ORIGINAL PAPER

INTERESTING PROPERTIES OF A SUBGROUP

GEORGIANA VELICU[1], SIMONA MINCU[1]

Manuscript received: 11.08.2014; Accepted paper: 17.09.2014;

Published online: 30.09.2014.

Abstract. *The basic ideas and ways of thought of algebra permeate nearly every part of mathematics. Moreover, modern algebra cultivates the ability to handle abstract ideas. From the most basic ideas of the modern and abstract algebra, the notions of group and subgroup are fundamental. We all know that a group G is an algebraic structure, more precisely a nonempty set endowed with an operation which combines between them two elements from G, obtaining in this way new and spectacular results and properties for the elements and also, for the subsets of G. In this article, we present how a subgroup of a group can receive interesting properties by using nonempty subsets of the main group and a positive integer previously fixed. Also, in this paper we give a few applications which are related to the new construction, namely the radical of a subgroup of a group.*

Keywords: *subgroup, application, radical.*

1. PRELIMINARY

Modern algebra's objective is to study several algebraic structures. By an algebraic structure we understand a nonempty set M, endowed with a low of composition φ, ψ, ... , which satisfies some properties called axioms: associability, commutability, the existence of the neutral element and/or the existence of symmetrical elements.

The notion of group is the most important algebraic notion and is linked with the names of two famous mathematicians Évariste Galois (1811-1832) and Augustin Louis Cauchy (1789-1857). The notion of group appeared for the first time in the study of polynomial equations, and this study was made by Évariste Galois in 1830. After the contributions received from other domains like number theory and geometry, the notion of group was generalized in the 70's. To explore groups, the mathematicians developed several notations to split groups in smaller parts more easier to understand and study, like subgroups and simple groups. A theory of groups was developed for the finite groups, which culminated with the classification of simple and finite groups in 1983. The number of examples of groups is considerably and from this point of view, it was necessary a classification of groups. Also, the large number of properties of groups and the numerous applications of groups in areas of mathematics, determined the algebraists to study them. The fundamental problem in the group's theory is to describe all types of possible groups, all types of subgroups of a group and to find isomorphisms between them.

[1] Valahia University of Targoviste, Faculty of Sciences and Arts, 130024 Targoviste, Romania.
E-mail: georgiana.velicu@yahoo.com; mincu_simona@yahoo.com.

2. THE RADICAL OF A SUBGROUP AND APPLICATIONS

Application 1. Let *G* be a group and *H* a subgroup of *G*. Let *p* be a positive integer greater than or equal to 2 and two sets: $A = \{x \in G / x^p \in H\}$ and $B = \{x \in G / x^{p+1} \in H\}$. Then the following assertions are true:

1. *A* and *B* are nonempty sets, $A, B \neq \phi$;
2. $(A - B) \cap H = \phi$;
3. $(B - A) \cap H = \phi$;
4. $A \cap B \subset H$

Solution.

1. If e is the neutral element of G, then it is obvious that $e \in A$ and $e \in B$, so *A* and *B* are nonempty subsets of *G*.

2. Let suppose now that $(A - B) \bigcap H \neq \phi$. We have:

$$\exists x_0 \in (A - B) \cap H \Rightarrow x_0 \in H, x_0 \in A \text{ and } x_0 \notin B \Leftrightarrow x_0 \in H, x_0^p \in H \text{ and } x_0^{p+1} \notin H,$$

but *H* is a subgroup in *G* and this implies that $x_0 \cdot x_0^p = x_0^{p+1} \in H$, which contradicts the fact that $x_0 \notin B$. In conclusion, the assumption made is false and so we have $(A - B) \bigcap H = \phi$.

3. The proof of the assertion 3 is similar to 2.

4. We prove that any element from the intersection $A \cap B$ is also from the subgroup *H*.

In this sense, let consider the element $x_0 \in A \cap B \Rightarrow x_0 \in A$ and $x_0 \in B \Rightarrow x_0^p \in H$ and $x_0^{p+1} \in H$. But $H \leq G$ is a subgroup in *G*, so: $\left(x_0^p\right)^{-1} \cdot x_0^{p+1} = x_0 \in H$. But the element $x_0 \in A \cap B$ was arbitrary choose and so we have the inclusion $A \cap B \subset H$.

