Arch. Math. 117 (2021), 9–18

0003-889X/21/010009-10
published online March 3, 2021
https://doi.org/10.1007/s00013-021-01589-x

Archiv der Mathematik

Generalized bases of finite groups

Benjamin Sambale

Abstract. Motivated by recent results on the minimal base of a permutation group, we introduce a new local invariant attached to arbitrary finite groups. More precisely, a subset Δ of a finite group G is called a *p-base* (where p is a prime) if $\langle\Delta\rangle$ is a p-group and $\mathrm{C}_G(\Delta)$ is p-nilpotent. Building on results of Halasi–Maróti, we prove that p-solvable groups possess p-bases of size 3 for every prime p. For other prominent groups, we exhibit p-bases of size 2. In fact, we conjecture the existence of p-bases of size 2 for every finite group. Finally, the notion of p-bases is generalized to blocks and fusion systems.

Mathematics Subject Classification. 20D20, 20B05.

Keywords. Base, p-nilpotent centralizer, Fusion.

1. Introduction. Many algorithms in computational group theory depend on the existence of small bases. Here, a *base* of a permutation group G acting on a set Ω is a subset $\Delta \subseteq \Omega$ such that the pointwise stabilizer G_Δ is trivial (i.e. if $g \in G$ fixes every $\delta \in \Delta$, then $g = 1$). The aim of this short note is to introduce a generalized base without the presence of a group action. To this end, let us first consider a finite group G acting faithfully by automorphisms on a p-group P. If p does not divide $|G|$, then G always admits a base of size 2 by a theorem of Halasi–Podoski [5]. Now suppose that G is p-solvable, P is elementary abelian, and G acts completely reducibly on P. Then G has a base of size 3 (2 if $p \geq 5$) by Halasi–Maróti [4]. In those situations, we may form the semidirect product $H := P \rtimes G$. Now there exists $\Delta \subseteq P$ such that $|\Delta| \leq 3$ and $\mathrm{C}_H(\Delta) = \mathrm{C}_H(\langle\Delta\rangle) \leq P$. This motivates the following definition.

Definition 1. Let G be a finite group with Sylow p-subgroup P. A subset $\Delta \subseteq P$ is called a *p-base* of G if $\mathrm{C}_G(\Delta)$ is p-nilpotent, i.e. $\mathrm{C}_G(\Delta)$ has a normal p-complement.

Clearly, any generating set of P is a p-base of G since $\mathrm{C}_G(P) = \mathrm{Z}(P) \times \mathrm{O}_{p'}(\mathrm{C}_G(P))$ (this observation is generalized in Lemma 7 below).

Our main theorem extends the work of Halasi–Maróti as follows.

Theorem 2. *Every p-solvable group has a p-base of size 3 (2 if $p \geq 5$).*

Although Halasi–Maróti's theorem does not extend to non-p-solvable groups, the situation for p-bases seems more fortunate. For instance, if V is a finite vector space in characteristic p, then every base of $\mathrm{GL}(V)$ (under the natural action) contains a *basis* of V, so its size is at least $\dim V$. On the other hand, $G = \mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V)$ possesses a p-base of size 2. To see this, let P be the Sylow p-subgroup of $\mathrm{GL}(V)$ consisting of the upper unitriangular matrices. Let $x \in P$ be a Jordan block of size $\dim V$. Then $\mathrm{C}_{\mathrm{GL}(V)}(x) \leq P\mathrm{Z}(\mathrm{GL}(V))$. For any $y \in \mathrm{C}_V(x) \setminus \{1\}$, we obtain a p-base $\Delta := \{x, y\}$ such that $\mathrm{C}_G(\Delta) \leq VP$. We have even found a p-base consisting of *commuting* elements. After checking many more cases, we believe that the following might hold.

Conjecture 3. *Every finite group has a (commutative) p-base of size 2 for every prime p.*

The role of the number 2 in Conjecture 3 appears somewhat arbitrary at first. There is, however, an elementary dual theorem: A finite group is p-nilpotent if and only if every 2-generated subgroup is p-nilpotent. This can be deduced from the structure of minimal non-p-nilpotent groups (see [6, Satz IV.5.4]). It is a much deeper theorem of Thompson [8] that the same result holds when "p-nilpotent" is replaced by "solvable". Similarly, 2-generated subgroups play a role in the Baer–Suzuki theorem and its variations.

