Note di Matematica ISSN 1123-2536, e-ISSN 1590-0932
Note Mat. **30** (2010) no. 2, 149–153. doi:10.1285/i15900932v30n2p149

A characterization of groups of exponent p which are nilpotent of class at most 2

Domenico Lenzi
Dipartimento di Matematica "E. De Giorgi"
Università degli Studi di Lecce 73100-LECCE
domenico.lenzi@unile.it

Received: 2.8.2009; accepted: 8.11.2010.

Abstract. Let $(\mathbf{G},+)$ be a group of prime exponent $p = 2n+1$. In this paper we prove that $(\mathbf{G},+)$ is nilpotent of class at most 2 if and only if one of the following properties is true:

i) $\mathbf{G}$ is also the support of a commutative group $(\mathbf{G},+')$ such that $(\mathbf{G},+)$ and $(\mathbf{G},+')$ have the same cyclic cosets [cosets of order p].

ii) the operation $\oplus$ defined on $\mathbf{G}$ by putting $x \oplus y = x/2 + y + x/2$, gives $\mathbf{G}$ a structure of commutative group.

Keywords: nilpotent groups, group partition

MSC 2000 classification: 03G25

1 Some remarks on the nilpotent groups of class at most 2

We will call *quasi-commutative* any group $(\mathbf{G},+)$ with the following property:

1) $\forall x, z \in \mathbf{G} : -x - z + x + z = x + z - x - z$;

Now we recall that a group $(\mathbf{G},+)$ is nilpotent of class at most 2 if and only if the commutator subgroup $\mathbf{G}'$ of $(\mathbf{G},+)$ is included in the center $\mathbf{Z_G}$ of $(\mathbf{G},+)$. Obviously, this property is equivalent to the following one:

2) $\forall x, y, z \in \mathbf{G} : -x - z + x + z + y = y - x - z + x + z$.

Therefore any nilpotent group of class at most 2 is quasi-commutative. Indeed, if in 2) we put $y = z + x$, then we easily get property 1).

Remark 1. We point out that a group $(\mathbf{G},+)$ is nilpotent of class at most 2 if and only if the following property holds:

3) $\forall x, y, z \in \mathbf{G} : x + z + y + z + x = z + x + y + x + z$.

Indeed, by 1), property 2) is equivalent to the following one:

4) $\forall x, y, z \in \mathbf{G} : -x - z + x + z + y = y + x + z - x - z$.

Moreover, it is clear that 4) and 3) are equivalent.

In the sequel $(\mathbf{G},+)$ shall be a torsion group with non zero elements of odd order. Thus, if $a \in \mathbf{G}$, there is a unique $d \in \mathbf{G}$, denoted by $a/2$, such that $2d = a$. Then we can define on $\mathbf{G}$ an operation $\oplus$ by putting, for any $a, b \in \mathbf{G}$:

6) $a \oplus b = a/2 + b + a/2$.

Clearly, $+$ and $\oplus$ coincide on the commutative subgroups of $(\mathbf{G},+)$; in particular on the cyclic subgroups. Thus, for any $x \in \mathbf{G}$, $x \oplus (-x) = 0 = (-x) \oplus x$.

Theorem 1. *If* $(\mathbf{G}, \oplus)$ *is a commutative group, then* $(\mathbf{G}, +)$ *and* $(\mathbf{G}, \oplus)$ *have the same cyclic cosets.*

PROOF. Indeed $(\mathbf{G}, +)$ and $(\mathbf{G}, \oplus)$ have the same cyclic subgroups. Therefore, if $\mathbf{H}$ is such a subgroup, then we have:

$$a \oplus \mathbf{H} = a/2 + \mathbf{H} + a/2 = a + (-a/2 + \mathbf{H} + a/2);$$
$$a + \mathbf{H} = a/2 + (a/2 + \mathbf{H} - a/2) + a/2 = a \oplus (a/2 + \mathbf{H} - a/2).$$

QED

Theorem 2. *Let the group* $(\mathbf{G}, +)$ *be nilpotent of class at most 2. Then* $(\mathbf{G}, \oplus)$ *is a commutative group.*

PROOF. Being $(\mathbf{G}, +)$ nilpotent of class at most 2, $+$ is quasi-commutative and hence $\oplus$ is commutative. Therefore, since $+$ and $\oplus$ coincide on the cyclic subgroups of $(\mathbf{G}, +)$, in order to prove that $(\mathbf{G}, \oplus)$ is a group, it remains to see that, for any $a, b, c \in \mathbf{G}$, $a \oplus (c \oplus b) = c \oplus (a \oplus b)$; i. e. $a/2 + c/2 + b + c/2 + a/2 = c/2 + a/2 + b + a/2 + c/2$. This equality is true by Remark 1. QED

2 Some remarks on the groups of exponent p

In the sequel we shall consider only groups of prime exponent $p = 2n + 1$. We recall that if $(\mathbf{G}, +)$ is such a group, then the subgroups of order p represent a group partition of $(\mathbf{G}, +)$ [wiz. they encounter only in 0; moreover, their union is $\mathbf{G}$ (see [1], p.16)]. Therefore, the set $\mathcal{L}_+$ of the cyclic cosets determines a line space $(\mathbf{G}, \mathcal{L}_+)$ on $\mathbf{G}$; precisely, for any two distinct elements $a, b \in \mathbf{G}$, there is a unique cyclic coset containing them.

