ORIGINAL PAPER

SOME APPLICATIONS FROM STUDENT'S CONTESTS ABOUT THE GROUP OF AUTOMORPHISMS OF Z_n

GEORGIANA VELICU[1], ELENA CATALINA GRINDEI[2]

Manuscript received: 16.04.2015; Accepted paper: 28.05.2015;
Published online: 30.06.2015.

Abstract. *This article is a collection of a few interesting applications on finite groups and morphisms of groups, applications which already have been given to undergraduate's international and national contests, some of them using only basic ideas of modern and abstract algebra. Students studying algebra in school will obviously go further, as will those who are interested in one or more of the applications. The aim of this paper is to sustain students studying algebra and improve their ability to handle abstract ideas.*
Keywords: *group, generator, automorphism.*

1. INTRODUCTION

In mathematics a group is an algebraic structure, more specifically a nonempty set endowed with a low of composition which combine between them two elements, obtaining in this way a third element of the considered set. But to become a group, the set with its low of composition must satisfy some conditions, named the axioms of the group: associability, the existence of the neutral element and the existence of the symmetric of any element from the considered set. Although these properties called axioms are common for many algebraic structures like the sets of numbers, particularly the set of positive integers, the formulation of these axioms is well detached by the nature of the group and from its law. The existence of the groups in many domains of mathematics, but not only, makes them a principle of organization in contemporary mathematics.

The concept of group appeared in connection with the study of the polynomial equations, study made by the French mathematician Évariste Galois in the years 1830. After the contributions obtained from other domains, like number theory and geometry, the notion of group was generalized in the 70'. Studying groups, mathematicians developed several notations to split them in smaller parts 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 classification of all finite groups is a very difficult work. By Lagrange's theorem all finite groups of order *p*, where *p* is a prime positive integer, are cyclic groups and, obviously, commutative groups, which are denoted (up to an isomorphism) by Z_p. It is easy to prove that every group of order p^2 is also a commutative one, but this assertion can't be generalized to groups of order p^3; we have in this sense the example of the dihedral group D_4

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

of order 8 = 2^3, which is not a commutative one. Some algorithms can be used to generate lists of small groups, but we don't have yet a classification of all finite groups. An intermediate step was the classification of the finite and simple groups. We remind that a nontrivial group is a simple group if it's only normal subgroups is itself and the trivial subgroup, means the subgroup generated by the neutral element. Jordan-Hölder's theorem presents the simple groups like the constituents of all finite groups.

Making a list of all finite and simple groups was a great achievement in the group's theory and it is due to Richard Borcherds, laureate of Fields Medal in 1998 for the monstrous moonshine conjecture, an amazing connection between the largest sporadic group finite and simple and ,,the monster group" of order

$$|M| = 808\ 017\ 424\ 794\ 512\ 875\ 886\ 459\ 904\ 961\ 710\ 757\ 005\ 754\ 368\ 000\ 000\ 000$$
$$= 2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71$$

We also have to specify that the morphisms and isomorphisms are very important in the study of finite groups. Remind that in algebra an isomorphism (in Greek: isos = "equal" and morphe = "form") is an application between two sets equipped with an algebraic structure, application which satisfies two conditions:

1. is a morphism (means that the algebraic structure is preserved)
2. any isomorphism have an inverse, which is also a morphism (if f:A→B is an isomorphism, then does exist g:B→A , also a morphism so that g∘f = 1_A and f∘g = 1_B).

In this way, any two algebraic structures with the property that does exist between them an isomorphism are called **isomorphe**. As a consequence, any two algebraic structure being isomorphe, have the same properties. A special class of isomorphisms is the class of the **automorphisms** of a group. An automorphism of a group G is an isomorphism from G to G. The set of all automorphism of G is denoted by Aut(G).

Next, we present some important applications related to the automorphisms of an important group: the additive group of classes modulo-n, Z_n.

2. AUTOMORPHISMS FOR Z_n

First, we remind some properties of the automorphisms of $(Z_n,+)$, and next, we present a way to determine the number of the automorphisms of the additive group $Z_{p^2}\times Z_p$, where *p* is a prime number.

