12-2015

The Bourbaki-Jacobson correspondence

Jose R. Vera
The University of Texas Rio Grande Valley

THE BOURBAKI-JACOBSON CORRESPONDENCE

A Thesis

By

JOSE R. VERA

Submitted to the Graduate College of
The University of Texas Rio Grande Valley
In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

December 2015

Major Subject: Mathematics

THE BOURBAKI JACOBSON CORRESPONDENCE

A Thesis
by
JOSE R. VERA

COMMITTEE MEMBERS

Dr. habil. Paul-Hermann Zieschang
Commitee Member

Dr. Timothy Huber
Commitee Member

Dr. Jacob White
Commitee Member

December 2015

ABSTRACT

Vera, Jose R., The Jacobson Bourbaki Jacobson Correspondence. Master of Science (MS), December, 2015, 24 pp., references.

A general ring theoretic correspondence between subrings of the endomorphism ring of the additive group of a commutative field will be established. This correspondence (called Bourbaki-Jacobson Correspondence) provides the ordinary Galois correspondence when applied to specific group rings. Throughout this thesis, we will work with finite dimensional field extensions.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

In this thesis, we present a generalisazion of the classical Galois Theory to rings which has been introduced by Nathan Jacobson in 1944. We define E to be the endomorphism ring of the additive group of a commutative field R and consider R to be a subring of E. To each subring T of E which contains R and has finite dimension over R, we associate the centralizer $C_R(T)$ of T in R. Conversely, for each subfield S of R such that R has finite dimension over S, we associate the centralizer $C_E(S)$ of S in E. Jacobson's main observation is that the two functors which we described are inverses of each other.

In Chapter II, we cover the definitions and notation that are critical for understanding this thesis. In Chapter III, we define how a dual basis is formed and some properties that can be applied to it. In Chapter IV, we prove the two propositions which are needed to prove the main theorem of the Bourbaki-Jacobson Correspondence.

CHAPTER II

DEFINITIONS AND NOTATION

Let S be a set. A map from $S \times S$ to S is called an *operation* on S.

Let S be equipped with an operation which we denote by $\cdot$. Then S is called a (*multiplicative*) *monoid* if the following conditions hold.

(i) For any three elements a, b, c in S, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(ii) There exists an element e in S such that $e \cdot s = s \cdot e = s$ for each element s in S.

The element e in (ii) is called a *neutral element* of S, and it is easy to see that monoids cannot have more than one neutral element.

Sometimes the operation of a monoid is denoted by $+$ instead of $\cdot$. In this case we speak about an *additive* monoid.

Let G be an additive monoid. Then G is called a *group* if the following condition holds.

(iii) For each element g in G, there exists an element h in G such that $g + h = e = h + g$.

The element h in (iii) is called an *inverse* of g, and it is easy to see that each element in a group has only one inverse.

The unique neutral element in an additive monoid is usually denoted by 0 instead of e and in a multiplicative monoid by 1 instead of e. The inverse element of an additive group element g is usually denoted by $-g$ and of a multiplicative group by g^{-1}.

Let R be an additive group which, at the same time, is a multiplicative monoid. Assume additionally that

$$(s+t)u = su + tu \qquad \text{and} \qquad s(t+u) = st + su$$

for any three elements s, t, u in R. Then R is then called a *ring*.

A ring element r is called a *unit* of R if it has a multiplicative inverse.

If every non-zero element of a ring R is a unit, then R is called a *field*.

Let R be a ring, and let M be an additively written commutative group. This means that $k+l = l+k$ for any two elements k and l in M.

We define

$$\lambda\colon\ M \times R \longrightarrow M,\ (m,r) \longmapsto mr$$

Then M is called a module over R if the following conditions hold.

(i) $m \cdot 1 = m$.

(ii) $\forall\, m \in M\ \forall\, s, t$ in R, we have $m(st) = (ms)t$.

(iii) $\forall\, m$ in $M\ \forall\, s, t$ in R, we have $m(s+t) = ms + mt$.

(iv) $\forall\, k, l$ in M and $\forall\, r$ in R, we have $(k+l)r = kr + lr$.

If R is a field, then the module M is called a *vector space* over R.

Let V be a vector space over a field R, let B be a finite subset of V. Then B is called a *basis* of V if the following conditions hold.

(i) The set B is linearly independent.

(ii) Each element of V is a linear combination of the elements in B.

