ISRAEL JOURNAL OF MATHEMATICS 77 (1992), 17–31

STRUCTURE OF $R(3,3)$-GROUPS

BY

GREGORY A. FREIMAN

School of Mathematics
Institute for Advanced Study, Princeton, NJ 08540, USA; and
School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Ramat Aviv, Tel Aviv, Israel

AND

BORIS M. SCHEIN

Department of Mathematical Sciences
University of Arkansas, Fayetteville, AR 72701, USA

ABSTRACT

We describe groups G in which the set $\{abc, acb, bac, bca, cab, cba\}$ contains three different elements at most for any $a, b, c \in G$ and show how this type of problem is connected with the rewritability (or permutation) properties of groups.

In this paper we solve a problem connected with a rewritability property in groups. This type of problem is explained in more detail in our paper [4]. This general direction studies properties of groups and semigroups determined by multiplication of subsets. Analogous problems are considered in the book by Arad and Herzog [1] and in a survey by Blyth and Robinson [2]. For other references see the bibliography at the end of [4].

For an m-element subset $A = \{a_1, a_2, \ldots, a_m\}$ of a group G let $A^{[m]}$ denote the set of all products $a_{\pi(1)}a_{\pi(2)}\cdots a_{\pi(m)}$ for all permutations π of the set $\{1, 2, \ldots, m\}$. Clearly, $A^{[m]}$ cannot contain more than $m!$ different elements. The cardinality $|A^{[m]}|$ of $A^{[m]}$, however, may be much smaller. For example, if G is abelian, then $|A^{[m]}| = 1$ for every such subset A. A group G is called

Received August 21, 1990 and in revised form March 10, 1991

an $R(m,n)$-group if $|A^{[m]}| \leq n$ for all m-element subsets A of G. We can assume that n is a natural number such that $1 \leq n \leq m!$ and, for convenience sake, the symbol $R(m,n)$ will denote the class of all $R(m,n)$-groups. Clearly, $R(m,n) \subset R(m,n+1)$. In particular, we obtain a chain

$$R(m,1) \subset R(m,2) \subset \ldots \subset R(m,m!).$$

If $m = 1$, then $R(m,n)$ is the class of all groups, and so we assume that $m > 1$. Then $R(m,1)$ is the class of all abelian groups and $R = (m,m!)$ the class of all groups. For $m = 2$ we have the trivial cases of $R(2,1)$ and $R(2,2)$. For $m = 3$ there are four nontrivial classes: $R(3,n)$ for $2 \leq n \leq 5$. We described $R(3,2)$ in our previous paper [4] (it consists of all those groups G for which $|G'| \leq 2$, where G' is the commutator subgroup of G). In this paper we describe $R(3,3)$. A description of $R(3,5)$ is a known group theory problem, for $R(3,5)$ coincides with the so-called Q_3-groups whose structure is not known (see [2] and [4]). We hope that describing classes $R(3,n)$ when n grows may shed light on the structure of Q_3-groups and help solve similar problems. At the end of this paper we list a few natural unsolved problems.

THEOREM: *A group G is an $R(3,3)$-group if and only if $|G'| \leq 3$. If $|G'| = 1$, then G is abelian; if $|G'| = 2$, then G is an $R(3,2)$-group; and if $|G'| = 3$ then either $G/Z(G)$ is a group of exponent 3 or $G/Z(G)$ is isomorphic to S_3, the symmetric group of degree 3.*

Proof: We use the classification of three-element subsets from [4]. If $A = \{x,y,z\}$ is a three-element subset of a group, then $|A^{[3]}| \leq 3$ if and only if one of the following nine systems of equalities holds, where the elements x, y and z are renamed as a, b, and c in a certain order:

(1) $abc = acb = bac = bca = cab = cba$ (all elements of A commute);

(2) $abc = bac = bca$ and $acb = cab = cba$ (two pairs of elements of A commute);

(3) $abc = bac = cab = cba$ and $acb = bca$ (one pair of elements of A commutes);

(4) $abc = bca = cab$ and $acb = bac = cba$;

(5) $abc = bac$, $cab = cba$, and $acb = bca$ (one pair of elements of A commutes);

(6) $abc = bac = cab = cba$, with acb and bca isolated (one pair of elements of A commutes);

(7) $abc = bca$, $bac = cab$, and $acb = cba$;

(8) $abc = cba$, $acb = bca$, and $bac = cab$;

(9) $acb = bac = cba$, $bca = cab$, and abc isolated (that is, not equal to the product of a, b, and c in any other order).

Each of these systems is called a Type, and only those equalities of products of a, b, and c, which are specifically mentioned, hold in each Type. For example, the equality $abc = bac$ is not listed in Type (7), and hence $abc \neq bac$ in this Type. In Type (9) abc is not equal to any other product in $A^{[3]}$, which is why we say that abc is isolated.