Remak. A class $\hat{a}\in Z_n = Z/nZ$ is a generator for the additive group Z_n if and only if the great common divisor of *a* and *n* is 1, $(a,n)=1$. In consequence, the number of the generators for Z_n is given by the Euler's function $\varphi(n)$.

Proof. First, we have: if $\hat{a}\in Z_n$ is a generator for Z_n, $Z_n = <\hat{a}>$, then there exist an element $u\in Z$ so that $\hat{1} = u\cdot\hat{a} \Rightarrow ua \equiv 1(\mathrm{mod}\, n) \Rightarrow n \mid ua-1 \Rightarrow \exists v\in Z$, and we obtain $ua - nv = 1 \Rightarrow (a,n)=1$.

Inverse, we have: $(a,n)=1 \Rightarrow \exists u,v\in Z$, then $au+nv=1$, so $au\equiv 1(\mathrm{mod}\, n) \Rightarrow \widehat{au} = \hat{1}$. Also, for any class $\hat{b}\in Z_n$ we have $\hat{b} = \hat{1}\cdot\hat{b} = \widehat{au}\cdot\hat{b} = \widehat{bu}\cdot\hat{a} \in <\hat{a}>$, then we have $<\hat{a}> = Z_n$.

Example. The additive group Z_{24}, $24 = 2^3 \cdot 3$, have $\varphi(24) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 8$ generators, and the set of generators is

$$Gen(Z_{24}) = \{\hat{k} \in Z_{24} \ / \ (k,24) = 1\} = \{\hat{1},\hat{5},\hat{7},\widehat{11},\widehat{13},\widehat{17},\widehat{19},\widehat{23}\}.$$

Remak. If $\hat{a} \in Z_n = Z/nZ$ is a generator for Z_n, then $\varphi : Z_n \to Z_n$, $\varphi(\hat{k}) = \widehat{ka}, \forall \hat{k} \in Z_n$, is an automorphism of Z_n, $\varphi \in Aut(Z_n)$.

Proof. It is obvious that φ is a morphism of groups:

$$\varphi(\hat{k_1} + \hat{k_2}) = \varphi(\widehat{k_1 + k_2}) = (\widehat{k_1 + k_2)a} = \widehat{k_1 a} + \widehat{k_2 a} = \varphi(\hat{k_1}) + \varphi(\hat{k_2}), \ \forall \hat{k_1}, \hat{k_2} \in Z_n.$$

The injectivity of φ: $\varphi(\hat{k_1}) = \varphi(\hat{k_2}),\ \hat{k_1}, \hat{k_2} \in Z_n \Rightarrow \widehat{k_1 a} = \widehat{k_2 a} \Rightarrow k_1 a \equiv k_2 a \,(\mathrm{mod}\, n) \Leftrightarrow (k_1 - k_2)a \equiv 0 \,(\mathrm{mod}\, n)$, but $\hat{a}$ is a generator for Z_n, so $(a,n) = 1$, and so we obtain $k_1 \equiv k_2 (\mathrm{mod}\, n) \Leftrightarrow \hat{k_1} = \hat{k_2}$. Because φ is defined fron Z_n to Z_n and it is injective, it is obvious that φ is a bijection. Finally we have that φ is an automorphism of Z_n.

Examples. By the previous remark we have:

$$|Aut(Z_2)| = 1;\ Aut(Z_3) \cong Z_2;\ Aut(Z_4) \cong Z_2;\ Aut(Z_p) \cong Z_{p-1}, p \text{ is a prime number}.$$

