10-1991

Cyclicizers, Centralizers, and Normalizers

David Patrick
Rose-Hulman Institute of Technology

Eric Wepsic
Rose-Hulman Institute of Technology

CYCLICIZERS, CENTRALIZERS and NORMALIZERS

David Patrick and Eric Wepsic

MS TR 91-05

October 1991

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198

Phone: (812) 877-8391

Cyclicizers, Centralizers, and Normalizers

David Patrick* and Eric Wepsic*

Abstract

Our goal is to define the cyclicizer, which is analogous to the centralizer and normalizer, and to examine groups in which these subsets have certain special properties.

1 Definitions

Note: In this paper, all of the groups mentioned are finite. Also, for notational convenience, $G^\times$ denotes G without the identity element.

We begin by restating a familiar definition.

Definition: The *centralizer* of an element $x \in G$, denoted $C(x)$, is defined by

$$C(x) = \{y \in G \mid xy = yx\}.$$

We will also define the normalizer of an element.

Definition: The *normalizer* of an element $x \in G$, denoted $N(x)$, is defined by

$$N(x) = \{y \in G \mid y^{-1}xy \in \langle x \rangle\}.$$

*The authors' work was supported by NSF grant number DMS-910059.

Note that this is equivalent to $N(\langle x\rangle)$ under the more customary definition of normalizer.

Finally, we define a new subset of G, analogous to the two defined above:

Definition: The *cyclicizer* of an element $x \in G$, denoted $\mathrm{Cyc}(x)$, is defined by

$$\mathrm{Cyc}(x) = \{y \in G \mid \langle x, y\rangle \text{ is cyclic}\}.$$

In general, $\mathrm{Cyc}(x)$ is not a subgroup. For example, in the group $\mathbf{Z}_2 \oplus \mathbf{Z}_4$, we have $\mathrm{Cyc}((0,2)) = \{(0,0),(0,1),(0,2),(0,3),(1,1),(1,3)\}$, which is not a subgroup. Groups in which all the cyclicizers are subgroups are referred to as *tidy* groups; such groups are discussed in **[1]**.

2 The Fundamental Sequence

It is clear that for all groups G and all $x \in G$,

$$\langle x\rangle \subseteq \mathrm{Cyc}(x) \subseteq C(x) \subseteq N(x).$$

We now consider necessary and sufficient conditions for equality of terms in the above sequence.

2.1 Groups in which $\langle x\rangle = \mathrm{Cyc}(x)$

Theorem 1 *A group G satisfies $\langle x\rangle = \mathrm{Cyc}(x)$ for all $x \in G^\times$ if, and only if, every element of $G^\times$ is of prime order.*

Proof: Suppose there exists $x \in G^\times$ such that x is not of prime order.

Choose k such that k properly divides the order of x. Then $x^k \neq e$ and $x \in \mathrm{Cyc}(x^k)$, since $\langle x, x^k \rangle = \langle x \rangle$, but $x \notin \langle x^k \rangle$. Hence $\langle x^k \rangle \neq \mathrm{Cyc}(x^k)$.

Conversely, suppose every non-identity element of G is of prime order. Then every non-identity element x of G is contained in exactly one cyclic subgroup of G, namely $\langle x \rangle$. Therefore, $\mathrm{Cyc}(x) = \langle x \rangle$. $\square$

Finite groups in which every non-identity element has prime order are classified in **[2]**; the only such groups are p-groups of exponent p, certain non-nilpotent groups of order $p^a q$ (where p and q are distinct primes), and A_5.

2.2 Groups in which $\langle x \rangle = \mathrm{Cyc}(x) = C(x)$

We will refer to groups satisfying this condition as *anti-abelian.*

Theorem 2 *A group G satisfies $\langle x \rangle = \mathrm{Cyc}(x) = C(x)$ for all $x \in G^\times$ if, and only if, G is either cyclic of prime order or nonabelian of order pq, where p and q are distinct primes.*

Proof: If $|G| = p$, then $\langle x \rangle = G = C(x)$ for all $x \in G^\times$. If $|G| = pq$, and G is not abelian, then $|Z(G)| = 1$, since G/Z is not cyclic. Therefore, for any $x \in G^\times$, we have $\langle x \rangle \leq C(x) < G$. But $[G : \langle x \rangle]$ is prime, so we must have $\langle x \rangle = C(x)$.

Conversely, suppose G is anti-abelian, but not cyclic of prime order. First, we note that for any prime p, we have $p^2 \nmid |G|$. Otherwise, G contains a subgroup H of order p^2, which must be abelian, and must contain an element h of order p. But then $C(h)$ includes H, so $|C(h)| \geq p^2$, a contradiction since $|h| = p$. Therefore, G is of square-free order, and hence **[3]** must be metacyclic, with generators a and b such that $|a||b| = |G|$. It follows by Theorem 1 that $|a| = p$ and $|b| = q$, where p and q are distinct primes. Finally, if G is abelian, then $\langle a \rangle = C(a) = G$, a contradiction. $\square$

2.3 Groups in which $\mathrm{Cyc}(x) = C(x)$

We will arrive at the classification of such groups via a series of lemmas. But first we define a property of finite groups.