Apart from Theorem 2 we give some more evidence of Conjecture 3.

Theorem 4. *Let G be a finite group with Sylow p-subgroup P. Then Conjecture 3 holds for G in the following cases:*

(i) *P is abelian.*
(ii) *G is a symmetric group or an alternating group.*
(iii) *G is a general linear group, a special linear group, or a projective special linear group.*
(iv) *G is a sporadic simple group or an automorphism group thereof.*

Our results on (almost) simple groups carry over to the corresponding quasisimple groups by Lemma 8 below. The notion of p-bases generalizes to blocks of finite groups and even to fusion systems.

Definition 5.
- Let B be a p-block of a finite group G with defect group D. A subset $\Delta \subseteq D$ is called *base* of B if B has a nilpotent Brauer correspondent in $\mathrm{C}_G(\Delta)$ (see [1, Definition IV.5.38]).
- Let $\mathcal{F}$ be a saturated fusion system on a finite p-group P. A subset $\Delta \subseteq P$ is called *base* of $\mathcal{F}$ if there exists a morphism φ in $\mathcal{F}$ such that $\varphi(\langle\Delta\rangle)$ is fully $\mathcal{F}$-centralized and the centralizer fusion system $\mathcal{C} := \mathrm{C}_{\mathcal{F}}(\varphi(\langle\Delta\rangle))$ is trivial, i.e. $\mathcal{C} = \mathcal{F}_{\mathrm{C}_P(\Delta)}(\mathrm{C}_P(\Delta))$ (see [1, Definition I.5.3, Theorem I.5.5]).

By Brauer's third main theorem, the bases of the principal p-block of G are the p-bases of G (see [1, Theorem IV.5.9]). Moreover, if $\mathcal{F}$ is the fusion system attached to an arbitrary block B, then the bases of B are the bases of $\mathcal{F}$ (see [1, Theorem IV.3.19]). By the existence of exotic fusion systems, the following conjecture strengthens Conjecture 3.

Conjecture 6. *Every saturated fusion system has a base of size* 2.

We show that Conjecture 6 holds for p-groups of order at most p^4.

2. Results.

Proof of Theorem 2. Let G be a p-solvable group with Sylow p-subgroup P. Let $N := \mathrm{O}_{p'}(G)$. For $Q \subseteq P$, $\mathrm{C}_G(Q)N/N$ is contained in $\mathrm{C}_{G/N}(QN/Q)$. Hence, $\mathrm{C}_G(Q)$ is p-nilpotent whenever $\mathrm{C}_{G/N}(QN/Q)$ is p-nilpotent. Thus, we may assume that $N = 1$. Instead we consider $N := \mathrm{O}_p(G)$. Since G is p-solvable, $N \neq 1$. We show by induction on $|N|$ that there exists a p-base $\Delta \subseteq N$ such that $\mathrm{C}_G(\Delta) \leq N$. By the Hall–Higman lemma (see [6, Hilfssatz VI.6.5]), $\mathrm{C}_{G/N}(N/\Phi(N)) = N/\Phi(N)$ where $\Phi(N)$ denotes the Frattini subgroup of N. It follows that $\mathrm{O}_{p'}(G/\Phi(N)) = 1$. Hence, by induction, we may assume that N is elementary abelian. Then $\overline{G} := G/N$ acts faithfully on N and it suffices to find a p-base $\Delta \subseteq N$ such that $\mathrm{C}_{\overline{G}}(\Delta) = 1$. Thus, we may assume that $G = N \rtimes H$ where $\mathrm{C}_G(N) = N$ and $\mathrm{O}_p(H) = 1$.

