CLT and non-CLT groups of order p^2q^2

by

S. Baskaran (Madras)

Abstract. A characterization of groups of order p^2q^2, p, q, primes, which have subgroups of all possible orders is given in this paper.

1. Introduction. In this paper, we consider only finite groups. A group G is said to be CLT if it possesses subgroups of every possible order and non-CLT otherwise. CLT groups are necessarily soluble (see [3]). The question arises as to which soluble groups are CLT. As a first step one is naturally tempted to consider groups G of order $|G| = p^\alpha q^\beta$, p, q distinct primes, $\alpha, \beta \geqslant 1$, which are necessarily soluble, and find out which of these groups are CLT. This general question does not seem to be amenable, as far as the author can see, of being dealt with at one stroke. This surmise sprouts out of the fact that the author's treatment of the case $|G| = p^2q^2$ in the present paper differs considerably from the case $|G| = pq^2$ dealt with earlier in [1]. To cite an explicit instance, every group of order $2q^2$, q a prime, is CLT (see e.g. [1]) whereas a group of order $4q^2$ may be CLT or non-CLT.

2. Notations and theorem. In the sequel we employ the following notations:

Z_m = the cyclic group of order m,
V_4 = the Klein-four group $\equiv \{e, u, v, uv\}$,
A_4 = the alternating group on four symbols,
S_3 = the symmetric group on three symbols,
$\operatorname{Aut} G$ = the group of automorphisms of G,
$A \otimes_s B$ = a semi-direct product of A with B, $\otimes_s$ denoting the operation in this semi-direct product,
$N_G(K)$ = the normalizer of the subgroup K of G in G,
$[G:K]$ = the index of the subgroup K of G in G,
$\langle x \rangle$ = the subgroup generated by x.

When dealing with the direct product of two copies of Z_q we write the two copies as A, B where

$$A = \{e_1, a, a^2, \ldots, a^{q-1}\}, \quad B = \{e_2, b, b^2, \ldots, b^{q-1}\}.$$

A typical automorphism of $A\times B$ will be denoted by σ; σ is determined by x_1, x_2, y_1, y_2 where $\sigma(e_1, b) = (a^{x_1}, b^{x_2})$, $\sigma(a, e_2) = (a^{y_1}, b^{y_2})$. We denote a generator of Z_4 by g and its identity by e. We prove here

THEOREM. *Let G be a non-abelian group of order p^2q^2, p, q primes, $p<q$. Then for G to be non-CLT it is necessary and sufficient that one of the following conditions holds.*

I. *p is odd and p divides $q+1$.*

II. *$p = 2$, $q \equiv 3 (\mathrm{mod}\, 4)$, $G \cong (Z_q\times Z_q)\otimes_s Z_4$ and the semi-direct product is induced by a monomorphism.*

III. *$G \cong V_4\otimes_s Z_9$ or $V_4\otimes_s(Z_3\times Z_3)$.*

The proof consists of a number of steps and is given in Section 3.

It is not known whether Theorem is independent of Chunikhin's [2] results on the existence of subgroups or is deducible from them.

3. Proof of Theorem.

Step (1). I *is sufficient*: Since $p<q$ and p and q are not adjacent primes, G contains a normal Sylow q-subgroup S_q. Let, if possible, G contain a subgroup M of order p^2q. Then M contains a Sylow p-subgroup S_p of G and

$$\begin{aligned} q \equiv -1 (\mathrm{mod}\, p) &\Rightarrow q \not\equiv 1 (\mathrm{mod}\, p) \text{ as } p \text{ is odd}\\ &\Rightarrow S_p \text{ is normal in } M\\ &\Rightarrow [G:N_G(S_p)] = q \text{ or } 1\\ &\Rightarrow \text{Number of distinct conjugates of } S_p \text{ in } G = q \text{ or } 1\\ &\Rightarrow S_p \text{ is normal in } G \text{ as } q \not\equiv 1 (\mathrm{mod}\, p)\\ &\Rightarrow G \cong S_p\times S_q \end{aligned}$$

and so G is abelian, a contradiction. This completes Step (1).

Step (2). *For odd prime p*, I *is necessary*: As in Step (1), G contains a normal Sylow q-subgroup S_q and the group product of S_q with a subgroup of order p gives a subgroup of order pq^2. As G is non-CLT, G contains no subgroup of order p^2q as, otherwise, the intersection of a subgroup of order pq^2 and a subgroup of order p^2q would be a subgroup of order pq making G CLT. Consequently G contains no normal subgroup of order q. Further this shows that S_q is non-cyclic and so S_q and hence G contains exactly $q+1$ subgroups of order q. As every subgroup of order q is normal in S_q, it is clear that $[G:N_G(H)]$ is divisible by p for every subgroup H of order q and so $q+1$ should be divisible by p, a divisor of the greatest common divisor of the number of distinct conjugates in G of various subgroups of order q which equalize the indices of the normalizers of these subgroups of order q in G. Step (2) is complete.

