Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 38 (1997), No. 2, 399-410.

Galois Theory of Commutative Rings Revisited[1]

Miguel Ferrero **Antonio Paques**

Instituto de Matemática, Universidade Federal do Rio Grande do Sul, 91509-900, Porto Alegre, Brasil

Instituto de Matemática, Estatística e Ciência da Computação, Universidade Estadual de Campinas, 13083-970, Campinas, Brasil

Introduction. In [3], S. U. Chase, D. K. Harrison and A. Rosenberg developed a Galois theory for commutative ring extensions $S \supset R$ under the assumption that S is separable as an R-algebra and finitely generated and projective as an R-module, and the elements of the Galois group G are pairwise strongly distinct R-automorphisms of S. Among the main results of that paper, Theorem 1.3 gives several equivalent conditions for the definition of a Galois extension and Theorem 2.3 states a one-to-one correspondence between the subgroups of G and the R-subalgebras of S which are separable and G-strong.

On the other hand, recently A. W. Dress [5] showed that a simplification of Galois theory for fields is possible by combining Dedekind's lemma with some elementary facts on G-sets. The author also showed that the same approach can be used to obtain the basic results of Galois theory of skew-fields [6].

Dedekind's lemma states that for a field extension L of a field K the set $\mathrm{Alg}_K(A, L)$ of all K-algebra homomorphisms of a K-algebra A into L is a linearly independent subset of the L-vector space $\mathrm{Hom}_K(A, L)$. It turns out that strongly distinct homomorphisms of separable algebras are the kind of homomorphisms which satisfy a version of Dedekind's lemma. This simple remark is the starting point of this paper, and from this point of view, is not surprising that the approach by A. W. Dress in [5] can also be used to obtain the main results on Galois theory of commutative rings.

The purpose of this paper is twofold. First, we show that the above approach can in fact be used in Galois theory of commutative rings. Second, as a natural sequel of this method we obtain some new results.

[1]This paper was partially supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq, Brazil) and Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES, Brazil)

Section 1 is an introductory section. In Sections 2 and 3 we give new proofs for several known results which are simpler than the proofs in former papers, including a proof of the fundamental theorem of Galois theory given in [3]. We point out that the results of Section 2 are slightly more general than the results in [3], because we will need this later on. Also, to make the paper more self contained, throughout those sections we only assume the reader is familiar with Linear Algebra and basic facts on Commutative Algebra and separable algebras. However, in many cases our arguments have been borrowed from former papers.

The main result in Section 4 is a theorem giving several equivalent conditions for a faithfully projective R-algebra to be self-split. In particular, the theorem makes it clear once more the relevance of strongly distinct algebra homomorphisms. In the last Section 5 we give a new proof of Theorem 3.1 of [12] showing that a faithfully projective algebra over R which is a splitting ring of a separable polynomial is a weakly Galois extension of R, using again the same approach of [5].

Throughout R is always a commutative ring with identity element and algebras over R are always associative and commutative algebras. Ring homomorphisms carry the identity into the identity. Unadorned $\otimes$ means $\otimes_R$.

1. Prerequisites

Recall that a commutative R-algebra A is said to be separable over R if A is an $A \otimes A$-projective module [1]. This is equivalent to the existence of an idempotent $e = \sum_{i=1}^{n} x_i \otimes y_i \in A \otimes A$ such that $\mu(e) = \sum_{i=1}^{n} x_i y_i = 1$ and $xe = ex$, for all $x \in A$, where $\mu : A \otimes A \to A$ is the multiplication map. In this paper we use only some basic results on separable algebras which can be found for example in [4] and [9].

The following result will be used throughout the paper.

Lemma 1.1. *Assume that $A \subset B$ are R-algebras which are finitely generated and projective as R-modules and A is separable over R. If $rank_{R_p} A_p = rank_{R_p} B_p$, for every prime ideal p of R, then $A = B$.*

Proof. It is enough to prove the result when R is a local ring. Let $\mathbf{m}$ be the maximal ideal of R. By ([7], Lemma 1.1) we have $\mathbf{m}B \subseteq J(B)$ and $\mathbf{m}A = J(A)$, where J denotes the Jacobson radical. Also, B is a finitely generated and projective A-module ([7], Lemma 1.2). Hence B is a faithfully projective algebra over A and using ([9], Lemma I 3.2) we obtain $J(B) \cap A \subseteq J(A)$. Thus $\mathbf{m}A \subseteq \mathbf{m}B \cap A \subseteq J(B) \cap A \subseteq J(A) = \mathbf{m}A$, i.e. $\mathbf{m}B \cap A = \mathbf{m}A$. Then we can consider $\overline{A} = A/\mathbf{m}A \subseteq \overline{B} = B/\mathbf{m}B$. Since A and B are free R-modules of the same rank over R, $\overline{A}$ and $\overline{B}$ are vector spaces of the same dimension over $\overline{R} = R/\mathbf{m}$. Consequently $\overline{A} = \overline{B}$ and the result easily follows. $\square$

If a separable algebra A over R is, in addition, finitely generated and projective as an R-module, then we will say, following [8], that A is strongly separable over R.

Distinct homomorphisms $f_1, ..., f_n : T \to S$ of strongly separable R-algebras are not necessarily free over S in $\mathrm{Hom}_R(T, S)$. So if we want to have a Galois theory similar to the one we have for fields we must restrict the homomorphisms somehow. Two homomorphisms of R-algebras $f, g : T \to S$ are said to be strongly distinct if for every non-zero idempotent $e \in S$ there exists $x \in S$ such that $f(x)e \neq g(x)e$ (see [3]).

