

THE MULTIPLICATIVE GROUP OF UNITS OF A RING

GHIODEL GROZA

*Department of Mathematics,
Technical University of Civil Engineering,
Lacul Tei 124, Bucharest 020396, Romania.
E-mail: grozag@mail.utcb.ro*

Abstract

Let R be a ring with a multiplicative identity. This paper is an introduction to the study of multiplicative group of units $U(R)$ of the ring R . Here we recall briefly those notions needed to understand some results on this subject.

Introduction

Throughout this paper the symbol R will be used to denote an associative ring with a multiplicative identity. An element of R is called a *unit* if it has an inverse. If ' a ' and ' b ' are units, then a^{-1} and ab are units. Hence it follows that the units of a ring R form a group $U(R)$ with respect to multiplication.

The study of the group of units of a ring plays a dominant role in algebra. Traditionally this study consists of two distinct directions. The first of these deals with the properties of the group of units of a particular ring whereas the second one concerns with all the rings that have their groups of units isomorphic to a given group. In this article we offer a collection of notions and results on these subjects.

1. The group of units of particular rings

There are many important results on the group of units of particular rings. For example it is well-known that the multiplicative group Q^* of rational numbers is isomorphic with a direct sum of the additive group $Z/(2)$ and a countable direct sum of infinite cyclic groups and the multiplicative group of the finite field $Z/(p)$ is a cyclic group of order $p-1$.

A multiplicative group G is *periodic* if each $g \in G$ is a finite order, that is, $g^m = 1$ for some positive integer m . If K is a field, the elements of finite order of K^* form a periodic subgroup PK^* whose structure is given in the following theorem ([4], Ch. XVIII):

Theorem 1. *If K is a field of characteristic zero, a periodic group is isomorphic with PK^* if and only if it is isomorphic with a subgroup of the additive group \mathbf{Q}/\mathbf{Z} having elements of order 2.*

An abelian multiplicative group G is *divisible* if for every $g \in G$, and every integer m there exists an element h in G with $h^m = g$. It is easy to see that the additive group of rational numbers \mathbf{Q} is a divisible group. If p is prime number, the subgroup of C^* of all p^n -th roots of units for $n = 0, 1, 2, \dots$ is also a divisible group denoted by $\mathbf{Z}(p^\infty)$. the next theorem gives a complete determination of divisible abelian group ([4], Ch. IV or [8], §5).

Theorem 2. *A divisible abelian group is a direct sum of groups each isomorphic to the additive group of rational numbers or to $\mathbf{Z}(p^\infty)$ for various primes p .*

By Theorems 1 and 2 it follows the structure of the group K^* , if K is either an algebraically closed field, or a field which is a finite extension of its prime field ([4], Ch. XVIII).

Theorem 3. *If K is an algebraically closed field, then a group is isomorphic with K^* if and only if it is isomorphic with a group which has either the form*

$$\mathbf{Q}/\mathbf{Z} \oplus \bigoplus_n \mathbf{Q},$$

If the characteristic of K is zero, or

$$\bigoplus_{p_i \neq p} \mathbf{Z}(p_i^\infty) \oplus \bigoplus_n \mathbf{Q},$$

if the characteristic of K is $p \neq 0$. Here n is an infinite cardinal number or $n = 0$ (only in the second case), p_i are prime numbers and the groups $\mathbf{Z}(p_i^\infty)$ are considered additive groups.

Theorem 4. *If K is a field which is a finite extension of its prime field, then a group is isomorphic with K^* if and only if it is isomorphic with a group which has either the form*

$$\mathbf{Z}/(m) \oplus \bigoplus_{\aleph_0} \mathbf{Z},$$

where m is an even positive integer, if the characteristic of K is zero, or

$$\mathbf{Z}/(p^n - 1),$$

with n a positive integer, if the characteristic of K is $p \neq 0$.

If K be a number field, that is a subfield of the field of complex numbers C which is a finite extension of the field of rational numbers Q , an element x of K is called an *algebraic integer* if it is a root of a monic polynomial with coefficients in Z . All algebraic integers of K form a ring called the *number ring* of K . It is well known *the unit theorem* of Dirichlet in a number ring ([9], Ch. 5).

