Journal de Mathématiques
Mathématiques et Applications
Fondamentales & Informatique
JMMAFI, ISSN 2411-7188, **vol.5**,
2018, pp. 1-5

REMARK ON FINITE COMMUTATIVE RINGS

Harinaivo ANDRIATAHINY[1]

Mention: Mathématiques et Informatique,
Domaine: Sciences et Technologies,
Université d' Antananarivo, B.P. 906 Ankatso,
101 Antananarivo, Madagascar

Résumé
On sait que tout anneau commutatif fini se décompose de façon unique en une somme directe d'anneaux locaux. Dans ce papier, une nouvelle approche pour prouver ce résultat important est présentée.

Mots-clés. Anneau commutatif fini, anneau local, idéal, élément nilpotent, idempotent.

abstract
It is known that every finite commutative ring decomposes uniquely as a direct sum of local rings. In this paper, a new approach to prove this important result is presented.

Keywords. Finite commutative ring, local ring, ideal, nilpotent element, idempotent.

1 Introduction

The structure theorem of finite commutative rings states that any finite commutative ring may be expressed uniquely as a direct sum of finite local comutative rings. Therefore, the theory of finite commutative rings is reduced to a characterization of local commutative rings. Local rings have an important geometric aspect (cf M. Nagata [7]).
The structure theorem of finite commutative rings may be considered as a special case of the Krull-Remak-Schmidt decomposition theorem (cf S. Lang [5]).
Finite commutative ring theory has important applications in various areas like algebraïc cryptography, analysis of algorithms and coding theory.
Many authors studied the structure theorem of finite commutative rings, for instance cf B.R. McDonald [6] and G. Bini, F. Flamini [1].
We give here a new proof of this famous theorem. In fact, we provide an internal decomposition of a finite commutative ring.

[1]E-mail: hariandriatahiny@gmail.com

This paper is organized as follows. In section 2, we recall a property of finite domains. The section 3 is devoted to develop the new approach for the study of the structure of finite commutative rings. In section 4, an example is given.

2 Preliminaries

All rings will be commutative with identity $1 \neq 0$. Ideals do not contain 1. The divisors of 1 are called units. A ring D without zero-divisors is called a domain. This means that for any $a \in \mathrm{D}^\star := \mathrm{D}\backslash\{0\}$, the endomorphism

$$\begin{aligned} \phi : \quad & \mathrm{D} \longrightarrow \mathrm{D} \\ & x \longmapsto a \cdot x \end{aligned}$$

is injective.
If D is finite, these maps are also surjective, so D is a field.

3 The decomposition

From now on, we consider a finite ring R and its prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$. The residue class rings $\mathrm{R}/\mathfrak{P}_\tau$ are finite domains, so they are fields and it follows that the $\mathfrak{P}_\tau$ are maximal ideals.
Put

$$\mathfrak{A}_\tau := \bigcap_{\sigma \neq \tau} \mathfrak{P}_\sigma.$$

3.1 Proposition. *The ideal sum* $\mathfrak{P}_\tau + \mathfrak{A}_\tau$ *equals* R.

Proof. We have $\mathfrak{P}_i + \mathfrak{P}_j = \mathrm{R}$ for $i \neq j$. Let $\tau \in \{1, \ldots, t\}$. We have $\mathfrak{A}_\tau = \bigcap_{\sigma \neq \tau} \mathfrak{P}_\sigma = \prod_{\sigma \neq \tau} \mathfrak{P}_\sigma$. And $\prod_{\sigma \neq \tau} (\mathfrak{P}_\tau + \mathfrak{P}_\sigma) = \mathfrak{P}_\tau \cdot \mathcal{I} + \mathfrak{A}_\tau = \mathrm{R}$ where $\mathcal{I}$ is an ideal of R. Since $\mathfrak{P}_\tau \cdot \mathcal{I} \subseteq \mathfrak{P}_\tau$, then the proposition is proved. □

Therefore, the intersection $\mathfrak{P}_\tau \cap \mathfrak{A}_\tau$ is equal to the ideal product $\mathfrak{P}_\tau \cdot \mathfrak{A}_\tau$. We have also the following property.