Our starting point is the following slight extension of Lemma 1.2 in [3], whose proof is the same given in that paper.

Lemma 1.2. *Assume that T is a separable algebra over R and $f : T \to R$ is a homomorphism of R-algebras. Then there exists a unique idempotent $e \in T$ such that $f(e) = 1$ and $f(x)e = xe$, for every $x \in T$. Furthermore, if $\{f_j : j \in J\}$ is a non-empty set of pairwise strongly distinct homomorphisms of R-algebras from T into R, then the corresponding idempotents $e_j, j \in J$, are pairwise orthogonal and $f_i(e_j) = \delta_{ij}$, for all $i, j \in J$.*

2. Basic results

Lemma 1.2 has the following consequence which gives the version of Dedekind's lemma we will frequently use in the paper.

Proposition 2.1. *Assume that T and S are R-algebras with T separable over R, and V is a non-empty set of homomorphisms of R-algebras from T into S. Then the following conditions are equivalent.*

(i) *The elements of V are pairwise strongly distinct.*

(ii) *For every $\sigma \in V$ there exist $x_{i\sigma} \in S$, $y_{i\sigma} \in T$, $1 \le i \le m_\sigma$, such that $\sum_{i=1}^{m_\sigma} x_{i\sigma}\tau(y_{i\sigma}) = \delta_{\tau,\sigma}$, for all $\tau \in V$.*

(iii) *V is free over S in $Hom_R(T, S)$.*

Proof. (i) $\to$ (ii) Since T is separable over R, $S \otimes T$ is separable over S ([9], Proposition III 2.1). Also the mappings $f_\tau : S \otimes T \to S$ defined by $f_\tau(x \otimes y) = x\tau(y)$, for $x \otimes y \in S \otimes T$ and $\tau \in V$, are pairwise strongly distinct homomorphisms of S-algebras. Then there exist $e_\sigma = \sum_{i=1}^{m_\sigma} x_{i\sigma} \otimes y_{i\sigma} \in S \otimes T$ such that $f_\tau(e_\sigma) = \delta_{\tau,\sigma}$, for τ, $\sigma \in V$. Now (ii) follows.

(ii) $\to$ (iii) Assume that V' is a finite subset of V and $\sum_{\tau\in V'} s_\tau\tau = 0$ in $\mathrm{Hom}_R(T, S)$, $s_\tau \in S$. For $\sigma \in V'$ we have $s_\sigma = \sum_{\tau\in V'} \delta_{\tau,\sigma}s_\tau = \sum_{\tau\in V'}(\sum_{i=1}^{m_\sigma} x_{i\sigma}\tau(y_{i\sigma}))s_\tau = \sum_{i=1}^{m_\sigma} x_{i\sigma}(\sum_{\tau\in V'} \tau(y_{i\sigma})s_\tau)$ $= 0$.

(iii) $\to$ (i): Obvious. □

Corollary 2.2. *Assume that T is a strongly separable extension of R, S is an R-algebra and V is a non-empty set of pairwise strongly distinct homomorphisms of R-algebras from T into S. Then $\#V \le rank_{R_p}T_p$, for every prime ideal p of R.*

Proof. Since V is free over S, we have $V_p = \{\tau_p : \tau \in V\} \subset \mathrm{Hom}_{R_p}(T_p, S_p)$ and we see that V_p is free over S_p and $\#V = \#V_p$. Then it is enough to prove the result when R is a local ring. In this case T is free as an R-module and we may assume $T \simeq R^n$, for $n = rank_RT$. Consequently $\mathrm{Hom}_R(T, S) \simeq S^n$ as an S-module and hence $\#V \le n$. □

Lemma 2.3. *Assume that T and S are R-algebras, where S is faithfully projective, and $V \subseteq \mathrm{Alg}_R(T, S)$ is a non-empty finite set. Then the following conditions are equivalent.*

(i) *T is a strongly separable extension of R, $rank_RT = \#V$ and the elements of V are pairwise strongly distinct.*

(ii) *T is faithfully projective over R, $rank_R T = \#V$ and for every $\sigma \in V$ there exist $x_{i\sigma} \in S$, $y_{i\sigma} \in T$, $1 \leq i \leq m_\sigma$, such that $\sum_{i=1}^{m_\sigma} x_{i\sigma}\tau(y_{i\sigma}) = \delta_{\tau,\sigma}$, for all $\tau \in V$.*

(iii) *The mapping $\varphi : S \otimes T \to S^n$ given by $\varphi(s \otimes t) = (s\tau(t))_{\tau \in V}$ is an isomorphism of S-algebras, where $n = \#V$.*

Proof. (i) $\to$ (ii): Proposition 2.1.

(ii) $\to$ (iii) φ is clearly an S-algebra homomorphism. For $(s_\tau)_{\tau \in V} \in S^n$, take $z = \sum_{\sigma \in V} \sum_{i=1}^{m_\sigma} s_\sigma x_{i\sigma} \otimes y_{i\sigma} \in S \otimes T$ and verify $\varphi(z) = (s_\tau)_{\tau \in V}$. Then φ is an epimorphism. Also, since $rank_S(S \otimes T) = rank_R T = \#V = rank_S(S^n)$, φ is an isomorphism.