Step (3). II *is sufficient*: Let G be defined *via* the monomorphism ψ and $\psi(g) = \sigma \in \mathrm{Aut}(Z_q\times Z_q)$, g a generator of Z_4. Then σ is of order 4. Since $q \equiv 3 (\mathrm{mod}\, 4)$, σ is determined by x_1, x_2, y_1, y_2 where $x_1 \not\equiv 0 (\mathrm{mod}\, q)$, $x_2 \equiv -y_1 (\mathrm{mod}\, q)$ and $x_1y_2 \equiv -1-y_1^2 (\mathrm{mod}\, q)$ (cf. Appendix (III)). Let, if possible, G contain a subgroup M of order $4q$. Since q is odd it is clear that there is no non-trivial semi-direct product of Z_4 with Z_q and thus M cannot have a Sylow 2-subgroup normal in it unless M is abelian. In any case, M contains a subgroup H of order q such that H is normal in M. By II G contains a unique Sylow q-subgroup S_q and H is normal in S_q. It follows that H is normal in G. As S_q and hence G contains precisely $q+1$ subgroups of order q, H must be either the subgroup $N = \langle (e_1, b, e)\rangle$ or the subgroup $H_k = \langle (a, b^k, e)\rangle$ for some integer k. Since $x_1 \not\equiv 0 (\mathrm{mod}\, q)$, N is not normal in G and so $H \neq N$. Thus H_k is normal in G which implies that the element $(e_1, e_2, g) \in N_G(H_k)$. Hence

$$\begin{aligned} &(e_1, e_2, g)\otimes_s(a, b^k, e)\otimes_s(e_1, e_2, g)^{-1} \in H_k\\ \Rightarrow &((e_1, e_2)\sigma(a, b^k), g)\otimes_s(e_1, e_2, g^{-1}) \in H_k\\ \Rightarrow &(a^{y_1+x_1k}, b^{y_2+x_2k}, e) \in H_k\\ \Rightarrow &y_2+x_2k \equiv k(y_1+x_1k) (\mathrm{mod}\, q)\\ \Rightarrow &x_1^2k^2+x_1(y_1-x_2)k-x_1y_2 \equiv 0 (\mathrm{mod}\, q)\\ \Rightarrow &x_1^2k^2+2x_1y_1k-(-1-y_1^2) \equiv 0 (\mathrm{mod}\, q)\\ \Rightarrow &(x_1k+y_1)^2 \equiv -1 (\mathrm{mod}\, q). \end{aligned}$$

Thus the residue class containing (x_1k+y_1) is an element of order 4 in the multiplicative group of non-zero residue classes modulo q and, by Lagrange's Theorem, 4 must divide $q-1$, a contradiction to II.

Step (4). III *is sufficient*: Let, if possible G contain a subgroup M of order 18. Then a Sylow 3-subgroup of G contained in M is normal in M and hence normal in G since M is maximal and normal in G, a contradiction.

Step (5). *Necessity of* II *or* III *for* $p = 2$:

(5.1) *If G contains a normal Sylow q-subgroup S_q (which will be the case when $q>3$) Sylow 2-subgroups of G should be cyclic*: By a reasoning similar to what is contained in Step (2), we can show that G contains no subgroup of order $4q$ and $S_q \cong Z_q\times Z_q \equiv A\times B$, say. Also G contains no normal Sylow 2-subgroup as G is non-abelian. Thus, if Sylow 2-subgroups of G are not cyclic, then properly $G \cong (A\times B)\otimes_s V_4$. The homomorphism ψ of V_4 into $\mathrm{Aut}(A\times B)$ defining G must map at least two of the three elements u, v, uv to automorphisms of order 2. Let them be u and v and let $\psi(u) = \sigma$.

Since none of the Sylow subgroups of G are cyclic, it is clear that the element (e_1, b, u) is of order 2 or $2q$. Let, if possible, (e_1, b, u) have order $2q$. If $M = \langle (e_1, b, u)\rangle$ then $K = \{(e_1, e_2, e), (e_1, b, u)^q\}$ is a subgroup of order 2 and K is normal in M. Also K is normal in a Sylow 2-subgroup of G in which it is contained. It follows that $N_G(K)$ is of index q or 1. In the former case, G contains a subgroup of order $4q$ namely $N_G(K)$, a contradiction. In the latter case, G/K is a group of order $2q^2$ and so contains a subgroup of order $2q$ (see § 1). In this case also, G contains a subgroup of order $4q$, a contradiction.