Proof: *Sufficiency.* Let $|G'| \leq 3$. If $|G'| = 1$, then G is an abelian group. If $|G'| = 2$, then, by Theorem 2, G is an $R(3,2)$-group and hence an $R(3,3)$-group. Now let $|G'| = 3$ and consider a subset $A = \{a, b, c\}$ of G. If more than one pair of elements of A commutes, then A belongs to Types (1) or (2). If a and b are the only commuting elements of A, consider $[ab, c^{-1}]$. If $[ab, c^{-1}] = 1$, then $abc = cab$, and hence A belongs to Type (3) or Type (6). Let $[ab, c^{-1}] \neq 1$. If $[ab, c^{-1}] = [a, c^{-1}]$, then an easy calculation shows that $bc = cb$, contrary to our assumption. Thus, $[ab, c^{-1}] \neq [a, c^{-1}]$. Analogously, $[ab, c^{-1}] = [b, c^{-1}]$ leads to $ac = ca$, and hence $[ab, c^{-1}] \neq [b, c^{-1}]$. Since c commutes neither with a nor with b, we see that $[a, c^{-1}]$, $[b, c^{-1}]$, and $[ab, c^{-1}]$ are three elements of G', all different from 1. It follows that $[a, c^{-1}] = [b, c^{-1}]$. An easy calculation shows that this equality means $acb = bca$, that is A belongs to Types (3) or (5).

Suppose that no two elements of A commute. Let $abc \neq cab$ and $abc \neq cba$. Then $[ab, c] \neq 1$. It is easy to see that $[ab, c] = [b, c] \Leftrightarrow ac = ca$ and $[ab, c] = [b, a] \Leftrightarrow abc = cba$. Therefore, $[ab, c] \notin \{[b, a], [b, c]\}$. Thus, $[b, a] = [b, c]$. Also, $[ab, c] \neq [b, c]$ means that $[ab, c] = [b, c]^2 = [b, a][b, c]$. Now, the equality $[ab, c] = [b, a][b, c]$ is easily shown to mean $acb = cba$.

We have proved that $abc \neq cab$ and $abc \neq cba$ imply $acb = cba$. Interchanging here b and c, we obtain that $acb \neq bac$ and $acb \neq bca$ imply $abc = bca$.

Suppose that $|A|^{[3]}| > 3$. Then $A^{[3]}$ contains at least two isolated products (that is, products that are not equal to any other product in $A^{[3]}$). Without loss of generality, assume that abc is an isolated product. Then $abc \neq cab$ and $abc \neq cba$. Therefore, as we have proved earlier, $acb = cba$. Also, $abc \neq bca$, and hence $acb = bca$ or $acb = bac$. If $acb = bca$, then $cba = acb = bca$, so that $cb = bc$, contrary to our assumption. Thus, $acb \neq bca$. It follows that $acb = bac$. We proved that if abc is an isolated product, then $acb = bac = cba$. Then $|A^{[3]}| > 3$ implies that abc, bca and cab are isolated products in $A^{[3]}$ and the commutators $[a, bc]$, $[b, ca]$, and $[c, ab]$ differ from 1. If $[a, bc] = [ab, c]$, an easy argument shows that $bca = cab$, and so bca and cab are not isolated. Then $[a, bc] \neq [ab, c]$ and, since $|G'| = 3$, we obtain $[a, bc] = [ab, c]^{-1} = [c, ab]$. Analogously, $[c, ab] = [b, ca]$, and hence $[a, bc] = [b, ca] = [c, ab]$. Now, $[b, ca] = [b, a] \Leftrightarrow bc = cb$, so that $[b, ca] = [b, a]^{-1} = [a, b]$. Analogously, $[c, ab] = [b, c]$, so that $[a, b] = [b, c]$. But we have seen earlier that $[b, a] = [b, c]$. Then $[a, b] = [b, a] = [a, b]^{-1}$, which, together with $[a, b]^3 = 1$, shows that $[a, b] = 1$, contradicting $ab \neq ba$. Thus, $|A^{[3]}| > 3$ leads to a contradiction. It follows that $|A^{[3]}| \leq 3$, and hence G is an $R(3, 3)$-group.

Necessity: Let G be an $R(3, 3)$-group. For $a, b \in G$ we consider two cases: $ab \neq ba$ and $ab = ba$. Assume that $ab \neq ba$. The only commuting elements of $\{a, a^2, b\}$ are a and a^2, and possibly b and a^2. If $ba^2 \neq a^2 b$ then $\{a, a^2, b\}$ satisfies one of (3), (5) or (6). In each of these cases $baa^2 = aa^2 b$ or $aba^2 = a^2 ba$. The latter possibility yields $ab = ba$, which is impossible. Therefore, if $ba^2 \neq a^2 b$ then $ba^3 = a^3 b$. Thus, $C(a^2) \cup C(a^3) = G$ for all $a \in G$. Since $C(a^2)$ and $C(a^3)$ are subgroups of G, we obtain $C(a^2) = G$ or $C(a^3) = G$, so that for each $a \in G$ either $a^2 \in Z(G)$ or $a^3 \in Z(G)$. ∎

LEMMA 1: *One of the following four possibilities holds for every $R(3, 3)$-group G:*

(1) *G is abelian;*

(2) *$a^2 \in Z(G)$ for every $a \in G$ (that is $G/Z(G)$ is a group of exponent 2);*

(3) *$a^3 \in Z(G)$ for every $a \in G$ (that is, $G/Z(G)$ is a group of exponent 3);*

(4) *$G/Z(G) \cong S_3$, where S_3 denotes a symmetric group of degree 3.*

Proof: Suppose that the possibilities (1), (2) and (3) do not hold, that is, G possesses non-central elements whose squares belong to the center as well as those whose cubes belong to the center. Consider $H = G/Z(G)$. Clearly, H is an $R(3, 3)$-group in which all elements are of orders 1, 2, or 3. It suffices to prove that $H \cong S_3$.