(iii) $\to$ (i) By ([9], Lemma III 1.9) T is a direct summand of $S \otimes T \simeq S^n$. So T is a finitely generated and projective R-module. Comparing ranks, $rank_R T = \#V$. Hence T is faithful over R. Also, S^n is S-separable and so by ([9], Proposition III 2.2) T is separable over R. Finally, given $\sigma \in V$ consider $\alpha = (\delta_{\tau,\sigma})_{\tau \in V} \in S^n$. Then there exists $z = \sum_{i=1}^{m_\sigma} s_{i\sigma} \otimes t_{i\sigma} \in S \otimes T$ such that $\varphi(z) = \alpha$. Therefore by Proposition 2.1 the elements of V are pairwise strongly distinct. The proof is complete. □

If $S = T$, the equivalent conditions of Lemma 2.3 are satisfied and V is a group, we say that S is a Galois extension of R with Galois group V (c.f. [1] p. 396; [3], Theorem 1.3).

On the other hand, recall that S is said to be a weakly Galois extension of R [14] if S is a strongly separable extension of R and there exists a finite group (or set) H of R-automorphisms of S such that the fixed subring $S^H = \{x \in S : \sigma(x) = x, \text{for all}\, \sigma \in H\}$ equals R. We have

Corollary 2.4. *If $S = T$ and the equivalent conditions of Lemma 2.3 are satisfied, then $S^V = R$. In particular, if in addition the elements of V are R-automorphisms of S, then S is a weakly Galois extensions of R of constant rank.*

Proof. If $s \in S^V$, then using (iii) of Lemma 2.3 we easily get $s \otimes 1 = 1 \otimes s$ in $S \otimes S$. By ([9], Lemma III 1.9) R is a direct summand of S and so there exists an R-submodule M of S with $S = R \oplus M$. Write $s = r + x$, $r \in R$, $x \in M$. Then $x \otimes 1 = 1 \otimes x$ and they are in different direct summands of $S \otimes S$. Hence $x \otimes 1 = 0$ and it follows that $x = 0$ because the map $S \to S \otimes S$ is injective. Thus $s \in R$. □

In Section 4 we will see that the converse of Corollary 2.4 is also true.

3. The Fundamental Theorem of Galois Theory

Assume that S is a Galois extension of R with Galois group G. Recall that a subring T of S containing R is said to be G-strong if the restrictions to T of any two elements of G are either equal or strongly distinct as maps from T into S.

The purpose of this section is to give an elementary proof of Theorem 2.3 of [3].

Theorem 3.1. *Assume that S is a Galois extension of R with Galois group G. Then the correspondence $H \mapsto S^H$ gives a one-to-one correspondence between the set of subgroups of G and the set of R-subalgebras of S which are separable and G-strong.*

Following [5], for a group G and G-sets X and Y denote by $\mathrm{Map}(X, Y)$ the set of all the applications from X into Y. Then $\mathrm{Map}(X, Y)$ is a G-set via the action given by $\tau * f = \tau f \tau^{-1}$, $\tau \in G$, $f \in \mathrm{Map}(X, Y)$. Denote by $\mathrm{Hom}_G(X, Y)$ the subset of $\mathrm{Map}(X, Y)$ of all f with $\tau * f = f$, for all $\tau \in G$.

Let H be a subgroup of G and put $X_H = \{\tau H : \tau \in G\}$, the set of all the left cosets of H in G. Then X_H is a G-set via the action $\tau(\sigma H) = \tau\sigma H$, for τ, $\sigma \in G$. Also, it can easily be verified that for every G-set Y there is a canonical bijection $\theta : \mathrm{Hom}_G(X_H, Y) \to Y^H$ given by $\theta(f) = f(H)$.

Now, assume that S is an algebra over R and G is a group of R-automorphisms of S. If X is a G-set, $\mathrm{Map}(X, S)$ is an S-algebra under pointwise operations and $\mathrm{Hom}_G(X, S)$ is an R-algebra. Finally, when H is a subgroup of G the bijection $\theta : \mathrm{Hom}_G(X_H, S) \to S^H$ is an isomorphism of algebras over R.

For a finite G-set X we put $A(X) = \mathrm{Hom}_G(X, S)$. If $x \in X$, φ_x denotes the R-algebra homomorphism from $A(X)$ into S defined by $\varphi_x(f) = f(x)$, for all $f \in A(X)$.

The following lemma is a particular reformulation of Lemma 2.3.

Lemma 3.2. *Assume that S is a faithfully projective algebra over R, G is a group of R-automorphisms of S, and X is a finite G-set. Then the following conditions are equivalent.*

(i) *$A(X)$ is a strongly separable extension of R with $rank_R A(X) = \#X$ and the elements $(\varphi_x)_{x \in X}$ are pairwise strongly distinct.*

(ii) *The application $\varphi : S \otimes A(X) \to S^n$ given by $\varphi(s \otimes f) = (sf(x))_{x \in X}$, $s \in S, f \in A(X)$, is an isomorphism of S-algebras, where $n = \#X$.*

Proof. It is enough to show that under the assumption (ii) the mapping $x \mapsto \varphi_x$ defines a bijection from X onto $\{\varphi_x : x \in X\}$. In fact, if $\varphi_x = \varphi_y$ then $f(x) = f(y)$, for every $f \in A(X)$. Also, since $S \otimes A(X) \simeq S^n \simeq \mathrm{Map}(X, S)$ we easily obtain that $f(x) = f(y)$, for all $f \in \mathrm{Map}(X, S)$. Hence $x = y$ and the result follows. $\square$

Lemma 3.3. *Assume that S is a Galois extension of R with Galois group G and X is a finite G-set. Then the application $\varphi : S \otimes A(X) \to S^n$, $n = \#X$, given above is an isomorphism of S-algebras.*