Definition: For all $n \geq 2$, a group has the *cyclic if commutative* property, denoted CC_n, if for each n-tuple $(x_1, \ldots, x_n)$ of group elements, $\langle x_1, \ldots, x_n \rangle$ abelian implies $\langle x_1, \ldots, x_n \rangle$ cyclic.

Note that the condition that $\mathrm{Cyc}(x) = C(x)$ for all $x \in G^\times$ is equivalent to CC_2.

We now show that the CC_n condition is independent of the choice of n.

Lemma 3 *For all groups G and all $n \geq 2$, G has property CC_n if, and only if, G has property CC_2.*

Proof: Assume G has property CC_n, and let $x, y \in G$ be given such that $xy = yx$. Then the n-tuple $(x, y, e, \ldots, e)$ generates an abelian subgroup, and hence, by hypothesis, a cyclic one. But $\langle x, y, e, \ldots, e \rangle = \langle x, y \rangle$, so $\langle x, y \rangle$ is cyclic. Hence G has property CC_2.

We prove $CC_2 \Rightarrow CC_n$ by induction on n. Let $n > 2$ be given, and assume that CC_2 implies CC_{n-1} for G. Consider G with property CC_2, and let $x_1, \ldots, x_n$ be given such that $\langle x_1, \ldots, x_n \rangle$ is abelian. Then $\langle x_1, \ldots, x_{n-1} \rangle \leq C(x_n) = \mathrm{Cyc}(x_n)$. But $\langle x_1, \ldots, x_{n-1} \rangle$ is cyclic by the inductive hypothesis; let g be a generator. Then $g \in \mathrm{Cyc}(x_n)$, so $\langle x_1, \ldots, x_n \rangle = \langle g, x_n \rangle$ is cyclic. Hence G has property CC_n. □

Call a group G a *CC-group* if G satisfies the CC_n condition for all $n \geq 2$. Next we give an alternative characterization of the CC property, one that will be more useful when we attempt to classify such groups.

Lemma 4 *For all groups G, G is a CC-group if, and only if, each abelian subgroup of G is cyclic.*

Proof: Suppose each abelian subgroup of G is cyclic. Let $x, y \in G$ be given such that $xy = yx$. Consider $H = \langle x, y \rangle$. H is abelian, and therefore by hypothesis is cyclic. So x and y generate a cyclic subgroup, and thus $\mathrm{Cyc}(x) = C(x)$ for all $x \in G^{\times}$. So G is a CC-group.

Conversely, suppose G is a CC-group. Then any abelian subgroup of G is finitely generated, and therefore cyclic. □

We also need the following result:

Proposition 5 *A p-group has all its abelian subgroups cyclic if, and only if, it is cyclic or a generalized quaternion group.* **[4]**

Now we may give a more precise characterization of CC-groups.

Theorem 6 *G is a CC-group if, and only if, every Sylow subgroup of G is either cyclic or a generalized quaternion group.*

Proof: If G is a CC-group, then every subgroup of G must also have this property; in particular so must the Sylow subgroups of G. Thus, by Lemma 4, all the abelian subgroups of the Sylow subgroups must be cyclic, and by Proposition 5, all of the Sylow subgroups of G must be cyclic or generalized quaternion groups.

To prove the converse, suppose that all the Sylow subgroups of G are either cyclic or generalized quaternion groups. Let an abelian subgroup A of G be given. Then A is a direct product of its Sylow subgroups, as follows:

$$A = A_{p_1} \oplus \cdots \oplus A_{p_k}.$$

But then for each i we have $A_{p_i} \leq P_i$, where P_i is a Sylow subgroup of G, so by Proposition 5, A_{p_i} is cyclic. Hence, A is cyclic. Thus, since every abelian subgroup of G is cyclic, G is a CC-group by Lemma 4. □

2.4 Groups in which $\mathrm{Cyc}(x) = C(x) = N(x)$

Such groups have a simple classification:

Theorem 7 *A group G satisfies* $\mathrm{Cyc}(x) = C(x) = N(x)$ *for all* $x \in G^\times$ *if, and only if, G is cyclic.*

Proof: Cyclic groups clearly satisfy the condition. For the converse, suppose that G is a non-cyclic group in which $\mathrm{Cyc}(x) = C(x)$ for all $x \in G^\times$. Then by Theorem 6 there are two cases.