Let $x, y, z \in H$, $x \neq y$, and $1 \neq o(x) = o(y) \neq o(z) \neq 1$, where $o(u)$ denotes the order of u.

If x commutes with z, then $o(xz) = 6$, which is impossible, and hence elements of orders 2 and 3 never commute. Thus, the only commuting elements in $X = \{x, y, z\}$ may be x and y. If $xy = yx$, then X is of Types (3), (5) or (6), and hence $(xy)z = z(xy)$ in Types (3) and (6), or $xzy = yzx$ in Types (3) and (5). Since x and y are commuting elements of the same order, $o(xy)$ divides $o(x)$, that is, either $o(xy) = 1$ or $o(xy) = o(x)$. In Types (3) or (6) $o((xy)z)$ is the least common multiple of $o(xy)$ and $o(z)$, and hence $o(xy) = 1$. Then $xy = 1$ and $x = y^{-1}$. If $o(y) = 2$, then $x = y$, which contradicts $x \neq y$; and if $o(y) = 3$, then $x = y^2$. In Type (5)

$$xyz = (xyz)x^{o(x)} = x(yzx)x^{o(x)-1} = x(xzy)x^{o(x)-1} = (x^2z)yx^{o(x)-1}.$$

If $o(x) = 2$, then $xyz = zyx$, contrary to (5). Therefore, no two different elements of order 2 commute. If $o(x) = 3$, then $(x^2y)z = x(xyz) = (x^3z)yx^2 = zyx^2 = z(x^2y)$. Since x and y commute, $o(x^2y)$ divides $o(x^2) = o(y) = 3$. It cannot be 3, for x^2y commutes with z and $o(z) = 2$. Therefore, $o(x^2y) = 1$, and hence $x^2y = 1$, so that $y = x^{-2} = x$, contrary to $x \neq y$. Thus, two different elements of order 3 can commute only if one of them is a square of the other.

If $xy \neq yx$ and $o(x) = o(y) \neq o(z)$, then X has no commuting elements and so it is of Types (4), (7), (8), or (9). Also, $xy \neq 1$, because $xy \neq yx$. Thus, $o(xy)$ is 2 or 3. Another fact we will use is that $(yx)^{o(xy)+1} = y(xy)^{o(xy)}x = yx$ implies $(yx)^{o(xy)} = 1$, and hence $o(xy) = o(yx)$.

If (4) holds, then z commutes with xy, and hence $o(xy) = o(z)$. If $o(z) = 2$, then $xy = z$, for no two different elements of order 2 commute. If $o(z) = 3$, then $xy \in \{z, z^2\}$, for if two different elements of order 3 commute, then each of them is the square of the other.

Let (7) hold. Call a the **middle** element of (7). Let $o(x) = o(y) = 2$. If x is the middle element, then

$$xzy = y^2xzy = y(yxz)y = y(zxy)y = yzxy^2 = yzx.$$

If y is the middle element, then

$$xzy = xzyx^2 = x(zyx)x = x(xyz)x = x^2yzx = yzx.$$

If z is middle, then

$$xyz = xyzx^2 = x(yzx)x = x(xzy)x = x^2zyx = zyx.$$

Each of the equalities $xzy = yzx$ and $xyz = zyx$ contradicts (7).

Now let $o(x) = o(y) = 3$ and $o(z) = 2$. If x is middle, then

$$xyz = z^2xyz = z(zxy)z = z(yxz)z = zyxz^2 = zyx.$$

The equality $xyz = zyx$ contradicts (7).

If y is middle, then

$$yxz = z^2yxz = z(zyx)z = z(xyz)z = zxyz^2 = zxy.$$

The equality $yxz = zxy$ contradicts (7). If z is middle, it follows from (7) that z commutes with xy. Then $xy = z$ and $o(xy) = 2$.

If (8) holds and $o(z) = 3$, then

$$xy = xyz^3 = (xyz)z^2 = (zyx)z^2 = z(yxz)z$$

$$= z(zxy)z = z^2(xyz) = z^2(zyx) = z^3(yx) = yx.$$

If $o(x) = 2$, then $o(x) = 3$ and

$$yz = yzx^3 = (yzx)x^2 = (xzy)x^2 = x(zyx)x$$

$$= x(xyz)x = x^2(yzx) = x^2(xzy) = x^3zy = zy.$$

Thus, y commutes either with x or with z, which contradicts (8). Therefore, Type (8) cannot hold.

It is easy to see that in Type (9) z commutes with xy or with yx. It follows from $xy \neq 1$ that $o(z) = o(xy)$ or $o(z) = o(yx)$. Since $o(xy) = o(yx)$, we obtain $o(xy) = o(z)$. As in Type (4) above, we conclude that $xy = z$ or $xy = z^2$.