Proof. Clearly φ is an S-algebra homomorphism. By Lemma 2.3 there exist x_i, $y_i \in S$, $1 \leq i \leq m$, such that $\sum_{i=1}^m x_i \tau(y_i) = \delta_{1,\tau}$, for all $\tau \in G$. Take $\alpha = (s_x)_{x \in X} \in S^n$ and define $\alpha_i' : X \to S$ by $\alpha_i'(x) = \sum_{\tau \in G} \tau(y_i s_{\tau^{-1}(x)})$, for $1 \leq i \leq m$, $x \in X$. We easily see that $\alpha_i' \in A(X)$. Put $\psi(\alpha) = \sum_{i=1}^m x_i \otimes \alpha_i'$. Hence $\psi : S^n \to S \otimes A(X)$ is the inverse of φ. $\square$

Remark 3.4. Actually Lemma 3.3. is a direct consequence of ([3], Theorem 1.3 (d)).

Lemma 3.5. *Assume that S is a Galois extension of R with Galois group G and T is a subalgebra of S which is R-separable and G- strong. Then there exist elements x_i, $y_i \in T$, $1 \leq i \leq m$, such that $\sum_{i=1}^m x_i \tau(y_i) = \delta_{1,\tau|_T}$, for all $\tau \in G$. In particular, T is finitely generated and projective as an R-module.*

Proof. Assume that $e = \sum_{i=1}^m x_i \otimes y_i \in T \otimes T$ satisfies $\mu(e) = \sum_{i=1}^m x_i y_i = 1$ and $xe = ex$ for every $x \in T$, where $\mu : T \otimes T \to T$ is the multiplication mapping. We can easily see that

$e_\tau = \sum_{i=1}^m x_i\tau(y_i) = \mu(1\otimes\tau)(e)$ is an idempotent of S and $xe_\tau = \tau(x)e_\tau$, for all $\tau \in G$, $x \in T$. Since T is G-strong we necessarily have $e_\tau = 0$ in case $\tau|_T \neq id_T$ and $e_\tau = 1$ if $\tau|_T = id_T$. The first part follows.

Put $H_T = \{\tau \in G : \tau|_T = id_T\}$ and denote by $\tau_1, ..., \tau_r \in G$ a set of representatives of the left cosets of H_T in G, where $\tau_1 = id$. Since $S^G = R$ we have $\sum_{j=1}^r \tau_j(y_i x) \in R$ for all $x \in T$, $1 \leq i \leq m$. Clearly the mappings $f_i : T \to R$ defined by $f_i(x) = \sum_{j=1}^r \tau_j(y_i x)$ are homomorphisms of R-modules and $x = \sum_{i=1}^m f_i(x)x_i$, for every $x \in T$. The last part follows. □

Now we are in position to prove the theorem.

Proof of Theorem 3.1. If H is a subgroup of G, put $T_H = S^H$. Then $T_H \simeq A(X_H)$ is a separable and faithfully projective R-algebra with $rank_R T_H = \#X = [G : H]$, which is G-strong by Lemmas 3.2 and 3.3. Conversely, assume that T is a separable R-subalgebra of S which is G-strong and put $H_T = \{\tau \in G : \tau|_T = id_T\}$. By Lemma 3.5, T is finitely generated and projective as an R-module and since $T \subseteq S^{H_T}$, $rank_{R_p} T_p \leq rank_R S^{H_T} = [G : H_T]$, for every prime ideal p of R. On the other hand, since the representatives of the left cosets of H_T in G induce R-algebra homomorphisms from T into S which are pairwise strongly distinct, by Corollary 2.2 $[G : H_T] \leq rank_{R_p} T_p$, for every p. Thus $rank_R T = rank_R S^{H_T}$ and it follows that $T = S^{H_T}$ by Lemma 1.1. Finally, if $T = T_H$ then $H \subset H_T$ and $[G : H] = rank_R T = rank_R S^{H_T} = [G : H_T]$. Consequently $H = H_T$ and the proof is complete. □

4. Self-split algebras

Let S be a given algebra over R. Recall that an R-algebra T is said to be S-split if $S\otimes T \simeq S^n$, as S-algebras, for some $n \geq 1$. In particular, if S is an S-split algebra we say that S is a self-split algebra.

In this section we study self-split algebras which are faithfully projective. Our purpose here is to prove the following.

Theorem 4.1. *Let S be a faithfully projective algebra over R. Then the following conditions are equivalent*

(i) *S is self-split.*
(ii) *S is separable over R, $rank_R S$ is constant and there exists a finite set of pairwise strongly distinct elements $V \subset \mathrm{Alg}_R(S, S)$ such that $rank_R S = \#V$.*
(iii) *S is of constant rank and a homomorphic image of an S-split R-algebra.*
(iv) *There exists a finite number of pairwise orthogonal idempotents $e_1, ..., e_m$ of R whose sum is 1 such that Se_i is a Galois extension of Re_i with Galois group G_i and $o(G_i) = o(G_j)$, for all i, j.*
(v) *S is a weakly Galois extension of constant rank of R.*

To prove the theorem we need some preparation. We begin with the following proposition which is an easy consequence of Lemma 2.3 and gives a characterization of S-split algebras. In particular, this shows (i)↔(ii) of Theorem 4.1.