CASE 1: All of the Sylow subgroups of G are cyclic. Then G must be metacyclic, and is given by the presentation

$$\langle a, b \mid a^m = b^n = e, b^{-1}ab = a^r \rangle$$

for certain values of m, n and r. Then $b \in N(a)$ but $b \notin C(a)$.

CASE 2: G has a generalized quaternion 2-Sylow subgroup. This subgroup is given by the presentation

$$\langle x, y \mid x^{2^n} = e, y^2 = x^{2^{n-1}}, y^{-1}xy = x^{-1} \rangle$$

for some value of $n > 1$. Then $y \in N(x)$ but $y \notin C(x)$. $\square$

2.5 Groups in which $\langle x \rangle = \mathrm{Cyc}(x) = C(x) = N(x)$

These groups also belong to a very restrictive class.

Theorem 8 *A group G satisfies* $\langle x \rangle = \mathrm{Cyc}(x) = C(x) = N(x)$ *for all* $x \in G^\times$ *if, and only if, G is cyclic of prime order.*

Proof: If G is cyclic of prime order, then $\langle x \rangle = \mathrm{Cyc}(x) = C(x) = N(x) = G$ for all $x \in G^\times$. Conversely, if $\langle x \rangle = \mathrm{Cyc}(x) = C(x) = N(x)$ for all $x \in G^\times$, then by Theorem 2, G is either cyclic of prime order or nonabelian of order pq. Furthermore, Theorem 7 implies G is cyclic, so G is cyclic of prime order. $\square$

2.6 Groups in which $C(x) = N(x)$

Unfortunately, we cannot classify groups which satisfy $C(x) = N(x)$ for all $x \in G^{\times}$. However, we do know some facts about this property.

- If G is abelian, then $C(x) = N(x) = G$ for all $x \in G^{\times}$.
- If G is a group with this property, then any normal cyclic subgroup of G must be contained in the center of G (since if h is a generator of $H \triangleleft G$, we must have $C(h) = N(h) = G$).
- If G is a nonabelian p-group with this property, then there is no element $x \in G$ such that $[G : \langle x \rangle] = p$ (since if such an x exists, we must have $N(x) = G$, so $C(x) = G$, which implies $\langle x \rangle \leq Z(G)$; but then $G/Z(G)$ is cyclic, a contradiction).
- The smallest nonabelian group with this property is A_4.

3 Some special classes of centralizers

We will now give some results on groups in which we restrict the centralizers of the group.

3.1 Groups in which the centralizers are cyclic

We first prove the following lemma about groups with cyclic cyclicizers:

Lemma 9 *A group G is such that* $\mathrm{Cyc}(x)$ *is a cyclic subgroup for all $x \in G^{\times}$ if, and only if, each element $x \in G^{\times}$ is contained in exactly one maximal cyclic subgroup.*

Proof: Suppose every element of G is contained in exactly one maximal cyclic subgroup. Let $x \in G^{\times}$ be given, and choose y such that $x \in \langle y \rangle$, where $\langle y \rangle$ is a maximal cyclic subgroup. Then if $g \in \mathrm{Cyc}(x)$, we must have $\langle x, g \rangle \le \langle y \rangle$, so $g \in \langle y \rangle$. Also, if $h \in \langle y \rangle$, then $\langle x, h \rangle \le \langle y \rangle$, so $\langle x, h \rangle$ is cyclic, giving $h \in \mathrm{Cyc}(x)$. Therefore $\mathrm{Cyc}(x) = \langle y \rangle$, and hence $\mathrm{Cyc}(x)$ is cyclic.

Conversely, suppose there exists $x \in G^\times$ such that $x \in \langle y \rangle$ and $x \in \langle z \rangle$, where $\langle y \rangle$ and $\langle z \rangle$ are distinct maximal cyclic subgroups. Suppose $\mathrm{Cyc}(x)$ is cyclic. Then since $\langle y \rangle \le \mathrm{Cyc}(x)$, we have $\langle y \rangle = \mathrm{Cyc}(x)$. Similarly $\langle z \rangle = \mathrm{Cyc}(x)$, and hence $\langle y \rangle = \langle z \rangle$, a contradiction. □

This allows us to give a characterization of all groups in which $C(x)$ is cyclic for all x. Clearly, if G is abelian, then $C(x)$ is cyclic for all $x \in G^\times$ if, and only if, G is cyclic. The following theorem deals with the case in which G is nonabelian. ((m, n) denotes the greatest common divisor of m and n.)

Theorem 10 *G is a nonabelian group such that $C(x)$ is cyclic for all $x \in G^\times$ if, and only if, G is given by the presentation*

$$\langle a, b \mid a^m = b^n = e, b^{-1}ab = a^r \rangle,$$

where $(m, n) = 1, (r^j - 1, m) = 1$ *for* $1 \le j < n$, *and* $r^n \equiv 1 \pmod{m}$.