3.2 Corollary. $\mathfrak{P}_\tau^n + \mathfrak{A}_\tau^n = \mathrm{R}$ *for* $n = 1, 2, \ldots$.

Proof. We have $\mathfrak{P}_\tau + \mathfrak{A}_\tau = \mathrm{R}$. Thus $1 = a_1 + a_2$ with $a_1 \in \mathfrak{P}_\tau$ and $a_2 \in \mathfrak{A}_\tau$. Then $1 = (a_1 + a_2) \cdot (a_1 + a_2) = a_1^2 + 2a_1a_2 + a_2^2 = a_1^2 + 2a_1a_2(a_1 + a_2) + a_2^2 = (a_1^2 + 2a_1^2a_2) + (2a_1a_2^2 + a_2^2) \in \mathfrak{P}_\tau^2 + \mathfrak{A}_\tau^2$. Thus, $\mathfrak{P}_\tau^2 + \mathfrak{A}_\tau^2 = \mathrm{R}$. The result is obtained by continuing in this way. □

Define the radical $\mathfrak{R} := \mathrm{Rad}(\mathrm{R})$ of the ring R by

$$\mathfrak{R} := \mathfrak{P}_1 \cap \ldots \cap \mathfrak{P}_t.$$

Therefore,

$$\mathfrak{R} := \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_t.$$

If x is in $\mathfrak{R}$, so are its powers x^i ($i \in \mathbb{N}$), but these are not all different, since $\mathfrak{R}$ is finite. So there is a first $j \in \mathbb{N}$ with $x^j = x^{j+k}$ for some $k > 0$. We get $x^j(1 - x^k) = 0$. Since $x^k \in \mathfrak{R}$, the element $1 - x^k$ cannot be in any $\mathfrak{P}_\tau$. So $1 - x^k$ is a unit in R. And we get $x^j = 0$. Clearly, j is the smallest integer with $x^j = 0$. We call j the depth of x. So all elements of $\mathfrak{R}$ are nilpotent. Since $\mathfrak{R}$ is finite, some ideal product $\mathfrak{R} \cdot \ldots \cdot \mathfrak{R} = \mathfrak{R}^m$ is zero. The depth of $\mathfrak{R}$ is the smallest such $m \geq 0$. So we have

$$\mathfrak{P}_1^m \cdot \ldots \cdot \mathfrak{P}_t^m = \{0\} \tag{1}$$

for $m = \text{Depth}(\mathfrak{R})$.
Put

$$\mathfrak{Q}_\tau := \mathfrak{P}_\tau^m.$$

Then, (1) may be interpreted as the Noether-Lasker decomposition of $\{0\}$ in the ring R (cf O.Zariski, P. Samuel [8]), i.e.

$$\{0\} = \mathfrak{Q}_1 \cap \ldots \cap \mathfrak{Q}_t.$$

3.3 Proposition. *We have* $\mathfrak{P}_\tau^m = \{x \in \text{R} \mid x \cdot \mathfrak{A}_\tau^m = \{0\}\}$.

Proof. Since $\mathfrak{P}_\tau^m \cdot \mathfrak{A}_\tau^m = \{0\}$, then $\mathfrak{P}_\tau^m \subseteq \{x \in \text{R} \mid x \cdot \mathfrak{A}_\tau^m = \{0\}\}$. Conversely, let $x \in \text{R}$ such that $x \cdot \mathfrak{A}_\tau^m = \{0\}$. We have $1 = a + b \in \mathfrak{P}_\tau^m + \mathfrak{A}_\tau^m$, and then $x = xa + xb = xa \in \mathfrak{P}_\tau^m$. □

3.4 Proposition. *We have*

$$\text{R} = \mathfrak{A}_1 + \ldots + \mathfrak{A}_t.$$

Proof. The ideal sum is not contained in any maximal ideal of R. □

And we also have

3.5 Proposition.

$$\text{R} = \mathfrak{A}_1^m + \ldots + \mathfrak{A}_t^m. \tag{2}$$

Proof. The sum $\mathfrak{A}_1^m + \ldots + \mathfrak{A}_t^m$ is not contained in any maximal ideal of R. □

3.6 Corollary. *We have*

$$1 = e_1 + \ldots + e_t \tag{3}$$

with $e_\tau \in \mathfrak{A}_\tau^m$ *for all* τ,

$$e_\sigma \cdot e_\tau = 0 \quad \textit{for} \quad \sigma \neq \tau \tag{4}$$

and

$$e_\tau = e_\tau \cdot e_\tau \quad \textit{for all} \quad \tau. \tag{5}$$

Proof. (3) comes from (2).
We have $\mathfrak{A}_\sigma^m \cdot \mathfrak{A}_\tau^m \subseteq \mathfrak{P}_1^m \cdot \ldots \cdot \mathfrak{P}_t^m = \{0\}$ for $\sigma \neq \tau$. So we have (4).
By (3), $e_\tau = 1 \cdot e_\tau = e_\tau \cdot e_\tau$. Thus, we have (5). □

The set $\{e_1, \ldots, e_t\}$ in the above Corollary is called an orthogonal set of idempotents (cf C.W. Curtis and I. Reiner [3]).

