HAL
open science

p-Rank and p-groups in algebraic groups

Adrien Deloro

To cite this version:

Adrien Deloro. p-Rank and p-groups in algebraic groups. Turkish Journal of Mathematics, 2012, 36 (4), pp.578-582. 10.3906/mat-1103-52 . hal-01303309

HAL Id: hal-01303309

https://hal.science/hal-01303309

Submitted on 17 Apr 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Turk J Math
36 (2012) , 578 – 582.
© TÜBİTAK
doi:10.3906/mat-1103-52

p-Rank and p-groups in algebraic groups

Adrien Deloro

Abstract

A few remarks on the measures of the p-rank of a group equipped with a dimension, including the refutation of a result of Burdges and Cherlin.

Key Words: Algebraic groups, groups of finite Morley rank, torsion, p-groups

Groups of finite Morley rank are abstract analogues of algebraic groups; like them they bear a dimension enabling various genericity arguments. They do not come from geometry but from logic; yet the Cherlin-Zilber conjecture and related work suggest tight relationships between both aspects. My reader may thus view what follows as naive properties of algebraic groups obtained by elementary means; the word "definable" stands for "constructible". Should he desire more on groups of finite Morley rank, [1] would provide references.

I wish to thank Éric Jaligot for his many suggestions.

A group of finite Morley rank is *connected* if it has no proper definable subgroup of finite index. One lets H° be the *connected component* of a definable subgroup H, i.e. its smallest definable connected subgroup of finite index. This extends to arbitrary H: H is included in a smallest definable subgroup $d(H)$, one takes the connected component $d(H)^\circ$ and sets $H^\circ = H \cap d(H)^\circ$.

Throughout, p will be a prime (possibly 2). A *p-torus* T is a finite power of the Prüfer quasi-cyclic p-group $\mathbb{Z}_{p^\infty}$; $T \simeq \mathbb{Z}_{p^\infty}^d$ is injective among abelian groups. For $H \leq T$, H° consistently denotes the maximal subtorus of H.

A group of finite Morley rank is $U_p^\perp$ if it has no infinite elementary abelian p-subgroup. $U_p^\perp$ groups conjugate their *Sylow p-subgroups* [3, Theorem 4], i.e. their maximal (non-necessarily definable) p-subgroups; these are finite extensions of p-tori. Hence, for S a Sylow p-subgroup of a $U_p^\perp$ group, S° is a p-torus.

Given a $U_p^\perp$ group, 3 measures of its Sylow p-subgroups are available. One can consider the *Prüfer p-rank* $\mathrm{Pr}_p(G)$, which is the number of $\mathbb{Z}_{p^\infty}$ factors in a Sylow p-subgroup. One can also estimate the *normal p-rank* $n_p(G)$, which is the maximal p-rank of an elementary abelian p-group normal in a Sylow p-subgroup. Or one can simply compute the *p-rank* $m_p(G)$, which is the maximal p-rank of an elementary abelian p-subgroup. All 3 numbers are well defined by conjugacy of the Sylow p-subgroups, and $m_p(G) \geq n_p(G) \geq \mathrm{Pr}_p(G)$.

2010 *AMS Mathematics Subject Classification:* 20F11 (primary); 20G07, 20C11, 20D15.

1. The n-rank

Lemma 1 *If G is a connected, $U_p^\perp$ group, then $n_p(G) = \mathrm{Pr}_p(G)$.*

Proof. Let S be a Sylow p-subgroup of G, $V \lhd S$ an elementary abelian normal subgroup, and $v \in V$. As $V \lhd S$, $v^{S^\circ} \subseteq V$ which is finite; by connectedness, S° centralizes v. So $v \in C_S(S^\circ) = S^\circ$ by [3, Corollary 3.1], and $V \leq S^\circ$. □

2. Not quite a digression

For a p-torus $T \simeq \mathbb{Z}_{p^\infty}^d$, $\Omega_{p^n}(T)$ denotes the set of elements of order at most p^n.

Fact 1 *Let φ be an automorphism* of finite order *of a p-torus $T \simeq \mathbb{Z}_{p^\infty}^d$.*

1. *Suppose $\Omega_{p^2}(T) \leq C_T(\varphi)$. Then $\varphi = \mathrm{Id}$.*
2. *Suppose $\Omega_p(T) \leq C_T(\varphi)$. If $p = 2$, then $\varphi^2 = \mathrm{Id}$. If $p \neq 2$, then $\varphi = \mathrm{Id}$.*

Proof. This must be classical but I know no reference.

