Доклади на Българската академия на науките
Comptes rendus de l'Académie bulgare des Sciences
Tome 66, No 2, 2013

MATHEMATIQUES
Algèbre

PAIRS OF ELEMENTS OF ORDERS 2 AND 3 IN THE REE GROUPS $^2G_2(3^n)$

Konstantin Tabakov, Kerope Tchakerian

(*Submitted by Corresponding Member V. Drensky on September 24, 2012*)

Abstract

We classify all pairs of elements x and y with $|x| = 2$ and $|y| = 3$ in the group $G = {}^2G_2(3^n)$ (odd $n > 1$) such that either $|xy| = 7$ or $G = \langle x, y\rangle$.
Key words: (2,3)-generated group, Hurwitz group
2000 Mathematics Subject Classification: 20F05, 20D06

Introduction. A group is said to be $(2,3)$-generated if it is generated by two elements x and y of orders 2 and 3, respectively, and $(2,3,7)$-generated or Hurwitz group if, in addition, the product xy has order 7. Malle [5] proved that the Ree group $G = {}^2G_2(3^n)$ (n odd) is Hurwitz for any $n > 1$, and later the second author found in [7] explicit Hurwitz generators x and y of G. Malle's result, Macbeath's classification [4] of Hurwitz subgroups of $PSL_2(q)$ (q a prime power), and the known subgroup structure of G [3, 9, 2] easily imply that G contains exactly the following Hurwitz groups: $SL_2(8)$, $PSL_2(27)$ if $3|n$, and $^2G_2(3^m)$ for each divisor $m > 1$ of n if $n > 1$. The first aim of the present paper is to provide an alternative proof of this based on the papers [7, 9] and, moreover, to classify all Hurwitz pairs of elements x and y in G (that is, nonidentity elements with $x^2 = y^3 = (xy)^7 = 1$). Then the second aim is to classify all $(2,3)$-generations of G, that is, all pairs of elements x and y with $x^2 = y^3 = 1$ and $G = \langle x, y\rangle$. We note that some of the arguments below essentially appear in [7] and will be reproduced here for the sake of completeness and reader's convenience. Note also that case (i) of Theorem 1 below follows from the more general considerations in [8].

We fix the notation $G = {}^2G_2(q)$ where $q = 3^n$ and $n > 1$ is odd, $F = GF(q)$, and $\theta = 3^{\frac{n-1}{2}}$ (so that $q = 3\theta^2$). Now our results are as follows:

This work is partially supported by the Scientific Research Fund of St. Kl. Ohridski University of Sofia under Contract No 27, 2012.

Theorem 1. *Let x and y be nonidentity elements of G and $x^2 = y^3 = (xy)^7 = 1$. Then up to a conjugation in G exactly one of the following holds:*

(*i*) $x = \omega_0$, $y = \gamma(1)$, *and* $\langle x, y\rangle \cong SL_2(8)$;

(*ii*) $3|n$, $x = h(z)\omega_0$, $y = \beta(\varepsilon)$, *where* $\varepsilon = \pm 1$, $z \in F$ *and* $z^3 + z^2 = 1$, *and* $\langle x, y\rangle \cong PSL_2(27)$;

(*iii*) $x = h(z)\omega_0$, $y = \beta(\varepsilon)\gamma(t)$, *where* $\varepsilon = \pm 1$, $z, t \in F^*$ *and* $t^2 = z^{6\theta+3} - z^{3\theta} - 1$, *and* $\langle x, y\rangle \cong {}^2G_2(3^m)$ *where* $m > 1$ *is the least divisor of* n *for which* $z \in GF(3^m)$.

Remark. The lemma in [7] implies that case (*iii*) really holds for every divisor $m > 1$ of n.

Theorem 2. *Let x and y be elements of G such that $x^2 = y^3 = 1$ and $G = \langle x, y\rangle$. Then up to a conjugation in G exactly one of the following holds:*

(*i*) $x = h(z)\omega_0$ *and* $y = \gamma(1)$, *where* $F = \mathbb{Z}_3(z)$;

(*ii*) $x = h(z)\omega_0$ *and* $y = \beta(\varepsilon)\gamma(t)$, *where* $\varepsilon = \pm 1$, $t \neq 0$, $z \neq -t^{2\theta} - 1$, *and* $F = \mathbb{Z}_3(z, t)$.