Note that $\Phi(G) \leq \mathrm{F}(G) = N$ where $\mathrm{F}(G)$ is the Fitting subgroup of G. Since H is contained in a maximal subgroup of G, we even have $\Phi(G) < N$. Let $K \trianglelefteq H$ be the kernel of the action of H on $N/\Phi(G)$. By way of contradiction, suppose that $K \neq 1$. Since K is p-solvable and $\mathrm{O}_p(K) \leq \mathrm{O}_p(H) = 1$, also $K_0 := \mathrm{O}_{p'}(K) \neq 1$. Now K_0 acts coprimely on N and we obtain

$$N = [K_0, N]\mathrm{C}_N(K_0) = \Phi(G)\mathrm{C}_N(K_0)$$

as is well-known. Both $\Phi(G)$ and $\mathrm{C}_N(K_0)H$ lie in a maximal subgroup M of G. But then $G = NH = \Phi(G)\mathrm{C}_N(K_0)H \leq M$, a contradiction. Therefore, H acts faithfully on $N/\Phi(G)$ and we may assume that $\Phi(G) = 1$. Then there exist maximal subgroups $M_1, \ldots, M_n$ of G such that $N_i := M_i \cap N < N$ for $i = 1, \ldots, n$ and $\bigcap_{i=1}^n N_i = 1$. Since $G = M_iN$, the quotients N/N_i are simple $\mathbb{F}_pH$-modules and N embeds into $N/N_1 \times \cdots \times N/N_n$. Hence, the action of H on N is faithful and completely reducible. Now, by the main result of Halasi–Maróti [4], there exists a p-base with the desired properties. □

Next we work towards Theorem 4.

Lemma 7. *Let P be a Sylow p-subgroup of G. Let $Q \trianglelefteq P$ such that $\mathrm{C}_P(Q) \leq Q$. Then every generating set of Q is a p-base of G.*

Proof. Since $P \in \mathrm{Syl}_p(\mathrm{N}_G(Q))$, we have $\mathrm{Z}(Q) = \mathrm{C}_P(Q) \in \mathrm{Syl}_p(\mathrm{C}_G(Q))$ and therefore $\mathrm{C}_G(Q) = \mathrm{Z}(Q) \times \mathrm{O}_{p'}(\mathrm{C}_G(Q))$ by the Schur–Zassenhaus theorem. □

Lemma 8. *Let Δ be a p-base of G and let $N \leq \mathrm{Z}(G)$. Then $\overline{\Delta} := \{xN : x \in \Delta\}$ is a p-base of G/N.*

Proof. Let $gN \in \mathrm{C}_{G/N}(\overline{\Delta})$. Then g normalizes the nilpotent group $\langle\Delta\rangle N$. Hence, g acts on the unique Sylow p-subgroup P of $\langle\Delta\rangle N$. Since g centralizes

$$\langle\overline{\Delta}\rangle = \langle\Delta\rangle N/N = PN/N \cong P/P\cap N$$

and $P \cap N \le N \le \mathrm{Z}(G)$, g induces a p-element in $\mathrm{Aut}(P)$ and also in $\mathrm{Aut}(\langle\Delta\rangle N)$. Consequently, there exists a p-subgroup $Q \le \mathrm{N}_G(\langle\Delta\rangle N)$ such that $\mathrm{C}_{G/N}(\overline{\Delta}) = Q\mathrm{C}_G(\Delta N)/N = Q\mathrm{C}_G(\Delta)/N$. Since $\mathrm{C}_G(\Delta)$ is p-nilpotent, so is $Q\mathrm{C}_G(\Delta)$ and the claim follows. □

The following implies the first part of Theorem 4.

Proposition 9. *Let P be a Sylow p-subgroup of G with nilpotency class c. Then G has a p-base of size $2c$.*

Proof. The p'-group $\mathrm{N}_G(\mathrm{Z}(P))/\mathrm{C}_G(\mathrm{Z}(P))$ acts faithfully on $\mathrm{Z}(P)$. By Halasi–Podoski [5], there exists $\Delta_0 = \{x, y\} \subseteq \mathrm{Z}(P)$ such that $\mathrm{N}_H(\mathrm{Z}(P)) \le \mathrm{C}_H(\mathrm{Z}(P))$ where $H := \mathrm{C}_G(\Delta_0)$. If $c = 1$, then $P = \mathrm{Z}(P)$ is abelian and Burnside's transfer theorem implies that H is p-nilpotent. Hence, let $c > 1$. By a well-known fusion argument of Burnside, elements of $\mathrm{Z}(P)$ are conjugate in H if and only if they are conjugate in $\mathrm{N}_H(\mathrm{Z}(P))$. Consequently, all elements of $\mathrm{Z}(P)$ are isolated in our situation. By the Z^*-theorem (assuming the classification of finite simple groups), we obtain

$$\mathrm{Z}(H/\mathrm{O}_{p'}(H)) = \mathrm{Z}(P)\mathrm{O}_{p'}(H)/\mathrm{O}_{p'}(H).$$