The element (e_1, b, u) must therefore be of order 2 which forces $x_1 \equiv 0 \pmod{q}$. This in turn implies that each of (e_1, e_2, u), (e_1, e_2, v) (by a similar reasoning) normalizes $N = \langle(e_1, b, e)\rangle$. It follows that $N_G(N)$ contains a Sylow 2-subgroup of G. As N is normal in S_q also, it follows that N is normal in G and the group product of N with a subgroup of order 4 gives a subgroup of order $4q$, a contradiction. Hence (5.1).

(5.2) *Under* (5.1), *the automorphism* σ *which is the image of a generator* g *of* Z_4 *under the homomorphism* ψ *defining the semi-direct product, cannot be of order* 2 *and so* ψ *is a monomorphism*: Let, if possible σ be of order 2. Then we have

(i) $$y_1 x_1 + x_1 x_2 \equiv 0 \pmod{q},$$

(ii) $$x_1 y_2 + x_2^2 \equiv 1 \pmod{q}.$$

Also the element (e_1, b, g) has order a multiple of 4 and it can be supposed to have order 4. Then we have

(iii) $$x_1 + y_1[x_1 y_1 + x_1(1+x_2)] + x_1[x_1 y_2 + x_2(1+x_2)] \equiv 0 \pmod{q},$$

(iv) $$1 + x_2 + y_2[x_1 y_1 + x_1(1+x_2)] + x_2[x_1 y_2 + x_2(1+x_2)] \equiv 0 \pmod{q}.$$

Using (i) and (ii) in (iii) we have

$$x_1 + x_1 y_1 + x_1(1+x_2) \equiv 0 \pmod{q},$$

i.e.

$$2x_1 + (x_1 y_1 + x_1 x_2) \equiv 0 \pmod{q},$$

i.e.

$$2x_1 \equiv 0 \pmod{q} \quad \text{or} \quad x_1 \equiv 0 \pmod{q},$$

finally by (i). Hence (e_1, e_2, g) normalizes $N = \langle(e_1, b, e)\rangle$. As (e_1, e_2, g) is of order 4 and N is normal in S_q, N is normal in G and this makes G CLT, a contradiction.

(5.3) $q \not\equiv 1 \pmod 4$ *and so* $q \equiv 3 \pmod 4$: By Step (5.2), σ^2 is of order 2 and so we have either of the following two sets of conditions (cf. Appendix (II)).

(v)
$$y_1^2 + x_1 y_2 \equiv x_1 y_2 + x_2^2 \equiv -1 \pmod{q},$$
$$(y_1 + x_2) y_2 \equiv (y_1 + x_2) x_1 \equiv 0 \pmod{q}.$$

(vi)
$$y_1^2 + 2x_1 y_2 + x_2^2 \equiv 0 \pmod{q},$$
$$x_1 y_2 (y_1 + x_2)^2 \equiv 1 - (y_1^2 + x_1 y_2)^2 \pmod{q}.$$

If $q \equiv 1 \pmod 4$, these relations help us to conclude that the congruence equation

$$x_1 k^2 + (y_1 - x_2) k - y_2 \equiv 0 \pmod{q}$$

has an integral solution (cf. Appendix (IV)) which implies that the element (e_1, e_2, g) normalizes $H_k = \langle(a, b^k, e)\rangle$ for some integer k. It follows that G contains H_k as a normal subgroup. But then G is CLT, a contradiction, proving (5.3).

The next stage is in the form of an interesting lemma which can be proved in several ways. The proof given here is, however, elementary.

(5.4) LEMMA. *Any group of order* 36 *has a normal Sylow subgroup.*

Proof. Let G be a group of order 36 and suppose G has no normal subgroup of order 9 or 4. Then G has no subgroup of order 18. If P and Q are two subgroups of order 9 then $P \cap Q = H$ is a subgroup of order 3 which is normal in both P and Q and hence normal in G. G/H then has a normal subgroup of order 4 and G has a normal subgroup M of order 12 containing H. Let S be a subgroup of order 4 contained in M. Since $N_G(S) \neq S$ or M (as, otherwise, M would be self-normalizing) and since $N_G(S) \neq G$ by supposition, it follows that $N_G(S)$ is a subgroup R of order 12. Obviously R will not be normal in G. Now $SH = M$ and since R contains S and $R \neq M$, R cannot contain H. Hence $R \cap H = \{e\}$ and $RH = G$. It follows that $G \cong H \otimes_s R$ properly. Hence R cannot be isomorphic to A_4 and so R contains a subgroup K of order 6 where $K \cap H = \{e\}$. Then HK is a subgroup of order 18 a contradiction. Hence the lemma.

