**TEORÍA DE LOS GRUPO-ANILLOS**

**Y SUS APLICACIONES**

*Hugo Allan García Monterrosa*

*hugoallangm@gmail.com*

*Licenciado en Matemática Aplicada*

*Asesor: Licenciado en Matemática Aplicada, William Roberto Gutiérrez Herrera*

**RESUMEN**

Se realizó el desarrollo de los grupo-anillos, una nueva estructura algebraica generada a partir de un grupo y un anillo dado, estudiando las conexiones entre la nueva estructura y las anteriores. Luego de estudiar las propiedades algebraicas de los grupo-anillos se hace un breve estudio de los códigos correctores, para finalizar con la relación que existe entre los códigos cíclicos y las grupo-álgebras.

***Palabras clave:*** *álgebra, grupos, anillos, códigos.*

**CUERPO**

El trabajo está estructurado en seis capítulos, cuyo contenido se describe a continuación:

El primer capítulo contiene todo el bagaje matemático que sirve de cimiento para un estudio adecuado de los grupo-anillos.

En el segundo capítulo se da la definición de un grupo-anillo y una grupo-álgebra, caso especial del anterior. Posteriormente, se establecen las condiciones necesarias y suficientes para que un grupo-anillo sea semisimple.

En el tercer capítulo se estudia la teoría de representación de grupos y su relación con los módulos de los grupo-anillos.

En el cuarto capítulo se estudian algunos elementos algebraicos de un grupo-anillo como los elementos nilpotentes, los idempotentes y las unidades de torsión.

En el quinto capítulo se da una breve introducción al estudio de las unidades de un grupo-anillo, mostrando algunas construcciones de unidades no triviales para los mismos.

Finalmente en el sexto capítulo se da una introducción a la teoría de códigos correctores, dando relevancia a los códigos cíclicos y mostrando que dichos códigos tienen una fuerte conexión con las grupo-álgebras.

**RESULTADOS**

Del estudio de los grupo-anillos se obtuvo:

1. Sea G un p-grupo abeliano finito. Entonces G se puede escribir como producto directo de p-subgrupos cíclicos. Dicha composición es única.
2. El grupo-anillo RG es semisimple si y sólo si las siguientes condiciones son verdaderas:

* R es un anillo semisimple
* G es finito
* |G| es invertible en R

1. Existe una biyección entre las representaciones de G en R y los RG-módulos libres de rango finito.
2. Si la característica del del campo no divide al orden del grupo, entonces el estudio de los grupos cíclicos es equivalente al estudio de ideales en grupo-álgebras.

**CONCLUSIONES**

1. Para el estudio de los grupo-anillos es importante conocer la estructura de los grupos abelianos y hamiltonianos, así como la teoría de módulos y el teorema de Wedderburn-Artin.
2. Las condiciones necesarias y suficientes para que un grupo-anillo sea semisimple, vienen dadas por el teorema de Maschke.
3. Toda representación de un anillo conmutativo sobre un grupo dado,
4. corresponde a un módulo del grupo-anillo correspondiente.
5. En general no es fácil encontrar unidades no triviales en grupo-anillos, pero es posible construir algunas usando elementos idempotentes.
6. Las grupo-álgebras dan estructura matemática a los códigos correctores conocidos como códigos cíclicos.
7. Cuando la característica del campo no divide al orden del grupo el estudio de los códigos cíclicos se reduce a estudiar los ideales de grupo-álgebras generadas por elementos idempotentes.

**RECOMENDACIONES**

1. Usar el primer capítulo como guía de temas para el desarrollo de un curso de álgebra moderna de pregrado.
2. Para el estudio de los códigos cíclicos, se puede utilizar los resultados del capítulo 2, en especial los de las secciones 2.3 y 2.4.
3. Estudiar la teoría de códigos correctores desde el punto de vista algebraico, permitiendo así dictaminar la capacidad correctora de los mismos.
4. Para la lectura de los capítulos 2 y 3 es importante tener conocimientos previos de teoría de grupos y anillos.
5. Implementar el estudio de teoría de módulos en el curso de álgebra 2 de la licenciatura en Matemática Aplicada de la USAC.

**BIBLIOGRAFÍA**

1. BELL, Eric. *Los grandes matemáticos*. Argentina: Editorial Losada, 1948.
2. BLAKE, Ian. *The mathematical theory of coding*. Estados Unidos: Academic Press Inc, 1975.
3. BURNSIDE, William. *The theory of groups of finite order*. 2da ed. Cambridge: Cambridge University Press, 1911.
4. CAUCHY, Augustin-Louis. Oeuvres complètes. 1era ed. Cambridge: Cambridge University Press, 2009.
5. DESKINS, Eugene.”Finite abelian groups with isomorphic group algebras". *Duke Mathematical Journal*. 1956, vol 23, núm. 1, p. 35-40.
6. FEIT, Walter, et al. “The solvability of groups of odd order". *Pacific J. Math*. 1963, vol 13, núm 3, p. 775-1029.
7. GOLDSHMIDT, David. “A group theoretic proof of the theorem for odd primes".*Mathematische Zeitschrift*. 1970, vol 113, núm. 5, p. 373-375.
8. HAWKINS, Thomas. “The origins of the theory of group characters". *Archive for History of Exact Sciences*. 1971, vol 7, núm. 2, p. 142-170.
9. HERSTEIN, Nathain. *Topics in algebra*. 2da ed. New York: Macmillah, 1986.
10. IAN, Connell. “On the group ring". *Canad. J. Math*. 1963, vol 15, núm 1, p. 650-685.
11. ISAACS, Martin. *Algebra: a graduate course*. Estados Unidos: Editorial Pacific Grove, 1940.

