prod_{r|d} M \cap \mathbb{F}_p^{(r)} \subseteq \mathbb{F}_p \subset M \tag{2}$$

and such that for every $1 \leqq i \leqq d$ there exists a prime $l_i' > l_k$ and a point

$$P_i' \in D_n(\tilde{\mathbb{F}}_p)$$

of order l_i' such that

$$\varepsilon^i P_i' = \pi_q P_i', \quad \text{for} \quad i = 1, \ldots, d \tag{3}$$

The relation (3) together with the simple observation that $\varepsilon \pi_q = \pi_q \varepsilon$ imply that $\pi_{q^d} P_i' = \pi_q^d P_i' = \varepsilon^{id} P_i' = P_i'$ for $i = 1, \ldots, d$. Hence $P_i' \in D_n(\mathbb{F}_{q^d})$. The restriction of σ to $\mathbb{F}_{q^d}$ generates the cyclic group $\mathcal{G}(\mathbb{F}_{q^d}/\mathbb{F}_q)$, since $[M : \mathbb{F}_q]$ is relatively prime to d and hence $M \cap \mathbb{F}_{q^d} = \mathbb{F}_q$. The restriction of π_q to $\mathbb{F}_{q^d}$ also generates this group. Hence there exists a $1 \leqq j < d$ which is relatively prime to d such that

$$\sigma \,|\, \mathbb{F}_{q^d} = \pi_q^j \,|\, \mathbb{F}_{q^d} .$$

Let $1 \leqq i < d$ be an integer such that $ij \equiv 1 \bmod d$. Then we have, by (3), that

$$\sigma P_i' = \pi_q^j P_i' = \varepsilon^{ij} P_i' = \varepsilon P_i' .$$

Define therefore $l_{k+1} = l_i'$ and $P_{k+1} = P_i'$ and the induction is completed. ∎

We apply Proposition 2.3 to obtain the analogue to Proposition 1.3 for tori in characteristic p.

Lemma 2.4. *Let K be a finitely generated field over $\mathbb{F}_p$ and let T be a torus which is defined over K. Then for almost all $\sigma \in \mathcal{G}(K_s/K)$ there exist infinitely many primes l such that $T_l(\tilde{K}(\sigma)) \neq 1$.*

Proof. The field $K_0 = \tilde{\mathbb{F}}_p \cap K$ is a finite extension of $\mathbb{F}_p$. Hence, the set S of all $\sigma \in \mathcal{G}(K_s/K)$ whose restriction to $\tilde{\mathbb{F}}_p$ satisfy the result of Proposition 2.3 is of measure 1.

Let L be a finite normal extension of K over which there exists an isomorphism $\varphi\colon T \to D_n$, where $n = \dim(T)$. (Actually one can choose L even as a Galois extension of K; c.f. Borel [1, p. 211].) Let $\sigma \in S$. Then $\varepsilon_\sigma = \sigma\varphi \circ \varphi^{-1}$ is an auto-

morphism of D_n, hence it is defined over K, by Lemma 1.1. It follows that $\mathrm{ord}(\varepsilon_\sigma)$ is finite, by the arguments preceding Lemma 1.3. Using Proposition 2.3 for $\varepsilon = \varepsilon_\sigma$ and (3) of Section 1, we conclude that there exist infinitely many primes l for which there exists a point $P \in D_n(\tilde{K})$ of order l such that $\sigma P = P$. ■

3. End of the proof of Theorem C. Relying on Lemma 1.3 and Lemma 2.4 we conclude the proof of Theorem C for a finitely generated field K of an arbitrary characteristic.

Let L be a finite extension of K and let T be a torus defined over L. Denote by L_0 the maximal separable extension of K which is contained in L. Define $S(L, T)$ to be the set of all $\sigma \in \mathcal{G}(K_s/K)$ such that $T_l(\tilde{K}(\sigma)) \neq 1$ for infinitely many primes l. Observe that $\tilde{L}_0(\sigma) = \tilde{L}(\sigma) = \tilde{K}(\sigma)$. Hence $\mathcal{G}(K_s/K) - S(L, T)$ is a zero set in $\mathcal{G}(K_s/K)$ by Lemmas 1.3 and 2.4.