The group $\overline{H} := H/\mathrm{Z}(P)\mathrm{O}_{p'}(H)$ has Sylow p-subgroup $\overline{P} \cong P/\mathrm{Z}(P)$ of nilpotency class $c - 1$. By induction on c, there exists a p-base $\overline{\Delta_1} \subseteq \overline{P}$ of $\overline{H}$ of size $2(c - 1)$. We may choose $\Delta_1 \subseteq P$ such that $\overline{\Delta_1} = \{\overline{x} : x \in \Delta_1\}$. Since $\overline{\mathrm{C}_H(\Delta_1)} \le \mathrm{C}_{\overline{H}}(\overline{\Delta_1})$ is p-nilpotent, so is

$$\big(\mathrm{C}_H(\Delta_1)\mathrm{Z}(P)\mathrm{O}_{p'}(H)/\mathrm{O}_{p'}(H)\big)/\mathrm{Z}(H/\mathrm{O}_{p'}(H)).$$

It follows that $\mathrm{C}_H(\Delta_1)\mathrm{Z}(P)\mathrm{O}_{p'}(H)/\mathrm{O}_{p'}(H)$ and $\mathrm{C}_H(\Delta_1) = \mathrm{C}_G(\Delta_0 \cup \Delta_1)$ are p-nilpotent as well. Hence, $\Delta := \Delta_0 \cup \Delta_1$ is a p-base of G of size (at most) $2c$. □

Proposition 10. *The symmetric and alternating groups S_n and A_n have commutative p-bases of size 2 for every prime p.*

Proof. Let $n = \sum_{i=0}^{k} a_i p^i$ be the p-adic expansion of n. Suppose first that $G = S_n$. Let

$$x = \prod_{i=0}^{k}\prod_{j=1}^{a_i} x_{ij} \in G$$

be a product of disjoint cycles x_{ij} where x_{ij} has length p^i for $j = 1, \ldots, a_i$. Then x is a p-element and

$$\mathrm{C}_G(x) \cong \prod_{i=0}^{k} C_{p^i} \wr S_{a_i}.$$

Since $a_i < p$, $P := \langle x_{ij} : i = 0, \dots, k, j = 1, \dots, a_i \rangle$ is an abelian Sylow p-subgroup of $\mathrm{C}_G(x)$. Let $y := \prod_{i=0}^{k} \prod_{j=1}^{a_i} x_{ij}^{j} \in P$. It is easy to see that $\Delta := \{x, y\}$ is a commutative p-base of G with $\mathrm{C}_G(\Delta) = P$.

Now let $G = A_n$. If $p > 2$, then x, y lie in A_n as constructed above and the claim follows from $\mathrm{C}_{A_n}(\Delta) \leq \mathrm{C}_{S_n}(\Delta)$. Hence, let $p = 2$. If $\sum_{i=1}^{k} a_i \equiv 0 \pmod 2$, then we still have $x \in A_n$ and $\mathrm{C}_G(x) = \langle x_{ij} : i, j \rangle$ is already a 2-group. Thus, we have a 2-base of size 1 in this case. In the remaining case, let $m \geq 1$ be minimal such that $a_m = 1$. We adjust our definition of x by replacing x_{m1} with a disjoint product of two cycles of length 2^{m-1}. Then $x \in A_n$ and $\mathrm{C}_G(x)$ is a 2-group or a direct product of a 2-group and S_3 (the latter case happens if and only if $m = 1 = a_0$). We clearly find a 2-element $y \in \mathrm{C}_G(x)$ such that $\mathrm{C}_G(x, y)$ is a 2-group. □

The following elementary facts are well-known, but we provide proofs for the convenience of the reader.