The *centralizer* of an element z of a group G is defined to be the set of elements of G which commute with z:

$$C_G(z) = \{x \in G \mid xz = zx\}.$$

Let G and H be groups. A map f from G to H is called a *homomorphism* if $f(g_1g_2) = f(g_1)f(g_2)$ for any two elements g_1 and g_2 in G.

A bijective homomorphism from a group to a group is called an *isomorphism*. Two groups G and H are called *isomorphic* if there exists an isomorphism from G to H.

Let G be a commutative additively written group, and let d and e be endomorphisms of G. We define

$$(d+e)(g) := d(g) + e(g)$$

for each element g in G. The addition which we define this way on the set of all endomorphisms of G is called the *componentwise* addition.

An *endomorphism* is a homomorphism from a group to itself. It is well-known that the set of all endomorphisms of a commutative additively written group is a ring with respect to componentwise addition and composition as multiplication.

A bijective endomorphism is called an *automorphism*.

Let R be a ring and let E be the endomorphism ring of the additive group of R.

$$\begin{aligned} \rho\colon\ R &\longrightarrow E \\ r &\longmapsto \rho_r\colon\ R \longrightarrow R \\ &\qquad\qquad x \longmapsto x{\cdot}r \end{aligned}$$

For each subring S of R, we set $S^\rho := \{s^\rho \mid s \in S\}$, so that S^ρ is the image of S under ρ.

CHAPTER III

DUAL BASIS

Let R be a commutative field. Let V be a vector space. We define $\mathrm{Hom}_R(V, R)$ to be the set of all vector-space homomorphisms from V to R and set

$$V^* := \mathrm{Hom}_R(V, R).$$

The vector space V^* is called the dual vector space of V.

Lemma 3.1 *Let $\{v_1, \ldots, v_n\}$ be a basis of V. Then V^* possesses a basis $\{\tau_1, \ldots, \tau_n\}$ such that $v^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$.*

PROOF: For every j in $\{1, \ldots, n\}$ we define τ_j to be uniquely determined element in V^* which satisfies

$$r_i^{\tau_j} = \delta_{ij} := \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

for each element i in $\{1, \ldots, n\}$. We claim that $\{\tau_1, \ldots, \tau_n\}$ is a basis of V^* over R. First we must show the set $\{\tau_1, \ldots, \tau_n\}$ is linearly independent. We fix elements $r_1, \ldots, r_n$ in R and assume that $\tau_1 r_1 +, \ldots, +\tau_n r_n = 0$. Then

$$v_i^{\tau_1 r_1 + \ldots + \tau_n r_n} = 0$$

for each i in $\{1, \ldots, n\}$. Let us now expand the map being applied to the element v_i as follows:

$$v_i^{\tau_1 r_1 + \ldots + \tau_n r_n} = v_i^{\tau_1 r_1} + \ldots + v_i^{\tau_n r_n} = v_i^{\tau_1} r_1 + \ldots + v_i^{\tau_n} r_n = r_i.$$

Therefore, from the previous equation $r_i = 0$ for every i in $\{1, \ldots n\}$.

To show the set $\{\tau_1, \ldots, \tau_n\}$ spans V^*, we must fix an element ϕ in V^*. We set $r_i := v_i^\phi$ for each element i in $\{1, \ldots, n\}$. Then it follows that

$$v_i^\phi = r_i = v_i^{\tau_1 r_1 + \ldots + \tau_n r_n}$$

for each element i in $\{1, \ldots, n\}$. Since $\{v_1, \ldots, v_n\}$ is a basis of V we conclude that $\phi = \tau_1 r_1 + \ldots + \tau_n r_n$. As a consequence of Lemma 3.1 we obtain that $dim_R(V) = dim_R(V^*)$. For an element v in V we define ψ_v to be a map from V^* to R sending each element ϕ in V^* to v^ϕ

We also set $V^{**} := \mathrm{Hom}_R(V^*, R)$. For each element v in V we define

$$\zeta\colon\ V \longrightarrow V^{**},\ \ v^\zeta \longmapsto \psi_v.$$

□

We now prove a converse of Lemma 3.1.

Lemma 3.2 *Let $\{\tau_1, \ldots, \tau_n\}$ be a basis of V^*. Then V possesses a basis $\{v_1, \ldots, v_n\}$ such that $v_i^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$.*

PROOF: By Lemma 3.1, there exist elements $\sigma_1, \ldots, \sigma_n$ in V^{**} such that

$$\tau_i^{\sigma_j} = \delta_{ij}$$

for any two elements i and j in $\{1, \ldots, n\}$.

