CAHIERS DE TOPOLOGIE ET GEOMETRIE DIFFERENTIELLE CATEGORIQUES

Vol. LVII-3 (2016)

ON A CONJECTURE OF DEGOS

by Nick GILL

Résumé. Dans cette note nous prouvons une conjecture de Degos à propos des groupes engendrés par des matrices compagnons dans $\mathrm{GL}_n(q)$.

Abstract. In this note we prove a conjecture of Degos concerning groups generated by companion matrices in $\mathrm{GL}_n(q)$.

Keywords. Companion matrices; finite fields; general linear group; group generation.

Mathematics Subject Classification (2010). 20H30; 15A99.

1. Introduction

Let $\mathbb{F}$ be a field, and let $f \in \mathbb{F}[X]$ be a polynomial of degree n, i.e.

$$f(X) = a_n X^n + a_{n-1} X_{n-1} + \cdots + a_1 X + a_0$$

where $a_0, \ldots, a_n \in \mathbb{F}$. Recall that the *companion matrix* of f is the $n \times n$ matrix

$$C_f := \begin{bmatrix} 0 & \cdots & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & & & 0 & -a_1 \\ 0 & 1 & 0 & & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & 1 & 0 & -a_{n-2} \\ 0 & \cdots & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}.$$

The matrix C_f has the property that its minimal polynomial and its characteristic polynomial are both equal to f. Conversely, if $g \in \mathrm{GL}_n(\mathbb{F})$ has minimal polynomial and characteristic polynomial both equal to some polynomial f, then g is conjugate in $\mathrm{GL}_n(\mathbb{F})$ to C_f.

Recall in addition that if $\mathbb{F}$ has order q and $f \in \mathbb{F}[X]$ has degree n, then f is called *primitive* if it is the minimal polynomial of a primitive element $x \in \mathbb{F}$. In [Deg13], J.-Y. Degos makes the following conjecture.

Conjecture 1. *Let $\mathbb{F}$ be a field of order p a prime, let $g = X^n - 1$ and let $f \in \mathbb{F}[X]$ be a primitive polynomial of degree n. Then $\langle C_f, C_g\rangle = \mathrm{GL}_n(p)$.*

We will prove a stronger version of this conjecture. Specifically, we prove the following.

Theorem 2. *Let $\mathbb{F}$ be a finite field of order q and let $f, g \in \mathbb{F}[X]$ be distinct polynomials of degree n such that f is primitive, and the constant term of g is non-zero. Then $\langle C_f, C_g\rangle = \mathrm{GL}_n(q)$.*

For the rest of this paper $\mathbb{F}$ is a finite field of order q.

2. Field-extension subgroups

Let $\mathbb{K} = \mathbb{F}(\alpha)$ be an algebraic extension of $\mathbb{F}$ of degree d. Let $W = \mathbb{K}^a$, and observe that W is both an a-dimensional vector space over $\mathbb{K}$ and an ad-dimensional space over $\mathbb{F}$.

A $\mathbb{K}/\mathbb{F}$-*semilinear automorphism* of W, ϕ, is an invertible map $\phi : W \to W$ for which there exists $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ such that, for all $v_1, v_2 \in W$ and $k_1, k_2 \in \mathbb{K}$,

$$\phi(k_1 v_1 + k_2 v_2) = k_1^\sigma \phi(v_1) + k_2^\sigma \phi(v_2).$$

We define a group

$$\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W) = \{\phi : W \to W \mid \phi \text{ is a } \mathbb{K}/\mathbb{F}\text{-semilinear automorphism of } W\}.$$

The group $\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W)$ can be written as a product $\mathrm{GL}_a(\mathbb{K}).F$ where F is a cyclic group of degree d generated by the automorphism

$$W \to W,\ (w_1, \dots, w_d) \mapsto (w_1^q, \dots, w_d^q).$$

We will refer to elements of F as *field-automorphisms* of W.

Now, for $\mathcal{B} = \{v_1, \dots, v_{ad}\}$ an ordered $\mathbb{F}$-basis of W and $\phi \in \Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W)$, we define the following matrix

$$(\phi)_{\mathcal{B}} = \left[\ \phi(v_1) \mid \phi(v_2) \mid \cdots \mid \phi(v_{ad})\ \right].$$

It is a well-known fact that the map

$$\Phi_{\mathcal{B}} : \Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W) \to \mathrm{GL}_{ad}(q), \phi \mapsto (\phi)_{\mathcal{B}}$$

is a well-defined injective group homomorphism, the image of which is a group E known as a *field-extension subgroup of degree* d in $\mathrm{GL}_{ad}(q)$. Indeed, more is true: if we define

$$\theta : W \to \mathbb{F}^{ad}, w \mapsto [w]_{\mathcal{B}},$$

and consider $\Phi_{\mathcal{B}}$ to be a map $\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W) \to E$, then the pair (Φ, θ) is a permutation group isomorphism. (Here, and throughout this note, we consider groups acting on the left.)