Lemma 11. *Let p be a prime and let q be a prime power such that $p \nmid q$. Let $e \mid p-1$ be the multiplicative order of q modulo p. Let p^s be the p-part of $q^e - 1$. Then for every $n \geq 1$, the polynomial $X^{p^n} - 1$ decomposes as*

$$X^{p^n} - 1 = (X - 1) \prod_{k=1}^{(p^s-1)/e} \gamma_{0,k} \prod_{i=1}^{n-s} \prod_{k=1}^{\varphi(p^s)/e} \gamma_{i,k}$$

where the $\gamma_{i,k}$ are pairwise coprime polynomials in $\mathbb{F}_q[X]$ of degree ep^i for $i = 0, \dots, n - s$.

Proof. Let ζ be a primitive root of $X^{p^n} - 1$ in some finite field extension of $\mathbb{F}_q$. Then

$$X^{p^n} - 1 = \prod_{k=0}^{p^n-1} (X - \zeta^k).$$

Recall that $\mathbb{F}_q$ is the fixed field under the Frobenius automorphism $c \mapsto c^q$. Hence, the irreducible divisors of $X^{p^n} - 1$ in $\mathbb{F}_q[X]$ correspond to the orbits of $\langle q + p^n\mathbb{Z} \rangle$ on $\mathbb{Z}/p^n\mathbb{Z}$ via multiplication. The trivial orbit corresponds to $X - 1$. For $i = 1, \dots, s$, the order of q modulo p^i is e by the definition of s. This yields $(p^s - 1)/e$ non-trivial orbits of length e in $p^{n-s}\mathbb{Z}/p^n\mathbb{Z}$. The corresponding irreducible factors are denoted by $\gamma_{0,k}$ for $k = 1, \dots, (p^s - 1)/e$.

For $i \geq 1$, the order of q modulo p^{s+i} divides ep^i (it can be smaller if $p = 2$ and $s = 1$). We partition $(p^{n-s-i}\mathbb{Z}/p^n\mathbb{Z})^\times$ into $\varphi(p^{s+i})/(ep^i) = \varphi(p^s)/e$ unions of orbits under $\langle q + p^n\mathbb{Z} \rangle$ such that each union has size ep^i. The corresponding polynomials $\gamma_{i,1}, \dots, \gamma_{i,\varphi(p^s)/e}$ are pairwise coprime (but not necessarily irreducible). □

Lemma 12. *Let A be an $n \times n$-matrix over an arbitrary field F such that the minimal polynomial of A has degree n. Then every matrix commuting with A is a polynomial in A.*

Proof. By hypothesis, A is similar to a companion matrix. Hence, there exists a vector $v \in F^n$ such that $\{v, Av, \ldots, A^{n-1}v\}$ is a basis of F^n. Let $B \in F^{n\times n}$ such that $AB = BA$. There exist $a_0, \ldots, a_{n-1} \in F$ such that $Bv = a_0v + \cdots + a_{n-1}A^{n-1}v$. Set $\gamma := a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$. Then

$$BA^iv = A^iBv = a_0A^iv + \cdots + a_{n-1}A^{n-1}A^iv = \gamma(A)A^iv$$

for $i = 0, \ldots, n-1$. Since $\{v, Av, \ldots, A^{n-1}v\}$ is a basis, we obtain $B = \gamma(A)$ as desired. □

Proposition 13. *The groups* $\mathrm{GL}(n, q)$, $\mathrm{SL}(n, q)$, *and* $\mathrm{PSL}(n, q)$ *possess commutative* p*-bases of size* 2 *for every prime* p.

Proof. Let q be a prime power. By Lemma 8, it suffices to consider $\mathrm{GL}(n, q)$ and $\mathrm{SL}(n, q)$. Suppose first that $p \mid q$. Let $x \in G := \mathrm{GL}(n, q)$ be a Jordan block of size $n\times n$ with eigenvalue 1. Then x is a p-element since $x^{p^n} - 1 = (x-1)^{p^n} = 0$. Moreover, $\mathrm{C}_G(x)$ consists of polynomials in x by Lemma 12. In particular, $\mathrm{C}_G(x)$ is abelian and therefore p-nilpotent. Hence, we found a p-base of size 1. Since $(q-1, p) = 1$, this is also a p-base of $\mathrm{SL}(n, q)$.