Proof. For Z_2 we obtain only one automorphism: $id_{Z_2} : Z_2 \to Z_2, id_{Z_2}(\hat{k}) = \hat{k}$, so $|Aut(Z_2)| = 1$. Also, the additive group Z_3 have two generators: $\hat{1}$ and $\hat{2}$, and for $\hat{1}$ we have the identity automorphism id_{Z_3}, and for $\hat{2}$ we have $\varphi : Z_3 \to Z_3$. $\varphi(\hat{k}) = \widehat{2k}$, with $\varphi(\hat{0}) = \hat{0}, \varphi(\hat{1}) = \hat{2}$ *and* $\varphi(\hat{2}) = \hat{1}$. In the same way, the group Z_4 have two generators: $\hat{1}$ and $\hat{3}$, and so, two automorphisms: the identity map id_{Z_4} and $\varphi : Z_4 \to Z_4$. $\varphi(\hat{k}) = \widehat{3k}$, with $\varphi(\hat{0}) = \hat{0}, \varphi(\hat{1}) = \hat{3}, \varphi(\hat{2}) = \hat{2}$ and $\varphi(\hat{3}) = \hat{1}$. In general, for a prime number *p*, the condition $(a, p) = 1$ implies $a \in \{1,2,..., p-1\}$, so Z_p have $p-1$ generators, and for every such a generator we obtain an automorphism of Z_p, $\varphi : Z_p \to Z_p, \varphi(\hat{k}) = \widehat{ka}, a \in \{1,2,..., p-1\}$, totally, $p-1$ automorhisms, and $Aut(Z_p) \cong Z_{p-1}$. Below we present the tables for the following groups: $(Aut(Z_4),\circ)$ and $(Z_2,+)$, from where we observe that they are isomorphe:

$(Aut(Z_4),\circ)$	id_{Z_4}	φ
id_{Z_4}	id_{Z_4}	φ
φ	φ	id_{Z_4}

$(Z_2,+)$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

An interesting question about the automorphisms of a group is: which of the automorphisms admits fixed points? For that we have the following affirmation:

Remark. The group Z_p, where *p* is a prime number, it's a group in which any automorphism, other than the identity, is an automorphism who admit a fixed point.

Proof. Let consider $f \in Aut(Z_p)$. We have: $f(\hat{k}) = a\hat{k}, a \in \{1,2,..., p-1\}$. If f have at least two fixed points, then $\exists \hat{k} \neq \hat{0}$ so that $f(\hat{k}) = \hat{k}$, then $a\hat{k} = \hat{k} \Rightarrow (a-1)\hat{k} = \hat{0} \Rightarrow p \mid a-1$, but $a \in \{1,2,..., p-1\}$, then $a = 1$. Finally we have: $f(\hat{k}) = \hat{k} \Leftrightarrow f = 1_{Z_p}$.

Consequence. $Aut(Z_n) \cong U(Z_n)$.

Proof. $Aut(Z_n) = \{ f : Z_n \to Z_n \,/\, f(\hat{x}) = xf(\hat{1}), \forall \hat{x} \in Z_n \text{ } and < f(\hat{1}) >= Z_n \} \Leftrightarrow$

$Aut(Z_n) = \{ f : Z_n \to Z_n \,/\, f(\hat{x}) = xf(\hat{1}), \forall \hat{x} \in Z_n$ and $f(\hat{1}) = \hat{k}, (k,n) = 1\}$, then $Aut(Z_n) \cong U(Z_n)$, much more, we have $|Aut(Z_n)| = \varphi(n)$, where $\varphi(n)$ is Euler's function.

We saw above, that the set of all automorphisms of the additive group Z_n is well defined. We are interested now to determine the group of automorphisms of the Cartesian product $Z_m \times Z_n, m,n \in N, m,n \geq 2$, which is also an additive group. We know that there exist an isomorphism $Z_m \times Z_n \cong Z_{mn}$ when $m,n \in N, m,n \geq 2$ are two positive integers with $(m,n) = 1$. Another important result is:

$$Aut(Z_2 \times Z_2) \cong S_3.$$

A simple proof of the existence of this isomorphism is: if we consider the set

$$A = \left\{ \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} \,/\, \hat{a},\hat{b},\hat{c},\hat{d} \in Z_2, (\hat{a} \neq \hat{0} \text{ } or \, \hat{b} \neq \hat{0}) \text{ } and \text{ } (\hat{c} \neq \hat{0} \text{ } or \, \hat{d} \neq \hat{0}) \text{ } and \text{ } (\hat{a} \neq \hat{c} \text{ } or \text{ } \hat{b} \neq \hat{d}) \right\}$$

$$\Leftrightarrow A = \left\{ \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix} \right\},$$

then it is obvious that $A \cong S_3$, and $\varphi : Aut(Z_2 \times Z_2) \to S_3$, defined by $\varphi(f) = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$, where $f(\hat{0},\hat{1}) = (\hat{a},\hat{b})$ and $f(\hat{1},\hat{0}) = (\hat{c},\hat{d})$, is an isomorphism of groups, then we have $Aut(Z_2 \times Z_2) \cong S_3$.