Note that the group $\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W)$ contains a unique normal subgroup N isomorphic to $\mathrm{GL}_a(\mathbb{K})$. Then $H = \Phi_{\mathcal{B}}(N)$ is a subgroup of $\mathrm{GL}_{ad}(q)$ isomorphic to $\mathrm{GL}_a(\mathbb{K})$ and, writing $G = \mathrm{GL}_{ad}(q)$, one can check that $N_G(H) = E$, the associated field-extension subgroup. (To see this, note, firstly, that $E \leq N_G(H) \leq N_G(Z(H))$; now [KL90, Proposition 4.3.3 (ii)] asserts that $N_G(Z(H))) = E$ and we are done.)

3. Singer cycles

Recall that a *Singer subgroup* of the group $\mathrm{GL}_n(q)$ is a cyclic subgroup of order $q^n - 1$. In this section we prove the following lemma.

Lemma 3. *Let $g \in \mathrm{GL}_n(q)$ and let f be its minimal polynomial. Then $\langle g \rangle$ is a Singer subgroup if and only if f is primitive of degree n.*

What is more, if $S = \langle g \rangle$ is a Singer subgroup, then $\langle g \rangle$ is conjugate to $\langle C_f \rangle$, and $S = \Phi_{\mathcal{B}}(GL_1(\mathbb{K}))$, where $\mathbb{K}$ is a degree n extension of $\mathbb{F}$, and $\mathcal{B}$ is an ordered $\mathbb{F}$-basis of $\mathbb{K}$.

Proof. Suppose that $S = \langle g \rangle$ is a Singer subgroup. Then g contains an eigenvalue α that lies in $\mathbb{K}$, a degree n extension of $\mathbb{F}$, and no smaller field. What is more, since g has order $q^n - 1$, so does α and so the minimal polynomial of g is primitive of degree n as required.

Suppose, on the other hand, that f is primitive of degree n. Then the eigenvalues of g are $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$; in particular they are all distinct. Elementary linear algebra implies that g is conjugate to C_f, the companion matrix of f. It is enough, then, to prove that $\langle C_f \rangle$ is a Singer cycle.

Let α be a primitive element of degree n over $\mathbb{F}$ and a root of f; let $\mathbb{K} = \mathbb{F}(\alpha)$, an extension of $\mathbb{F}$ of degree n. We construct a field-extension subgroup

G of degree n in $\mathrm{GL}_n(q)$ as the image of the map $\Phi_{\mathcal{B}} : \Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(\mathbb{K}) \to \mathrm{GL}_n(q)$ where $\mathcal{B} = \{\alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

By construction H is isomorphic to $\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(\mathbb{K})$ and, in particular, contains a subgroup isomorphic to $\mathrm{GL}_1(\mathbb{K}) \cong \mathbb{K}^*$. This subgroup is cyclic of order $q^n - 1$ and is generated by the invertible linear transformation

$$L_\alpha : \mathbb{K} \to \mathbb{K}, x \mapsto \alpha \cdot x.$$

Now our construction guarantees that $\Phi_{\mathcal{B}}(L_\alpha) = C_f$ and we conclude, as required, that C_f generates a cyclic subgroup of $\mathrm{GL}_n(q)$ of order $q^n - 1$. In fact we have shown that $\langle C_f \rangle = \Phi_{\mathcal{B}}(GL_1(\mathbb{K}))$ and the final statement follows. □

4. Two companion matrices

Lemma 4. *Let H be a field-extension subgroup of degree a in $\mathrm{GL}_{ad}(q)$. A non-trivial element of H fixes at most $(q^a)^{d-1}$ elements of $V = (\mathbb{F})^{ad}$.*

Proof. We observed in §2 that the action of H on V is isomorphic to the action of $\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W)$ on $W = \mathbb{K}^a$ where $\mathbb{K}$ is a degree d extension of $\mathbb{F}$. Thus we set ϕ to be a non-trivial element of $\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W)$.

If ϕ lies in $\mathrm{GL}_a(\mathbb{K})$ and is non-trivial, then basic linear algebra implies that the fixed-point set is a proper $\mathbb{K}$-subspace of W and so fixes at most $(q^a)^{d-1}$ elements of W.