Propositon 4.2. *Let S be a faithfully projective R-algebra and let T be an R-algebra. Then the following conditions are equivalent.*

(i) *T is S-split.*

(ii) *T is a strongly separable extension of R, $rank_R T$ is constant and there exists a finite set $V \subset \mathrm{Alg}_R(T,S)$ whose elements are pairwise strongly distinct with $\#V = rank_R T$.*
Moreover, under the above conditions for every $g \in \mathrm{Alg}_R(T,S)$ and $f \in \mathrm{Alg}_R(S,S)$ there exists a unique set $\{e_v : v \in V\}$ of pairwise orthogonal idempotents of S whose sum is 1 such that $g(t) = \sum_{v\in V} f(v(t))e_v$, for all $t \in T$.

Proof. Let $\varphi : S\otimes T \to S^n$ be an isomorphism of S-algebras, $n \geq 1$. Denote by $\eta : T \to S\otimes T$ the canonical mapping and by $\pi_i : S^n \to S$ the ith projection, and put $\varphi_i = \pi_i\varphi\eta$. Clearly $\varphi_i \in \mathrm{Alg}_R(T,S)$, $\varphi_i \neq \varphi_j$ for all $i \neq j$, and $\varphi(s\otimes t) = (s\varphi_i(t))_{1\leq i\leq n}$, for every $s\otimes t \in S\otimes T$. Now take $V = \{\varphi_i : 1 \leq i \leq n\}$ and apply Lemma 2.3. The converse follows directly from this lemma.

The last part follows as in Theorem 3.1 of [3]. Denote by θ the homomorphism of R-algebras given by the composition $S^n \overset{\varphi^{-1}}{\to} S\otimes T \overset{f\otimes g}{\to} S\otimes S \overset{\mu}{\to} S$, where μ is the multiplication mapping. Then $e_j = \theta((\delta_{ij})_{1\leq i\leq n})$, $1 \leq j \leq n$, are the required idempotents. □

Proposition 4.3. *Let S be a faithfully projective algebra over R which has no non-trivial idempotents. If S is a homomorphic image of an S-split R-algebra, then $\mathrm{Alg}_R(S,S) = \mathrm{Aut}_R(S)$, $\#\mathrm{Aut}_R(S) = rank_R S$ and S is a Galois extension of R with Galois group $\mathrm{Aut}_R(S)$.*

Proof. Assume that T is an R-algebra, $\varphi : S\otimes T \to S^n$ an isomorphism of S-algebras and $\psi : T \to S$ is an epimorphisms of R-algebras.

From Proposition 4.2 it follows that T is faithfully projective and separable over R and $rank_R T = n$. Also, $\varphi(s\otimes t) = (s\varphi_i(t))_{1\leq i\leq n}$, where $V = \{\varphi_i : 1 \leq i \leq n\}$ is a set of n pairwise strongly distinct elements of $\mathrm{Alg}_R(S,S)$. Since T is R-separable so is S and by ([8], Lemma 1.6) there exists an idempotent $e \in T$ with $Ker\psi = Te$.

Every $v \in V$ with $v(e) = 0$ induces a homomorphism of R-algebras $\bar{v} : T/Te \to S$, so a homomorphism $\tilde{v} : S \to S$ because $S \simeq T/Te$. Denote by $\tilde{V}$ the set of all such homomorphisms, i. e., $\tilde{V} = \{\tilde{v} : v \in V, v(e) = 0\} \subseteq \mathrm{Alg}_R(S,S)$.

We claim that $\#\tilde{V} = rank_R S$. In fact, this is obvious if $e = 0$ and so we may assume $e \neq 0$. Since S has no non-trivial idempotents it follows from Corollary 2.2 that $rank_R S \geq \#\tilde{V} = \#V - \#\{v \in V : v(e) \neq 0\} = rank_R T - \#\{v \in V : v(e) \neq 0\}$. Furthermore, $T = Te \oplus T(1-e)$ and $T(1-e) \simeq S$ as R-algebras. So Te is a separable faithfully projective algebra over R. Again since S has no non-trivial idempotents for $v \in V$ with $v(e) \neq 0$ we have $v(e) = 1$. So every $v \in V$ with $v(e) \neq 0$ induces, by restriction, an R-algebra homomorphism $v|_{Te} : Te \to S$ and $\#V_e = \#\{v \in V : v(e) \neq 0\}$, where $V_e = \{v|_{Te} : v \in V, v(e) \neq 0\}$. Hence by Corollary 2.2 we have $\#V_e \leq rank_R Te$ and thus $rank_R S \geq \#\tilde{V} \geq rank_R T - rank_R Te = rank_R(T/Te) = rank_R S$.

Finally, by Proposition 4.2 given $g \in \mathrm{Alg}_R(S,S)$ there exists unique $\tilde{v} \in \tilde{V}$ with $g = id_S\tilde{v} = \tilde{v}$. Hence $\mathrm{Alg}_R(S,S) = \tilde{V}$. Also, again by 4.2 given $\tilde{v} \in \tilde{V}$ there exists $\tilde{u} \in \tilde{V}$ with $id_S = \tilde{v}\tilde{u}$. This shows that $\mathrm{Alg}_R(S,S) = \mathrm{Aut}_R(S)$. The result follows by Lemma 2.3. □

Now we prove an interesting particular case of Theorem 4.1.

