Advances in Group Theory and Applications
© 2019 AGTA - www.advgrouptheory.com/journal
8 (2019), pp. 155–162 ISSN: 2499-1287
DOI: 10.32037/agta-2019-015

"In re mathematica ars proponendi quaestionem pluris facienda est quam solvendi"

Georg Cantor

ADV Perspectives in Group Theory

– an open space –

ADV – 8A *Gareth Tracey*

A subset

$$\{g_1, g_2, \dots, g_d\}$$

of a group G is said to *invariably generate* G if $\{g_1^{x_1}, g_2^{x_2}, \dots, g_d^{x_d}\}$ generates G for each d-tuple $(x_1, x_2 \dots, x_d) \in G^d$. An easy exercise shows that if G is finite then such a set always exists, and in this case the *Chebotarev invariant* $C(G)$ of G is defined to be the expected value of the random variable n which is minimal subject to the requirement that n randomly chosen elements of G invariably generate G. The study of the invariant $C(G)$ has deep motivations coming from computational Galois Theory and the Inverse Galois Problem (see [D] and [KZ] for more information).

Indeed, in this direction the case $G = \mathrm{Sym}(n)$, which was first proposed by B.L. van der Waerden [vdW] in 1936 (albeit in a different form), is particularly important. With this in mind, Pemantle, Peres and Rivin (2016) and Eberhard, Ford and Green (2017) proved seminal results which combine to give the following theorem; for a finite group G, let $P_{I,G}(k)$ denote the probability that k randomly chosen elements of G invariably generate G.

Theorem (see Theorem 1.5 of [PPR] and Theorem 1.2 of [EFG])
Let $G = \mathrm{Sym}(n)$.

1. *There exists a constant* ϵ *such that* $P_{I,G}(4) > \epsilon$ *for all* $n \in \mathbb{N}$.

2. $P_{I,G}(3) \to 0$ *as* $n \to \infty$.

An easy exercise in Probability Theory allows one to deduce from the Theorem that $C(Sym(n))$ is absolutely bounded, and that

$$C(Sym(n)) \geqslant 4$$

if n is large enough. However, sharp bounds for $C(Sym(n))$ are unknown, and this leads us to propose the following question.

Question 1 *Find the infimum of* $C(Sym(n))$ *as* n *runs over the natural numbers.*

It is also unclear whether or not $C(Sym(n))$ depends on the the arithmetic of n, or if the limit exists (the limit $\lim_{n\to\infty} e(Sym(n))$ of the expected number $e(Sym(n))$ of uniform random elements required to *generate* $Sym(n)$ exists - see Theorem 8 of [L]). This leads us to our next suggested open problem.

Question 2 *Does* $\lim_{n\to\infty} C(Sym(n))$ *exist?*

With the motivation from Galois Theory again in mind, it is also natural to consider the more general case of G being a subgroup of the symmetric group $Sym(n)$. Indeed, we do not know any examples where $C(G)$ is not linear in n, where $G \leqslant Sym(n)$.

Question 3 *Does there exist a constant* β *such that* $C(G) \leqslant \beta n$ *whenever* $G \leqslant Sym(n)$*?*

We remark that in a forthcoming paper, Lucchini and the author prove that $C(G)$ is polynomial in n whenever $G \leqslant Sym(n)$ is either primitive or soluble.

Finally, we remark that for any $\epsilon > 0$ there exists and absolute constant $k = k(\epsilon)$ such that $P_{I,G}(k) \geqslant 1 - \epsilon$ whenever $k \geqslant c$. This is proved for groups of Lie type in [FG], and for alternating groups in [LP]. In particular, it follows that there exists an absolute constant γ such that $C(G) \leqslant \gamma$ whenever G is a non-abelian finite simple group. Our final open problem then reads as follows.

Question 4 *Find the infimum of* $C(G)$ *as* G *runs over the set of finite simple groups.*

References

[D] J.D. Dixon: "Random sets which invariably generate the symmetric group", *Discrete Math.* 105 (1992), 25–39.

[EFG] S. Eberhard – K. Ford – B. Green: "Invariable generation of the symmetric group",. *Duke Math. J.* 166 (2017), 1573–1590.

[FG] J. Fulman – R. Guralnick: "Derangements in simple and primitive groups", in *Groups, combinatorics and Geometry (Durham, 2001)*, 99–121, World Sci. Publ, River Edge, NJ (2003).