Theorem 5. *Let K be a number field and let r and $2s$ denote the number of real and non-real embedding of K in C . If R is the number ring of K , then $U(R)$ is the direct product $G \times H$, where G is a finite cyclic group consisting of the roots of 1 in K and H is a free abelian group of rank $r+s-1$.*

A field K is called *formally real* if the only relations of the form $\sum_{i=1}^r x_i^2 = 0$ in K are those for which every $x_i = 0$. K is called *real closed* if it is formally real and no proper algebraic extension of K is formally real. Any real closed field can be ordered in one and only one way. The following theorem gives the structure of the multiplicative group of units of a real closed field ([4], Ch. XVIII).

Theorem 6. *Let K be a real closed field. Then a group is isomorphic with K^* if and only if it is isomorphic with a group which has the form*

$$\mathbf{Z}/(2) \oplus_n \mathbf{Q},$$

where n is an infinite cardinal number.

If we consider Q_p the field of p -adic numbers and Z_p the ring of p -adic integers, where p is a prime number, then it is known the following result ([4], Ch. XVIII).

Theorem 7. *A group is isomorphic with Q_p^* if and only if it is isomorphic with an additive group that has either the form*

$$\mathbf{Z} \oplus \mathbf{Z}/(p-1) \oplus \mathbf{Z}_p,$$

if p is an odd prime number, or the form

$$\mathbf{Z} \oplus \mathbf{Z}/(2) \oplus \mathbf{Z}_2,$$

if $p=2$.

If R is a commutative ring and G is a multiplicative group, then the *group ring* $R[G]$ consists of all formal finite sums of the form $\sum_{g \in G} a_g g$ with a_g in R . Then $R[G]$ is an associative R -algebra with multiplication defined distributively using the

group multiplication in G . If K is a field, one of the interesting problems in-group rings concerns classifying those situations in which $U(K[G])$ have particularly nice properties.

A group G is *nilpotent* if it possesses a finite normal series $G = A_0 \supseteq A_1 \supseteq \dots \supseteq A_r = \{1\}$, in which A_{i-1}/A_i is in the center of G/A_i for $i=1,2,\dots,r$. If G is a group, the subgroup G' generated by all the commutators $(x, y) = x^{-1}y^{-1}xy$, where $x, y \in G$, is called *commutator subgroup* or *derived group*. A group G is said to be *solvable* if the sequence $G \supseteq G' \supseteq G'' \supseteq \dots \supseteq G^{(i)} \supseteq \dots$, where each $G^{(i)}$ is the derived group of the preceding, terminates in the identity in a finite number of steps, say, $G^{(r)} = \{1\}$.

The case in which $U(K[G])$ is assumed to be nilpotent has been completely settled by Khripta and by Fisher, Parmenter and Sehgal. On the other hand, the complete determination of those situation with $U(K[G])$ solvable is more difficult. If K is a field and G a finite group the problem was solved by Passman ([10], p. 1132) and by Bovdi for a field of characteristic p and a nilpotent group. In [1] Bovdi gave a survey of results and unsolved problems concerning the group of units of $U(K[G])$, where K is a field of characteristic p . A group P is a *p-group* if every element of P except the identity has order a power of a prime p . Here we are given only the following two results.

Theorem 8. *Let K be a field of characteristic $p > 2$ and let P be a nontrivial p -Sylow subgroup of the torsion group G . The non abelian group $U(K[G])$ is solvable if and only if the commutator subgroup of G is a finite p -group or K is the field of three elements, the 3-Sylow subgroup P is a finite normal subgroup and the factor group $\bar{G} = G/P$ satisfies one of the following conditions:*

- a) \bar{G} is an extension of an elementary abelian 2-group A by a group $\langle b \rangle$ of order 2;
- b) \bar{G} is an extension of an abelian group A of exponent 4 by a group $\langle b \rangle$ of order 2 and $bab^{-1} = a^{-1}$ for all $a \in A$;
- c) \bar{G} is an extension of an abelian group A of exponent 8 by a group $\langle b \rangle$ of order 2 and $bab = a^3$ for all $a \in A$;
- d) \bar{G} is a direct product of the group.

$$\langle a, b \mid a^4 = b^4 = 1, (a, b)^2 = 1, (a, b, a) = (a, b, b) = 1 \rangle$$

of order 32 and the elementary abelian 2-group.