Proofs. The general theory of the groups of Lie type is developed in [1]. Notation and detailed information on the Ree groups can be found in [6] and [10]. For our present purposes, it is most convenient to adopt the notation and make use of the information gathered in [9]. Also, we make essential use of the well-known 7-dimensional matrix representation of the group G over the field F (for details, see [9], p. 220).

Proof of Theorem 1. The group G has three conjugacy classes of elements of order 3 with representatives $\gamma(1)$, $\beta(1)$, and $\beta(-1) = \beta(1)^{-1}$.

Let first $y = \gamma(1)$. Then $x \notin UH = P$ as $|P| = q^3(q-1)$ is not divisible by 7. So $x \in UH\omega_0U$ and $|x| = 2$ exactly when $x = uh(z)\omega_0u^{-1}$ ($z \in F^*$) where $u \in U$. As $\gamma(1) \in Z(U)$, conjugating by u we can assume $x = h(z)\omega_0$ and $y = \gamma(1)$. In matrix form

$$x = -(z^{-3\theta-2}E_{-33} + zE_{-22} + z^{3\theta+1}E_{-11} + E_{00} + z^{-3\theta-1}E_{1-1} + z^{-1}E_{2-2} + z^{3\theta+2}E_{3-3}),$$
$$y = E + E_{-21} + E_{-1-3} - E_{-12} + E_{0-3} - E_{3-3} + E_{30} - E_{31}.$$

Now we have

$$\begin{aligned} xy = z^{-3\theta-2}E_{-3-3} - z^{-3\theta-2}E_{-30} + z^{-3\theta-2}E_{-31} - z^{-3\theta-2}E_{-33} \\ -zE_{-22} - z^{3\theta+1}E_{-11} - E_{0-3} - E_{00} - z^{-3\theta-1}E_{1-3} - z^{-3\theta-1}E_{1-1} \\ +z^{-3\theta-1}E_{12} - z^{-1}E_{2-2} - z^{-1}E_{21} - z^{3\theta+2}E_{3-3}. \end{aligned}$$

Set $\eta = tr(xy) = z^{-3\theta-2} - 1$. Then one computes that the characteristic polynomial of xy is

$$X^7 - \eta X^6 + (\eta^{3\theta} - \eta)X^5 + (\eta^{3\theta} - \eta^2 + \eta)X^4 - (\eta^{3\theta} - \eta^2 + \eta)X^3 - (\eta^{3\theta} - \eta)X^2 + \eta X - 1.$$

On the other hand, G has a single conjugacy class of elements of order 7, with characteristic polynomial $X^7 - 1$. Thus $|xy| = 7$ if and only if $\eta = 0$ which yields $z = 1$. Now $x = \omega_0$ and $y = \gamma(1)$ both lie in the subgroup $G_1 \cong {}^2G_2(3)$ of G. As $\langle x, y\rangle$ is a perfect group, it is contained in $G_1' \cong SL_2(8)$ and (by the structure of $SL_2(8)$) it follows that $\langle x, y\rangle \cong SL_2(8)$. This is (i) of the theorem.

Now let $y = \beta(\varepsilon)$ where $\varepsilon = \pm 1$. Just as above, $x = uh(z)\omega_0 u^{-1}$ $(z \in F^*)$ with $u \in U$ and conjugation by u transforms y into $\beta(\varepsilon)\gamma(t)$ for some $t \in F$. Thus we can assume $x = h(z)\omega_0$ and $y = \beta(\varepsilon)\gamma(t)$. In matrix form, x is given above and

$$y = E + \varepsilon E_{-2-3} + t^\theta E_{-21} + (t - \varepsilon t^\theta)E_{-1-3} - \varepsilon E_{-10} - E_{-11} - t^\theta E_{-12} + t^\theta E_{0-3} \\ -\varepsilon E_{01} + \varepsilon E_{2-3} - (t^{2\theta} + 1)E_{3-3} - \varepsilon E_{3-2} + t^\theta E_{30} - (t + \varepsilon t^\theta)E_{31} - \varepsilon E_{32}.$$