(5.5) *For* $p = 2$, II *or* III *holds*: From (5.1), (5.2), (5.3) and Lemma in (5.4) we conclude that either II holds or G is a non-CLT group of order 36 with a normal Sylow 2-subgroup. In the latter case, it is clear that the Sylow 2-subgroup of G cannot be cyclic and thus III holds.

4. Concluding remarks. We observe that each of the classes of groups satisfying I, II or III is non-vacuous. For, when I holds $\mathrm{Aut}(Z_q \times Z_q)$ has order $(q^2-1)(q^2-q)$ divisible by p and so has an element of order p. If $p = 2$, we choose $x_1 \not\equiv 0 \pmod{q}$, y_1 arbitrary, $x_2 \equiv -y_1 \pmod{q}$ and y_2 with $x_1 y_2 \equiv -1 - y_1^2 \pmod{q}$ to determine a $\sigma \in \mathrm{Aut}(Z_q \times Z_q)$ of order 4. This determines the non-trivial semi-direct product $(Z_q \times Z_q) \otimes_s Z_4$ when $q \equiv 3 \pmod 4$ as in II. The class of groups satisfying III is non-vacuous since $\mathrm{Aut}\, V_4 \cong S_3$.

As regards the class of CLT groups we have an interesting phenomenon where *there exist two non*-CLT *groups whose direct product is* CLT. Groups G_1, G_2 of order 36, respectively satisfying II and III, serve this purpose. We note that G_1 has a subgroup of index 2 and G_2 has a subgroup of index 3.

Appendix. In this appendix we reduce the study of $\mathrm{Aut}(Z_q \times Z_q)$ to the study of the linear group $L_2(Z_q)$ where Z_q is now the prime field of characteristic q. This reduction becomes possible because of the association $\sigma \leftrightarrow \begin{pmatrix} y_1 & y_2 \\ x_1 & x_2 \end{pmatrix}$ where σ is determined by x_1, x_2, y_1, y_2, integers modulo q.

We have the following results.

(I) *If* $E = \begin{pmatrix} y_1 & y_2 \\ x_1 & x_2 \end{pmatrix}$ *has order* 2 *then one of the following two sets of conditions holds.*

(1) $$y_1 = x_2 = -1 \quad \text{and} \quad x_1 = y_2 = 0,$$

(2) $$x_2 = -y_1 \quad \text{and} \quad x_1 y_2 = 1 - y_1^2.$$

Proof. Since $E^2 = I$ we have

(i) $y_1^2 + x_1 y_2 = 1$,

(ii) $(y_1 + x_2)x_1 = 0$,

(iii) $(y_1 + x_2)y_2 = 0$,

(iv) $x_2^2 + x_1 y_2 = 1$.

From (ii) and (iii) we have either $x_2 = -y_1$ or $x_1 = y_2 = 0$.

From (i) and (iv) we have $x_2^2 = y_1^2$ and so $x_2 = \pm y_1$. If $x_2 = -y_1$ then (2) holds by (i). If $x_2 = y_1$ then $x_1 = y_2 = 0$ and so (1) is seen to hold by using (i) and (iv) and noting that $E \neq I$, the unit matrix.

(II) *If* $E = \begin{pmatrix} y_1 & y_2 \\ x_1 & x_2 \end{pmatrix}$ *has order* 4 *then one of the following two sets of conditions holds.*

(α) $$y_1^2 + x_1 y_2 = x_2^2 + x_1 y_2 = -1, \quad (y_1 + x_2)x_1 = (y_1 + x_2)y_2 = 0.$$

(β) $$y_1^2 + 2x_1 y_2 + x_2^2 = 0, \quad x_1 y_2 (y_1 + x_2)^2 = 1 - (y_1^2 + x_1 y_2)^2.$$

These conditions are got at once by applying (I) for the matrix E^2 which has order 2.

(III) *If* $E = \begin{pmatrix} y_1 & y_2 \\ x_1 & x_2 \end{pmatrix}$ *has order* 4 *and* $q \equiv 3 (\mathrm{mod}\, 4)$ *then* $x_1 \neq 0$, $x_2 = -y_1$ *and* $x_1 y_2 = -1 - y_1^2$.