Next, we will specify the number of automorphisms of $Z_{p^2} \times Z_p$, where *p* is a prime number, and how they are defined on the generators. It is obvious that the identity map is an automorphism and, also, because $Z_{p^2} \times Z_p$ is an commutative group, we have that its interior automorphisms coincide with the identity map.

Remember that: if $(G,\cdot)$ is a group and $a \in G$ is an element from *G*, the application $\varphi_a : G \to G$, $\varphi_a(g) = a \cdot g \cdot a^{-1}, \forall g \in G$, is an automorphism of *G*, called *the interior automorphism of G.*

Application. If *p* is a prime number, then $\left|Aut(Z_{p^2} \times Z_p)\right| = p^3(p-1)^2$.

(Berkeley, 2003)

Solution. It is obvious that an automorphism of $Z_{p^2} \times Z_p$ is well determinated by the images of the generators $(\overline{1},\overline{\overline{0}})$ and $(\overline{0},\overline{\overline{1}}) \in Z_{p^2} \times Z_p$. So, the following map:

$$f : Z_{p^2} \times Z_p \to Z_{p^2} \times Z_p , \begin{cases} f(\overline{1},\overline{\overline{0}}) = (\overline{a},\overline{\overline{b}}) \\ f(\overline{0},\overline{\overline{1}}) = (\overline{c},\overline{\overline{d}}) \end{cases}, \text{ where } (\overline{a},\overline{\overline{b}}),(\overline{c},\overline{\overline{d}}) \in Z_{p^2} \times Z_p ,$$

is an automorhism if and only if $\overline{a} \in Z_{p^2}$ and $\overline{a} \notin pZ / p^2Z$, $\overline{\overline{b}} \in Z_p$, $\overline{c} \in Z_{p^2}$ and $\overline{c} \in pZ / p^2Z$, and also, $\overline{\overline{d}} \in (Z_p)^*$.

The direct implication is obvious, because if f is an automorphism of $Z_{p^2} \times Z_p$ with $f(\overline{1},\overline{\overline{0}}) = (\overline{a},\overline{\overline{b}})$ and $f(\overline{0},\overline{\overline{1}}) = (\overline{c},\overline{\overline{d}})$, then $(\overline{a},\overline{\overline{b}})$ is not canceled by p, but $(\overline{c},\overline{\overline{d}})$ must be canceled by *p*, and so we obtain that $\overline{a} \notin pZ / p^2Z$ and $\overline{c} \in pZ / p^2Z$. More, $(\overline{c},\overline{\overline{d}})$ can't be a multiple of $p(\overline{a},\overline{\overline{b}}) = (p\overline{a},\overline{\overline{0}})$, then $\overline{\overline{d}} \neq \overline{\overline{0}}$.

The reverse implication: considering two elements $(\overline{a},\overline{\overline{b}})$ and $(\overline{c},\overline{\overline{d}}) \in Z_{p^2} \times Z_p$ having the above properties, we have a morphism $g : Z_{p^2} \times Z_p \to Z_{p^2} \times Z_p$ so that $g(\overline{1},\overline{\overline{0}}) = (\overline{a},\overline{\overline{b}})$ and $g(\overline{0},\overline{\overline{1}}) = (\overline{c},\overline{\overline{d}})$, because $(\overline{a},\overline{\overline{b}})$ is canceled by p^2 and $(\overline{c},\overline{\overline{d}})$ by *p*. The condition $\overline{a} \notin pZ / p^2Z$ implies that $ord(\overline{a},\overline{\overline{b}}) = p^2$. The pair $(\overline{c},\overline{\overline{d}})$ can't be a multiple of $p(\overline{a},\overline{\overline{b}}) = (p\overline{a},\overline{\overline{0}})$, because $\overline{\overline{d}} \in (Z_p)^*$. Then we have, by the Lagrange's theorem, $\left|g(Z_{p^2} \times Z_p)\right| > p^2$. But $\left|g(Z_{p^2} \times Z_p)\right| = p^3$, then *g* is a surjective morphism and considering the fact that $Z_{p^2} \times Z_p$ is a finite group, we obtain *g* also injective, the *g* is an automorphism.