1. LANG, Serge. *Linear algebra*. 3ra ed. Nueva York: Springer-Verlag, 2004. 308 p.
2. POLCINO, César; SEHGAL, Sudarshan. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, 2002. 371 p.

**AGRADECIMIENTOS**

A Dios y a mi familia.

**AUTOR**

****

*Hugo Allan García Monterrosa*

*Licenciado en Matemática Aplicada*

*Facultad de Ingeniería*

*Universidad de San Carlos de Guatemala*

**THEORY OF GROUP RINGS**

**AND ITS APLICATTIONS**

*Hugo Allan García Monterrosa*

*hugoallangm@gmail.com*

*Degree in applied mathematics*

*Advisor: William Roberto Gutiérrez Herrera, Degree in applied mathematics*

**ABSTRACT**

Group Rings are developed from groups and rings, generating a new algebraic structure. In this paper connections between group rings and group and rings are made. After studying properties of group rings a very short study of correcting codes is made. Finally it is showed that there exists a relationship between cyclic codes and group algebras.

***Keywords:*** *algebra, groups, rings, codes.*

**BODY**

The paper is structured in six chapters. The first three have a similar structure, developing a theoretical description of each disciplines used for the application described in the fourth chapter.

In the first chapter the main concepts of algebra are developed, working harder in the main points to understand the theory of group rings.

In the second chapter group rings and group algebras are defined, showing that the second case is an especial one of the first case. Conditions for semisimplicity of a group rings are given in the Maschkes theorem.

The relationship between representations of a given group over a ring and modules over a group ring are given in the third chapter.

In the fourth chapter some algebraic elements are studied such as nilpotent elements, idempotent elements and torsion units.

In the fifth chapter a short introduction of units of group rings is given, showing that there are some recipes to build non trivial units.

Finally, in the sixth chapter it is presented a short introduction to code theory giving relevant importance to cyclic codes and showing that there exist a strong relationship between those kind of codes and group algebras.

**RESULTS**

Some highlights of this investigation are:

1. Let G be an abelian finite p-group, then G can be written as direct product of cyclic subgroups. This composition is unique.
2. RG is semisimply if and only if the following conditions are meet:

* R is a semisimple ring
* G is finite
* |G| is invertible in R.

1. There exists a bijection between representations of G over R and free RG-modules of finite rank.
2. If characteristic of the filed does not divide to the order of the group, then the study of cyclic codes is equivalent to the study of ideals in group algebras.

**CONCLUTIONS**

1. For the study of group rings it is important to know the structure of abelian and Hamiltonian groups and theory of modules and the Wedderburn-Artin theorem.
2. The necessary and sufficient conditions for a group ring to be semi simple are given by Maschke's theorem.
3. Any representation of a commutative ring over a given group corresponds to a module of the corresponding group ring.
4. In general it is not easy to find non-trivial units in group rings, but you can build some using idempotent elements.
5. The group algebras give mathematical support to correcting codes known as cyclic codes structure.

**RECOMMENDATIONS**

1. Use the first chapter as a guide of topics to develop a course of undergraduate modern algebra.
2. To study cyclic codes, you can use the results of Chapter 2, especially sections 2.3 and 2.4.
3. Study the theory of correcting codes from algebraic point of view to know in that way the corrective capacity of them.
4. To read Chapters 2 and 3 is important to have prior knowledge of the theory of groups and rings.
5. To implement the study of theory modules during algebra 2 degree in Applied Mathematics at USAC.

**BIBLIOGRAPHY**

1. BELL, Eric. *Los grandes matemáticos*. Argentina: Editorial Losada, 1948.
2. BLAKE, Ian. *The mathematical theory of coding*. Estados Unidos: Academic Press Inc, 1975.
3. BURNSIDE, William. *The theory of groups of finite order*. 2da ed. Cambridge: Cambridge University Press, 1911.
4. CAUCHY, Augustin-Louis. Oeuvres complètes. 1era ed. Cambridge: Cambridge University Press, 2009.
5. DESKINS, Eugene.”Finite abelian groups with isomorphic group algebras". *Duke Mathematical Journal*. 1956, vol 23, núm. 1, p. 35-40.
6. FEIT, Walter, et al. “The solvability of groups of odd order". *Pacific J. Math*. 1963, vol 13, núm 3, p. 775-1029.
7. GOLDSHMIDT, David. “A group theoretic proof of the theorem for odd primes".*Mathematische Zeitschrift*. 1970, vol 113, núm. 5, p. 373-375.
8. HAWKINS, Thomas. “The origins of the theory of group characters". *Archive for History of Exact Sciences*. 1971, vol 7, núm. 2, p. 142-170.
9. HERSTEIN, Nathain. *Topics in algebra*. 2da ed. New York: Macmillah, 1986.
10. IAN, Connell. “On the group ring". *Canad. J. Math*. 1963, vol 15, núm 1, p. 650-685.
11. ISAACS, Martin. *Algebra: a graduate course*. Estados Unidos: Editorial Pacific Grove, 1940.
12. LANG, Serge. *Linear algebra*. 3ra ed. Nueva York: Springer-Verlag, 2004. 308 p.
13. POLCINO, César; SEHGAL, Sudarshan. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, 2002. 371 p.

**ACKNOWLEDGEMENTS**

To God and my family.

**AUTHOR**

****

*Hugo Allan García Monterrosa*

*Degree in applied mathematics*

*Engineering School*

*Universidad de San Carlos de Guatemala*