We know that ζ is a bijective map from V to V^{**}.

Therefore, there exists an element v_i in V such that $v_i^\zeta = \sigma_i$ for each i in $\{1, \ldots, n\}$.

Thus, we have

$$v_i^{\tau_j} = \tau_j^{\psi_{v_i}} = \tau_j^{v_i^\zeta} = \tau_j^{\sigma_i} = \delta_{ij}$$

for any two elements i and j in $\{1, \ldots, n\}$. □

CHAPTER IV

THE THEOREM OF N. BOURBAKI - N. JACOBSON

In this chapter, the letter R will stand for a commutative field, the letter E for the endomorphism ring of the additive group of R.

Recall that for any element $r \in R$ ρ_r is the map from R to itself sending any element x in R to $x \cdot r$.

Let S be a subfield of R. An element e in E is called an *S-endomorphism* if $r^e s = (rs)^e$ for any two elements s in S and r in R. The set of all S-endomorphisms of R will be denoted by $\mathrm{End}_S(R)$.

Lemma 4.1 *Let S be a subfield of R. Then $C_E(S^\rho) = \mathrm{End}_S(R)$.*

PROOF: Let e be an element in $C_E(S^\rho)$. Then $e\rho_s = \rho_s e$ for each element s in S. It follows that

$$r^e s = r^{e\rho_s} = r^{\rho_s e} = (rs)^e$$

for any two elements s in S and r in R. Therefore, we conclude that e is in $\mathrm{End}_S(R)$.

Conversely, let e be an element in $\mathrm{End}_S(R)$. Then

$$r^{e\rho_s} = r^e s = (rs)^e = r^{\rho_s e}$$

for any two elements s in S and r in R, and that means that $e\rho_s = \rho_s e$ for each element s in S. It follows that $e \in C_E(S^\rho)$. □

Proposition 4.2 *Let S be a subfield of R, and assume R to be finitely generated over S. Set $T := C_E(S^\rho)$. Then T is a subring of E with $R^\rho \subseteq T$, and T is finitely generated over R^ρ with $dim_S(R) = dim_{R^\rho}(T)$.*

PROOF: We first show that T is a subring of R. Let s be an element in S. Then we have $t_1\rho_s = \rho_s t_1$ and $t_2\rho_s = \rho_s t_2$ for any two elements t_1 and t_2 in T. Thus,

$$(t_1 + t_2)\rho_s = t_1\rho_s + t_2\rho_s = \rho_s t_1 + \rho t_2 = \rho_s(t_1 + t_2)$$

and

$$(t_1t_2)\rho_s = t_1(t_2\rho_s) = t_1(\rho_s t_2) = (t_1\rho_s)t_2 = (\rho_s t_1)t_2 = \rho_s(t_1t_2)$$

for any two elements t_1 and t_2 in T. Thus, $t_1 + t_2 \in T$ and $t_1t_2 \in T$ for any two elements t_1 and t_2 in T. For each element t in T, we also have

$$(-t)\rho_s = -(t\rho_s) = -(\rho_s t) = \rho_s(-t).$$

Thus, $-t \in T$ for each element t in T. Note finally that $1 \in T$, since $1\cdot\rho_s = \rho_s\cdot 1$.

This shows that T is a subring of E.

Since R is assumed to be commutative we have that $R^\rho \subseteq T$.

We assume R is finitely generated over S. Thus, there exist elements r_1, ..., r_n in R such that $\{r_1, \ldots, r_n\}$ is a basis of R over S.

For every element j in $\{1, \ldots, n\}$, we define τ_j to be uniquely determined element in $\mathrm{Hom}_S(R, S)$ which satisfies

$$r_i^{\tau_j} = \delta_{ij} := \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

for any two elements i and j in $\{1, \ldots, n\}$. We claim that $\{\tau_1, \ldots, \tau_n\}$ is a basis of T over R^ρ.