Let $u, v, x, y \in H$ and $o(u) = o(v) = 2$, $o(x) = o(y) = 3$. Then either $uv = 1$, in which case $u = v$, or $u \neq v$, in which case $uv \neq vu$ and, as we have just seen, $uv \in \{x, x^2\}$. Analogously, $uv \in \{y, y^2\}$. Therefore, either $x = y$, or $x = y^2$. Thus, H contains exactly two elements of order 3, namely x and x^2. Suppose that u, v, w, z are four different elements of order 2. Then each of the products uz, vz, and wz has order 3, and hence equals x or x^2. It follows that at least two of these products are equal, and so at least two elements in $\{u, v, w\}$ are equal. Therefore, H cannot contain more than three elements of order 2. Thus, H contains 1, two elements of order 3, and at most three elements of order 2. Since all groups with less than six elements are abelian, $|H| = 6$. The only nonabelian group of order six is isomorphic to S_3. This completes the proof of Lemma 1. ∎

LEMMA 2: *If G is an $R(3,3)$-group and $G/Z(G)$ is a group of exponent 2, then G is an $R(3,2)$-group.*

Proof: Let G be a nonabelian $R(3,3)$-group with $G/Z(G)$ a group of exponent 2 (that is, $a^2 \in Z(G)$ for all $a \in G$). To prove that G is an $R(3,2)$-group consider a subset $A = \{a,b,c\}$ of G.

If A is of Type (5), then $acb = bca$ implies $b^2ac = acb^2 = (acb)b = (bca)b = b(cab)$. Cancelling b we obtain $bac = cab$, which contradicts (5).

If A is of Types (6) or (7), then $bac = cab$, and hence $acb^2 = b^2ac = b(bac) = b(cab) = (bca)b$. Cancelling b we obtain $acb = bca$, which contradicts both (6) and (7).

If A is of Type (9), then b commutes with ac. No two other elements of the set $C = \{a, b, ac\}$ commute, because no elements of A commute. Thus C belongs to one of the Types (3), (5), or (6). But Types (5) and (6) are impossible, and hence C is of Type (3). Thus $b \cdot a \cdot ac = ac \cdot a \cdot b$. Since $a^2 \in Z(G)$, we obtain $a^2bc = ba^2c = acab$. This yields $abc = cab$, which contradicts (9).

If A is of Type (8), consider C again. No two elements of C commute, as now $b(ac) \neq (ac)b$. Thus C belongs to one of the Types (4), (7), (8), or (9). But we have just seen that Types (7)–(9) are impossible, and hence C belongs to (4). Then $ac \cdot b \cdot a = a \cdot ac \cdot b$. Cancelling a we obtain $cba = acb$, contrary to (8) for A.

Thus, A can belong only to one of the Types (1)–(4). By Theorem 2 of [4], G is an $R(3,2)$-group. ∎

LEMMA 3: *If G is an $R(3,3)$-group and $G/Z(G)$ is a group of exponent 3, then $|G'| \leq 3$.*

Proof: Let G be a nonabelian $R(3,3)$-group and $G/Z(G)$ a group of exponent 3. First we prove that no subset $A = \{a,b,c\}$ of G can belong to Types (3), (8) and (9).

Let A be of Type (9). Consider $B = \{a, b, ca\}$. Only b and ca commute in this set. Thus, B belongs to the Types (3), (5), or (6). If (3) or (5) hold, then $ca \cdot a \cdot b = b \cdot a \cdot ca$. Thus, $ca^2b = (bac)a = (cba)a$. Cancelling c we obtain $a^2b = ba^2$ Thus, both a^2 and a^3 commute with b, and hence $ab = ba$, contrary to our assumption about A. If (6) holds, then $a \cdot b \cdot ca = b \cdot ca \cdot a$. Cancelling a we obtain $abc = bca$, which contradicts (9). Thus, Type (9) is impossible.

Let A be of Type (8). No elements of the set $C = \{a, b, ac\}$ commute, and hence C belongs to Types (4), (7), (8), or (9). As we have just seen, Type (9) is impossible. If C is of Type (4), then $ac \cdot b \cdot a = a \cdot ac \cdot b$. Cancelling a we obtain $cba = acb$, contrary to (8) for A. Let C be of Type (7). If a is the middle element, then $ac\cdot a\cdot b = b\cdot a\cdot ac$, and hence $(ab)(ac) = a(bac) = a(cab) = ba^2c$. Cancelling ac we obtain $ab = ba$, which is false. If b is the middle element, then $ac\cdot b\cdot a = a\cdot b\cdot ac$. Cancelling a we obtain $cba = bac$, which fails in A. If ac is the middle element, then $a\cdot ac\cdot b = b\cdot ac\cdot a$, so that $abca = a(bca) = a(acb) = a^2cb = baca$. Cancelling a we obtain $abc = bac$, which fails in A. Thus, C cannot be of Type (7). If C is of Type (8), then $ac \cdot b \cdot a = a \cdot b \cdot ac$. Cancelling a we obtain $cba = bac$, which fails in A. Thus, C cannot belong to any of the Types (1)–(9). This shows that A cannot belong to Type (8).