Proof. Since E has order 4, (α) or (β) in (II) holds. Let, if possible, (β) hold. Then $2x_1 y_2 = -(y_1^2 + x_2^2)$ and

$$\begin{aligned} & x_1 y_2 (y_1 + x_2)^2 = 1 - (y_1^2 + x_1 y_2)^2 \\ \Rightarrow\ & 4x_1 y_2 (y_1 + x_2)^2 = 4 - (2y_1^2 + 2x_1 y_2)^2 \\ \Rightarrow\ & -2(y_1^2 + x_2^2)(y_1 + x_2)^2 = 4 - (y_1^2 - x_2^2)^2 \\ \Rightarrow\ & (y_1 + x_2)^2 [2(y_1^2 + x_2^2) - (y_1 - x_2)^2] = -4 \\ \Rightarrow\ & (y_1 + x_2)^4 = -4, \end{aligned}$$

which is impossible when $q \equiv 3 (\mathrm{mod}\, 4)$. Hence (α) holds and we have the required condition arguing as in (I) and noting that $x_1 = 0$ or $x_1 = y_2 = 0 \Rightarrow y_1^2 = -1$, which is impossible when $q \equiv 3 (\mathrm{mod}\, 4)$.

(IV) *If* $E = \begin{pmatrix} y_1 & y_2 \\ x_1 & x_2 \end{pmatrix}$ *has order* 4 *and* $q \equiv 1 (\mathrm{mod}\, 4)$ *then the equation* $x_1 t^2 + (y_1 - x_2)t - y_2 = 0$ *has a solution for* t *in the field* Z_q.

Proof. Since E has order 4, (α) or (β) in (II) holds. Suppose (α) holds. Then arguing as in (I) we have either $x_1 = y_2 = 0$ or $x_2 = -y_1$ and $x_1 y_2 = -1 - y_1^2$.

In the former case, $t = 0$ is obviously a solution. In the latter case, the equation becomes $x_1 t^2 + 2y_1 t - y_2 = 0$. Now if $x_1 = 0$ then $x_1 y_2 = -1 - y_1^2 \Rightarrow y_1^2 = -1 \Rightarrow y_1 \neq 0$ and so the equation has a solution in Z_q. So let $x_1 \neq 0$. Then

$$\begin{aligned} & x_1 t^2 + 2y_1 t - y_2 = 0 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & x_1^2 t^2 + 2x_1 y_1 t - x_1 y_2 = 0 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & (x_1 t + y_1)^2 = x_1 y_2 + y_1^2 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & (x_1 t + y_1)^2 = -1 \quad \text{for some } t \in Z_q, \end{aligned}$$

which is true since $q \equiv 1 (\mathrm{mod}\, 4)$ and $x_1 \neq 0$.

Now let (β) hold. If $x_1 = 0$ then $y_1 - x_2 \neq 0$ as, otherwise, we have from the first part of (β) $y_1 = 0 = x_2$ and so the second part of (β) does not hold. Thus if $x_1 = 0$ then the equation has a solution in Z_q. So let $x_1 \neq 0$. Then we have $2x_1 y_2 = -(y_1^2 + x_2^2)$ and

$$\begin{aligned} & x_1 t^2 + (y_1 - x_2)t - y_2 = 0 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & 4x_1^2 t^2 + 4x_1 (y_1 - x_2)t - 4x_1 y_2 = 0 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & [2x_1 t + (y_1 - x_2)]^2 = 4x_1 y_2 + (y_1 - x_2)^2 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & [2x_1 t + (y_1 - x_2)]^2 = -2(y_1^2 + x_2^2) + (y_1 - x_2)^2 \quad \text{for some } t \in Z_q \\ \Leftrightarrow\ & [2x_1 t + (y_1 - x_2)]^2 = -(y_1 + x_2)^2 \quad \text{for some } t \in Z_q, \end{aligned}$$

which is true since $q \equiv 1 (\mathrm{mod}\, 4)$ and $x_1 \neq 0$.

Added in proof. Steps (2), (3), (5.2) and (5.3) can be treated without explicit computations too.

References

[1] S. Baskaran, CLT *and non*-CLT *groups* I, Indian J. Math. 14 (1972), pp. 81–82.

[2] S. A. Chunikhin, *Subgroups of finite groups*, Groningen 1969.

[3] D. H. McLain, *The existence of subgroups of given order in finite groups*, Proc. Cambridge Philos. Soc. 53 (1957), pp. 278–285.

THE RAMANUJAN INSTITUTE
UNIVERSITY OF MADRAS
Madras, India

Accepté par la Rédaction le 4. 4. 1974