First we must show the set $\{\tau_1, \ldots, \tau_n\}$ is linearly independent, so we fix elements q_1, ..., q_n in R and assume that $\tau_1\rho_{q_1} + \ldots + \tau_n\rho_{q_n} = 0$. Then we have

$$0 = r_i^{\tau_1\rho_{q_1}+\ldots+\tau_n\rho_{q_n}} = r_i^{\tau_1\rho_{q_1}} + \ldots + r_i^{\tau_n\rho_{q_n}} = r_i^{\tau_1}q_1 + \ldots + r_i^{\tau_n}q_n = q_i$$

for all i in $\{1, \ldots, n\}$.

Now we must show that the set $\{\tau_1, \ldots, \tau_n\}$ generates T as an R^ρ module we fix an element τ in T and set $q_i := r_i^\tau$ for all i in $\{1, \ldots, n\}$. Then

$$r_i^{\tau_1\rho_{q_1}+\ldots+\tau_n\rho_{q_n}} = q_i = r_i^\tau$$

for each element i in $\{1, \ldots, n\}$. $\square$

Lemma 4.3 *Let T be a subring of E with $R^\rho \subseteq T$, and assume T to be finitely generated over R^ρ. Then there exist a basis $\{\tau_1, \ldots, \tau_n\}$ of T over R^ρ and elements $r_1, \ldots, r_n$ in R such that $r_i^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$.*

PROOF: Let r be an element in R, and let τ be an element in T. We define

$$\tau^{\sigma_r} := \rho_{r^\tau}$$

and note that σ_r is a map from T to R^ρ.

For any two elements τ_1 and τ_2 in T we have

$$(\tau_1 + \tau_2)^{\sigma_r} = \rho_{r^{\tau_1+\tau_2}} = \rho_{r^{\tau_1}+r^{\tau_2}} = \rho_{r^{\tau_1}} + \rho_{r^{\tau_2}} = \tau_1^{\sigma_r} + \tau_2^{\sigma_r}.$$

For any two elements τ in T and q in R we have

$$(\tau\rho_q)^{\sigma_r} = \rho_{r^{\tau\rho_q}} = \rho_{(r^\tau)^{\rho_q}} = \rho_{r^\tau q} = \rho_{r^\tau}\rho_q = \tau^{\sigma_r}\rho_q.$$

Thus, we have shown that $\sigma_r \in \mathrm{Hom}_{R^\rho}(T, R^\rho)$.

Now we let K denote the subspace of the R-vector space $\mathrm{Hom}_{R^\rho}(T, R^\rho)$ generated by the $\{\sigma_r \mid r \in R\}$. We claim $K = \mathrm{Hom}_{R^\rho}(T, R^\rho)$, and in order to prove this we assume, by way of contradiction, that $K \neq \mathrm{Hom}_{R^\rho}(T, R^\rho)$.

There exist element $\sigma_1, \ldots, \sigma_n$ in $\mathrm{Hom}_{R^\rho}(T, R^\rho)$ and an integer $m \leq n-1$ such that $\{\sigma_1, \ldots, \sigma_n\}$ is a basis of $\mathrm{Hom}_{R^\rho}(T, R^\rho)$ and $\{\sigma_1, \ldots, \sigma_m\}$ is a basis of K. Since $\{\sigma_1, \ldots, \sigma_m\}$ is a basis of $\mathrm{Hom}_{R^\rho}(T, R^\rho)$, T possesses a basis $\{\tau_1, \ldots, \tau_n\}$ such that $\tau_i^{\sigma_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$. This implies $\tau_n^{\sigma_j} = 0$ for all j in $\{1, \ldots, m\}$, since $\{\sigma_1, \ldots, \sigma_m\}$ is a basis of K and $\tau_n^{\sigma_j} = 0$ for all j in $\{1, \ldots, m\}$. Therefore $\rho_r^{\tau_n} = 0 \Rightarrow r^{\tau_n} = 0 \ \forall r \in R \Rightarrow \tau_n = 0$ contrary to the fact that τ_n is a basis element.