Theorem 9. *Let K be a field of characteristic 2 and assume that 2-Sylow subgroup of the torsion group G is nontrivial. The non abelian group $U(K[G])$ is*

solvable if and only if there exists a finite normal 2-group N such that the factor group $\bar{G} = G/N$ satisfies one of the following conditions:

- a) \bar{G} is abelian;
- b) $|K|=2$ and \bar{G} is an extension of an abelian group A by a group $\langle b \rangle$ of order 2, where A is a direct product of a bounded abelian 2- group of finite exponent and an elementary 3-group W and $bab = a^3$ for all $a \in W$;
- c) \bar{G} is a direct product of an abelian group W having no element of order 2 and a 2-group B with the following properties:

- 1. B has an abelian normal subgroup of index 2;
- 2. $B/C(B)$ is a group of finite exponent, where $C(B)$ is the center of B .

2. Rings, which have their groups of units isomorphic to a given group

If R is a ring, the intersection of the maximal right ideals of R is a two-sided ideal $J(R)$ of R which is called the *Jacobson radical* of R . A ring R is called a *ring with minimum condition* for right (left) ideals (a right (left) *artinian ring*) if and only if in every non-empty set of right (left) ideals in R , partially ordered by inclusion, there exists a minimal element. If R is a right (left) artinian ring and $R/J(R)$ is isomorphic to the complete matrix ring over a division ring, then R is called a *primary ring* and if $R/J(R)$ is a division ring, R is called a *completely primary ring*. We remark that a commutative artinian ring is a primary ring if and only if it is a completely primary ring.

In [5] Gilmer determined those finite commutative rings R having a cyclic multiplicative group of units. Since R is a direct sum of primary rings R_1, R_2, \dots, R_n and $U(R)$ is the direct product of $U(R_1), U(R_2), \dots, U(R_n)$, $U(R)$ is cyclic if and only if each $U(R_i)$ is cyclic and for $1 \leq i < j \leq n$, $\left(\left| U(R_i) \right|, \left| U(R_j) \right| \right) = 1$. Hence it follows that we can consider R a finite commutative primary ring. The main result of Gilmer is the following:

Theorem 10. *Each of the following classes consists of finite primary commutative rings R having a cyclic multiplicative group of units. Any finite commutative primary ring with a cyclic multiplicative group of units is isomorphic to an element of one and only one of these classes.*

- a) $GF(p^k)$;
- b) $Z/(p^m)$, where p is an odd prime and $m > 1$;
- c) $Z/(4)$;
- d) $Z/(p)[X]/(X^2)$, where p is a prime;
- e) $Z/(2)[X]/(X^3)$;
- f) $Z/(4)[X]/(2X, X^2-2)$.

This result was extended ([3], p. 248) to artinian rings having a cyclic group of units and then ([6], p. 148) to artinian rings R having all Sylow subgroups of $U(R)$ cyclic groups.

A commutative ring such that its non-units form an ideal is called a *local ring*. If R is a finite completely primary ring it is known that the following result ([7], p. 256) which gives a representation of all finite completely primary rings having a nilpotent group of units by means of a finite p -group and homomorphic image of a polynomial ring.

Theorem 11. *Let R be a finite completely primary ring. Then $U(R)$ is a nilpotent group if and only if R is a homomorphic image of the group algebra $C[P]$ so that the following holds:*

P is a finite p -group, where p is a prime number; C is a homomorphic local image of the ring $\mathbf{Z}/(p^r)[X]/(X^{p^s}-1)$, where r and s are positive integers.

A crossed product $S(G, \gamma, \sigma)$ is an associative ring determined by a ring S with a multiplicative identity, a multiplicative group G , a map $\sigma : G \rightarrow \text{Aut } S$ and a factor set γ , that is a map $\gamma : G \times G \rightarrow U(S)$ such that, for all $a \in S$ and $g_1, g_2, g_3 \in G$,

$$\gamma(g_1, g_2 g_3) \gamma(g_2, g_3) = \gamma(g_1 g_2, g_3) \gamma(g_1, g_2)^{g_3 \sigma}$$

and

$$a^{g_1 \sigma g_2 \sigma} = \gamma(g_1, g_2)^{-1} a^{(g_1 g_2) \sigma} \gamma(g_1, g_2).$$

The elements of $S(G, \gamma, \sigma)$ are expressions $\sum_{g \in G} t_g a_g$, where $a_g \in S$ and $a_g = 0$ for all but a finite number of $g \in G$. We consider

$$\sum_{g \in G} t_g a_g = \sum_{g \in G} t_g b_g$$

if and only if $a_g = b_g$ for all $g \in G$ and we define

$$\sum_{g \in G} t_g a_g + \sum_{g \in G} t_g b_g \equiv \sum_{g \in G} t_g (a_g + b_g),$$

$$\left(\sum_{g \in G} t_g a_g \right) \left(\sum_{h \in G} t_h b_h \right) \equiv \sum_{g, h \in G} t_{gh} \gamma(g, h) a_g^{h \sigma} b_h.$$