The elements of $\mathbf{G}$ and $\mathcal{L}_+$ are respectively called *points* and *lines* of $(\mathbf{G}, \mathcal{L}_+)$. Points on a same line are said *collinear*.

A *subspace* of $(\mathbf{G}, \mathcal{L}_+)$ is a subset $\mathbf{K}$ of $\mathbf{G}$ such that either its cardinality is less than 2, or it contains the lines connecting pairs of its distinct points. Thus the set of the subspaces of $(\mathbf{G}, \mathcal{L}_+)$ is a closure system of $\mathbf{G}$.

If $\mathbf{K}$ is a set of points, we will represent by $((\mathbf{K}))$ [$((a_1, ..., a_n))$, whenever $\mathbf{K} = \{a_1, ..., a_n\}$] the minimum subspace containing $\mathbf{K}$ [*the subspace generated* by $\mathbf{K}$]. Whenever a and b are points, it is clear that $((a, b)) = a + < -a + b >$.

A *plane* is the subspace $((a, b, c))$ generated by three non collinear points a, b and c. Points and lines in a same plane are said *coplanar*.

Obviously, if $\mathbf{l}$ is a line and a is a point not belonging to $\mathbf{l}$, then the lowest subspace containing a and $\mathbf{l}$ [in symbols, $((a, \mathbf{l}))$] is a plane. Indeed, for any distinct points b and c of $\mathbf{l}$, we have $((a, \mathbf{l})) = ((a, b, c))$.

Theorem 3. *Let the group* $(\mathbf{G}, +)$ *be nilpotent of class at most 2. Then* $(\mathbf{G}, \oplus)$ *is a commutative group of exponent* p*. Moreover,* $(\mathbf{G}, \mathcal{L}_+)$ *and* $(\mathbf{G}, \mathcal{L}_\oplus)$ *coincide.*

PROOF. $(\mathbf{G}, \oplus)$ is a commutative group by Theorem 2. The remaining part of the proof is trivial by Theorem 1. QED

If $a \in \mathbf{G}$, both the left translation l_a and the right translation r_a of $(\mathbf{G}, +)$ are bijective functions on $\mathbf{G}$ that map cyclic cosets in cyclic cosets. This means that l_a and r_a are automorphisms of $(\mathbf{G}, \mathcal{L}_+)$, hence they map subspaces in subspaces. Also the function $[-]$ that maps any $b \in \mathbf{G}$ in $-b$ is an automorphism.

Clearly, any coset $\mathbf{K}$ of $(\mathbf{G}, +)$ is a subspace. But there can be subspaces which are not cosets (see Remark 3 below).

If a and b are two points, then $a+(-a+b)/2 \in ((a,b))$. Indeed $a+(-a+b)/2 \in a+<(-a+b)/2> = a+<-a+b> = ((a,b))$.

Remark 2. Now assume that the group $(\mathbf{G},+)$ is commutative. We have the following properties:

a) Any subspace $\mathbf{K_0}$ containing 0 is a subgroup. Indeed, if $a,b \in \mathbf{K_0}$, then $-a \in <a> = ((0,a)) \subseteq \mathbf{K_0}$; moreover, $a+(-a+b)/2 \in ((a,b)) \subseteq \mathbf{K_0}$, hence $a+b = 2[a+(-a+b)/2] \in ((0,a+(-a+b)/2)) \subseteq \mathbf{K_0}$.

As a consequence, since the translations are automorphisms of $(\mathbf{G},\mathcal{L}_+)$, any subspace is a coset of $(\mathbf{G},+)$. Thus in the commutative case all the planes have p^2 points.

a') In $\mathcal{L}_+$ there is a natural equivalence relation $//$: the *parallelism*. Precisely, two lines $\mathbf{l}$ and $\mathbf{l}'$ of $(\mathbf{G},\mathcal{L}_+)$ are said to be *parallel* [in symbols, $\mathbf{l}//\mathbf{l}'$] if and only if $\mathbf{l}$ and $\mathbf{l}'$ are cosets of a same [cyclic] subgroup of $(\mathbf{G},+)$.