What we have seen is that $K = \mathrm{Hom}_{R^\rho}(T, R^\rho)$

There exist elements r_1, ..., r_n in R such that $\{\sigma_{r_1}, \ldots, \sigma_{r_n}\}$ is a basis of $\mathrm{Hom}_{R^\rho}(T, R^\rho)$. Recall from Lemma 3.2 that T possesses a basis $\{t_1, \ldots, t_n\}$ over R^ρ such that $\tau_j^{\sigma_{r_i}} = \delta_{ij} \Rightarrow r_i^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$. $\square$

Lemma 4.4 *Let T be a subring of E with $R^\rho \subseteq T$, and assume T to be finitely generated over R^ρ. Let $\{\tau_1, \ldots, \tau_n\}$ be a basis of T over R^ρ, and let $r_1, \ldots, r_n$ be elements in R such that $r_i^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$. Then we have $\tau = \tau_1\rho_{r_1{}^\tau} + \ldots + \tau_n\rho_{r_n{}^\tau}$ for each element τ in T.*

PROOF: Let τ be an element in T. Since $\{\tau_1, \ldots, \tau_n\}$ is a basis of T over R^ρ, there exist elements $q_1, \ldots, q_n$ in R such that $\tau = \tau_1\rho_{q_1} + \ldots + \tau_n\rho_{q_n}$. Thus,

$$r_i^\tau = r_i^{\tau_1\rho_{q_1}+\ldots+\tau_n\rho_{q_n}} = r_i^{\tau_1\rho_{q_1}} + \ldots + r_i^{\tau_n\rho_{q_n}} = r_i^{\tau_i\rho_{q_i}} = q_i$$

for each element i in $\{1, \ldots, n\}$. It follows that $\tau = \tau_1\rho_{r_1{}^\tau} + \ldots + \tau_n\rho_{r_n{}^\tau}$. □

Lemma 4.5 *Let T be a subring of E with $R^\rho \subseteq T$, and assume T to be finitely generated over R^ρ. Then T possesses a basis $\{\tau_1, \ldots, \tau_n\}$ over R^ρ such that $\tau_i\rho_r\tau_j = \tau_i\rho_{r^{\tau_j}}$ for any three elements r in R and i, j in $\{1, \ldots, n\}$.*

PROOF: By Lemma 4.3, there exists a basis $\{\tau_1, \ldots, \tau_n\}$ of T over R^ρ and elements $r_1, \ldots, r_n$ in R such that $r_i^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$.
Let r be an element in R, and let i, and j be elements in $\{1, \ldots, n\}$. Then we have

$$r_k^{\tau_i\rho_r\tau_j} = (r_k^{\tau_i})^{\rho_r\tau_j} = \delta_{ki}^{\rho_r\tau_j} = (\delta_{ki}^{\rho_r})^{\tau_j} = (\delta_{ki}r)^{\tau_j}$$

for each element k in $\{1, \ldots, n\}$. Since T is assumed to be a subring of E with $R^\rho \subseteq T$, we have $\tau_i\rho_r\tau_j \in T$. Thus, by applying Lemma 4.4 to $\tau_i\rho_r\tau_j$ in place of τ we have

$$\tau_i\rho_r\tau_j = \tau_1\rho_{r_1^{\tau_i\rho_r\tau_j}} + \ldots + \tau_n\rho_{r_n^{\tau_i\rho_r\tau_j}} = \tau_i\rho_{r^{\tau_j}},$$

and that finishes the proof. □

Lemma 4.6 *Let T be a subring of E with $R \subseteq T$, and assume T to be finitely generated over R^ρ. Then we have $\rho_{r^\tau} \in C_{R^\rho}(T)$ for any two elements r in R and τ in T.*

PROOF: By lemma 4.5, T possesses a basis $\{\tau_1, \ldots, \tau_n\}$ over R^ρ such that $\tau_i\rho_r\tau_j = \tau_i\rho_{r^{\tau_j}}$ for any three elements r in R and i, j in $\{1, \ldots, n\}$.
Let $r \in R$, and let i and j be elements in $\{1, \ldots, n\}$. Then we have

$$q^{\rho_{r^{\tau_i}}\tau_j} = (q^{\rho_{r^{\tau_i}}})^{\tau_j} = (qr^{\tau_i})^{\tau_j} = (r^{\tau_i}q)^{\tau_j} = r^{\tau_i\rho_q\tau_j} = r^{\tau_i\rho_{q^{\tau_j}}} = (r^{\tau_i})^{\rho_{q^{\tau_j}}} = r^{\tau_i}q^{\tau_j} = q^{\tau_j}r^{\tau_i} = q^{\tau_j\rho_{r^{\tau_i}}}$$

for each element q in R. Thus, $q^{\rho_{r^{\tau_i}}\tau_j} = q^{\tau_j\rho_{r^{\tau_i}}}$ for each element q in R implying $\rho_{r^{\tau_i}}\tau_j = \tau_j\rho_{r^{\tau_i}}$ so $\rho_{r^{\tau_i}} \in C_{R^\rho}(\tau_j)$. Since $\{\tau_1, \ldots, \tau_n\}$ is a basis of T over R^ρ and i and j were chosen arbitrarily in $\{1, \ldots, n\}$, we then have that $\rho_{r^\tau} \in C_{R^\rho}(T)$. □