The set of all $\sigma \in \mathcal{G}(K_s/K)$ that do not satisfy the conclusion of Theorem C is contained in the union of all the sets $\mathcal{G}(K_s/K) - S(L, T)$. Hence it is a zero set, since there are only countably many pairs (L, T) as above. ■

4. Linear algebraic groups. We recall that a quadratic matrix A with entries in a field L is said to be *unipotent* if all of its characteristic roots are equal to 1. In this case A is conjugate (over $\tilde{L}$) to an upper triangular matrix with 1's in the main diagonal. If $A \neq 1$ and if $\mathrm{char}(L) = 0$, then $\mathrm{ord}(A) = \infty$. If $\mathrm{char}(L) = p$, then $\mathrm{ord}(A)$ is a finite power of p.

A linear algebraic group is said to be *unipotent* if all of its elements are unipotent.

Lemma 4.1. *Let G be a connected linear algebraic group defined over a field L. Then G contains a torus T which is also defined over L or G is unipotent.*

Proof. If G contains a torus, then G contains a maximal torus T which is defined over K (c.f. Borel [1, p. 382]). The dimension of T is >0, since all the maximal tori of G are conjugate (c.f. [1, p. 263]). If G does not contain a torus, then G is unipotent (c.f. [1, p. 264]). ■

Proof of Theorem D. Let σ be an element of $\mathcal{G}(K_s/K)$ that satisfies the conclusion of Theorem C and such that $\tilde{K}(\sigma)$ is a infinite field. By Theorem C and by [4, Lemma 7.1] almost all σ have these properties.

Let $L = \tilde{K}(\sigma)$ and consider a connected linear algebraic group G defined over L such that $G_{\mathrm{tor}}(\tilde{K})$ is an infinite set. If G contains a torus which is defined over L, then $G_{\mathrm{tor}}(L)$ is infinite, by choice of σ. Otherwise G is unipotent, by Lemma 4.1. The assumption that $G_{\mathrm{tor}}(\tilde{K})$ is infinite implies now that $\mathrm{char}(L) = p$ and that $\dim(G) > 0$. The field L is infinite and perfect, hence there is an embedding of the additive group of L into $G(L)$ (c.f. [1, p. 362]). In particular $G(L)$ is an infinite torsion group. ■

Proof of Theorem E. Let σ be an element of $\mathcal{G}(K_s/K)$ that satisfies the conclusion of Theorem C and let $L = \tilde{K}(\sigma)$. Consider a linear algebraic group G defined over L such that the order of the torsion of $G(\tilde{K})$ is not bounded. Then the

connected component G^0 of the unit element of G is also defined over (c.f. [1, p. 86]). We claim that G^0 contains a torus defined over L, and hence there exist infinitely many primes l such that $G_l(L) \neq 1$.

Indeed, otherwise G^0 is an unipotent group and there exists an n such that G^0 can be embedded in the subgroup U_n of all upper triangular matrices of GL_n with 1's in the main diagonal (c.f. [1, p. 158]). If $\mathrm{char}(K) = 0$, then G^0 is torsion-free; if $\mathrm{char}(K) = p$, then every element of G^0 has an order which is a power of p not bigger then p^{n-1}, (c.f. [4, Lemma 9.3]). Since G^0 has a finite index in G (c.f. [1, p. 86]), it follows that the order of the torsion of $G(\tilde{K})$ is bounded, a contradiction to our assumption. ■

References

[1] A. Borel, Linear algebraic groups. New York 1961.
[2] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. Annals of Math. **15**, 30–70 (1913–1914).
[3] W.-D. Geyer and M. Jarden, Torsion points of elliptic curves over large algebraic extensions of finitely generated fields. Israel J. Math. **31**, 257–297 (1978).
[4] M. Jarden, Roots of unity over large algebraic fields. Math. Ann. **213**, 109–127 (1975).

Eingegangen am 28. 2. 1979

Anschrift des Autors:

M. Jarden
Department of Mathematics
Tel-Aviv University
Ramat-Aviv, Tel-Aviv
Israel