[KZ] E. Kowalski – D. Zywina: "The Chebotarev invariant of a finite group", Exp. Math. 21 (2012), 38–56.

[L] A. Lucchini: "The expected number of random elements to generate a finite group", *Monatsh. Math.* 181 (2016), 123–142.

[LP] T. Luczak – L. Pyber: "On random generation of the symmetric group", *Combin. Probab. Comput.* 2 (1993), 505–512.

[PPR] R. Pemantle – Y. Peres – I. Rivin: "Four random permutations conjugated by an adversary generate S_n with high probability", *Random Structures Algorithms* 49 (2016), 409–428.

[vdW] B.L. van der Waerden: "Die Seltenheit der Gleichungen mit Affekt", *Math. Ann.* 109 (1934), 13–16.

ADV – 8B *Andreas Bächle*

All groups considered here are finite. Rationality questions are classical and at the very heart of finite group theory. An element $x \in G$ is called *rational in* G if it is conjugate in G to all generators of $\langle x \rangle$, the cyclic subgroup generated by x. A group G is called *rational* if every element is rational in G. This is equivalent to the character table being a rational matrix (whence the name). The notion of rational groups was generalized by D. Chillag and S. Dolfi in [CD]: an element $x \in G$ is called *inverse semi-rational in* G if every generator of $\langle x \rangle$ is conjugate to x or to x^{-1} in G; a group G is called *inverse semi-rational* if every element is inverse semi-rational in G. It turned out that this has nice interpretations of different flavor. The following are equivalent for a group G (see e.g. [BCJM]):

(i) G is inverse semi-rational.

(ii) $Z(U(\mathbb{Z}G))$, the center of the unit group of the integral group ring of G, is finite.

(iii) $K_1(\mathbb{Z}G)$, the Whitehead group of the integral group ring of G, is finite.

(iv) For all rows of the character table of G, the field extension of $\mathbb{Q}$ generated by the entries of this row equals $\mathbb{Q}$ or an imaginary quadratic extension.

(v) For all columns of the character table of G, the field extension of $\mathbb{Q}$ generated by the entries this column equals $\mathbb{Q}$ or an imaginary quadratic extension.

This is a surprisingly frequently happening phenomenon: for instance, about 86.62% of all groups up to order 512 are inverse semi-rational (mainly due to the fact that many 2-groups are inverse semi-rational) whereas 0.57% of the groups of order at most 512 are rational, see Section 7 of [BCJM]. Due to the characterization (ii) above, inverse semi-rational groups are also called *cut groups* (for central units trivial, a name coined by Bakshi-Maheshwary-Passi [BMP]) and for brevity this is also the term we will also use in what follows

Denote by $\mathbb{Q}(G)$ the field extension of the rationals generated by all entries of the character table of G. Clearly, $|\mathbb{Q}(G) : \mathbb{Q}| = 1$ if and only if G is rational. Is there a natural class comprising the rational groups such that the degrees of the fields $\mathbb{Q}(G)$ is uniformly bounded?

Question 1 *Is there* $c > 0$ *such that* $|\mathbb{Q}(G) : \mathbb{Q}| \leqslant c$ *for all cut groups?*

J. Tent proved in [T], Theorem B, that $|\mathbb{Q}(G) : \mathbb{Q}| \leqslant 2^7$ (or actually $\leqslant 2^5$) for solvable cut groups. There is also an affirmative answer to Question 1 for all quasi or almost simpel groups (in particular for all simple groups), cf. Theorem 5.1 of [BCJM] and S. Trefethen's article [Tr].

On the other hand, the answer to Question 1 is no, if one considers the slightly larger classes of semi-rational or quadratic rational groups (i.e. groups where one allows arbitrary quadratic extensions for each row or column of the character table, respectively) instead of cut groups, as can be seen from the alternating groups.

Since non-trivial rational groups have even order, the Sylow 2-subgroups play a fundamental role in these groups. In particular it was conjectured that they should again be rational! This was refuted by I.M. Isaacs and G. Navarro in the article [IN] providing counterexamples of order $2^9 \cdot 3$, where they also proved that the Sylow 2-subgroup of a rational group is rational again in certain classes of groups. Since every non-trivial cut group has an order divisbile by 2 or 3 (see

Theorem 1 of [BMP]), one might wonder what can be said about the corresponding Sylow subgroups. It is not hard to find examples of cut groups having Sylow 2-subgroups that fail to be cut. However for Sylow 3-subgroups the situation seems to be different; see also Question 6.8 of [BCJM].