Suppose that ϕ does not lie in $\mathrm{GL}_a(\mathbb{K})$. Thus we can write $\phi = h\sigma$ where h is linear and σ is a non-trivial field automorphism of W that fixes $(\mathbb{F})^a$.

Thus if $v \in \mathbb{K}^a$ and $v^\phi = v$ we obtain immediately that $v^h = v^{\sigma^{-1}}$. Now if c is a scalar that is not fixed by σ, then we obtain immediately that $(cv)^h \neq (cv)^{\sigma^{-1}}$. Since v and c were arbitary we conclude immediately that g fixes at most $(q^b)^d$ elements where b is some proper-divisor of a. The result follows. □

Corollary 5. *If C_f and C_g are companion matrices of distinct monic polynomials $f, g \in \mathbb{F}[x]$ of degree n, then $\langle C_f, C_g \rangle$ does not lie in a field-extension subgroup of $\mathrm{GL}_n(q)$.*

Proof. We consider the action of $\mathrm{GL}_n(q)$ on $V = \mathbb{F}^n$. Observe that the images of the first $n - 1$ elementary basis vectors are the same for both

C_f and C_g. In particular, then, the matrix $C_f^{-1}C_g$ fixes the $\mathbb{F}$-span of these $n-1$ vectors and so fixes at least q^{n-1} vectors. The previous lemma implies that, since $C_f \neq C_g$, we can conclude that $\langle C_f, C_g\rangle$ is not a subgroup of a field-extension subgroup of $\mathrm{GL}_n(q)$. □

5. A result about subgroups

To complete the proof of Theorem 2 we will need the result below, Theorem 7. In an earlier draft of this article, we attributed this result to Kantor [Kan80]. We are grateful to Peter Mueller who pointed out that Kantor's result relies on another paper – [CK79] – which has subsequently been found to contain a number of errors.

In fact it is clear that the errors in [CK79] are not fatal and that, with a little adjustment, the result still holds [Cam]. However, since no proof exists in the literature, we will sketch one below. Our approach uses a theorem of Hering [Her85], a proof of which can be found in [Lie87, Appendix 1]. The disadvantage of our proof is that it relies on the Classification of Finite Simple Groups (CFSG), which Kantor's original approach did not.

Lemma 6. *Suppose that S is a Singer cycle in $\mathrm{GL}_n(q)$. Then, for each integer d dividing n, there is a unique field-extension subgroup $\Phi_{\mathcal{B}}(\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(W))$ (where $\mathbb{K}$ is a field extension of $\mathbb{F}$ of degree d) that contains S.*

Proof. Let H be a subgroup of $\mathrm{GL}_n(q)$ that contains S and suppose that $H \cong \mathrm{GL}_{n/d}(q^d)$ for some divisor d of n. Now S is a Singer cycle in H and so $S = \Phi_{\mathcal{C}}(\mathrm{GL}_1(\mathbb{L}))$ where $\mathbb{L}$ is a degree n/d extension of $\mathbb{F}_{q^d}$.

Write Z for the unique subgroup of S of order q^d-1. Direct calculation confirms that Z coincides with the center of H. Thus $H \leq C_{\mathrm{GL}_n(q)}(Z)$. But Z is precisely the $\mathbb{F}_{q^d}$-scalar maps on $\mathbb{L}$, and so (as we saw earlier, using [KL90, Proposition 4.3.3(ii)]) $N_{\mathrm{GL}_n(q)}(Z)$ is a field-extension subgroup $\Phi_{\mathcal{B}}(\Gamma\mathrm{L}_{\mathbb{K}/\mathbb{F}}(\mathbb{L}))$ where $\mathbb{K}$ is a field extension of $\mathbb{F}$ of degree d. But now H must be the unique normal subgroup of this field-extension subgroup that is isomorphic to $\mathrm{GL}_{n/d}(q^d)$ and we are done. □

In the proof above we refer to two ordered $\mathbb{F}$-bases of $\mathbb{L}$, namely $\mathcal{B}$ and $\mathcal{C}$. It is an easy exercise to see that we can take $\mathcal{B}$ to be equal to $\mathcal{C}$.