1. Up to taking a power of φ, we may assume that φ has prime order q. Let $x \notin C_T(\varphi)$ have minimal order. Then $\varphi(x^p) = x^p$ so there is $y \in \Omega_p(T) \setminus \{1\}$ with $\varphi(x) = xy$. By assumption $y \in C_T(\varphi)$, so $x = \varphi^q(x) = xy^q$ and $q = p$. Let $\hat{x}$ and $\hat{y}$ be such that $\hat{x}^p = x$ and $\varphi(\hat{x}) = \hat{x}\hat{y}$. Then $\hat{y}^p = y$ so $\hat{y} \in \Omega_{p^2}(T) \leq C_T(\varphi)$ and $\hat{x} = \varphi^p(\hat{x}) = \hat{x}\hat{y}^p = \hat{x}y$, a contradiction.
2. Since φ centralizes $\Omega_p(T)$, for $x \in \Omega_{p^2}(T)$ there is $y \in \Omega_p(T)$ with $\varphi(x) = xy$; hence $\varphi^p(x) = xy^p = x$ and $\Omega_{p^2}(T) \leq C_T(\varphi^p)$. So $\varphi^p = \mathrm{Id}$; we may assume $p \neq 2$. Represent $\varphi_{|\Omega_{p^3}(T)}$ by a matrix $M \in \mathrm{GL}_d(\mathbb{Z}/p^3\mathbb{Z})$. As $\Omega_p(T) \leq C_T(\varphi)$, the reduction of M modulo p is the identity: there is a matrix N with $M = \mathrm{Id} + pN$. Since $\varphi^p = \mathrm{Id}$,
$$0 \equiv \sum_{\ell=1}^{p} \binom{p}{\ell} p^\ell N^\ell \equiv p^2 N + \frac{p(p-1)}{2} p^2 N^2 \quad [p^3].$$
Since $p \neq 2$, p divides $\frac{p(p-1)}{2}$, so $p^2 N \equiv 0[p^3]$ and $N \equiv 0[p]$. Hence the reduction of $M = \mathrm{Id} + pN$ modulo p^2 is the identity: M centralizes $\Omega_{p^2}(T)$, and φ is trivial. □

Consequence *If $p \neq 2$, the restriction map $\rho : \mathrm{Aut}(T) \to \mathrm{Aut}(\Omega_p(T))$ kills no element of finite order. In particular if W is a finite subgroup of $\mathrm{Aut}(T)$ then W embeds into $\mathrm{Aut}(\Omega_p(T)) \simeq \mathrm{GL}_d(\mathbb{F}_p)$. If $p = 2$ then $\ker \rho_{|W} \hookrightarrow (\mathbb{Z}/2\mathbb{Z})^d$.*

Proof. The only non-immediate claim is about the rank of $K = \ker \rho_{|W}$ when $p = 2$. Observe that K has exponent 2, so it is abelian. We go in a direction that will prove fruitful. Taking automorphism groups changes inductive limits to projective limits, so $\mathrm{Aut}(T) \simeq \varprojlim \mathrm{Aut}((\mathbb{Z}/p^n\mathbb{Z})^d) = \varprojlim \mathrm{GL}_d(\mathbb{Z}/p^n\mathbb{Z}) = \mathrm{GL}_d(\mathbb{Z}_p)$. Hence K embeds into $\mathrm{GL}_d(\mathbb{Z}_2)$. Now elements of K are simultaneously diagonalizable over $\bar{\mathbb{Q}}_2$ with eigenvalues ± 1, so

K embeds into $\{\pm 1\}^d$. □

We could use a similar method to get a lazy bound on $\operatorname{rk} W$ for $W \leq \operatorname{Aut}(T)$ an elementary abelian p-group; observe how we are naturally moving towards the p-adic representation. Anyway, embedding into $\mathrm{GL}_d(\mathbb{F}_p)$, i.e. restricting to $\Omega_p(T)$, was too clumsy in the first place. For instance, any element of $\mathrm{GL}_d(\mathbb{F}_p)$ comes from an element of $\mathrm{GL}_d(\mathbb{Z}_p)$, but not necessarily from one of finite order. (The reader may check that $\mathrm{GL}_2(\mathbb{Z}_5)$ has no element of order 5.) Representation-theoretically speaking, embedding into $\mathrm{GL}_d(\mathbb{Z}_p)$ is more appropriate, and this is what we shall now do.