Now let $ab = ba$, and suppose that A belongs to Type (3). Then no two elements of the set $E = \{a, bc, c\}$ commute, and hence E is of Type (4) or (7). In the former case $bac^2 = abc^2 = a \cdot bc \cdot c = bc \cdot c \cdot a = bc^2a$. Cancelling b we obtain $ac^2 = c^2a$. Thus, a commutes both with c^2 and c^3, and hence $ac = ca$, contrary to our assumption about A. So E must be of Type (7). If a is the middle element of E, then $bc \cdot a \cdot c = c \cdot a \cdot bc$, and hence $bca = cab$, which fails in A. If bc is the middle element of E, then $cabc = a \cdot bc \cdot c = c \cdot bc \cdot a$. Cancelling c we obtain $abc = bca$. Since $ab = ba$, we obtain $bac = bca$, whence $ac = ca$, which contradicts our assumption about A. Thus, Type (3) is impossible.

To complete our proof of Lemma 3 we need another Lemma.

LEMMA 4: *Let G be an $R(3,3)$-group with $G/Z(G)$ a group of exponent 3. For every $a, b, c \in G$, if c commutes neither with a nor with b, then $[a,c] = [b,c]$ or $[a,c] = [b,c]^{-1}$.*

Proof: Let $ab \neq ba$. Then no two elements of the set $\{a, b, ab\}$ commute, and so this set is of Type (4) or (7). If (4) holds, then $b \cdot a \cdot ab = a \cdot ab \cdot b$. Cancelling b we obtain $a^2b = ba^2$, which, as we have seen, implies $ab = ba$, contrary to our assumption. Therefore, (7) holds. If a or b is the middle element, then either $b \cdot a \cdot ab = ab \cdot a \cdot b$ or $a \cdot b \cdot ab = ab \cdot b \cdot a$. In both cases, cancelling ab we obtain $ab = ba$, which is impossible. Therefore, ab is the middle element, and so $a \cdot ab \cdot b = b \cdot ab \cdot a$ and $b \cdot a \cdot ab = ab \cdot b \cdot a$.

We proved that G satisfies the identities $a^2b^2 = (ba)^2$ and $ab^2a = ba^2b$. It follows that $a^3b^3 = a(a^2b^2)b = a(baba)b = (ab)^3$, and so the mapping $f : G \to G$ defined by $f(a) = a^3$ for all $a \in G$ is an endomorphism of G. Since f maps G into $Z(G)$, we see that $G' \subset \mathrm{Ker} f$, and hence $[a,b]^3 = 1$ for all $a, b \in G$. Also,

$(ab)^3 = a^3b^3 = b^3a^3 = (ba)^3$. Now we have

$$[a,b] = (ba)^{-2}(ba)(ab) = (ba)^{-2}(ba^2b) = (ba)^{-2}(ab^2a) = (ba)^{-3}b(a^2b^2)a$$

$$= (ba)^{-3}b(ba)^2a = b(ba)^{-3}(ba)^2a = b(ba)^{-1}a = [b^{-1},a].$$

Thus $[a,b] = [b,a]^{-1} = [a^{-1},b]^{-1} = [b,a^{-1}]$.

Again, consider $A = \{a,b,c\}$, in which c commutes neither with a nor b. Let $ab = ba$. Then $ab^{-1} = b^{-1}a$. Thus A belongs to one of Type (5) or (6), and hence $acb = bca$ or $abc = cab$. In the former case,

$$[a,c][c,b] = a^{-1}c^{-1}acc^{-1}b^{-1}cb = a^{-1}c^{-1}ab^{-1}cb$$

$$= a^{-1}c^{-1}b^{-1}acb = (bca)^{-1}(acb) = 1,$$

and hence $[a,c] = [c,b]^{-1} = [b,c]$. If (6) holds, we obtain

$$(ca)(ac)^2(cb) = (ca)c^2a^2cb = (cac)(ca^2c)b = (cac)(ac^2a)b = (ca)^2c(cab)$$
$$= (ca)^2c(abc) = (ca)^3bc = (bc)(ca)^3 = (bc)(ac)^3,$$

and hence

$$cac^{-1}a^{-1}cb = (ca)(ac)^{-1}(cb) = (ca)(ac)^2(ac)^{-3}(cb) = (ca)(ac)^2(cb)(ac)^{-3} = bc.$$

Therefore, $[c^{-1},a^{-1}] = cac^{-1}a^{-1} = bcb^{-1}c^{-1} = [b^{-1},c^{-1}]$. This equality follows from $ab = ba$ and $abc = cab$. If we replace a, b, and c by a^{-1}, b^{-1}, and c^{-1}, respectively, we obtain the equality $[c,a] = [b,c]$. Therefore, $[a,c] = [c,a]^{-1} = [b,c]^{-1}$.

Now suppose that $ab \neq ba$. Then A satisfies (4) or (7). Let (4) hold. Then $abc = cab$, and

$$[a,c][c,b^{-1}] = a^{-1}c^{-1}ac \cdot c^{-1}bcb^{-1} = b(b^{-1}a^{-1}c^{-1}abc)b^{-1}$$

$$= b(cab)^{-1}(abc)b^{-1} = 1.$$

We obtain $[a,c] = [c,b^{-1}]^{-1} = [b^{-1},c] = [c,b] = [b,c]^{-1}$.