Now we have

$$xy = z^{-3\theta-2}(t^{2\theta} + 1)E_{-3-3} + \varepsilon z^{-3\theta-2}E_{-3-2} - z^{-3\theta-2}t^\theta E_{-30} + z^{-3\theta-2}(t + \varepsilon t^\theta)E_{-31} \\ +\varepsilon z^{-3\theta-2}E_{-32} - z^{-3\theta-2}E_{-33} - \varepsilon z E_{-2-3} - zE_{-22} - z^{3\theta+1}E_{-11} - t^\theta E_{0-3} - E_{00} \\ +\varepsilon E_{01} + z^{-3\theta-1}(\varepsilon t^\theta - t)E_{1-3} - z^{-3\theta-1}E_{1-1} + \varepsilon z^{-3\theta-1}E_{10} + z^{-3\theta-1}E_{11} \\ +z^{-3\theta-1}t^\theta E_{12} - \varepsilon z^{-1}E_{2-3} - z^{-1}E_{2-2} - z^{-1}t^\theta E_{21} - z^{3\theta+2}E_{3-3}.$$

Set $\tau = tr(xy) = z^{-3\theta-2}(t^{2\theta} + 1) + z^{-3\theta-1} - 1$. Then the characteristic polynomial of xy is again

$$X^7 - \tau X^6 + (\tau^{3\theta} - \tau)X^5 + (\tau^{3\theta} - \tau^2 + \tau)X^4 - (\tau^{3\theta} - \tau^2 + \tau)X^3 - (\tau^{3\theta} - \tau)X^2 + \tau X - 1.$$

This polynomial is $X^7 - 1$ if and only if $\tau = 0$ or, equivalently,

$$t^{2\theta} = z^{3\theta+2} - z - 1 \quad (z \in F^*,\ t \in F). \tag{1}$$

Thus $|xy| = 7$ exactly when (1) holds.

Denote $N = \langle x, y\rangle$. Let $t = 0$; then both x and y are centralized by the involution $h(-1)$. Now (1) implies consecutively

$$z^{3\theta+2} = z + 1,\quad z^{6\theta+3} = z^{3\theta} + 1,\quad (z + 1)^2 = z(z^{3\theta} + 1),\quad z^{3\theta+1} = z^2 + z + 1, \\ z(z^2 + z + 1) = z + 1,\quad z^3 + z^2 = 1.$$

The last equality easily produces $z^{13} = 1$. Hence $13 | q - 1$ so $3|n$. Conversely, let $3|n$. Then there is a $z \in GF(3^3) \le F$ with $z^3 + z^2 = 1$ (whence $z + 1 = z^{-2}$). As $\frac{n-3}{2}$ is divisible by 3, we have $3^{\frac{n-3}{2}} \equiv 1 \pmod{13}$ and hence $3\theta + 2 = 3^{\frac{n+1}{2}} + 2 \equiv 9 + 2 \equiv -2 \pmod{13}$. Then $z^{3\theta+2} = z^{-2} = z + 1$ and therefore $|xy| = 7$. Now $x = h(z)\omega_0$ and $y = \beta(\varepsilon)$ both lie in the subgroup $G_3 \cong {}^2G_2(3^3)$ of G. Since $N \le C_{G_3}(h(-1)) \cong Z_2 \times PSL_2(27)$ and N is a perfect group, the structure of $PSL_2(27)$ implies $N \cong PSL_2(27)$. This is (ii) of the theorem.