Theorem 7. *Let L be a proper subgroup of $G = \mathrm{GL}_n(q)$ that contains a Singer cycle. Then L contains a normal subgroup H isomorphic to $\mathrm{GL}_a(q^c)$ with $n = ac$ and $c > 1$. What is more H is equal to $\Phi_{\mathcal{B}}(\mathrm{GL}_a(\mathbb{K}))$ for $\mathbb{K}$ some field extension of $\mathbb{F}$ of degree c, and $\mathcal{B}$ some ordered $\mathbb{F}$-basis of $\mathbb{K}^a$.*

Proof. It is convenient, first, to deal with the case when $n = 2$. If L lies inside the normalizer of a non-split torus, then L contains a normal subgroup $H \cong \mathrm{GL}_1(q^2)$, as required. Furthermore, order considerations imply that L is a subgroup of neither the normalizer of a split torus, nor a Borel subgroup of $\mathrm{GL}_2(q)$.

The remaining subgroups of $\mathrm{GL}_2(q)$ can be deduced from a classical theorem of [Dic58]. In particular, $L \cap \mathrm{SL}_2(q)$ is isomorphic to either A_4, S_4, A_5 or a double cover of one of these. In particular the maximal order of an element of $L \cap \mathrm{SL}_2(q)$ is 10. Since $L \cap \mathrm{SL}_2(q)$ must contain an element of order $q + 1$, we conclude that $q \leq 9$. Now computation in the remaining groups (using, for example, [GAP15]) rules out the remaining possibilities.

Assume, then that $n \geq 3$, and we refer to Hering's Theorem, as presented in [Lie87, Appendix 1]. This result lists those subgroups of $\mathrm{GL}_\ell(p)$ (for $\ell \in \mathbb{Z}^+$) that act transitively on the set of non-zero vectors of $(\mathbb{F}_p)^\ell$. Since G embeds naturally (inside a field extension subgroup) in $\mathrm{GL}_\ell(p)$ for $\ell = n \log_p q$ and, since a Singer cycle acts transitively (via this embedding) on the set of non-zero vectors in $(\mathbb{F}_p)^\ell$, this list contains all the possible groups L. In what follows we fix a field-extension embedding

$$\Phi_{\mathcal{D}} : G \hookrightarrow \mathrm{GL}_\ell(p)$$

for $\ell = n \log_p q$, and $\mathcal{D}$ an ordered $\mathbb{F}_p$-basis of $(\mathbb{F})^n$. We obtain an associated action on the vector space $V = (\mathbb{F}_p)^\ell$, and apply the theorem.

According to Hering's Theorem, the group L lies in one of three class (A), (B) and (C). Given that $\ell \geq n \geq 3$, the classes (B) and (C) reduce to the following possibilities:

1. $L = A_6, A_7$ or $\mathrm{SL}_2(13)$; $G = \mathrm{GL}_4(2), \mathrm{GL}_6(3)$ or $\mathrm{GL}_3(9)$.

2. L has a normal subgroup $R \cong D_8 \circ Q_8$, $L/R \leq S_5$ and $G = \mathrm{GL}_4(3)$.

In the first case, we note that all elements of L have order less than or equal to 14, and this case is immediately excluded. Similarly, in the second case, all elements of L have order less than or equal to 48, and this case is immediately excluded.

We are left with groups in Liebeck's class A. These come in four families; we examine them one at a time. For family (1), L is a subgroup of the normalizer of a Singer cycle. The result follows immediately in this case. For the remaining families, L has a normal subgroup N isomorphic to $\mathrm{SL}_a(q_0)$, $\mathrm{Sp}_a(q_0)$ or $G_2(q_0)$ with $q_0 = p^d$ and $\ell = ad$.

By examining the proof in [Lie87], we find that, in all cases, L lies in a field-extension subgroup $\Phi_{\mathcal{C}}(\Gamma\mathrm{L}_{\mathbb{K}_0/\mathbb{F}_p}(W))$ of $\mathrm{GL}_\ell(p)$, for $\mathbb{K}_0$ some field extension of $\mathbb{F}_p$ of degree $d \in \mathbb{Z}^+$ and $\mathcal{C}$ some ordered $\mathbb{F}_p$-basis of $W = (\mathbb{K}_0)^a$. What is more $q_0 = q^d$ and $N \leq \Phi_{\mathcal{C}}(\mathrm{GL}_a(\mathbb{K}_0))$.

In the symplectic case, this means that the action of N on $(\mathbb{K}_0)^a$ yields the natural module for $\mathrm{Sp}_a(\mathbb{K}_0)$ (see, for instance, [KL90, Proposition 5.4.13]). Now one can check that an irreducible cyclic subgroup of $\mathrm{Sp}_a(q_0)$ in the natural module has size dividing $q_0^{a/2} + 1$ (see, for instance, [Ber00]). Now Schur's Lemma implies that an irreducible cyclic subgroup of L has order dividing $(q_0^{a/2} + 1)2(q_0 - 1)\log_p(q_0)$. Since this must be at least $q_0^a - 1$, one immediately obtains that $a/2 = 1$ and, since $\mathrm{Sp}_2(\mathbb{K}_0) \cong \mathrm{SL}_2(\mathbb{K}_0)$ we are in one of the remaining cases.