3.7 Proposition. *The kernel of the homomorphism*

$$\begin{aligned} \psi : \quad \text{R} &\longrightarrow \text{R} \cdot e_\tau \\ x &\longmapsto x \cdot e_\tau \end{aligned}$$

is $\mathfrak{P}_\tau^m$.

Proof. Let $x \in \mathfrak{P}_\tau^m$. We have $x \cdot e_\tau \in \mathfrak{P}_\tau^m \cdot \mathfrak{A}_\tau^m = \{0\}$. Then $x \in \ker(\psi)$.
Conversely, let $x \in \mathrm{R}$ such that $\psi(x) = 0$, i.e. $x \cdot e_\tau = 0$. Let $a \in \mathfrak{A}_\tau^m$. By (3), we have $a = e_\tau \cdot a$. Then $x \cdot a = (x \cdot e_\tau) \cdot a = 0$. Thus $x \in \mathfrak{P}_\tau^m$ from Proposition 3.3. □

But $\mathrm{R}/\mathfrak{P}_\tau^m$ have the only maximal ideal $\mathfrak{P}_\tau/\mathfrak{P}_\tau^m$, then the ring $\mathrm{R}/\mathfrak{P}_\tau^m$ is local. Furthermore, we have

$$\mathrm{R}/\mathfrak{P}_\tau^m \cong \mathrm{R} \cdot e_\tau. \tag{6}$$

3.8 Theorem. *We have the unique direct sum decomposition of the finite commutative ring* R*:*

$$\mathrm{R} = \mathrm{L}_1 \oplus \ldots \oplus \mathrm{L}_t \tag{7}$$

where $\mathrm{L}_\tau := \mathrm{R} \cdot e_\tau$ *is local and* e_τ *is defined by (3) for all* $\tau \in \{1, \ldots, t\}$.

Proof. By (6), the L_τ are local. From (3), we have $\mathrm{R} = \mathrm{L}_1 + \ldots + \mathrm{L}_t$. This is a direct sum because if $a_1 + \ldots + a_t = 0$ with $a_i \in \mathrm{R} \cdot e_i$ for all i, then $0 = e_1(a_1 + \ldots + a_t) = e_1 \cdot a_1 = e_1(x_1 \cdot e_1) = x_1 \cdot e_1^2 = x_1 \cdot e_1 = a_1$ where $x_1 \in \mathrm{R}$. In the same manner, we have $a_i = 0$ for all i. The unicity of the decomposition is straightforward. □

4 Example

Consider $\mathrm{R} = \mathbb{Z}/\mathbb{Z}n$ with $n = p_1^{i_1} \cdot \ldots \cdot p_t^{i_t}$. In this case, we have $m = \max(i_1, \ldots, i_t)$, $\mathfrak{R} = \mathbb{Z}p_1 \cdot \ldots \cdot p_t/\mathbb{Z}n$, and $\mathrm{L}_\tau \cong \mathbb{Z}/p_\tau^{i_\tau}$. Then we have the decomposition

$$\mathbb{Z}/p_1^{i_1} \cdot \ldots \cdot p_t^{i_t} \;\cong\; \mathbb{Z}/p_1^{i_1} \times \ldots \times \mathbb{Z}/p_t^{i_t}.$$

References

[1] G. Bini, F. Flamini, Finite commutative rings and their applications, *Kluwer Academic Publishers*, 2002.

[2] N. Bourbaki, Algèbre Commutative, Chapitre 3, *Masson*, 1983.

[3] C.W. Curtis and I. Reiner, Representations Theory of Finite Groups and Associative Algebras, *Interscience*, 1962.

[4] Jacobson, Basic Algebra, vol.II, *Freeman*, 1980.

[5] S. Lang, Algebra , 3th ed., *Addison-Wesley*, 1993.

[6] B.R. McDonald, Finite Rings with identity, *Marcel Dekker.*, 1974.

[7] M. Nagata, Local rings, *Interscience Publishers*, 1962.

[8] O. Zariski, P. Samuel, Commutative algebra, vol.I, *D. Van Nostrand Company Inc.*, 1958.