Now we assume $t \ne 0$. Let m be the least divisor of n for which $z \in GF(3^m) = K \le F$. If $m = 1$, then $z = \pm 1$ and $z^{3\theta+2} - z - 1 = -1$ is not a square in F so

(1) does not hold, that is $|xy| \neq 7$. Thus $m > 1$, and set $\theta_0 = 3^{\frac{m-1}{2}}$. Equality (1) is equivalent to $t^2 = z^{6\theta+3} - z^{3\theta} - 1$, and hence $t^2 \in K$. As $t \in F$ and as $GF(3^n)$ (n odd) has no subfield $GF(3^{2m})$, it follows that $t \in K$. It is easy to see that $\theta - \theta_0$ is a multiple of $3^m - 1$, hence $z^\theta = z^{\theta_0}$, $t^\theta = t^{\theta_0}$ and (1) becomes

$$t^{2\theta_0} = z^{3\theta_0+2} - z - 1. \tag{2}$$

Then the lemma in [7] implies that for any $m > 1$ there exists $z, t \in K^*$ such that (2) holds (so $|xy| = 7$) and z in fact lies in no proper subfield of K. Now $x = h(z)\omega_0$ and $y = \beta(\varepsilon)\gamma(t)$ both belong to the subgroup $G_m \cong {}^2G_2(3^m)$ of G. Just as in [7], the list of maximal subgroups of G_m (see the next section) implies $N = G_m$, i.e. $N \cong {}^2G_2(3^m)$. This is (iii) of the theorem.

The proof of Theorem 1 is completed.

Proof of Theorem 2. We shall need the list of maximal subgroups of G determined in [3, 9, 2]. In the notation of [9], this list implies that if M is a maximal subgroup of G then one of the following holds:

1) $M \cong Z_2 \times PSL_2(q)$ is the centralizer of an involution;
2) $M \cong (E_8 Z_{\frac{q+1}{4}})Z_3$ is the normalizer of a four-group;
3) M is conjugate to $P = UH = N_G(U)$, a parabolic subgroup;
4) M is a Frobenius group of order $6(q+1-\sqrt{3q})$ or $6(q+1+\sqrt{3q})$;
5) M is conjugate to the subgroup $G_m \cong {}^2G_2(3^m)$ for some divisor m of n with $\frac{n}{m}$ prime.

Now, starting with an element y of order 3 as in the previous section, we have $y \in P$ and this forces $x \notin P$. So we can again assume that (up to a conjugation in G) $x = h(z)\omega_0$ ($z \in F^*$) and $y = \gamma(1)$ or $y = \beta(\varepsilon)\gamma(t)$ ($\varepsilon = \pm 1,\ t \in F$). Let $N = \langle x, y \rangle$. Note that, in order to have $N = G$, necessarily $F = \mathbb{Z}_3(z)$ if $y = \gamma(1)$ and $F = \mathbb{Z}_3(z, t)$ if $y = \beta(\varepsilon)\gamma(t)$.

Let first $y = \gamma(1)$. We claim that (with the above choice of z) $N = G$. Assume false and let M be a maximal subgroup of G containing N. Note that $C_G(y) = U$ and, in particular, y is not centralized by any involution of G. Hence M is not of type 1). Similarly, M is not of type 4) because this Frobenius group has a cyclic complement of order 6, that is any element of order 3 in it is centralized by an involution. Further, as it is shown in [9], p.217 any element of order 3 of G normalizing a four-subgroup necessarily centralizes an involution; so M is not of type 2).

Next, assume that M is of type 3), that is $N \leq g^{-1}Pg$ for some $g \in G$. Then $y \in U$ and $y \in g^{-1}Ug$ (as $g^{-1}Ug$ is the unique Sylow 3-subgroup of $g^{-1}Pg$). However, any two distinct conjugates of U in G intersect trivially, see [9], Lemma 2.1. It follows that $g^{-1}Ug = U$ so $g \in N_G(U) = P$ and $x \in g^{-1}Pg = P$, a contradiction.

Last, suppose that M is of type 5), i.e. N is conjugate to a subgroup of G_m for some $m < n$. Then, in the 7-dimensional matrix representation of G, the trace of any element of N must lie in a proper subfield $K = GF(3^m)$ of F. But $tr(xy) = z^{-3\theta-2} - 1$ (see the previous section) and $tr(xy) \in K$ implies $z = (z^{-3\theta-2})^{3\theta-2} \in K$ which contradicts the choice of z.

Thus $N = G$, proving (i) of the theorem.

Remark. A few more arguments imply the following: if $x \in G$ is any involution and $y \in G$ is any element of order 3 conjugate to $\gamma(1)$, then the group $\langle x, y\rangle$ is isomorphic to S_3, $SL_2(8)$, or ${}^2G_2(3^m)$ for some divisor $m > 1$ of n.