Theorem 4.4. *Assume that S is a faithfully projective R-algebra and R has no non-trivial* *idempotents. If S is a homomorphic image of an S-split R-algebra, then S is a Galois extension of R.*

Proof. Assume that T is an S-split R-algebra and $\psi : T \to S$ is an epimorphism of R-algebras. By Proposition 4.2, T is separable over R and there exists $V \subset \mathrm{Alg}_R(T, S)$ whose elements are pairwise strongly distinct and $\#V = rank_R T$. So S is also separable over R and then ([13], Proposition 1.2) shows that there exists a family $(e_i)_{1\leq i\leq m}$ of minimal idempotents of S whose sum is one. Thus we have $S = S_1 \oplus ... \oplus S_m$, where $S_i = Se_i$ is a separable and faithfully projective algebra over R which has no non-trivial idempotents. Moreover, for $f, g \in \mathrm{Alg}_R(T, S)$, f and g are pairwise strongly distinct if and only if $e_i f \neq e_i g$ for all i. On the other hand, by ([8], Lemma 1.6) there exists an idempotent $e \in T$ such that $Ker\psi = Te$. Then $T = Te \oplus T(1-e)$ and $T(1-e) \simeq S$ as R-algebras. Consequently we can consider $T = Te \oplus S_1 \oplus ... \oplus S_m$. We divide the proof in several steps.

Claim 1. For every $1 \leq i, j \leq m$ there exists $v \in V$ with $e_j v(e_i) \neq 0$.
By the way of contradiction, assume that there exist i, j such that $e_j v|_{S_i} = 0$ for every $v \in V$. Then $e_j v$ induces a homomorphism $\overline{e_j v} : \overline{T} = Te \oplus S_1 \oplus ... \oplus \hat{S}_i \oplus ... \oplus S_m \to S_j$, $1 \leq j \leq m$, and the elements of $e_j V = \{\overline{e_j v} : v \in V\}$ are pairwise distinct. By Corollary 2.2 this is a contradiction since S_i has no non-trivial idempotents and $rank_R T > rank_R(\overline{T})$.

Claim 2. If $e_j v(e_i) \neq 0$, then $e_j v|_{S_i} : S_i \to S_j$ is an isomorphism of algebras over R. In particular, $S_i \simeq S_j$ for all i, j.
In fact, since e_j is minimal and $e_j v(e_i)$ is an idempotent, when $e_j v(e_i) \neq 0$ we necessarily have $e_j v(e_i) = e_j$. Hence $e_j v|_{S_i} : S_i \to S_j$ is a homomorphism of R-algebras. It follows that $e_j v|_{S_i}$ is a monomorphism, by ([8], Lemma 1.6). Also, there exists $v' \in V$ with $e_i v'(e_j) \neq 0$ and so $e_i v'|_{S_j} : S_j \to S_i$ is a monomorphism too. The claim follows by Lemma 1.1.

Claim 3. S_i is a Galois extension of R with Galois group $\mathrm{Aut}_R(S_i)$, for $1 \leq i \leq m$.
This follows from the assumption and Proposition 4.3. In fact, since T is S-split we can easily see that T is also S_i-split, for $1 \leq i \leq m$ and clearly S_i is a homomorphic image of T.

Now we complete the proof of the theorem. Put $H = \mathrm{Aut}_R(S_1)$. The argument that follows is the same as in ([14], (3.15)). For every $1 \leq i \leq m$ choose an isomorphism $\alpha_i : S_1 \to S_i$. So $\mathrm{Aut}_R(S_i) = \alpha_i H \alpha_i^{-1} = \{\tau_i = \alpha_i \tau \alpha_i^{-1} : \tau \in H\}$ and H can be seen as a group of R-automorphisms of S via the identification $\tau = e_1\tau_1 + ... + e_m\tau_m$, for every $\tau \in H$. Define an R-automorphism σ of S by demanding that σ restricted to S_i equals $\alpha_{i+1}\alpha_i^{-1}$, for $1 \leq i \leq m-1$, and σ restricted to S_m equals α_m^{-1}. It can easily be seen that $G = \cup_{1\leq i\leq m}\sigma^i H$ is a finite group of pairwise strongly distinct R-automorphisms of S and S is a Galois extension of R with Galois group G, by Lemma 2.3.

Remark 4.5. The group G constructed in the above theorem is not necessarily unique. In fact, if T is a Galois extension of R with Galois group H, T has no non-trivial idempotents, and $S = Te_1 \oplus Te_2 \oplus Te_3 \oplus Te_4$ we can take $G = \cup_{0\leq i\leq 3}\sigma^i H$, where $\sigma(e_i) = e_{i+1(\mathrm{mod} 4)}$, as in the proof of Theorem 4.4. Also, we can define $\rho_i \in \mathrm{Aut}_R(S)$ by demanding that $\rho_1(e_1) = e_2$, $\rho_1(e_2) = e_1$, $\rho_1(e_3) = e_4$ and $\rho_1(e_4) = e_3$. Similarly, ρ_2 is defined by $\rho_2^{\pm 1}(e_1) = e_3$ and $\rho_2^{\pm 1}(e_2) = e_4$ and $\rho_3 = \rho_1\rho_2$. Hence $F = \{id, \rho_1, \rho_2, \rho_3\}$ is a group of pairwise strongly distinct

R-automorphisms of S and S is a Galois extension of R with Galois group $G' = FH$. Finally, we easily see that G and G' are not isomorphic.

Now we are in position to prove the theorem.