Proposition 4.7 *Let T be a subring of E with $R^\rho \subseteq T$, and assume T to be finitely generated over R^ρ. Set $S := C_{R^\rho}(T)$. Then S is a subfield of R^ρ, R^ρ is finitely generated over S, and*

$dim_S(R^\rho) = dim_{R^\rho}(T)$.

PROOF: By Lemma 4.3, there exist a basis $\{\tau_1, \ldots, \tau_n\}$ of T over R^ρ and elements $r_1, \ldots, r_n$ in R such that $r_i^{\tau_j} = \delta_{ij}$ for any two elements i and j in $\{1, \ldots, n\}$. We claim that $\{\rho_{r_1}, \ldots, \rho_{r_n}\}$ is a basis of R^ρ over S.

In order to show that $\{\rho_{r_1}, \ldots, \rho_{r_n}\}$ is linearly independent we pick elements $\sigma_1, \ldots, \sigma_n$ in S and assume that $\rho_{r_1}\sigma_1 + \ldots + \rho_{r_n}\sigma_n = 0$. Let i be an element in $1, \ldots, n$. Then, as $\sigma_i \in S$,

$$0 = (\rho_{r_1}\sigma_1 + \ldots + \rho_{r_n}\sigma_n)\tau_i = \rho_{r_1}\sigma_1\tau_i + \ldots + \rho_{r_n}\sigma_n\tau_i = \rho_{r_1}\tau_i\sigma_1 + \ldots + \rho_{r_n}\tau_i\sigma_n.$$

Therefore, we have

$$0 = 1^{\rho_{r_1}\tau_i\sigma_1 + \ldots + \rho_{r_n}\tau_i\sigma_n} = r_1^{\tau_i\sigma_1} + \ldots + r_n^{\tau_i\sigma_n} = r_i^{\tau_i\sigma_i} = 1^{\sigma_i}.$$

Since $\sigma_i \in S$, there exists an element s_i in R such that $\sigma_i = \rho_{s_i}$. Thus, $s_i = 1^{\rho_{s_i}} = 1^{\sigma_i} = 0$. Thus, $\sigma_i = 0$.

In order to show that $\{\rho_{r_1}, \ldots, \rho_{r_n}\}$ generates R^ρ as an S-module, we fix an element r in R^ρ. For each element i in $\{1, \ldots, n\}$, we set $\sigma_i := \rho_{r^{\tau_i}}$. Then, by Lemma 4.6, $\sigma_i \in S$ for each element i in $\{1, \ldots, n\}$. Thus, for any two elements i and j in $\{1, \ldots, n\}$,

$$(r_i r^{\tau_i})^{\tau_j} = (r_i^{\sigma_i})^{\tau_j} = r_i^{\sigma_i\tau_j} = (r_i^{\tau_j})^{\sigma_i} = (r_i^{\tau_j})r^{\tau_i} = \delta_{ij}r^{\tau_i}.$$

Thus, setting $q := r_1 r^{\tau_1} + \ldots + r_n r^{\tau_n}$, we have

$$q^{\tau_j} = (r_1 r^{\tau_1} + \ldots + r_n r^{\tau_n})^{\tau_j} = (r_1 r^{\tau_1})^{\tau_j} + \ldots + (r_n r^{\tau_n})^{\tau_j} = r^{\tau_j}$$

for each element j in $\{1, \ldots, n\}$. It follows that $(r - q)^{\tau_j} = 0$ for each element j in $\{1, \ldots, n\}$. Thus, as $\{\tau_1, \ldots, \tau_n\}$ is a basis of T, we obtain that $(r - q)^\tau = 0$ for each element τ in T. Thus, as $1 \in T$, $r - q = 0$, and that means that $r = r_1 r^{\tau_1} + \ldots + r_n r^{\tau_n}$. It follows that

$$\rho_r = \rho_{r_1}\sigma_1 + \ldots + \rho_{r_n}\sigma_n,$$

so we are done. □

Theorem 4.8 *Let R be a commutative field, and let E denote the endomorphism ring of the additive group of R. Then we have the following.*

(i) *Let S be a subfield of R^ρ, and assume R^ρ to be finitely generated over S. Then $S = C_{R^\rho}(C_E(S))$.*

(ii) *Let T be a subring of E with $R^\rho \subseteq T$, and assume T to be finitely generated over R^ρ. Then*

$T = C_E(C_{R^\rho}(T))$.