Now let $y = \beta(\varepsilon)\gamma(t)$ $(\varepsilon = \pm 1,\ t \in F)$. Recall $x = h(z)\omega_0$ and $F = \mathbb{Z}_3(z, t)$. We also must have $t \neq 0$ since otherwise x and y are centralized by the involution $h(-1)$ and $N \neq G$. We shall use the matrices representing x, y, and xy and also the characteristic polynomial of xy, as given in the previous section.

First, we claim that $|xy| \geq 6$ and $|xy| = 6$ if and only if $z = -t^{2\theta} - 1$. Indeed, $|xy| > 2$ as clearly $xy = h(z)\omega_0\beta(\varepsilon)\gamma(t) \neq \beta(-\varepsilon)\gamma(-t)h(z)\omega_0 = (xy)^{-1}$. Assume that $|xy| = 3$, hence $(xy)^2 = y^2x$. Then a comparison of the $(3,2)$-entries and $(3,3)$-entries of these two matrices yields $-\varepsilon = -\varepsilon z$ and $1 = z^{-3\theta-2}(t^{2\theta} + 1)$, that is $z = 1$ and $t = 0$ which is not the case. Next, $|xy| \neq 4$ as a Sylow 2-subgroup of G is isomorphic to E_8 and $|xy| \neq 5$ as $|G|$ is not divisible by 5. Now G has two conjugacy classes of elements of order 6 with representatives $\beta(\varepsilon)h(-1)$ and characteristic polynomial $X^7 + X^6 - X - 1$. So $|xy| = 6$ implies $\tau = z^{-3\theta-2}(t^{2\theta}+1)+z^{-3\theta-1}-1 = -1$, i.e. $z = -t^{2\theta}-1$. Conversely, if $z = -t^{2\theta}-1$ then xy has the above characteristic polynomial and this easily yields $(xy)^{18} = 1$. As $|xy| \geq 6$, $|xy| \neq 9$ (the 3-elements in G have trace 1), and G has no element of order 18, it follows that $|xy| = 6$. This proves our claim.

Now if $|xy| = 6$ it is easily verified that $\langle (x, y), (x, y^{-1})\rangle$ is a nonidentity normal Abelian subgroup of N (in fact, it is well-known that N is a solvable group), hence $N \neq G$. So we must have $z \neq -t^{2\theta} - 1$ and then $|xy| > 6$.

Now, supposing $F = \mathbb{Z}_3(z, t)$, $t \neq 0$, and $z \neq -t^{2\theta} - 1$, we proceed to prove that $N = G$. Assume it is false and let M be a maximal subgroup of G with $N \leq M$.

Suppose that M is of type 1), then N is centralized by some involution. It is directly checked that the only involutions of G centralizing y are $v = \alpha(-\varepsilon t)\beta(t^{3\theta+1})\gamma(c)h(-1)$ $(c \in F)$. Then a glance at the canonical form of the elements vx and xv implies that v centralizes x only if $c = t = 0$, a contradiction.

Next, suppose that M is of type 2). Then $M = N_G(V)$ where $V \cong E_4$, $C_G(V) \cong E_8Z_{\frac{q+1}{4}}$, and $|N_G(V) : C_G(V)| = 3$. It follows that $x \in C_G(V)$ and $y \notin C_G(V)$ so $xy \notin C_G(V)$ but $(xy)^3 \in C_G(V)$. This implies that $3||xy|$. But an element of G conjugate to $\beta(\pm 1)$ is centralized by nonidentity elements of orders 3 and 6 only, hence $|xy| = 3$ or 6, an impossibility.

That M is not of type 3) follows (just as for $y = \gamma(1)$ above) by the fact that any two distinct conjugates of U in G intersect trivially. Further, let M be of type 4). Then xy is not in the Frobenius kernel $Z_{q+1\pm\sqrt{3q}}$ of M as otherwise $x^{-1}(xy)x = (xy)^{-1}$, i.e. $y = y^{-1}$, an absurd. But the elements of M, outside the kernel, have all orders dividing 6, that is $|xy||6$ which is again impossible.