Now let A satisfy (7). Suppose that a is the middle element. Then a and bc are the only commuting elements of the set $E = \{a, bc, c\}$, and so E is of Type (5) or (6). If (6) holds, then $c \cdot abc = abc \cdot c$, and hence $cab = abc$, which contradicts (7). If (5) holds, we have

$$(cb)(ac) = (cba)c = (acb)c = a \cdot c \cdot bc = bc \cdot c \cdot a = (bc)(ca).$$

Thus $ac = (cb)^{-1}(bc)(ca)$, so that $[a^{-1}, c^{-1}] = (ac)(ca)^{-1} = (cb)^{-1}(bc) = [b,c]$. Therefore,

$$[a,c] = [c,a]^{-1} = [c,a^{-1}] = [a^{-1},c]^{-1} = [a^{-1},c^{-1}] = [b,c].$$

Type (7) is invariant under the transposition of b and c. It follows that $[a,c] = [b,c]$ holds together with $[a,b] = [c,b]$, and hence $[a,b] = [c,b] = [c,a]$. If we apply a cyclic permutation (a,b,c) to (7), b becomes the middle element and we obtain the equalities $[b,c] = [a,c] = [a,b]$. Applying a cyclic permutation (a,c,b) to (7), we make c the middle element, and obtain the equalities $[c,a] = [b,a] = [b,c]$, which imply $[a,c] = [b,c]$. Thus, $[a,c] = [b,c]$ for any middle element of A. This proves Lemma 4. ∎

To complete the proof of Lemma 3 assume that $a,b,c,d \in G$ and consider $[a,b]$ and $[c,d]$. Suppose that these commutators differ from 1. There exists $e \in G$ which commutes with neither b nor c. Indeed, if there is no such e, then $C(b) \cup C(c) = G$, and hence $C(b) = G$ or $C(c) = G$, that is, $b \in Z(G)$ or $c \in Z(G)$. Then $[a,b] = 1$ or $[c,d] = 1$, contrary to our assumption.

Since a and e do not commute with b, obtain, by Lemma 4, that $[a,b] = [e,b]$ or $[a,b] = [e,b]^{-1}$. Since e does not commute with b and c, we obtain, again by Lemma 4, $[e,b] = [e,c]$ or $[e,b] = [e,c]^{-1}$. Now, c does not commute with e and d. Thus, by Lemma 4, $[e,c] = [d,c]$ or $[e,c] = [d,c]^{-1}$. Combining these possibilities, we see that $[a,b] = [c,d]$ or $[a,b] = [c,d]^{-1}$. Thus, $|G'| \leq 3$ (in fact, $|G'| = 3$). This proves Lemma 3. ∎

LEMMA 5: *Let G be a group such that $G/Z(G) \cong S_3$. Then $|G'| = 3, G$ is an $R(3,3)$-group and no three-element subset of G belongs to the Types (4) and (7).*

Proof: Let $f : G \to S_3$ be a homomorphism of G onto the group S_3 of all permutations of $\{1,2,3\}$ and let $Z = Z(G)$ be the kernel of f. Then G is a disjoint union of cosets $Z, G_{12}, G_{13}, G_{23}, G_{123}$, and G_{132} of Z. Here $G_{ij} = f^{-1}((i,j))$ and $G_{ijk} = f^{-1}((i,j,k))$. Choose $p \in G_{12}$ and $q \in G_{13}$. Then $pq \in G_{123}, qp \in G_{132}, pqp, qpq \in G_{23}, (pq)^2 \in G_{132}, (qp)^2 \in G_{123}$, and $p^2, q^2 \in Z$.

Consider a subset $A = \{a, b, c\}$ of G. If more than one pair of its elements commute, then A belongs to Type (1) or (2). Suppose that only a and b commute in A. Then $f(a)$ and $f(b)$ commute in S_3, and hence either $f(a) = f(b)$ or $f(a) \in \{(1,2,3),(1,3,2)\}$ and $f(a^2) = f(b)$.

Consider all possible cases when $ab = ba$. Let $f(a) = f(b)$. One possibility is that $a, b \in G_{ij}$. Without loss of generality we may assume that $a, b \in G_{12}$. Then $a = pu$ and $b = pv$ for certain $u, v \in Z$. Since c commutes neither with a nor b, we see that $c \notin Z \cup G_{12}$. Without loss of generality we may suppose that either $c \in G_{13}$ or $c \in G_{123}$. In the former case $c = qw$ for some $w \in Z$. Then

$$abc = (pu)(pv)(qw) = p^2quvw = q(p^2uvw) \in G_{13},$$

$$acb = (pu)(qw)(pv) = (pqp)(uvw) \in G_{123},$$

$$bca = (pv)(qw)(pu) = (pqp)(uvw) = acb,$$

$$cba = cab = (qw)(pu)(pv) = q(p^2uvw) = abc = bac.$$

Thus, A is of Type (3). If $c \in G_{123}$, then $c = pqw$ for some $w \in Z$. In this case

$$bac = abc = cba = cab = pq(p^2uvw) \in G_{123},$$

$$acb = bca = qp(p^2uvw) \in G_{132},$$

and hence A is of Type (3).