Remark. The assertions 2. and 3. from the above application, can be reformulated in the following way:

$$((A - B) \cup (B - A)) \cap H = \phi.$$

The proof of this relation is based only on the properties of the set's operations.

From (A-B)∩H=∅ and (B-A)∩H=∅ , we have

[(A-B)∩H]∪[(B-A)∩H]=∅
⇒[(A-B)∪(B-A)]∩[H∪(B-A)]∩[(A-B)∪H]∩[H∪H]=∅
⇒(A ΔB)∩[H∪((A-B)∩(B-A))]∩H=∅ ⇒(AΔB)∩[H∪(A ΔB)]∩H=∅
⇒[((AΔB)∩H)∪ (AΔB)∩ (AΔB)]∩H=∅ ⇒[((AΔB)∩H)∪(AΔB)]∩H=∅
⇒((AΔB)∩H∩H)∪ ((AΔB)∩H)=∅ ⇒((AΔB)∩H)∪(AΔB)∩H)=∅
⇒(AΔB)∩H=∅.

Application 2. Let $(G,\cdot)$ be a multiplicative and commutative group. Let *H* be a subgroup of G. For an integer $k \geq 2$ let's denote with $H_k = \{x \in G / x^k \in H\}$, the set of all elements *x* from G with the property that x^k is from H . Using this notation, we have the following assertions:

1) H_k is a subgroup of *G*, $H_k \leq G$, and also $H \subseteq H_k$.
2) For any positive integers $i, j \in N, i, j \geq 2$, we have: $(H_i)_j = H_{ij}$.
3) If $ord(H) = m < \infty$, then $H \subseteq (\{e\})_m$, where e is the neutral element of *G*.

Solution.
The assertion 1) is obvious because:
(1) $e \in H_k \Leftrightarrow e^k = e \in H$
(2) $\forall x \in H_k \Rightarrow x^k \in H, H \leq G \Rightarrow (x^k)^{-1} = (x^{-1})^k \in H \Rightarrow x^{-1} \in H_k$
(3) $\forall x, y \in H_k \Rightarrow x^k \in H, y^k \in H, H \leq G \Rightarrow x^k \cdot y^k = (xy)^k \in H$
(*G* is a commutative group) $\Rightarrow xy \in H_k$.
The inclusion $H \subseteq H_k$ is also obvious because *H* is a subgroup in *G*.

2) $(H_i)_j = \{x \in G / x^j \in H_i\} = \{x \in G / (x^i)^j \in H\} = \{x \in G / x^{ij} \in H\} = H_{ij}$.

3) If the order of the subgroup *H* is finite, $ord(H) = m < \infty$, then for any element $x \in H$ result $ord(x) \mid m$, and then $\exists d \in N^*, d \mid m$ such that $x^d = e$. This relation implies that $x \in (\{e\})_d \subseteq (\{e\})_m$, and so we have $H \subseteq (\{e\})_m$.

The inclusion $(\{e\})_d \subseteq (\{e\})_m$ is simple because for any $x_0 \in (\{e\})_d$, we have $(x_0)^d = e$. But $d \mid m$, so there exist d_1 such that $dd_1 = m$, and so $\left((x_0)^d\right)^{d_1} = e$, from where we have $(x_0)^m \in (\{e\})_m \Leftrightarrow (\{e\})_d \subseteq (\{e\})_m$.

Remark. The problem above can be reformulated for any group (not necessary commutative) in the following way:

Let $(G,\cdot)$ be a group and *H* a subgroup of G. For any integer $k \geq 2$ let's denote with $H_k = \{x \in G / x^k \in H\}$, the set of all elements *x* from G with the property that x^k is from H. If *m* and *n* are two positive integers such that g.c.d.$(m,n) = 1$, then $H_m \cap H_n$ is a subgroup of *G*.