If $G = G_2(q_0)$, then the proof in [Lie87] implies that, in fact, N is a subgroup of a symplectic group $\mathrm{Sp}_6(q_0)$ that acts on $(\mathbb{K}_0)^6$ via its natural module. Thus this situation can be excluded via the calculation of the previous paragraph.

We are left with the case where

$$N \cong \mathrm{SL}_a(q_0) \lhd L \leq \Phi_{\mathcal{C}}(\Gamma\mathrm{L}_{\mathbb{K}_0/\mathbb{F}_p}(W)) \leq \mathrm{GL}_\ell(p).$$

Direct computation inside $\Gamma\mathrm{L}_{\mathbb{K}_0/\mathbb{F}_p}(W)$ confirms that, since L contains a cyclic group of order $p^\ell - 1$, L must contain $M = \Phi_{\mathcal{C}}(\mathrm{GL}(W)) \cong GL_a(q_0)$ as a normal subgroup.

Observe, then, that the Singer cycle S lies in two field extension subgroups of $\mathrm{GL}_d(p)$, namely $N_{\mathrm{GL}_d(p)}(G)$ and $N_{\mathrm{GL}_d(p)}(M)$. Notice, though, that by Lemma 3, $S = \Phi_{\mathcal{B}}(GL_1(\mathbb{L}))$ for some ordered $\mathbb{F}_p$-basis $\mathcal{B}$ of $\mathbb{L}$, a degree n extension of $\mathbb{F}_p$. Clearly the groups $\Phi_{\mathcal{B}}(\Gamma\mathrm{L}_{\mathbb{F}/\mathbb{F}_p}(\mathbb{L}))$ and $\Phi_{\mathcal{B}}(\Gamma\mathrm{L}_{\mathbb{K}_0/\mathbb{F}_p}(\mathbb{L}))$ are also field extension subgroups that contain S.

Now Lemma 6 implies that $M = \Phi_{\mathcal{B}}(\mathrm{GL}_a(\mathbb{K}_0))$ and $G = \Phi_{\mathcal{B}}(\mathrm{GL}_n(\mathbb{F}))$. The second occurrence of the monomorphism $\Phi_{\mathcal{B}}$ here is simply a restriction of the first; it is an easy exercise to check that, in this situation, M is a field-extension subgroup of G as required. □

6. Proving Theorem 2

Observe that if f and g are as in Theorem 2, then they both have non-zero constant term and hence are invertible and so lie in $\mathrm{GL}_n(q)$. Now Lemma 3, Corollary 5 and Theorem 7 imply that $\langle C_f, C_g\rangle$ does not lie in a proper subgroup of $\mathrm{GL}_n(q)$. In other words $\langle C_f, C_g\rangle = \mathrm{GL}_n(q)$, as required.

References

[Ber00] Á. Bereczky. Maximal overgroups of Singer elements in classical groups. *J. Algebra*, 234(1):187–206, 2000.

[Cam] P. J. Cameron. Antiflag-transitive groups. 2015. Blogpost at: `https://cameroncounts.wordpress.com/2015/05/31/antiflag-transitive-groups/`.

[CK79] P. J. Cameron and W. M. Kantor. 2-transitive and antiflag transitive collineation groups of finite projective spaces. *J. Algebra*, 60:384–422, 1979.

[Deg13] J.-Y. Degos. Linear groups and primitive polynomials over $\mathbf{F}_p$. *Cah. Topol. Géom. Différ. Catég.*, 54(1):56–74, 2013.

[Dic58] L. E. Dickson. Linear groups. With an exposition of the Galois field theory, 1958.

[GAP15] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.8*, 2015.

[Her85] C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. II. *J. Algebra*, 93:151–164, 1985.

[Kan80] W. M. Kantor. Linear groups containing a Singer cycle. *J. Algebra*, 62:232–234, 1980.

[KL90] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[Lie87] M. W. Liebeck. The affine permutation groups of rank three. *Proc. Lond. Math. Soc. (3)*, 54:477–516, 1987.

Nick Gill
Department of Mathematics
University of South Wales
Treforest, CF37 1DL
U.K.
nicholas.gill@southwales.ac.uk