Finally, assume that M is of type 5), i.e. N is conjugate to a subgroup of $G_m \cong {}^2G_2(3^m)$ for some $m < n$. Then

$$tr(xy) = \tau = z^{-3\theta-2}(t^{2\theta}+1) + z^{-3\theta-1} - 1 \in GF(3^m) = K < F. \tag{3}$$

Now we find

$$\begin{aligned} xy^{-1} = {} & z^{-3\theta-2}(t^{2\theta}+1)E_{-3-3} - \varepsilon z^{-3\theta-2}E_{-3-2} + z^{-3\theta-2}t^{\theta}E_{-30} \\ & + z^{-3\theta-2}(\varepsilon t^{\theta} - t)E_{-31} - \varepsilon z^{-3\theta-2}E_{-32} - z^{-3\theta-2}E_{-33} + \varepsilon zE_{-2-3} - zE_{-22} \\ & - z^{3\theta+1}E_{-11} + t^{\theta}E_{0-3} - E_{00} - \varepsilon E_{01} + z^{-3\theta-1}(\varepsilon t^{\theta}+t)E_{1-3} - z^{-3\theta-1}E_{1-1} - \varepsilon z^{-3\theta-1}E_{10} \\ & + z^{-3\theta-1}E_{11} - z^{-3\theta-1}t^{\theta}E_{12} + \varepsilon z^{-1}E_{2-3} - z^{-1}E_{2-2} + z^{-1}t^{\theta}E_{21} - z^{3\theta+2}E_{3-3}. \end{aligned}$$

Then we compute the trace of the commutator $(x, y) = xy^{-1}.xy$:

$$tr(x,y) = z^{-6\theta-4}(t^{2\theta}+1)^2 - z^{-6\theta-3}(t^{2\theta}+t^2) + z^{-6\theta-2} - z^{-3\theta-3} + 1 \in K. \tag{4}$$

As (3) implies

$$t^{2\theta} = \tau z^{3\theta+2} + z^{3\theta+2} - z - 1 \text{ and hence } t^2 = \tau^{3\theta}z^{6\theta+3} + z^{6\theta+3} - z^{3\theta} - 1,$$

(4) becomes $tr(x, y) = \tau^2 - \tau - \tau^{3\theta} + 1 - z^{-6\theta-3}$. Since $tr(x, y) \in K$ and $\tau \in K$, it follows that $z^{-6\theta-3} \in K$ whence $z = (z^{-6\theta-3})^{1-2\theta} \in K$. Now $t^2 \in K$ and as $t \in F$ and F has no subfield $GF(3^{2m})$, it follows that $t \in K$. Then $\mathbb{Z}_3(z, t) \le K < F$, a contradiction.

Thus $N = G$, proving (ii) of the theorem. The proof of Theorem 2 is completed.

REFERENCES

[1] Carter R. Simple Groups of Lie Type, London, Wiley, 1972.
[2] Kleidman P. J. Algebra, **117**, 1988, 30–71.
[3] Levchuk V. M., Ya. N. Nuzhin. Algebra i Logika (Novosibirsk), **24**, 1985, 26–41.
[4] Macbeath A. M. Proc. Symp. Pure Math., **12**, 1969, 14–32.
[5] Malle G. Can. Math. Bull., **33**, 1990, 349–357.
[6] Ree R. Amer. J. Math., **83**, 1961, 432–462.
[7] Tchakerian K. Compt. rend. Acad. bulg. Sci., **58**, 2005, No 7, 749–752.
[8] Tchakerian K. Compt. rend. Acad. bulg. Sci., **65**, 2012, No 7, 875–880.
[9] Tchakerian K., N. Petrov. Ann. Univ. Sofia, **79**, 1985, 215–221.
[10] Ward H. Trans. Amer. Math. Soc., **121**, 1966, 62–89.

Faculty of Mathematics and Informatics
St. Kliment Ohridski University of Sofia
5, J. Bourchier Blvd
1164 Sofia, Bulgaria
e-mail: ktabakov@fmi.uni-sofia.bg