Now let $p \nmid q$. We "linearize" the argument from Proposition 10. Let e and s be as in Lemma 11. Let $0 \le a_0 \le e-1$ be such that $n \equiv a_0 \pmod e$. Let

$$\frac{n - a_0}{e} = \sum_{i=0}^{r} a_{i+1}p^i$$

be the p-adic expansion. Let $M_i \in \mathrm{GL}(ep^i, q)$ be the companion matrix of the polynomial $\gamma_{i,1}$ from Lemma 11 for $i = 0, \ldots, r$. Let $G_i := \mathrm{GL}(ea_{i+1}p^i, q)$ and $x_i := \mathrm{diag}(M_i, \ldots, M_i) \in G_i$. Then the minimal polynomial of

$$x := \mathrm{diag}(1_{a_0}, x_0, \ldots, x_r) \in G$$

divides $X^{p^{r+s}} - 1$ by Lemma 11. In particular, x is a p-element. Since the $\gamma_{i,1}$ are pairwise coprime, it follows that

$$\mathrm{C}_G(x) = \mathrm{GL}(a_0, q) \times \prod_{i=0}^{r} \mathrm{C}_{G_i}(x_i).$$

Since $a_0 < e$, $\mathrm{GL}(a_0, q)$ is a p'-group. By Lemma 12, every matrix commuting with M_i is a polynomial in M_i. Hence, the elements of $\mathrm{C}_{G_i}(x_i)$ have the form $A = (A_{kl})_{1\le k,l\le a_{i+1}}$ where each block A_{kl} is a polynomial in M_i. We define

$$y_i := \mathrm{diag}(M_i, M_i^2, \ldots, M_i^{a_{i+1}}) \in \mathrm{C}_{G_i}(x_i)$$

and $y := \mathrm{diag}(1_{a_0}, y_0, \ldots, y_r) \in \mathrm{C}_G(x)$. Let $A = (A_{kl}) \in \mathrm{C}_{G_i}(x_i, y_i)$. We want to show that $A_{kl} = 0$ for $k \ne l$. To this end, we may assume that $k < l$ and $A_{kl} = \rho(M_i)$ where $\rho \in \mathbb{F}_q[X]$ with $\deg(\rho) < \deg(\gamma_{i,1}) = ep^i$. Since $A \in \mathrm{C}_{G_i}(x_i, y_i)$, we have $M_i^kA_{kl} = M_i^lA_{kl}$ and $(M^{l-k} - 1)A_{kl} = 0$. It follows that the minimal polynomial $\gamma_{i,1}$ of M_i divides $(X^{l-k} - 1)\rho$. By way of contradiction, we assume that $\rho \ne 0$. Then $\gamma_{i,1}$ divides $X^{l-k} - 1$ and $X^{p^{r+s}} - 1$. However, $l - k \le a_{i+1} < p$ and γ_{i1} must divide $X - 1$. This contradicts the definition of $\gamma_{i,1}$ in Lemma 11. Hence, $A_{kl} = 0$ for $k \neq l$. We have shown that the elements of $\mathrm{C}_G(x, y)$ have the form

$$L \oplus \bigoplus_{i=0}^{r} \bigoplus_{j=1}^{a_{i+1}} L_{ij}$$

where $L \in \mathrm{GL}(a_0, q)$ and each L_{ij} is a polynomial in M_i. In particular, $\mathrm{C}_G(x, y)$ is a direct product of a p'-group and an abelian group. Consequently, $\mathrm{C}_G(x, y)$ is p-nilpotent.

Now let $G := \mathrm{SL}(n, q)$. If $p \nmid q-1$, then the p-base of $\mathrm{GL}(n, q)$ constructed above already lies in G. Thus, we may assume that $p \mid q-1$. Then $e = 1$ and $a_0 = 0$ with the notation above. We now have the polynomials $\gamma_{i,k}$ with $i = 0, \ldots, r$ and $k = 1, \ldots, p-1 \leq \varphi(p^s)$ at our disposal. Let $M_{i,k}$ be the companion matrix of $\gamma_{i,k}$. Define