3. Bounding the m-rank

Let φ be an automorphism of order p of a p-torus $T \simeq \mathbb{Z}_{p^\infty}^d$.

Fact 2 (Maschke's Theorem) *Let $T_1 \leq T$ be a φ-invariant subtorus. Then there is a φ-invariant subtorus $T_2 \leq T$ such that $T = T_1 + T_2$ and $T_1 \cap T_2 \leq \Omega_p(T_1)$.*

Proof. There is a subtorus $T_0 \leq T$ with $T = T_1 \oplus T_0$. Let π be the projection on T_1 along T_0 and $\hat{\pi} = \sum_{i=0}^{p-1} \varphi^i \pi \varphi^{-i}$. Then $\hat{\pi}$ is φ-covariant, $\operatorname{im} \hat{\pi} = T_1$, and $\hat{\pi}(t_1) = pt_1$ for $t_1 \in T_1$. Take T_2 to be the maximal subtorus of $\ker \hat{\pi}$. □

Fact 3 (φ, T as above) *If $C_T^\circ(\varphi) = 1$ then $p-1 | d$ and $\mathrm{Id} + \varphi + \cdots + \varphi^{p-1} = 0$.*

Proof. (This again must be well known.) We may assume $p \neq 2$. Let $\tau \leq T$ be isomorphic to $\mathbb{Z}_{p^\infty}$, and set $\Theta = \sum_{i=0}^{p-1} \varphi^i(\tau)$; Θ is φ-invariant and $\mathrm{Pr}_p(\Theta) \leq p$. So by Maschke's Theorem, we may assume $d \leq p$. As in the proof of the Consequence above, let us view φ as an element of order p of $\mathrm{GL}_d(\mathbb{Z}_p) \leq \mathrm{GL}_d(\mathbb{Q}_p)$. By assumption, 1 is not an eigenvalue.

The minimal polynomial μ of φ over $\mathbb{Q}_p$ divides $X^p - 1 = (X-1)(1 + X + \cdots + X^{p-1})$, so it divides $1 + X + \cdots + X^{p-1}$. The latter is irreducible over $\mathbb{Z}_p$ by Eisenstein's criterion, so $\mu = 1 + X + \cdots + X^{p-1}$. But μ divides the characteristic polynomial which has degree d. So $p - 1 \leq d \leq p$. Over $\bar{\mathbb{Q}}_p$, φ has $p-1$ eigenvalues, which sum to -1. So if $d = p$, one of them, say j, occurs twice: hence $1 + \operatorname{Tr} \varphi = j \in \mathbb{Q}_p$, against $p \neq 2$. So $d = p - 1$. □

Lemma 2 *For $W \leq \operatorname{Aut} \mathbb{Z}_{p^\infty}^d$ an elementary abelian p-group, $\operatorname{rk} W \leq \frac{1}{p-1} d$.*

Proof. $E = \mathbb{Q}_p^d$ is a sum of W-irreducible subspaces $\oplus_{i \in I} E_i \bigoplus \oplus_{j \in J} F_j$ with E_i's the W-trivial lines. Since W is abelian, it acts W-covariantly. Let $\rho_j : W \to \operatorname{Aut}_W(F_j)$ be the restriction map, with (non-trivial) image W_j and kernel K_j. Each $\operatorname{End}_W F_j$ is a skew-field by Schur's Lemma, so the abelian group W_j of exponent p has order p. As $C_W(E) = 1$, $W \hookrightarrow \prod_{j \in J} W/K_j$, and $\operatorname{rk} W \leq \# J$. By Fact 3, $\dim F_j \geq p - 1$, whence $\# J \leq \frac{d}{p-1}$. □

Corollary 1 *Let G be a connected, $U_p^\perp$ group. Then $m_p(G) \leq \frac{p}{p-1} \mathrm{Pr}_p(G)$.*