Question 2 *Let* G *be a cut group,* $P \in \mathrm{Syl}_3(G)$. *Is* P *cut?*

Why might there be more hope that this question has a positive answer compared to the question on rationality of the Sylow 2-subgroups in rational groups? One can prove the following: A 3-element of a group G is inverse semi-rational in G if and only if it is inverse semi-rational in some Sylow 3-subgroup P of G containing it (see Lemma 6.1 of [BCJM]). The basic fact behind this is that the automorphism group of a cyclic 3-group is cyclic, which is in general not the case for a cyclic 2-group, hence the corresponding proof does not work for rationality and 2-elements. In Section 6 of [BCJM] a positive answer to Question 2 is provided for supersolvable groups (or, more generally, for solvable groups of 3-length 1), Frobenius groups, for groups of small order and in several other situations. Moreover, the answer to Question 2 is yes for all groups of odd order (see Theorem C of [G]) and for all (quasi or almost) simpel groups as can be checked departing from the data in Theorem 5.1 of [BCJM] and [Tr]. N. Grittini also showed that Question 2 has an affirmative answer for solvable cut groups, if their Sylow 3-subgroup has nilpotency class at most 2, see Theorem A of [G]. Note that in case Question 2 has a positive answer, then P/P' is also cut, hence an elementary abelian 3-group. This is indeed always the case by a result of Isaacs-Navarro, Grittini (for solvable groups) or, in general, by Corollary D of [NT].

The only primes that divide the order of a solvable rational group are 2, 3 and 5 by a classical result of R. Gow. A striking result of P. Hegedűs asserts that 5 plays a very special rôle: the Sylow 5-subgroup is normal and elementary abelian in every solvable rational group [H]. The only primes that divide the order of a solvable cut group are 2, 3, 5 and 7 (see Theorem 1.2 of [B]). Yet one can construct examples of solvable cut groups with arbitrary large p-length and Sylow p-subgroups with arbitrary large exponent (for $p \in \{5, 7\}$ take the iterated wreath product of the normalizer of a Sylow p-subgroup in S_p, the symmetric group of degree p). But is at least the Hall $\{5, 7\}$-subgroup of each Fitting layer nice? As usual, $O_p(G)$ denotes the largest normal p-subgroup of G.

Question 3 *Let* G *be a solvable* cut *group. Is it true that* $\exp O_p(G) \mid p$ *for* $p \in \{5, 7\}$*?*

References

[B] A. Bächle: "Integral group rings of solvable groups with trivial central units", *Forum Math.* 30 (2018), 845–855.

[BCJM] A. Bächle – M. Caicedo – E. Jespers – S. Maheshwary: "Global and local properties of finite groups with only finitely many central units in their integral group ring", 12pp.; *arXiv*:1808.03546.

[BMP] G.K. Bakshi – S. Maheshwary – I.B.S. Passi: "Integral group rings with all central units trivial", *J. Pure Appl. Algebra* 221 (2017), 1955–1965.

[CD] D. Chillag – S. Dolfi: "Semi-rational solvable groups", *J. Group Theory* 13 (2010), 535–548.

[G] N. Grittini: "Sylow 3-subgroups of solvable cut groups", 12pp.; *arXiv*:1911.13196.

[H] P. Hegedűs: "Structure of solvable rational groups", *Proc. London Math. Soc.* 90 (2005), 439–471.

[IN] I.M. Isaacs – G. Navarro: "Sylow 2-subgroups of rational solvable groups", *Math. Z.* 272 (2012), 937–945.

[NT] G. Navarro – P.H. Tiep: 'Sylow subgroups, exponents, and character values", *Trans. Amer. Math. Soc.* 372 (2019), 4263–4291.

[T] J.F. Tent: "Quadratic rational solvable groups", *J. Algebra* 363 (2012), 73–82.

[Tr] S. Trefethen: "Non-Abelian composition factors of finite groups with the CUT-property", *J. Algebra* 522 (2019), 236–242.

