On abelian groups with the unique square root property

by José Morgado

Instituto de Física e Matemática, Universidade Federal de Pernambuco, Brasil

1. It is well known that, if G is a finite group (multiplicatively written), then each element of G has a square root, if and only if the order of G is odd ([1], Theorem 1, and [2]).

Recently, we have obtained a characterization of the groups which admit a JACOBI automorphism. We have stated that a group G has at most one JACOBI automorphism, and that such an automorphism exists, if and only if G is an abelian group having the unique square root property (i. e., for each element $x \in G$, there is exactly one element $y \in G$ satisfying the condition $y^2 = x$).

In this note we obtain some results about the abelian groups having the unique square root property.

2. Let us state the following

LEMMA 1. *If* x *is an element of odd order of a group* G *and* y *is a square root of* x, *then one has either* $\mathrm{ord\,y} = \mathrm{ord\,x}$ *or* $\mathrm{ord\,y} = 2 \cdot \mathrm{ord\,x}$.

PROOF. Indeed, let $ord\, x = 2n-1$. Since $y^2 = x$, one has

$$y^{2(2n-1)} = x^{2n-1} = 1$$

and so y is an element of finite order.

If $ord\, y$ is odd, say $2m-1$, then one has $(2m-1) \mid 2(2n-1)$, hence

$$(2m-1) \mid (2n-1).$$

On the other hand, one has

$$x^{2m-1} = y^{2(2m-1)} = 1$$

and so $(2n-1) \mid (2m-1)$.

Consequently, $ord\, y = ord\, x$.

If $ord\, y$ is even, say $2m$, then from $y^2 = x$, it follows

$$y^{2(2n-1)} = x^{2n-1} = 1 = y^{2m} = x^m,$$

meaning that $2m \mid 2(2n-1)$ and $(2n-1) \mid m$, hence $ord\, y = 2 \cdot ord\, x$, as wanted.

LEMMA 2. *If* x *is an element of odd order of a group* G, *then there is exactly one element* $\mathrm{y} \in \mathrm{G}$ *such that*

$$\mathrm{y}^2 = \mathrm{x} \textit{ and } \mathrm{ord\,y} = \mathrm{ord\,x}$$

and this element y *belongs to the cyclic subgroup generated by* x.

PROOF. Let $ord\, x = 2n-1$. Then, since

$$(x^n)^2 = x^{2n-1} \cdot x = x$$

one sees that x^n is a square root of x and obviously x^n belongs to the cyclic subgroup generated by x. Moreover, if $y^2 = x$ and $ord\,y = ord\,x$, then

$$y = y^{2(2n-1)+1} = (x^n)^{2(2n-1)+1} = x^n,$$

proving the lemma.

THEOREM 1. *If* T *is the set af all elements of odd order of an abelian group* G, *then* T *is a subgroup of* G *having the unique square root property.*

PROOF. The set T is clearly non void, since $1 \in T$. Moreover, since $ord(a^{-1}) = ord\,a$ and $ord(a\,b) = ord\,a \cdot ord\,b$ for all a, b in T, on sees that T is a subgroup of G. By Lemma 2, for each $a \in T$ there is exactly one element x such that $x^2 = a$ and $ord\,x = ord\,a$ and this element belongs to the cyclic subgroup generated by a, hence $x \in T$.

If $ord\,x \neq ord\,a$, then, by Lemma 1, one has $ord\,x = 2 \cdot ord\,a$ and so x does not belong to T.

3. If G is a torsion free abelian group such that for each element $a \in G$ there is some x satisfying the condition $x^2 = a$, then G has the unique square root property. In fact, if $x^2 = y^2 = a$ with $y \neq x$, then $(x\,y^{-1})^2 = x^2\,(y^{-1})^2 = a \cdot a^{-1} = 1$, contradicting the hypothesis that G is torsion free.

Let G be a group with the unique square root property. Then, there his no element x in G with even order. In fact, from $ord\,x = 2\,m$ it follows $(x^m)^2 = 1$ and so 1 and $x^m \neq 1$ would be square roots of 1, against the hypothesis. Thus, the set T formed by all elements in G having odd order is the maximal torsion subgroup of G and, therefore, the quotient group G/T is torsion free. If $a\,T \in G/T$ and $x^2 = a$, then it is immediate that $(x\,T)2 = a\,T$.

Consequently, the following holds:

THEOREM 2: *If* G *is an abelian group with the unique square root property and* T *is the set of all elements in* G *having odd order, then* G/T *is a torsion free abelian group with the unique square root property.*

4. Now, let H be a torsion free abelian group having the unique square root property. We shall denote by $x^{1/2}$ the (unique) square root of x. More generally, we shall denote by $x^{m/2^n}$, m and n integers, the square root of $x^{m/2^{n-1}}$.