Proof. For $V \leq S$ an elementary abelian subgroup of a Sylow p-subgroup S, write $V = (V \cap S^\circ) \oplus W$. By [3, Corollary 3.1], $C_S(S^\circ) = S^\circ$; use Lemma 2. □

4. Maximal abelian p-subgroups

Thesis [2, Theorem 1.2] *Let G be a connected, $U_p^\perp$ group with $m_p(G) \geq 3$. Then any maximal elementary abelian p-subgroup $V < G$ has p-rank at least 3.*

The flaw in [2] lies at the bottom of page 172. On the very last line, "commutation with v" need not in general be "a map from $\Omega_1(T)/A$ to A". Observe that in [2] Theorem 6.4 relies on Corollary 4.2, which relies on Theorem 1.2.

Counter-Example *In $\mathrm{PSL}_5(\mathbb{C})$ let Θ be the usual torus and σ be the Weyl element naturally associated with the 5-cycle (12345). Let $\theta \in C_\Theta(\sigma) \setminus \{1\}$. Then $\langle \theta, \sigma \rangle$ does not extend to an elementary abelian 5-group of rank 3.*

Proof. The actual computations will take place in $\mathrm{SL}_5(\mathbb{C})$. Let $\lambda = e^{\frac{2i\pi}{5}} \in \mathbb{C}$; then $Z(\mathrm{SL}_5(\mathbb{C})) = \{\lambda^k \,\mathrm{Id}\}$. The matrix $s = (\delta_{j,i+1}) \in \mathrm{SL}_5(\mathbb{C})$ (equality modulo 5) reduces modulo $Z(\mathrm{SL}_5(\mathbb{C}))$ to $\sigma \in \mathrm{PSL}_5(\mathbb{C})$; conjugation by s rotates coefficients of a matrix $(m_{i,j}) \in \mathrm{SL}_5(\mathbb{C})$ along the 5 (complete) diagonals. So given $\theta \in \Theta \leq \mathrm{PSL}_5(\mathbb{C})$ and a diagonal matrix $t \in \mathrm{SL}_5(\mathbb{C})$ representing it, one sees that $[\sigma, \theta] = 1$ iff $t_{i,i} = \lambda^{k+\ell i}$ for some integers k and ℓ; thus $C_\Theta(\sigma)$ has order 5. Fix $\theta \in C_\Theta(\sigma) \setminus \{1\}$. Conjugation by t on $(m_{i,j})$ multiplies $m_{i,j}$ by $\lambda^{\ell(j-i)}$. So $C(\theta) = \Theta \rtimes \langle \sigma \rangle$, and $\langle \theta, \sigma \rangle$ is maximal. □

The following merely serves the purpose of exposing an important method.

Observation *Let G be a connected, $U_p^\perp$ group, and $S \leq G$ a Sylow p-subgroup. Then S is connected iff abelian iff nilpotent.*

Proof. Only one claim is non-trivial; we prove it by induction on the Morley rank (read: dimension) of G. Suppose S nilpotent; let $\omega \in S$. Then by nilpotence, $\tau = C^\circ_{S^\circ}(\omega) \neq 1$. By [3, Corollary 3.1], ω lies in any maximal p-torus of $C^\circ(\omega)$, so $\omega \in C^\circ(\tau)$. Hence $\langle S^\circ, \omega \rangle \leq C^\circ(\tau)$. If $C^\circ(\tau) < G$ we are done by induction. Otherwise τ is central and we can factor by $Z^\circ(G)$, pursuing by induction. □

I shall now bring my reader some comfort.

Lemma 3 *The thesis of* [2, Theorem 1.2] *holds for $p = 2$, and so does* [2, Corollary 6.5].

Proof. Suppose $m_2(G) \geq 3$; clearly $\mathrm{Pr}_2(G) \geq 2$. Let i, j be 2 commuting involutions; by torality [3, Theorem 3] there is a Sylow 2-subgroup S with $i \in S^\circ$ and $j \in S$.

Suppose $\mathrm{Pr}_2(G) \geq 3$. If $j \in S^\circ$ we are done. If not, consider the map $\varphi(k) = [j, k] : \Omega_2(S^\circ) \to \Omega_2(S^\circ)$. Then $\mathrm{im}\,\varphi \leq \ker \varphi$ and $\mathrm{rk}\,\mathrm{im}\,\varphi + \mathrm{rk}\ker\varphi \geq 3$, so $\mathrm{rk}\ker\varphi \geq 2$ and we are done. From now on, suppose $\mathrm{Pr}_2(G) = 2$ (so $m_2(G) \leq 4$) and let $V = \Omega_2(S^\circ)$.