Now, let's count the pairs $(\overline{a},\overline{\overline{b}})$ and $(\overline{c},\overline{\overline{d}})$ with the above properties:

- for $\overline{a}$ we have $p^2 - p$ possibilities
- for $\overline{\overline{b}}$ we have *p* possibilities
- for $\overline{c}$ we have *p* possibilities
- for $\overline{\overline{d}}$ we have $p-1$ possibilities

totally there are $(p^2 - p) \cdot p^2 \cdot (p-1) = p^3(p-1)^2$ automorphisms of $Z_{p^2} \times Z_p$.

Examples: For $p = 2$, the group $Z_4 \times Z_2$ have 8 automorphisms. In the case of $p = 3$, the group $Z_9 \times Z_3$ have 108 automorphisms, and for $p = 5$, $Z_{25} \times Z_5$ have 2000 automorphisms. Next, we present the table for $Z_4 \times Z_2$, $p = 2$, and we specify all it's automorphisms and subgroups. Let's conside $Z_4 \times Z_2 = \{(\overline{x},\overline{\overline{y}}) / \overline{x} \in Z_4, \overline{\overline{y}} \in Z_2\}$.

+	$(\bar{0},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$
$(\bar{0},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$
$(\bar{0},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$
$(\bar{1},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$
$(\bar{1},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$
$(\bar{2},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$
$(\bar{2},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$
$(\bar{3},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$
$(\bar{3},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{1}})$	$(\bar{3},\bar{\bar{0}})$	$(\bar{0},\bar{\bar{1}})$	$(\bar{0},\bar{\bar{0}})$	$(\bar{1},\bar{\bar{1}})$	$(\bar{1},\bar{\bar{0}})$	$(\bar{2},\bar{\bar{1}})$	$(\bar{2},\bar{\bar{0}})$

Using Lagrange's theorem, if $H \le Z_4 \times Z_2$ is a subgroup, then $8 = |Z_4 \times Z_2| = |H| \cdot |Z_4 \times Z_2 : H|$, and we obtain $|H| \in \{1,2,4,8\}$. Analyzing the table we can specify the subgroups of $Z_4 \times Z_2$:

- one subgroup of order 1: $H_1^{(1)} = \{(\bar{0},\bar{\bar{0}})\}$;
- three subgroups of order 2: $H_2^{(1)} = \{(\bar{0},\bar{\bar{0}}),(\bar{0},\bar{\bar{1}})\} = <(\bar{0},\bar{\bar{1}})>$,
  $H_2^{(2)} = \{(\bar{0},\bar{\bar{0}}),(\bar{2},\bar{\bar{0}})\} = <(\bar{2},\bar{\bar{0}})>$ and
  $H_2^{(3)} = \{(\bar{0},\bar{\bar{0}}),(\bar{2},\bar{\bar{1}})\} = <(\bar{2},\bar{\bar{1}})>$
- four subgroups of order 4: $H_4^{(1)} = \{(\bar{0},\bar{\bar{0}}),(\bar{1},\bar{\bar{0}})\} = <(\bar{1},\bar{\bar{0}})>$
  $H_4^{(2)} = \{(\bar{0},\bar{\bar{0}}),(\bar{1},\bar{\bar{1}})\} = <(\bar{1},\bar{\bar{1}})>$
  $H_4^{(3)} = \{(\bar{0},\bar{\bar{0}}),(\bar{3},\bar{\bar{0}})\} = <(\bar{3},\bar{\bar{0}})>$ and
  $H_4^{(4)} = \{(\bar{0},\bar{\bar{0}}),(\bar{3},\bar{\bar{1}})\} = <(\bar{3},\bar{\bar{1}})>$
- one subgroup of order 8: $H_8^{(1)} = Z_4 \times Z_2$.