$$x_i := \mathrm{diag}(M_{i,1}, \ldots, M_{i,a_{i+1}})$$

for $i = 0, \ldots, r$. Then the minimal polynomial of $x := \mathrm{diag}(x_0, \ldots, x_r) \in \mathrm{GL}(n, q)$ has degree n and therefore $\mathrm{C}_{\mathrm{GL}(n,q)}(x)$ is abelian by Lemma 12. Let $i \geq 0$ be minimal such that $a_{i+1} > 0$. We replace the block $M_{i,1}$ of x by the companion matrix of $X^{p^i} - 1$. Then, by Lemma 11, the minimal polynomial of x still has degree n. Moreover, x has at least one block B of size 1×1. We may modify B such that $\det(x) = 1$. After doing so, it may happen that B occurs twice in x. In this case, $\mathrm{C}_G(x) \leq \mathrm{GL}(2, q) \times H$ where H is abelian. Then the matrix

$$y := \begin{cases} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \oplus 1_{n-2} & \text{if } p = 2, \\ \mathrm{diag}(M_{0,1}, M_{0,1}^{-1}, 1_{n-2}) & \text{if } p > 2 \end{cases}$$

lies in $\mathrm{C}_G(x)$ and $\mathrm{C}_G(x, y)$ is abelian. Hence, $\{x, y\}$ is a p-base of G. □

Proposition 13 can probably be generalized to classical groups. The next result completes the proof of Theorem 4.

Proposition 14. *Let S be a sporadic simple group and $G \in \{S, S.2\}$. Then G has a commutative p-base of size 2 for every prime p.*

Proof. If p^4 does not divide $|G|$, then the claim follows from Lemma 7. So we may assume that p^4 divides $|G|$. From the character tables in the Atlas [2], we often find p-elements $x \in G$ such that $\mathrm{C}_G(x)$ is already a p-group. In this case, we found a p-base of size 1 and we are done. If G admits a permutation representation of "moderate" degree (including Co_1), then the claim can be shown directly in GAP [3]. In the remaining cases, we use the Atlas to find p-elements with small centralizers:

- $G = Ly$, $p = 2$: There exists an involution $x \in G$ such that $\mathrm{C}_G(x) = 2.A_{11}$. By the proof of Proposition 10, there exists $y \in A_{11}$ such that $\mathrm{C}_{A_{11}}(y)$ is a 2-group. We identify y with a preimage in $\mathrm{C}_G(x)$. Then $\mathrm{C}_G(x, y)$ is a 2-group.

- $G = Ly$, $p = 3$: Here we find $x \in G$ of order 3 such that $\mathrm{C}_G(x) = 3.McL$. Since McL contains a 3-element y such that $\mathrm{C}_{McL}(y)$ is a 3-group, the claim follows.
- $G = Th$, $p = 2$: There exists an involution $x \in G$ such that $\mathrm{C}_G(x) = 2_+^{1+8}.A_9$. As before, we find $y \in \mathrm{C}_G(x)$ such that $\mathrm{C}_G(x, y)$ is a 2-group.
- $G = M$, $p = 5$: There exists a 5-element $x \in G$ such that $\mathrm{C}_G(x) = C_5 \times HN$. Since there is also a 5-element $y \in HN$ such that $\mathrm{C}_{HN}(y)$ is a 5-group, the claim follows.
- $G = M$, $p = 7$: In this case there exists a radical subgroup $Q \le G$ such that $\mathrm{C}_G(Q) = Q \cong C_7 \times C_7$ by Wilson [9, Theorem 7] (this group was missing in the list of local subgroups in the Atlas). Any generating set of Q of size 2 is a desired p-base of G.
- $G = HN.2$, $p = 3$: There exists an element $x \in G$ of order 9 such that $|\mathrm{C}_G(x)| = 54$. Clearly, we find $y \in \mathrm{C}_G(x)$ such that $\mathrm{C}_G(x, y)$ is 3-nilpotent. □

Finally, we consider a special case of Conjecture 6.

Proposition 15. *Let $\mathcal{F}$ be a saturated fusion system on a p-group P of order at most p^4. Then $\mathcal{F}$ has a base of size* 2.