Assume first that $j \in S \setminus S^\circ$. If j inverts S° then $\langle i, j \rangle \leq \langle V, j \rangle$: we are done. Otherwise $\tau = C^\circ_{S^\circ}(j) \neq 1$. If $i \notin \tau$ then $\langle i, j \rangle \leq \langle i, \Omega_2(\tau), j \rangle$: we are done. So assume $i \in \tau \leq C^\circ(j)$. By torality [3, Theorem 3 and Corollary 3.1], i lies in a 2-torus of $C^\circ(j)$ and j lies in *any* 2-torus of $C^\circ(j)$, so i and j are cotoral.

So assume that $j \in S^\circ$, that is $V = \langle i, j\rangle$. By assumption there is an elementary abelian 2-subgroup of rank 3: $A = \langle r, s, t\rangle \leq S$; clearly $A \cap S^\circ \neq 1$, say $r \in V$. If s or t is in V then $\langle i, j\rangle = V \leq A$: we are done. Suppose that s and t (hence st as well) lie in $S \setminus S^\circ$. Since $|\operatorname{Aut}(V)| = 6$, one of s, t, st must centralize $V = \langle i, j\rangle$: we are done again. □

Here is a final word on counter-examples.

Lemma 4 *Let G be a counter-example to* [2, Theorem 1.2]. *Then* $\mathrm{Pr}_p(G) = p - 1$. *In particular,* [2, Theorem 1.2] *also holds for* $p = 3$.

Proof. By Lemma 3, $p \geq 3$. As $m_p(G) \geq 3$, one sees with Corollary 1 that $\mathrm{Pr}_p(G) \geq 2$. Equality can hold only for $p = 3$; as there is an elementary 3-group of rank 3, there is an automorphism of order 3 fixing $\Omega_3(\mathbb{Z}_{3^\infty}^2)$, against Fact 1: equality cannot hold.

Hence $\mathrm{Pr}_p(G) \geq 3$. Let $V = \langle \alpha, \omega\rangle$ be a maximal abelian p-group and $S \geq V$ a Sylow p-subgroup. By torality we may assume $\alpha \in S^\circ$, so $\omega \in S \setminus S^\circ$. If $C^\circ_{S^\circ}(\omega) \neq 1$ then by maximality, $\alpha \in C^\circ_{S^\circ}(\omega) \leq C^\circ(\omega)$, and as in the proof of Lemma 3, α and ω are cotoral, a contradiction. Hence $C^\circ_{S^\circ}(\omega) = 1$. Let $\varphi \in \operatorname{End}\Omega_p(S^\circ)$ map x to $[x, \omega]$; writing ω as an automorphism, $\varphi(x) = \omega(x) - x$ and $\varphi^n(x) = \sum_{i=0}^n (-1)^i \binom{n}{i} \omega^i(x)$. As $(-1)^i \binom{p-1}{i} \equiv 1\ [p]$, $\varphi^{p-1} = \mathrm{Id} + \omega + \cdots + \omega^{p-1}$. But $C^\circ_{S^\circ}(\omega) = 1$, so Fact 3 applied to ω implies $\varphi^{p-1} = 0$. Since $\ker\varphi = C_{\Omega_p(S^\circ)}(\omega) = \langle\alpha\rangle$, one has $\operatorname{rk}\Omega_p(S^\circ) \leq p - 1$. □

References

[1] Borovik, A., Nesin, A.: Groups of Finite Morley rank, volume 26 of *Oxford Logic Guides*. New York. Clarendon 1994.

[2] Burdges, J., Cherlin, G.: A generation theorem for groups of finite Morley rank J. Math. Logic 8(2) 163–195, (2008).

[3] Burdges, J., Cherlin, G.: Semisimple torsion in groups of finite Morley rank. J. Math. Logic 9(2) 183–200, (2009).

Adrien DELORO
Institut de Mathématiques de Jussieu,
Université Paris 6; 4, place Jussieu
75252 Paris Cedex 05, FRANCE
e-mail: adeloro@math.jussieu.fr

Received: 01.04.2011