We note also that the element $t_1\gamma(1,1)^{-1}$ is the multiplicative identity for $S(G, \gamma, \sigma)$. Moreover the elements t_g are units and

$$t_g^{-1} = \left(\gamma(1,1)\gamma(g^{-1}, g) \right)^{-1} t_{g^{-1}} .$$

Let R be a right artinian ring. A two-sided ideal I in R is said to be *indecomposable* if it is impossible to express I as a direct sum of two non-zero two-sided ideals of R . If $R = I_1 \oplus I_2 \oplus \dots \oplus I_s$ is any decomposition of R into two-sided indecomposable ideals, the direct summands I_j are called the *blocks* of A ([2], Ch. VII). If $J(R) = (0)$, R is called a *semi-simple ring*. R is called a *simple ring*, if the only two-sided ideals of R are the trivial ones (0) and R . If R is a semi-simple ring, then R is the direct sum of a finite number of simple rings ([2], Ch. IV) which are called the *simple components* of R . Finally we give a representation of a large class of right artinian rings, including all the finite-dimensional algebras over a field of characteristic $p > 2$, having a nilpotent group of units ([7], p. 259).

Theorem 12. *The following properties of the ring R are equivalent:*

a) R is a right artinian ring finitely generated over its center, its prime subring R_0 is a finite ring, every block of R is an artinian ring such that at most one simple component of the ring $R/J(R)$ is a field of order 2 and $U(R)$ is a nilpotent group.

b) R is a direct sum of the rings R_1, R_2, \dots, R_n , where every R_i is a homomorphic image of a crossed product of the form $S(G, \gamma, \sigma)/I$ so that the following four conditions hold:

1) S is a completely primary artinian ring and there exists a finite p -group P , where p is a prime number, so that $S \cong C[P]/L$, where L is a two-sided ideal of the group algebra $C[P]$ of the p -group P over the local commutative artinian ring C of characteristic a power of p . Moreover $\bar{P}^{g\sigma} \subset \bar{P}$ for all $g \in G$, where \bar{P} is the image of P in S .

2) G is a direct product $G = \langle g_1 \rangle \times \dots \times \langle g_r \rangle$ of non-trivial cyclic groups.

3) $\gamma(g', g'') \in \bar{P}$ for all $g', g'' \in G$ and $\gamma(1,1) = 1$.

4) I is a finitely generated two-sided ideal so that

$$I = \sum_{i=1}^r S(G, \gamma, \sigma)x_i S(G, \gamma, \sigma) + \sum_{k=1}^s S(G, \gamma, \sigma)y_k S(G, \gamma, \sigma),$$

and every x_i is of the type $t_{g_i}^{n(i)} + t_{g_i}^{n(i)-1}a_{i1} + \dots + a_{in(i)}$, with $a_{ij} \in S$, $n(i)$ are positive integers and there exists a positive integer m such that

$$\{y_1, \dots, y_s\} = \{(z_1, \dots, z_m) - t_1 \mid z_i \in \{t_{g_1}, \dots, t_{g_r}\} \cup \bar{P}; i = 1, 2, \dots, m\},$$

where (z_1, \dots, z_m) are commutators.

References

- [1] A. Bovdi, *The group of units of group algebra of characteristic p*, Publ. Math. Debrecen, **52** (1998), No. 1-2, 193-244.
- [2] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons, Inc., New York, 1962.
- [3] K. E. Eldridge, I. Fischer, *D.C.C. rings with a cyclic group of units*, Duke Math. J., **34** (1967), 243-248.
- [4] L. Fuchs, *Infinite abelian groups*, vols. I, II, Academic Press, New York, 1973.
- [5] R.W. Gilmer, *Finite rings having a cyclic multiplicative group of units*, Amer. J. Math, **85** (1963), 447-452.
- [6] G. Groza, *on certain properties of rings with minimum condition*, Simon Stevin, **59** (1985), No.2, 141-151.
- [7] G. Groza, *Artinian rings having a nilpotent group of units*, J. Algebra, **121** (1989), No. 2, and 253-262.
- [8] I. Kaplansky, *Infinite abelian groups*, University of Michigan Press, 1956.
- [9] D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.
- [10] D. S. Passman, *Observations on group rings*, Comm. In Algebra, **5** (1977), 1119-1162.