This notation is consistent, since

$$x^{m/2^n} . x^{m'/2^{n'}} = x/^{m2^n + m'/2^{n'}} .$$

Let $a \in H$. It is immediate that the least subgroup of H containing a and having the unique square root property is the set of all elements a^r, where r is either 0 or a rational number of the form $\dfrac{2\,m+1}{2^n}$, where m and n are integers.

Let us denote this group by $S(a)$. It is immediate that this group is isomorphic to the additive group whose elements are 0 and the rational numbers of the form $\dfrac{2\,m+1}{2^n}$, with m and n integers.

THEOREM 3. *For each* $a \in H$, *the lattice of all subgroups of the group* S(a) *is distributive.*

PROOF. Indeed, as it was stated by ORE [4], the lattice of all subgroups of a group is distributive, if and only if the group is locally cyclic.

Let us see that the group $S(a)$ is locally cyclic, that is to say, if $x, y \in S(a)$, say

$$x = a^{(2m+1)/2^n} \text{ and } y = a^{(2r+1)/2^s}$$

then there is some $z \in S(a)$ such that x and y belong to the cyclic subgroup generated by z. It is sufficient to set $z = a^{1/2^p}$, where p is the greatest of the integers n and s.

THEOREM 4. *For each* $a \in H$, *the lattice of all subgroups of* $S(a)$ *having the unique square root property, is isomorphic to the lattice constituted by the set of all positive odd integers partially ordered by the relation* $m \leqq n$ *if and only if* m *is divisible by* n.

PROOF. Let A be a subgroup of $S(a)$ having the unique square root property. If $a^{(2m+1)/2^n} \in A$, then a^{2m+1} and $a^{-(2m+1)}$ belong to A. Let $2p+1$ be the least positive integer such that $a^{2p+1} \in A$. Then, if $x \in A$, one has $x = a^{(2p+1)(2q+1)/2^n}$ for some integers q and n.

This means that $A = S(a^{2p+1})$.

Thus, one sees that there is a one-one correspondence between the set of all subgroups of $S(a)$ having the unique square root property and the set of all positive odd integers.

Moreover, one has clearly

$$S(a^{2m+1}) \subseteq s(a^{2p+1})$$

if and only if

$$(2p+1) \mid (2m+1),$$

completing the proof.

The group H may be considered as a module over the ring R formed by all rational numbers $0, \frac{2m+1}{2^n}$, m and n integers, relatively to the ordinary addition and multiplication. The set $S(a)$ the cyclic submodule generated by a.

The theorem 4 above says that *the lattice of all submodules of* $S(a)$ *is isomorphic to the lattice of all positive odd integers,* $m \leqq n$ *meaning that* n *divides* m.

5. For each $a \in H$, let us denote by $C(a)$ the cyclic subgroup generated by a.

Let us consider the quotient group $S(a)/C(a)$ and let $a^{(2m+1)/2^n}$ be any element of $S(a)$. If $n \geqq 1$, by the division algorithm, one has

$$2m+1 = 2^n \cdot q + (2r+1), \text{ with } 0 < 2r+1 < 2^n$$

q and r integers.

From this it follows

$$\frac{2m+1}{2^n} = q + \frac{2r+1}{2^n}, \quad \text{with } 0 < 2r+1 < 2^n \tag{1}$$

and hence

$$a^{(2m+1)/2^n} = a^q \cdot a^{(2r+1)/2^n} \in a^{(2r+1)/2^n} C(a)$$

If $n < 1$, then $\frac{2m+1}{2^n}$ is an integer and so $a^{(2m+1)/2^n} \in C(a)$.

Thus, the elements of the group $S(a)/C(a)$ are $C(a)$ and the cosets of the form

$$a^{(2r+1)/2^n} C(a)$$

where n is a positive integer and r is an integer such that $0 < 2r+1 < 2^n$.

Let us consider the group $Z(2^\infty)$ ([5], p. 4). The elements of the group $Z(2^\infty)$ are

$$0, \frac{1}{2}, \frac{1}{4}, \frac{3}{4}, \frac{1}{8}, \frac{3}{8}, \ldots, \frac{2r+1}{2^n}, \ldots$$

with $0 < 2r+1 < 2^n$, the group operation being the addition modulo one.

Since the integers q and r in (1) are uniquely determined, one concludes the following

THEOREM 5. *For each* $a \in H$, *the quotient group* $S(a)/C(a)$ *is isomorphic to the group* $Z(2^\infty)$.

BIBLIOGRAPHY

[1] W. R. UTZ, *Square roots in groups,* Amer. Math. Monthly, **60** (1953), pp. 185-186.

[2] E. A. FAY, *Solution of the problem E 1794* [*1965, 545*], Amer. Math. Monthly, **73** (1966), pp.892-893.

[3] JOSÉ MORGADO, *Note on Jacobi endomorphisms,* in preparation.

[4] OYSTEIN ORE, *Structures and group theory II,* Duke Math. J., **4** (1938), pp. 247-269.

[5] IRVING KAPLANSKY, *Infinite abelian groups,* Ann Arbor, 1954.