PROOF: (i) Set $T := C_E(S)$. Then, by Proposition 4.2, T is a subring of E with $R^\rho \subseteq T$, and T is finitely generated over R^ρ with

$$dim_S(R^\rho) = dim_{R^\rho}(T).$$

Since T is a subring of E which is finitely generated over R^ρ, we obtain from Proposition 4.7 that R^ρ is finitely generated over $C_{R^\rho}(T)$ and that

$$dim_{C_{R^\rho}(T)}(R^\rho) = dim_{R^\rho}(T).$$

It follows that

$$dim_S(R^\rho) = dim_{C_{R^\rho}(T)}(R^\rho).$$

Thus, as $S \subseteq C_{R^\rho}(T)$, $S = C_{R^\rho}(T)$.

(ii) Set $S := C_{R^\rho}(T)$. Then, by Proposition 4.7, S is a subfield of R^ρ, R^ρ is finitely generated over S, and

$$dim_S(R^\rho) = dim_{R^\rho}(T).$$

Since R^ρ is finitely generated over S, we obtain from Proposition 4.2 that $C_E(S)$ is finitely generated over R^ρ and that

$$dim_S(R^\rho) = dim_{R^\rho}(C_E(S)).$$

It follows

$$dim_{R^\rho}(T) = dim_{R^\rho}(C_E(S)).$$

Thus, as $T \subseteq C_E(S)$, $T = C_E(S)$. □

Let R be a commutative field, let $\mathcal{S}(R)$ denote the set of all subfields S of R^ρ such that R^ρ is finitely generated over S, and let $\mathcal{T}(R)$ denote the set of all subrings T of E which contain R^ρ as subfield and are finitely generated over R^ρ. Note that $\mathcal{S}(R)$ and $\mathcal{T}(R)$ both are partially ordered with respect to set-theoretic containment.

For each element S in $\mathcal{S}(R)$, we set

$$S^\tau := C_E(S),$$

and, for each element T in $\mathcal{T}(R)$, we set

$$T^\sigma := C_{R^\rho}(T).$$

Note that $Q^\tau \subseteq P^\tau$ for any two elements P and Q in $\mathcal{S}(R)$ with $P \subseteq Q$. Similarly, $V^\sigma \subseteq U^\sigma$ for any two elements U and V in $\mathcal{T}(R)$ with $U \subseteq V$. From Theorem 4.8 we obtain that $S = S^{\tau\sigma}$ and $T = T^{\sigma\tau}$. Thus, the pair (τ, σ) is a Galois pair with respect to set-theoretic containment defined on $\mathcal{S}(R)$ and with respect to set-theoretic containment defined on $\mathcal{T}(R)$.

REFERENCES

[1] Jacobson, Nathan, Lectures in Abstract Algebra: III. Theory of Fields and Galois Theory (Graduate Texts in Mathematics). Van Nostrand, 1964.

[2] Zieschang, Paul-Hermann, *The Bourbaki-Jacabson Correspondence*, in: Lecture Notes on Galois Theory.

BIOGRAPHICAL SKETCH

Jose R. Vera is in his 5th year in the 4 plus 1 math program at The University of Texas Rio Grande Valley. In December 2015, he graduated with his Master of Science having a focus on abstract algebra. Aside from being a Member of the 4 plus 1 program, Mr. Vera also graduated from the Math and Science Academy. The Math and Science Academy is an early college program offered to a limited set of Juniors and Seniors from highschool to advance in their area of study.

His last three semesters Jose participated in weekly seminars with professors and students to discuss different topics in the area of mathematics. This gave him a stronger well rounded math background in other studied areas of mathematics. He is eager to begin his career as a math instructor. He also wishes to return and continue his studies and recieve a Masters in Business Administration.

Jose has assisted professors in many math courses including Contemporty Math, Math for teachers, and Calculus three. He has been a math tutor for four years, working with many departments on campus such as the learning enrichment, Math and Science Academy, and the Math department. He finds a satisfaction from helping many students triumph the considered to be complicated subject of mathematics.