Proof. Recall that $A := \mathrm{Out}_{\mathcal{F}}(P)$ is a p'-group and there is a well-defined action of A on P by the Schur–Zassenhaus theorem. If $\mathcal{F}$ is the fusion system of the group $P \rtimes A$, then the claim follows from Halasi–Podoski [5] as before. We may therefore assume that P contains an $\mathcal{F}$-essential subgroup. In particular, P is non-abelian. Let $Q < P$ be a maximal subgroup of P containing $\mathrm{Z}(P)$. The fusion system $\mathrm{C}_{\mathcal{F}}(Q)$ on $\mathrm{C}_P(Q) = \mathrm{Z}(Q)$ is trivial by definition. Hence, we are done whenever Q is generated by two elements.

It remains to deal with the case where $|P| = p^4$ and all maximal subgroups containing $\mathrm{Z}(P)$ are elementary abelian of rank 3. Since two such maximal subgroups intersect in $\mathrm{Z}(P)$, we obtain that $|\mathrm{Z}(P)| = p^2$ and $|P'| = p$ by [7, Lemma 1.9] for instance. By the first part of the proof, we may choose an $\mathcal{F}$-essential subgroup Q such that $\mathrm{Z}(P) < Q < P$. Let $A := \mathrm{Aut}_{\mathcal{F}}(Q)$. Since Q is essential, P/Q is a non-normal Sylow p-subgroup of A (see [1, Proposition I.2.5]). Moreover, $[P, Q] = P'$ has order p. By [7, Lemma 1.11], there exists an A-invariant decomposition

$$Q = \langle x, y\rangle \times \langle z\rangle.$$

We may choose those elements such that $\Delta := \{xz, y\} \nsubseteq \mathrm{Z}(P)$. Then $\mathrm{C}_P(\Delta) = Q$ and $\mathrm{C}_A(\Delta) = 1$. Let $\varphi : S \to T$ be a morphism in $\mathcal{C} := \mathrm{C}_{\mathcal{F}}(\Delta)$ where $S, T \le Q$. Then φ extends to a morphism $\hat{\varphi} : S\langle\Delta\rangle \to T\langle\Delta\rangle$ in $\mathcal{F}$ such that $\hat{\varphi}(x) = x$ for all $x \in \langle\Delta\rangle$. Hence, if $S \le \langle\Delta\rangle$, then $\varphi = \mathrm{id}$. Otherwise, $S\langle\Delta\rangle = Q$ and $\hat{\varphi} \in \mathrm{C}_A(\Delta) = 1$ since morphisms are always injective. In any case, $\mathcal{C}$ is the trivial fusion system and Δ is a base of $\mathcal{F}$. □

Acknowledgements. The author is supported by the German Research Foundation (SA 2864/1-2 and SA 2864/3-1).

Funding Open Access funding enabled and organized by Projekt DEAL.

References

[1] Aschbacher, M., Kessar, R., Oliver, B.: Fusion Systems in Algebra and Topology. London Mathematical Society Lecture Note Series, vol. 391. Cambridge University Press, Cambridge (2011)

[2] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A.: ATLAS of Finite Groups. Oxford University Press, Eynsham (1985)

[3] The GAP Group, GAP: Groups, Algorithms, and Programming, Version 4.11.0 (2020). http://www.gap-system.org

[4] Halasi, Z., Maróti, A.: The minimal base size for a p-solvable linear group. Proc. Amer. Math. Soc. **144**, 3231–3242 (2016)

[5] Halasi, Z., Podoski, K.: Every coprime linear group admits a base of size two. Trans. Amer. Math. Soc. **368**, 5857–5887 (2016)

[6] Huppert, B.: Endliche Gruppen. I. Grundlehren der Mathematischen Wissenschaften, vol. 134. Springer, Berlin (1967)

[7] Oliver, B.: Simple fusion systems over p-groups with abelian subgroup of index p: I. J. Algebra **398**, 527–541 (2014)

[8] Thompson, J.G.: Nonsolvable finite groups all of whose local subgroups are solvable. Bull. Amer. Math. Soc. **74**, 383–437 (1968)

[9] Wilson, R.A.: The odd-local subgroups of the Monster. J. Austral. Math. Soc. Ser. A **44**, 1–16 (1988)

Benjamin Sambale
Institut für Algebra, Zahlentheorie und Diskrete Mathematik
Leibniz Universität Hannover
Welfengarten 1
30167 Hannover
Germany
e-mail: sambale@math.uni-hannover.de

Received: 4 September 2020

Revised: 13 January 2021

Accepted: 28 January 2021.