Proof of Theorem 4.1.
(i) $\leftrightarrow$ (ii): Proposition 4.2.
(i) $\rightarrow$ (iii): Obvious.
(iii) $\rightarrow$ (v) For this part of the proof we use freely the result of [14]. Denote by $B(R)$ the Boolean ring of the ring R and by $X = X(R)$ the Boolean spectrum of R consisting of all the prime ideals of $B(R)$. Assume that S is a homomorphic image of an S-split R-algebra and let $x \in X$. Then R_x has no non-trivial idempotents and S_x is a faithfully projective R_x-algebra which is a homomorphic image of an S_x-split R_x-algebra. Hence Theorem 4.4 implies that S_x is a Galois extension of R_x with some Galois group G_x. Lift G_x to a finite set of R-automorphisms $F(x)$ of S and consider the (finite) subgroup $H(x)$ of $\mathrm{Aut}_R(S)$ generated by $F(x)$. Then $S_y^{H(x)_y} = R_y$ for all y in a neighborhood of x. By compactness, we get a finite number of these neighborhoods covering X and a finite number of subgroups of the type $H(x)$ which generate a finite group H of $\mathrm{Aut}_R(S)$. Since $S_z^{H_z} = R_z$ for every $z \in X$, we obtain $S^H = R$. Thus S is a weakly Galois extension of R.
(iv) $\leftrightarrow$ (v) It follows easily from (3.15) of [14], since a decomposition $S = \sum_{i=1}^m \oplus Se_i$ over $R = \sum_{i=1}^m \oplus Re_i$ has constant rank over R if and only if each Se_i has constant rank n_i over Re_i and all the n_i's are equal.
(iv) $\rightarrow$ (i) Assume that there exists a finite set of pairwise orthogonal idempotents $\{e_1, ..., e_m\}$ of R with $\sum_{1\leq i\leq m} e_i = 1$ and $S_i = Se_i$ is a Galois extension of $R_i = Re_i$ with a Galois group G_i, $o(G_i) = n$ for some $n \geq 1$ and for every $1 \leq i \leq m$. Then $S_i \otimes_{R_i} S_i \simeq S_i^n$ as S_i-algebras and it follows that $S \otimes_R S \simeq \sum_{1\leq i\leq m} \oplus S_i \otimes_{R_i} S_i \simeq \sum_{1\leq i\leq m} \oplus S_i^n \simeq S^n$ as S-algebras. □

Remark 4.6. Under the same notation of Theorem 4.1, the groups G_i are not uniquely determined. It is easy to prove that if we can select a set $\{G_1, ..., G_m\}$ such that $G_i \simeq G_j$, for all i, j, then S is a Galois extension of R with a Galois group $G \simeq G_i$.

5. Strongly separable splitting rings

Let S be an extension of R. Recall that S is said to be a splitting ring over R if there exist a monic polynomial $f \in R[X]$ and elements $x_1, ..., x_n \in S$ such that $S = R[x_1, ..., x_n]$ and $f = \Pi_{1\leq i\leq n}(X - x_i)$. In this case S is also called a splitting ring of the polynomial f over R. This notion is an extension of the notion of splitting field of a polynomial and has been studied for rings by several authors ([1], [2], [8], [11], [12], [15]).

A splitting ring over R is obviously a finitely generated extension of R, but it is not necessarily R-separable neither projective as an R-module. Several examples may be found even in field theory for the first affirmation. The following example, due to Janusz [8], shows the second.

Example 5.1. Let $\mathbf{Z}_{(2)}$ be the localization at 2 in the ring of all the rational integers and take $R = \mathbf{Z}_{(2)}[\sqrt{5}]$ and $S = R[2^{-1}(1 - \sqrt{5})]$. Then S is a splitting ring of the polynomial $f = X^2 + X - 1 \in R[X]$, but S is not projective over R.

A monic polynomial $f \in R[X]$ is said to be separable over R if the R-algebra $R[X]/\langle f\rangle$ is separable over R. The following lemma is an immediate consequence of Corollary 8 in [16] and Corollary 3 in [10].

Lemma 5.2. *Let f be a monic polynomial in $R[X]$ and $S = R[x_1, ..., x_n]$ a splitting ring of f over R. Then f is separable over R if and only if $\Pi_{1\leq i<j\leq n}(x_i - x_j)$ is invertible in S. In particular, in this case S is R-separable.*

We say that a splitting ring S of a monic polynomial $f \in R[X]$ is a strongly separable splitting ring over R if f is separable over R and S is projective as an R-module.

In ([12], Theorem 3.1) Nagahara proved that every strongly separable splitting ring S over R is a weakly Galois extension of R. The purpose of this section is to give a new proof of that result using the same approach of ([5], p. 136-137) and the results of the former section.

Theorem 5.3. *Let S be a strongly separable splitting ring over R and assume that $rank_R S$ is constant. Then S is a weakly Galois extension of R.*

Proof. Let $S = R[x_1, ..., x_n]$ with $\Pi_{1\leq i<j\leq n}(x_i - x_j)$ invertible in S and put $f = \Pi_{1\leq i\leq n}(X - x_i) = X^n - r_1X^{n-1} + ... + (-1)^n r_n \in R[X]$. Assume that S is projective as an R-module and $rank_R S$ is constant. For every $\tau \in S_{\underline{n}}$ (the symmetric group of degree n) there exists an R-algebra homomorphism $\tau^* : R[X_1, ..., X_n] \to S$ defined by $\tau^*(X_i) = x_{\tau(i)}$, $1 \leq i \leq n$. Denote by $s_k = s_k(X_1, ..., X_n) = \sum_{1\leq i_1<...<i_k\leq n} X_{i_1}X_{i_2}...X_{i_k}$ the kth elementary symmetric functions of $X_1, ..., X_n$. Then $\tau^*(s_k - r_k) = 0$ for $1 \leq k \leq n$; hence τ^* induces an R-algebra homomorphism (which we again denote by τ^*) $\tau^* : A \to S$ given by $\tau^*(t_i) = x_{\tau(i)}$ for $1 \leq i \leq n$, where $A = R[X_1, ..., X_n]/I$, I is the ideal of A generated by $\{s_k - r_k : 1 \leq k \leq n\}$ and $t_i = X_i + I$ in A. The set $V = \{\tau^* : \tau \in S_n\} \subset \mathrm{Alg}_R(A, S)$ is a set of $n!$ pairwise strongly distinct elements, since for $\tau(i) \neq \sigma(i)$ the difference $x_{\tau(i)} - x_{\sigma(i)}$ is invertible. It follows by ([11], Corollaries 1.1 and 1.2) that A is a free R-module of rank $n! = \#V$. Furthermore, A is also a splitting ring of the polynomial f and so A is separable over R, by Lemma 5.2. Then Proposition 4.2 shows that A is S-split. Finally, since S is a homomorphic image of A the result follows from Theorem 4.1. □