Since now any plane of $(\mathbf{G},\mathcal{L}_+)$ has p^2 points, it is easy to verify that $\mathbf{l}$ and $\mathbf{l}'$ are parallel if and only if they either coincide or are disjoint and coplanar.

Let the group $(\mathbf{G},+)$ be nilpotent of class at most 2; thus $(\mathbf{G},\mathcal{L}_+) = (\mathbf{G},\mathcal{L}_\oplus)$. Now if $a,b \in \mathbf{G}$, then $<b> // a \oplus <b> = a + (-a/2 + <b> + a/2)$. Hence $a+<b> // <b>$ if and only if a belongs to the normalizer of $<b>$.

Remark 3. Now assume that $(\mathbf{G},+)$ is a non abelian group of prime exponent $p=2n+1$ and order p^3. Thus $(\mathbf{G},+)$ is an extraspecial p-group (see [3], p.145); hence, since in this case $\mathbf{G}' = \mathbf{Z_G}$, $(\mathbf{G},+)$ is nilpotent of class 2. Therefore, if 0, a and b are not collinear points, the plane $((0,a,b))$ has p^2 point. Indeed, by a) of Remark 2, $((0,a,b))$ is the subgroup generated by a and b in the group $(\mathbf{G},\oplus)$. On the other hand, $((0,a,b))$ is not a coset of $(\mathbf{G},+)$. Indeed, $0 \in ((0,a,b))$, but $((0,a,b))$ is not a subgroup of $(\mathbf{G},+)$, since $<a,b> = \mathbf{G}$ and $(\mathbf{G},+)$ has order p^3.

3 The characterization

In this section we will prove that, being $(\mathbf{G},+)$ a group of a prime exponent $p=2n+1$, $(\mathbf{G},+)$ is nilpotent of class at most 2 if and only if one of the properties i) and ii) in Abstract is true.

We emphasize that Theorem 3 above already ensures that if $(\mathbf{G},+)$ is such a group, then both the properties i) and ii) hold [in i) the operation $+'$ is given by $\oplus$]. Conversely, if ii) is true, then also i) [with $+' = \oplus$] is true by Theorem 1. Thus, it remains to prove that property i) implies that $(\mathbf{G},+)$ is nilpotent of class at most 2.

Remark 4. We point out that property i) is equivalent to the following one:

i_0) $\mathbf{G}$ is also the support of a commutative group $(\mathbf{G},+')$ such that $(\mathbf{G},+)$ and $(\mathbf{G},+')$ have the same *zero* and the same cyclic cosets.

Indeed, if the *zero* of $(\mathbf{G},+')$ is the element a, then we can replace the group $(\mathbf{G},+)$ with the group $(\mathbf{G},+_a)$, where $+_a$ is defined by putting $b +_a c = b - a + c$, for any $b,c \in \mathbf{G}$. Thus, since $(\mathbf{G},+)$ and $(\mathbf{G},+_a)$ are isomorphic and have the same cosets, the claim is true.

We assume that in the sequel the group $(\mathbf{G},+)$ fulfills property i_0. Moreover, being $(\mathbf{G},+')$ commutative, we will consider – with respect to $(\mathbf{G},\mathcal{L}'_+)$ – the parallelism $//$ of a') in Remark 2.

Now consider the function $d_a = l_a \circ r_a \circ [-]$. Since l_a, r_a and $[-]$ are automorphisms of $(\mathbf{G},\mathcal{L}_+)$, also d_a is an automorphism. It is easy to verify that d_a is an involution; moreover, since p is an odd number, a is the unique fixed point of d_a.

Remark 5. Let $a, b \in \mathbf{G}$. Then $d_a b \in ((a, b))$. Indeed $d_a b = a - b + a \in a + < -b + a > = ((a, b))$.

Consequently, if $\mathbf{K}$ is a subspace of $(\mathbf{G}, \mathcal{L}_+)$ and $a, b \in \mathbf{K}$, then $d_a b \in \mathbf{K}$. □

Theorem 4. *If $\mathbf{K}$ is a subspace of $(\mathbf{G}, \mathcal{L}_+)$ and if a is a point, consider the subspace $d_a\mathbf{K}$. The following properties hold:*

1) *If $a \in \mathbf{K}$, then $d_a\mathbf{K} = \mathbf{K}$;*

2) *if $a \notin \mathbf{K}$, then $d_a\mathbf{K}$ and $\mathbf{K}$ are disjoint.*

Proof. Let b be an arbitrary point of $\mathbf{K}$.

1) If $a \in \mathbf{K}$, then $d_a\mathbf{K} \subseteq \mathbf{K}$ by Remark 5. Thus, being d_a an involution, $d_a\mathbf{K} = \mathbf{K}$.