Now assume that $a, b \in G_{ijk}$. Again, without loss of generality we can assume that $a, b \in G_{123}$. Then $a = pqu$ and $b = pqv$ for some $u, v \in Z$. Now, c does not commute with a and b, and hence $c \notin Z \cup G_{123} \cup G_{132}$. It follows that $c \in G_{ij}$. Without loss of generality assume that $c \in G_{12}$. Then $c = pw$ for some $w \in Z$. Computing all elements in $A^{[3]}$, we easily obtain:

$$bac = abc = pqpqpuvw \in G_{13}, \qquad acb = bca = p(p^2q^2uvw) \in G_{12},$$

$$\text{and} \qquad cba = cab = qpq(p^2uvw) \in G_{23}.$$

It follows that A belongs to Type (5).

Next we suppose that $ab = ba$, but $f(a) \neq f(b)$. Without loss of generality, $a \in G_{123}$ and $b \in G_{132}$. Thus, $a = pqu$ and $b = qpv$ for some $u, v \in Z$. Since

c does not commute with a and b, $c \in G_{ij}$. Without loss of generality we can assume that $c \in G_{12}$. Then

$$abc = cab = p(p^2q^2uvw) \in G_{12}, \qquad acb = pqpqpuvw \in G_{13},$$

$$\text{and} \qquad bca = qpq(p^2uvw) \in G_{23}.$$

Therefore, A is of Type (6).

Now suppose that no two elements of A commute. First consider the case when $f(A)$ does not contain a 3-cycle. Without loss of generality, we may assume that $a \in G_{12}$, $b \in G_{13}$, and $c \in G_{23}$. Therefore, $a = pu$, $b = qv$, and $c = pqpw$ for some $u, v, w \in Z$. Computing $A^{[3]}$ we obtain

$$abc = cba = pqpqpuvw \in G_{13}, \qquad acb = bca = qpq(p^2uvw) \in G_{23},$$

$$\text{and} \qquad bac = cab = p(p^2q^2uvw) \in G_{12}.$$

It follows that A is of Type (8).

Now let $f(A)$ contain a 3-cycle. As no two elements of A commute, assume without loss of generality that $b \in G_{123}$, $c \in G_{12}$ and $a \in G_{13}$. Then $a = qu$, $b = pqv$, and $c = pw$ for some $u, v, w \in Z$. Computing $A^{[3]}$ we obtain

$$abc = qpqpuvw \in G_{123}, \qquad bca = cab = pqpquvw \in G_{132},$$

$$acb = bac = cba = p^2q^2uvw \in Z,$$

and hence A is of Type (9).

We proved that A always belongs to one of the Types (1)–(3), (5)–(6), (8)–(9). Therefore, G is an $R(3,3)$-group. It follows that $a^2 \in Z$ or $a^3 \in Z$ for every $a \in G$.

To prove that $|G'| = 3$, describe $[x, y]$ for all $x, y \in G$. Clearly,

$$x \in \{u, pu, qu, pqu, pqpu, qpu\} \quad \text{and} \quad y \in \{v, pv, qv, pqv, pqpv, qpv\}$$

for some $u, v \in Z$. Since $[au, bv] = [a, b]$ for all $a, b \in G$ and $u, v \in Z$, we can assume that $x, y \in \{1, p, q, pq, pqp, qp\}$. Suppose that $[x, y] \neq 1$. Then $x \neq y$ and neither x nor y is 1. Note also the commutator identities $[p, q] = [q, p]^{-1}$ and $[p, pq] = p^{-1}q^{-1}p^{-1}ppq = p^{-1}q^{-1}pq = [p, q]$, and that $p^2, q^2 \in Z$. Now,

$$[p, pqp] = p^{-1}p^{-1}q^{-1}p^{-1}ppqp = p^{-2}p^2q^{-1}p^{-1}qp = q^{-1}p^{-1}qp = [q, p],$$

$$[p,qp]=p^{-2}q^{-1}pqp=q^{-1}p^{-2}pqp=[q,p],$$

$$[q,pq]=q^{-2}p^{-1}qpq=p^{-1}q^{-2}qpq=[p,q],$$

$$[q,pqp]=q^{-1}p^{-1}q^{-1}p^{-1}qpqp=q^{-1}p^{-1}q^{-1}p^{-1}q^2q^{-1}p^2p^{-1}qp$$

$$=q^{-1}p^{-1}q^{-1}q^2p^{-1}p^2q^{-1}p^{-1}qp=q^{-1}p^{-1}qpq^{-1}p^{-1}qp=[q,p]^2,$$

$$[q,qp]=q^{-1}p^{-1}q^{-1}qqp=[q,p],$$

$$[pq,pqp]=q^{-1}p^{-1}p^{-1}q^{-1}p^{-1}pqpqp=q^{-1}q^{-1}qpp^{-2}qp=[q,p],$$

$$[pq,qp]=q^{-1}p^{-1}p^{-1}q^{-1}pqqp=q^{-2}q^2p^{-2}p^2=1,$$

and

$$[pqp,qp]=p^{-1}q^{-1}p^{-1}p^{-1}q^{-1}pqpqp=p^{-1}q^{-1}q^{-1}pqp^{-2}pqp$$

$$=p^{-1}pq^{-2}qp^{-1}qp=q^{-1}p^{-1}qp=[q,p].$$

Thus, every commutator in G equals 1, $[q,p],[q,p]^{-1}$, or $[q,p]^2$. It remains to prove that $[q,p]^3=1$. Here we use the fact that $q^{-1}p^{-1}qpq^{-1}p^{-1}\in Z$. We see that