Remark 5.4. The proof of Theorem 5.3 together with Lemma 2.3 shows that the R-algebra A constructed in that proof is a Galois extension of R with Galois group $S_{\underline{n}}$ (cf. [2], Proposition 5; [11], Theorem 2.1). Also, by Theorem 4.4 it follows that if R has no non-trivial idempotents and S is a strongly separable splitting ring over R, then S is a Galois extension of R.

The following corollary gives the Nagahara's result mentioned above.

Corollary 5.5. *Every strongly separable splitting ring S over R is a weakly Galois extension of R.*

Proof. Note that there exists a finite set of pairwise orthogonal idempotents $\{e_1, ..., e_m\}$ of R whose sum is 1 and such that $rank_{Re_i} Se_i$ is constant. Clearly Se_i is a strongly separable splitting ring over Re_i, for every $1 \leq i \leq m$, and the result follows by Theorem 5.3. □

Nagahara ([12], Remark 2.1) showed that a strongly separable splitting ring S over R is not necessarily a Galois extension of R. However in his example the rank of S over R is not constant. The following example shows that the same holds even if S is a strongly separable splitting ring of constant rank over S.

Example 5.6. Denote by $\mathbf{Q}$ the field of rational integers and let $f_1 = X^4 + X^3 + X^2 + X + 1$, $f_2 = X^4 - 5X^2 + 6$ in $\mathbf{Q}[X]$. Then $\mathbf{Q}(w)$ is a splitting field of f_1 over $\mathbf{Q}$, where w is a primitive root of unit of order 5, and $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field of f_2 over $\mathbf{Q}$. Also the splitting ring of the polynomial $f = (1,1)X^4 + (1,0)X^3 + (1,-5)X^2 + (1,0)X + (1,6) \in R[X]$ over $R = \mathbf{Q} \times \mathbf{Q}$ is the strongly separable extension of constant rank 4 $S = R[(w, \sqrt{2}), (w^2, \sqrt{3}), (w^3, -\sqrt{2}), (w^4, -\sqrt{3})]$ which is a weakly Galois extension of R and it is not a Galois extension of R. In fact, this result easily follows from the observation that the Galois groups of $\mathbf{Q}(w)$ and $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$ are not isomorphic.

Acknowledgement. This paper was written while the second named author was visiting Universidade Federal do Rio Grande do Sul. He is grateful for the hospitality given by the members of the Instituto de Matemática.

References

[1] Auslander, M.; Goldman, O.: *The Brauer group of a commutative ring.* Trans. Amer. Math. Soc. **97** (1960), 367–409.

[2] Barnard, A. D.: *Commutative rings with operators (Galois theory and ramification).* Proc. London Math. Soc. **28** (1974), 274–290.

[3] Chase, S. U.; Harrison, D. K.; Rosenberg, A.: *Galois theory and Galois cohomology of commutative rings.* Mem. Amer. Math. Soc. **52** (1965), 15–33.

[4] DeMeyer, F.; Ingraham, E.: *Separable algebras over commutative rings.* Lecture Notes in Math. 181, Springer Verlag, 1971.

[5] Dress, A. W.: *One more shortcut to Galois theory.* Adv. Math. **110** (1995), 129–140.

[6] Dress, A. W.: *Basic non-commutative Galois theory.* Adv. Math. **110** (1995), 141–173.

[7] Ingraham, E.: *Inertial subalgebras of algebras over commutative rings.* Trans. Amer. Math. Soc. **124** (1966), 77–93.

[8] Janusz, G. J.: *Separable algebras over commutative rings.* Trans. Amer. Math. Soc. **122** (1966), 461–479.

[9] Knus, M.-A.; Ojanguren, M.: *Théorie de la descente et algèbres d'Azumaya.* Lecture Notes in Math. 389, Springer Verlag, 1974.

[10] Nagahara, T.: *On separable polynomials over a commutative ring.* Math. J. Okayama Univ. **14** (1970), 175–181.

[11] Nagahara, T.: *On separable polynomials over a commutative ring II.* Math. J. Okayama Univ. **15** (1972), 149–162.

[12] Nagahara, T.: *On separable polynomials over a commutative ring III.* Math. J. Okayama Univ. **16** (1973/74), 189–197.

[13] Villamayor, O. E.; Zelinsky, D.: *Galois theory for rings with finitely many idempotents.* Nagoya Math. J. **27** (1966), 721–731.

[14] Villamayor, O. E.; Zelinsky, D.: *Galois theory with infinitely many idempotents.* Nagoya Math. J. **35** (1969), 83–98.

[15] Wang, S. S.: *Splitting ring of a monic separable polynomial.* Pacific J. Math. **75** (1978), 293–296.

[16] Wang, S. S.: *A Jacobian criterion for separability.* J. Algebra **65** (1980), 453–494.

Received October 2, 1996