Proof: It is sufficient to prove that $H_m \cap H_n = H$.

Let consider an element from H, $x \in H \Rightarrow \begin{cases} x^m \in H \Rightarrow x \in H_m \\ x^n \in H \Rightarrow x \in H_n \end{cases} \Rightarrow x \in H_m \cap H_n$.

In this way we obtain that $H \subseteq H_m \cap H_n$. (1)

Let's now have $x \in H_m \cap H_n \Rightarrow \begin{cases} x \in H_m \\ x \in H_n \end{cases}$.

But because the g.c.d.$(m,n)=1$, we have two positive integers $k,l \in Z$, such that $mk+nl=1$. More, we have: $\begin{cases} x \in H_m \Rightarrow x^m \in H \Rightarrow (x^m)^k \in H \Rightarrow x^{mk} \in H \\ x \in H_n \Rightarrow x^n \in H \Rightarrow (x^n)^l \in H \Rightarrow x^{nl} \in H \end{cases}$.

But because H is a subgroup of G, we obtain $x^{mk} \cdot x^{nl} \in H \Leftrightarrow x^{mk+nl} \in H \Leftrightarrow x \in H$. Finally we have $H_m \cap H_n \subseteq H$. (2)

Using the relations (1) and (2) we obtain $H_m \cap H_n = H$, so the intersection $H_m \cap H_n$ is a subgroup of the group G.

Remark. The subgroup $H_k = \{x \in G / x^k \in H\} \leq (G,\cdot)$ can be named ***the radical of order k of the subgroup H***, which can also be denoted by $\sqrt[k]{H}$.

Using this notation, the assertion 2) from the Application 2 (for a commutative group) can be rewritten in the following way:

$$\sqrt[i]{\sqrt[j]{H}} = \sqrt[ij]{H}, \forall i,j \in N, i,j \geq 2 .$$

Property. Let $(G,\cdot)$ be a commutative group and H a subgroup of G. If H is a normal subgroup of G, $H \triangleleft G$, then the radical $\sqrt[k]{H}$ is also a normal subgroup in G, $\sqrt[k]{H} \triangleleft G, k \in N, k \geq 2$.

Proof: To prove that the radical $\sqrt[k]{H}$ is a normal subgroup in G, $\sqrt[k]{H} \triangleleft G, k \in N, k \geq 2$, is equivalent to prove that:

$$\forall x \in G, \forall h \in H_k \Rightarrow x \cdot h \cdot x^{-1} \in H_k$$
$$\Leftrightarrow (x \cdot h \cdot x^{-1})^k \in H .$$

For this we have:

$$(x \cdot h \cdot x^{-1})^k = \underbrace{(x \cdot h \cdot x^{-1}) \cdot (x \cdot h \cdot x^{-1}) \cdot \ldots \cdot (x \cdot h \cdot x^{-1})}_{k\ times} = x \cdot h^k \cdot x^{-1} .$$

Because H is a normal subgroup in G, $H \triangleleft G$, we have:

$$x \cdot h^k \cdot x^{-1} \in H, \forall x \in G, \forall h \in H_k \Leftrightarrow h^k \in H ,$$

which is equivalent to $\sqrt[k]{H} \triangleleft G$.

3. EXAMPLES

1. Let's now consider the group of three permutations S_3, and consider the cycles $\sigma = (2,3)$ and $\tau = (1,2,3)$. Then, we have the orders: $ord(\sigma) = 2$ and $ord(\tau) = 3$. Much more, the group S_3 is finite generated by these two permutations, means that $S_3 = <\sigma, \tau>$, and because σ and τ have the properties: $\sigma\tau = \tau^2\sigma$ and $\tau\sigma = \sigma\tau^2$, we obtain the following table of composition in S_3:

$\circ$	e	σ	τ	τ^2	$\sigma\tau$	$\sigma\tau^2$
e	e	σ	τ	τ^2	$\sigma\tau$	$\sigma\tau^2$
σ	σ	e	$\sigma\tau$	$\sigma\tau^2$	τ	τ^2
τ	τ	$\sigma\tau^2$	τ^2	e	σ	$\sigma\tau$
τ^2	τ^2	$\sigma\tau$	E	τ	$\sigma\tau^2$	σ
$\sigma\tau$	$\sigma\tau$	τ^2	$\sigma\tau^2$	σ	e	τ
$\sigma\tau^2$	$\sigma\tau^2$	τ	σ	$\sigma\tau$	τ^2	E

Analyzing this table and using the Lagrange's theorem we obtain all the subgroups of S_3:

- subgroups of order 1: $H^{(1)} = \{e\}$
- subgroups of order 2: $H^{(2)} =< \sigma >= \{e, \sigma\}$

  $H^{(3)} =< \sigma\tau >= \{e, \sigma\tau\}$

  $H^{(4)} =< \sigma\tau^2 >= \{e, \sigma\tau^2\}$
- subgroups of order 3: $H^{(5)} =< \tau >= \{e, \tau, \tau^2\}$

For example, we have the following radicals:

$$\sqrt[2]{H^{(2)}} = \{x \in S_3 / x^2 \in H^{(2)}\} = \{e, \sigma, \sigma\tau, \sigma\tau^2\}$$

$$\sqrt[3]{H^{(2)}} = \{x \in S_3 / x^3 \in H^{(2)}\} = \{e, \sigma, \tau, \tau^2\}$$

and

$$\sqrt[2]{\sqrt[3]{H^{(2)}}} = \sqrt[3]{\sqrt[2]{H^{(2)}}} = \sqrt[6]{H^{(2)}} = \{x \in S_3 / x^6 \in H^{(2)}\} = \{e, \sigma, \tau, \tau^2, \sigma\tau, \sigma\tau^2\} = S_3 .$$

Much more, the only one normal subgroup of S_3 is $H^{(5)} =< \tau >= \{e, \tau, \tau^2\}$, and so we have that it's radical of any order *k*, is also a normal one, means that: $\sqrt[k]{H^{(5)}} \lhd S_3, \forall k \in N, k \geq 2$.

2. Let's consider now the additive group $(Z_{12},+)$ of classes modulo – 12 and let $H =< \hat{4} >$ be the subgroup of Z_{12} generated by the class $\hat{4}$. Then we have $H = \{\hat{0}, \hat{4}, \hat{8}\}$. Calculating the radicals of order 2, 3 and 6 of this subgroup we obtain:

$$H_2 = \sqrt[2]{H} = \{\hat{x} \in Z_{12} / 2 \cdot \hat{x} \in H\} = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \widehat{10}\}$$

$$H_3 = \sqrt[3]{H} = \{\hat{x} \in Z_{12} / 3 \cdot \hat{x} \in H\} = \{\hat{0}, \hat{4}, \hat{8}\}$$

and

$$H_6 = \sqrt[6]{H} = \{\hat{x} \in Z_{12} / 6 \cdot \hat{x} \in H\} = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \widehat{10}\},$$

and, also, we have:

$$(H_3)_2 = \sqrt[2]{H_3} = \{\hat{x} \in Z_{12} / 2 \cdot \hat{x} \in H_3\} = \{\hat{0}, \hat{2}, \hat{4}, \hat{6}, \hat{8}, \widehat{10}\} = \sqrt[2]{\sqrt[3]{H}}$$

and

$$\sqrt[2]{\sqrt[3]{H}} = \sqrt[3]{\sqrt[2]{H}} = \sqrt[6]{H}\ .$$

For the orders 5 and 7 we have the following radicals:

$$\sqrt[5]{H} = \{\hat{x} \in Z_{12} \,/\, 5 \cdot \hat{x} \in H\} = \{\hat{0}, \hat{4}, \hat{8}\} = H$$

and

$$\sqrt[7]{H} = \{\hat{x} \in Z_{12} \,/\, 7 \cdot \hat{x} \in H\} = \{\hat{0}, \hat{4}, \hat{8}\} = H$$

by using the table below:

$\hat{x}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$	$\hat{8}$	$\hat{9}$	$\widehat{10}$	$\widehat{11}$
$2\hat{x}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{6}$	$\hat{8}$	$\widehat{10}$	$\hat{0}$	$\hat{2}$	$\hat{4}$	$\hat{6}$	$\hat{8}$	$\widehat{10}$
$3\hat{x}$	$\hat{0}$	$\hat{3}$	$\hat{6}$	$\hat{9}$	$\hat{0}$	$\hat{3}$	$\hat{6}$	$\hat{9}$	$\hat{0}$	$\hat{3}$	$\hat{6}$	$\hat{9}$
$6\hat{x}$	$\hat{0}$	$\hat{6}$	$\hat{0}$	$\hat{6}$	$\hat{0}$	$\hat{6}$	$\hat{0}$	$\hat{6}$	$\hat{0}$	$\hat{6}$	$\hat{0}$	$\hat{6}$
$5\hat{x}$	$\hat{0}$	$\hat{5}$	$\widehat{10}$	$\hat{3}$	$\hat{8}$	$\hat{1}$	$\hat{6}$	$\widehat{11}$	$\hat{4}$	$\hat{9}$	$\hat{2}$	$\hat{7}$
$7\hat{x}$	$\hat{0}$	$\hat{7}$	$\hat{2}$	$\hat{5}$	$\hat{4}$	$\widehat{11}$	$\hat{6}$	$\hat{1}$	$\hat{8}$	$\hat{3}$	$\widehat{10}$	$\hat{5}$

Consequence. Let consider the additive group of classes modulo – *n*, $(Z_n,+)$, $n \in N, n \geq 2$, and the cyclic subgroup $H = <\hat{a}>, \hat{a} \in Z_n$. If $m \in N$ is a positive integer such that g.c.d.$(m,n) = 1$, then the radical of order *m* of H coincide with H:

$$\sqrt[m]{H} = H\ .$$

Proof: We have $H = <\hat{a}>, \hat{a} \in Z_n \Rightarrow H = \{\hat{0}, \hat{a}, 2\hat{a}, ..., (k-1)\hat{a}\}$, where $k = ord(\hat{a})$ and $k \mid n$, with $n = |Z_n|$. More, we have:

$$\sqrt[m]{H} = \{\hat{x} \in Z_n \,/\, m \cdot \hat{x} \in H = <\hat{a}>\}.$$

Let's consider $\hat{x} \in \sqrt[m]{H} \Rightarrow m \cdot \hat{x} = q \cdot \hat{a}, q \in \{0,1,2,...,k-1\}$.

We have the following equivalences:

$$\text{g.c.d.}\,(m,n) = 1 \Leftrightarrow \exists u, v \in Z\ ,\ \ m \cdot u + n \cdot v = 1 \Leftrightarrow m \cdot u = 1 - n \cdot v\ \ \Rightarrow m \cdot u \cdot \hat{x} = qu \cdot \hat{a} \Leftrightarrow$$
$$\Leftrightarrow (1 - n \cdot v) \cdot \hat{x} = qu \cdot \hat{a} \Leftrightarrow \hat{x} = qu \cdot \hat{a} \Rightarrow \hat{x} \in uH \subseteq H\ .$$

Finally we obtain $\sqrt[m]{H} \subseteq H$, and because $H \subseteq \sqrt[m]{H}$, H being a subgroup in $(Z_n,+)$, we have the equality from the text.

REFERENCES

[1] Durbin, J.R., *Modern Algebra*, Ed.John Wiley, New York, 1985.

[2] Buşneag, D., Chirteş, F., Piciu, D., *Probleme de algebră*, Ed.Universitaria, Craiova, 2002.

[3] Buşneag, D., Piciu, D., *Lecţii de algebră*,Ed. Universitaria, Craiova, 2002.

[4] Năstăsescu, C., Niţă, C., Vraciu, C., *Bazele algebrei*, Ed.Academiei, Bucureşti, 1986.