ADV – 8C *Lev Kazarin*

Eugene P. Wigner introduced in 1940 the class of *simply reducible groups* (SR-groups). These are the real groups for which tensor product of any two irreducible representations are decomposable into the sum of irreducible representations of a group with coefficients not exceeding 1.

It was proved in [L.S. Kazarin – E.I. Chankov: "Finite simply reducible groups are solvable", *Sbornik Math.* 201 (2010), 655 – 668] that finite simply reducible groups are soluble.

Question 1 *Determine the structure of soluble* SR*-groups.*

In particular it is not known when the wreath product of two finite SR-groups is an SR-group. Is the derived length of a finite SR-group bounded?

The attempts to obtain a fast group-theoretic based algorithms of matrix multiplications lead to the investigations of finite groups for which the sums of the cubes of irreducible representations is not too far from $|G|\log|G|$. This is also interesting for the applications of a group-theoretic based algorithms for computing convolutions used in a signal processing.

It is also natural to study finite groups with extremely large degrees of irreducible characters.

Question 2 *Determine the structure of a finite group* G *admitting an irreducible character* χ *such that* $|G| < 3\chi(1)^2$*. Note that the sporadic Thompson group has such an irreducible character of degree* 190373976*.*

Clearly, it is interesting in general to study the behaviour of the set $\mathrm{cd}(G)$ of degrees of irreducible characters of a finite group G.

Question 3 *Is it true that every alternating group* A_n *for* $n > 20$ *has three irreducible complex characters* χ_1, χ_2, χ_3 *such that* $n!/2$ *divides* $\chi_1(1)\chi_2(1)\chi_3(1)$*?*

ADV – 8D *Francesco de Giovanni & Marco Trombetti*

Let $\mathfrak{X}$ be a class of groups. A group is said to be *minimal non-*$\mathfrak{X}$ (or an *opponent* of $\mathfrak{X}$) if it is not an $\mathfrak{X}$-group but all its proper subgroups belong to $\mathfrak{X}$. The structure of minimal non-$\mathfrak{X}$ groups has been investigated for several different choices of the group class $\mathfrak{X}$ since the beginning of twentieth century, when Šmidt on one side, Miller and Moreno on the other, studied in this context the behaviour of the class $\mathfrak{F}$ of finite groups and that of the class $\mathfrak{A}$ of abelian groups.

We shall denote by $\mathfrak{X}^\circ$ the *interior* of $\mathfrak{X}$, i.e. the subclass of $\mathfrak{X}$ consisting of all groups that occur as proper subgroups of some locally graded opponent of $\mathfrak{X}$. Of course, the class $\mathfrak{X}^\circ$ can be much smaller than $\mathfrak{X}$, and it is of interest to understand which groups must belong to $\mathfrak{X}^\circ$.

This problem is easily settled out for the classes $\mathfrak{F}$ and $\mathfrak{A}$ (see [dGT1]). Although also the structure of finite minimal non-nilpotent groups is well described (see [BER]), the situation is much more complicated in the infinite case (see for instance [M]), and so the following problem concerning the class $\mathfrak{N}$ of nilpotent groups naturally arises.

Question 1 *Determine the group class* $\mathfrak{N}^\circ$*, or at least give a satisfactory approximation of it.*

A similar question can be asked for the class ZA of hypercentral groups.

Question 2 *Determine the group class* ZA°*, or at least give a satisfactory approximation of it.*

Notice that answers to Question 2 will provide information also on the corresponding problem for the class of hypercyclic groups; indeed, it is known that an infinite locally graded group is minimal non-hypercyclic if and only if it is minimal non-hypercentral (see [dGT]).

The description of the main properties of the interior of a group class and related concepts can be found in [dGT1].

References

[BER] A. Ballester Bolinches – R. Esteban Romero – D.J.S. Robinson: "On finite minimal non-nilpotent groups", *Proc. Amer. Math. Soc.* 133 (2005), 3455–3462.

[dGT] F. de Giovanni – M. Trombetti: "Infinite minimal non-hypercyclic groups", *J. Algebra Appl.* 14 (2015), 1550143.

[dGT1] F. de Giovanni – M. Trombetti: "Cohopfian groups and accessible group classes", to appear.

[M] F. Menegazzo: "Groups of Heineken-Mohamed", *J. Algebra* 171 (1995), 807–825.