$$[q,p]^3=(q^{-1}p^{-1}qpq^{-1}p^{-1})qpq^{-1}p^{-1}qp=q(q^{-1}p^{-1}qpq^{-1}p^{-1})pq^{-1}p^{-1}qp$$

$$=p^{-1}qpq^{-1}q^{-1}p^{-1}qp=p^{-1}qpp^{-1}q^{-2}qp=p^{-1}qq^{-1}p=1.$$

Thus, $|G'|=3$, because $[q,p]\in G_{123}$, and hence $[q,p]\neq 1$. This completes the proof of Lemma 5. ∎

It follows from Lemmas 1, 2, 3, and 5 that if G is an $R(3,3)$-group, then $|G'|\leq 3$. This proves our Theorem. ∎

Examples: As examples of the four types of $R(3,3)$-groups described in Lemma 1 consider: (1) any abelian group; (2) any nonabelian group of order 8 (the quaternion group or D_4, the dihedral group of order 8); (3) the group of order 27 generated by elements x and y subject to defining relations $a^9=b^3=1$ and $ba=a^4b$; (4) S_6. ∎

In conclusion, we suggest some unsolved problems.

Problems: (1) The groups $R(3,n)$ have been described for $n = 2$ in [4] and for $n = 3$ here. Now the most natural problem is that of finding the structure of groups $R(3,4)$ (this problem has been discussed in our introduction). As we have already mentioned, the problem of describing the structure of $R(3,5)$ groups (that is, of Q_3-groups) is open.

(2) The next natural step would be studying groups $R(4,n)$ for various n, $4 \leq n \leq 23$. All elements of $A^{[m]}$ belong to the same coset of G' in G because G/G' is an abelian group. It follows that $|A^{[m]}| \leq |G'|$. Thus, as corollaries to the result of this paper, $R(4,2) = R(3,2)$ and $R(4,3) = R(3,3)$. A classification of four-element subsets analogous to that for three-element subsets obtained in [4] might be helpful in solving this and similar problems.

(3) We know that $R(3,2)$ are groups G such that $|G'| \leq 2$, while $R(3,3)$-groups are characterized by $|G'| \leq 3$. For $R(3,4)$ an analogous conjecture fails, because the infinite dihedral groups belongs to $R(3,4)$, while its commutator subgroup is infinite. Given m, find $s_0 = s_0(m)$ such that, for every $s \leq s_0$, a group G belongs to $R(m,s)$ if and only if $|G'| \leq s$.

(4) An ordered n-tuple $(a_1, a_2, \ldots, a_n)$ of elements of a semigroup S is called **rewritable** if there exists a nonidentity permutation τ of $\{1,2,\ldots,n\}$ such that $a_1 a_2 \cdots a_n = a_{\tau(1)} a_{\tau(2)} \cdots a_{\tau(n)}$. A semigroup S is called **totally n-rewritable** if every n-tuple of its elements is rewritable (see [4]). Let P_n denote the class of all n-rewritable groups (or semigroups).

It is easy to see that $P_n \subset R(n, n!/2)$. It was proved in [4] that $P_3 = R(3,2)$, and hence there exists a number $s \leq m!/2$ such that $P_m \subset R(m,s)$. Given m, what is the minimal s with this property?

(5) An element a of a group G is called a [3]-n-element if, for any $b, c \in G$, $|\{a,b,c\}^{[3]}| \leq n$ (see [4]). It was proved in [4] that [3]-2-elements of any group form a characteristic subgroup. Is this true for [3]-3-elements? What is the maximal n for which $[m]$-n-elements form a subgroup? (This subgroup is always characteristic.) For an analogous result see [3].

Call $a \in G$ a P_3-element if, for any $b, c \in G$, the ordered triples (a,b,c), (b,a,c), and (b,c,a) are rewritable. Is it true that the set of all P_3-elements of any group forms a characteristic subgroup? ∎

Problems (3) and (4) were suggested by Professor D. J. S. Robinson.

References

1. Z. Arad and M. Herzog (eds.), *Products of Conjugacy Classes in Groups*, Lecture Notes in Mathematics **1112**, Springer-Verlag, Berlin, 1985.
2. R. D. Blyth and D. J. S. Robinson, *Recent progress on rewritability in groups*, in *Group Theory*, Proceedings of the 1987 Singapore Conference, de Gruyter, Berlin, 1988.
3. L. V. Brailovsky, G. A. Freiman and M. Herzog, *Special elements in groups*, in *Group Theory*, Proceedings of the 2nd International Conference in Bressanone, Italy, 1989. Supplement to Rendiconti di Circolo Matematico di Palerma, II Ser. **23** (1990), 33–42.
4. G. A. Freiman and B. M. Schein, *Interconnections between two directions in the theory of groups: Structure theory of set addition and rewritability*, Proc. Am. Math. Soc. **113** (1991), 899–910.