2) If $a \notin \mathbf{K}$, then $a \neq b$ and hence $d_a b \neq b$; moreover, the line $((a, b))$ intersects $\mathbf{K}$ only in b. Therefore $d_a b \notin \mathbf{K}$; whence the claim. QED

We point out that in the sequel we will tacitly use the fact that $//$ is an equivalence relation.

Theorem 5. *The functions d_a, $[-]$ and $l_a \circ r_a$ are dilatations [wiz. they map any line $\mathbf{l}$ in a line $\mathbf{l}'$ parallel to $\mathbf{l}$].*

Proof. Since $[-] = d_0$, $l_a \circ r_a = d_a \circ [-]$ and $//$ is an equivalence relation, then it is sufficient to see that, whenever $\mathbf{l}$ is a line, then $\mathbf{l} // d_a\mathbf{l}$.

Let $d_a\mathbf{l} \neq \mathbf{l}$. Thus, by Theorem 4, $d_a\mathbf{l}$ and $\mathbf{l}$ are disjoint. Therefore, we have to prove that $d_a\mathbf{l}$ and $\mathbf{l}$ are coplanar. This is true; indeed, by 1) in Theorem 4, $d_a\mathbf{l}$ is included in the plane $((a, \mathbf{l}))$. QED

Theorem 6. *Consider a line $\mathbf{l}$. Then, for any element c of the commutator subgroup $\mathbf{G}'$ of $(\mathbf{G}, +)$, we have $c + \mathbf{l} // \mathbf{l} // \mathbf{l} + c$.*

Proof. Obviously, we can limit ourselves to prove that $c + \mathbf{l} // \mathbf{l}$.

To this purpose, it is sufficient to verify that, for any $x, z \in \mathbf{G}$, we have $-x - z + x + z + \mathbf{l} // \mathbf{l}$.

This is obvious, since by Theorem 5 we have:

$$-x - z + x + z + \mathbf{l} = (-x - z) + [x + (z + \mathbf{l} + z) + x] + (-x - z) // \mathbf{l}.$$

QED

Lemma 1. *For any $y \in \mathbf{G}$ and $c \in \mathbf{G}'$, $c + < y > = < y > + c$.*

Proof. If $y = 0$, the claim is trivial. Thus let $y \neq 0$, hence the subgroup $< y >$ is a line. Hence, by Theorem 6, we have $c + < y > // < y > + c$. Therefore, since c belongs to $(c + < y >) \cap (< y > + c)$, we obtain $c + < y > = < y > + c$. QED

And now we can prove the following Theorem 7, which concludes our characterization.

Theorem 7. *If a group $(\mathbf{G}, +)$ satisfies property $i)$ above, then it is nilpotent of class at most 2.*

Proof. We will prove that, for any $y \in \mathbf{G}$ and $c \in \mathbf{G}'$, $c + y = y + c$.

This is trivial whenever $< c > = < y >$, or $c = 0$, or $y = 0$. Therefore assume $< c > \neq < y >$, $c \neq 0$ and $y \neq 0$.

By Lemma 1, we have $c + y = hy + y + c$ [where $h \in \mathbb{N}$], hence hy is a commutator. We will prove that $hy = 0$. To this purpose we consider two cases: $y \notin \mathbf{G}'$, $y \in \mathbf{G}'$.

If $y \notin \mathbf{G}'$ and $hy \neq 0$, then $y \in < hy > \subseteq \mathbf{G}'$. This is absurd.

If $y \in \mathbf{G}'$, then in Lemma 1 we can interchange c with y. Therefore $c + y = kc + y + c$ and hence $hy = -kc$. Consequently, $hy = 0$. QED

We conclude by emphasizing that, with respect to the property i_0), if $\mathbf{H}$ is a cyclic subgroup of $(\mathbf{G},+)$ and of $(\mathbf{G},+')$, this fact does not say "a priori" that the groups $(\mathbf{H},+)$ and $(\mathbf{H},+')$ coincide. Nevertheless, since we have proved that by i_0) $(\mathbf{G},+)$ is nilpotent of class at most 2, "a posteriori" it is easy to verify that, if $\mathbf{G}$ has more than p elements and hence $(\mathbf{G},\mathcal{L}_+)$ is not a line, then $(\mathbf{G},+') = (\mathbf{G},\oplus)$. As a consequence, we get $(\mathbf{H},+) = (\mathbf{H},\oplus) = (\mathbf{H},+')$.

References

[1] P. Dembowski: Finite Geometries. Springer-Verlag, Berlin Heidelberg N. York (1968).

[2] D. Lenzi: *On the autodistributive Steiner triple systems.* Note di Matematica; in print.

[3] D. J. S. Robinson: A Course in the Theory of Groups. Springer-Verlag, N. York (1996).