Proof: Suppose G is nonabelian, and that $C(x)$ is cyclic for all $x \in G^\times$. Then $\mathrm{Cyc}(x) = C(x)$ for all $x \in G^\times$, since if $xy = yx$, then $\langle x, y \rangle$ is a subgroup of $C(x)$, and is thus cyclic. Therefore, by Theorem 6, every p-Sylow subgroup of G must be either cyclic or a generalized quaternion group. But G cannot have a generalized quaternion subgroup, since it would then contain a centralizer which is not cyclic (specifically, the centralizer of any element in the center of a quaternion group is the entire quaternion group, which is not cyclic). Therefore, every p-Sylow subgroup of G is cyclic, and hence G is metacyclic, with presentation

$$G = \langle a, b \mid a^m = b^n = e, b^{-1}ab = a^r \rangle,$$

where $(m, n) = 1, (r - 1, m) = 1$ and $r^n \equiv 1 \pmod{m}$. **[3]**

Now suppose there exists $1 < j < n$ such that $(r^j - 1, m) = k \neq 1$. Let $l = m/k$. Then the cyclic subgroup generated by b is $\{e, b, b^2, \ldots, b^{n-1}\}$, and the cyclic subgroup generated by $a^l b a^{-l}$ is $\{e, ba^{l(r-1)}, b^2 a^{l(r^2-1)}, \ldots, b^n a^{l(r^{n-1}-1)}\}$. In particular, $b^j = b^j a^{l(r^j - 1)}$, so these two maximal cyclic subgroups have a nontrivial intersection, which contradicts Lemma 9. Therefore, $(r^j - 1, m) = 1$ for all $1 \leq j < n$.

For the converse, suppose that G is given by the presentation above. Then every element of G is expressible in the form $b^i a^j$ for suitable i, j, and furthermore $b^i a^j b^k a^l = b^{i+k} a^{r^k j + l}$ for all $0 \leq i, k < n$ and $0 \leq j, l < m$. Thus, $b^i a^j$ and $b^k a^l$ commute if and only if $r^k j + l \equiv r^i l + j \pmod{m}$, which is equivalent to $(r^k - 1)j \equiv (r^i - 1)l \pmod{m}$.

So let $g = b^i a^j \in G^\times$ be given, and consider an element $b^k a^l$ in $C(g)$. We assume that $0 \leq i, k < n$ and $0 \leq j, l < m$. There are two cases:

CASE 1: $i = 0$. Then we must have $(r^k - 1)j \equiv 0 \pmod{m}$, so since $j \neq 0$ (we are only concerned with non-identity elements of G), we must have $(r^k - 1, m) \neq 1$. But then $k = 0$, by hypothesis, so $b^k a^l = a^l$, and hence $C(g) \leq \langle a \rangle$.

CASE 2: $i \neq 0$. Then for each value of k in $0, \ldots, n-1$, we must have $l \equiv \dfrac{r^k - 1}{r^i - 1} j \pmod{m}$, since $(r^i - 1, m) = 1$. Therefore there is exactly one element in $C(g)$ for each value of k in $0, \ldots, n-1$, and hence $|C(g)| = n$. But we know that $\langle g \rangle \leq C(g)$, and $|\langle g \rangle| = n$, so $C(g) = \langle g \rangle$.

In either case, $C(g)$ is cyclic. $\square$

3.2 Groups in which the centralizers are normal

We cannot fully classify these groups. We do, however, have the following:

Theorem 11 *If G is a group such that $G' \leq Z(G)$, then $C(x)$ is normal for every $x \in G$.*

Proof: Suppose $G' \leq Z(G)$, and let $x \in G$ be given. Then $G' \leq Z(G) \leq C(x)$, so $C(x) \triangleleft G$. $\square$

It is conjectured that the converse is also true; i.e. $C(x)$ is normal for all $x \in G$ if, and only if, $G' \leq Z(G)$. This conjecture has been verified, via CAYLEY, for all groups of order less than or equal to 100.

4 References

[1] K. O'Bryant, D. Patrick, L. Smithline, and E. Wepsic, *Some facts about cycels and tidy groups*, Rose-Hulman Technical Report (to appear).
[2] M. Deaconescu, *Classification of finite groups with all elements of prime order*, Proc. AMS #106 (1989), p.625-629.
[3] M. Hall, *The Theory of Groups*, New York: Macmillan, 1959.
[4] D. Gorenstein, *Finite Groups*, New York: Harper & Row, 1968.

The authors wish to acknowledge Martin Wattenberg for the final form of the proof of Theorem 1.

David Patrick
Carnegie Mellon University
Pittsburgh, PA 15213

Eric Wepsic
Harvard University
Cambridge, MA 02138