Because $Z_4 \times Z_2$ is a commutative group, all its subgroups are normal subgroups.

Now, let's present the set $Aut(Z_4 \times Z_2)$ of all automorphisms of $Z_4 \times Z_2$. From the above results we have $|Aut(Z_4 \times Z_2)| = 8$, where any isomorphism $f : Z_4 \times Z_2 \to Z_4 \times Z_2 \,/\, f$ have the properties $f(\bar{1},\bar{\bar{0}}) = (\bar{a},\bar{\bar{b}})$ and $f(\bar{0},\bar{\bar{1}}) = (\bar{c},\bar{\bar{d}})$, $(\bar{a},\bar{\bar{b}}),(\bar{c},\bar{\bar{d}}) \in Z_4 \times Z_2$, $\bar{a} \in Z_4$ and $\bar{a} \notin 2Z/4Z$, $\bar{\bar{b}} \in Z_2$, $\bar{c} \in Z_4$ and $\bar{c} \in 2Z/4Z$, and $\bar{\bar{d}} \in (Z_2)^*$.

We have: $2Z/4Z=\{\hat{x}/x\in 2Z\}$, $\hat{x}=\{y\in 2Z/x-y\in 4Z\}$, and if $x=2k_1$ and $y=2k_2$, where $k_1,k_2\in Z$, the condition $x-y\in 4Z$ is equivalent to $k_1-k_2\in 2Z \Leftrightarrow k_1\equiv k_2(\mathrm{mod}\,2)$, and then $k_1,k_2\in\{0,1\}$. In conclusion, we obtain $\hat{x}=\{\hat{0},\hat{2}\}$, $\forall x\in 2Z$, then $2Z/4Z=\{\hat{0},\hat{2}\}$. Finally, we have: $(\overline{a},\overline{\overline{b}})\in\{(\overline{1},\overline{\overline{0}}),(\overline{1},\overline{\overline{1}}),(\overline{3},\overline{\overline{0}}),(\overline{3},\overline{\overline{1}})\}$ and $(\overline{c},\overline{\overline{d}})\in\{(\overline{0},\overline{\overline{1}}),(\overline{2},\overline{\overline{1}})\}$, and we present all eight automorphisms of $Z_4\times Z_2$ in the table (1), of course how they are defined on generators, and in table (2) how they action on the elements of $Z_4\times Z_2$.

f_i	$f_i(\overline{1},\overline{\overline{0}})$	$f_i(\overline{0},\overline{\overline{1}})$
f_1	$(\overline{1},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{1}})$
f_2	$(\overline{1},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{1}})$
f_3	$(\overline{1},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$
f_4	$(\overline{1},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$
f_5	$(\overline{3},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{1}})$
f_6	$(\overline{3},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{1}})$
f_7	$(\overline{3},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$
f_8	$(\overline{3},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$	$(\overline{0},\overline{\overline{0}})$
$(\overline{0},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$
$(\overline{1},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{1}})$
$(\overline{1},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{0}})$
$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$	$(\overline{2},\overline{\overline{0}})$
$(\overline{2},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$	$(\overline{2},\overline{\overline{1}})$	$(\overline{0},\overline{\overline{1}})$
$(\overline{3},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{1}})$
$(\overline{3},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{1},\overline{\overline{1}})$	$(\overline{3},\overline{\overline{1}})$	$(\overline{1},\overline{\overline{0}})$	$(\overline{3},\overline{\overline{0}})$

REFERENCES

[1] J.R.Durbin, *Modern Algebra*, Ed.John Wiley, New York, 1985.
[2] D.Busneag, F.Chirtes, D.Piciu, *Probleme de algebra*, Ed.Universitaria, Craiova, 2002.
[3] C.Nastasescu, C.Nita, C.Vraciu, *Bazele algebrei*, Ed.Academiei, 1986.
[4] http://math.berkeley.edu/programs/graduate/prelim-exams/archive.