Ferrero, M.
Osaka J. Math,
7 (1970), 81-88

ON THE GALOIS THEORY OF NON-COMMUTATIVE RINGS

MIGUEL FERRERO

(Received July 3, 1969)

In this paper, some results of Galois theory for commutative rings without idempotents developed by Chase, Harrison and Rosenberg in [1], are generalized to non-commutative rings that verify a certain condition. Some proofs are similar to those appearing in [1].

The author wishes to thank Prof. O. Villamayor for his important suggestions. Some ideas here belong to a not yet published work by O. Villamayor and D. Zelinsky.

The final form of this paper was written while the author was under a fellowship granted by Consejo Nacional de Investigaciones Científicas y Técnicas.

1. Introduction

In this section, the previous definitions, already known, are remembered. As usual, all rings have units, all modules are unitary and ring homomorphisms carry the unit into the unit.

Let S be a ring, G a finite group of automorphisms of S and $R=S^G$, the fixed subring. We say that S is a Galois extension of R with group G, if there exist elements x_i, y_i $(i=1, 2, \cdots, n)$ in S, such that:

$$\sum_i x_i\sigma(y_i) = \delta_{1,\sigma}, \qquad \text{for all } \sigma\in G.$$

We indicate with $D=D(S, G)$ the crossed product of S with basis $(u_\sigma)_{\sigma\in G}$ and with tr the trace map, that is to say, the map of S into R defined by $tr(x) = \sum_{\sigma\in G}\sigma(x)$.

S^* shall denote the S structure as a right module, on the ring mentioned in each case.

The application $d: D\to \mathrm{Hom}_R(S^*, S^*)$, defined by $d(s\cdot u_\sigma)(x)=s\sigma(x)$, for each s, x in S and each σ in G, is a ring homomorphism and two-sided S-homomorphism.

As in [1], E designates the set of all functions of G into S. Then E is a ring

and a two-sided S-module in an obvious way. In addition, E is a direct sum of the S-submodules $S\cdot v_\sigma(\sigma\in G)$, where $v_\sigma\colon G\to S$ is defined by $v_\sigma(\tau)=\delta_{\sigma,\tau}$.

If M is a left D-module and M^G is the R-submodule, the elements of which are $m\in M$ such that $u_\sigma\cdot m=m$, $\forall\sigma\in G$, the map $\omega\colon S\otimes_R M^G\to M$ defined by $\omega(s\otimes m)=s\cdot m$, is an S-homomorphism.

If $h\colon S\otimes_R S\to E$ is defined by $h(s\otimes t)(\sigma)=s\cdot\sigma(t)$, then h is a two-sided S-homomorphism, that is an $S\otimes_Z S^0$-homomorphism (S^0 indicates the opposite ring of S and Z the ring of rational integers).

The definition of separable extension is the same as in [2], that is as follows:

Let $\Gamma\to\Lambda$ be a ring homomorphism (frequently the inclusion). Then Λ is a two-sided Γ-module and the abelian group $\Lambda\otimes_\Gamma\Lambda$ is a two-sided Λ-module. Therefore $\Lambda\otimes_\Gamma\Lambda$ is a left $\Lambda\otimes_Z\Lambda^0$-module with product defined by:

$$x\otimes y^0\in\Lambda\otimes_Z\Lambda^0\,,\quad u\otimes v\in\Lambda\otimes_\Gamma\Lambda\,,\quad (x\otimes y^0)\cdot(u\otimes v)=xu\otimes vy\,.$$

The multiplication $\Lambda\otimes_\Gamma\Lambda\to\Lambda$ is a $\Lambda\otimes_Z\Lambda^0$-homomorphism. We say that Λ is separable on Γ if there exists a $\Lambda\otimes_Z\Lambda^0$-homomorphism $\Lambda\to\Lambda\otimes_\Gamma\Lambda$such that the composition $\Lambda\to\Lambda\otimes_\Gamma\Lambda\to\Lambda$ is the identity in Λ.

This is equivalent to the existence of elements x_i, y_i $(i=1,2,\cdots,m)$ in Λ such that $\sum_i x_i\cdot y_i=1$ and $\sum_i x\cdot x_i\otimes y_i=\sum_i x_i\otimes y_i\cdot x$, $\forall x\in\Lambda$, in $\Lambda\otimes_\Gamma\Lambda$.

2. Galois extensions

The conditions of the following proposition are those given by Chase, Harrison and Rosenberg for the commutative case in the theorem 1.3 of [1].

The proof is a trivial extension of it, so we shall omit it. The equivalence between (a) and (b) has been proved by T. Kanzaki for the non-commutative rings in [3].

Proposition 2.1. *If S is a ring, G a finite group of automorphisms of S and $R=S^G$, the following statements are equivalent:*

(a) *S is a Galois extension of R with group G.*

(b) *S is finitely generated and projective as right R-module and $d\colon D\to \mathrm{Hom}_R(S^*, S^*)$ is an isomorphism.*

(c) *If M is a left D-module, $\omega\colon S\otimes_R M^G\to M$ is an isomorphism.*

(d) *$h\colon S\otimes_R S\to E$ is an isomorphism.*

On the other hand, Hirata and Sugano in [2] (prop. 3.3.), prove that if S is a Galois extension of R with group G, S is R-separable.

We shall consider here a case where the converse holds. Let $\mu\colon S\otimes_Z S^0\to S$ be the multiplication. We say that S verifies (H) if:

$$z\in S\otimes_Z S^0\,,\quad \mu(z)=\mu(z^2)\Rightarrow\mu(z)=0\quad\text{or}\quad\mu(z)=1\,.$$

Equivalently, S verifies (H) if for every finite family x_i, y_i in S:

$$\sum_{i,j} x_i \cdot x_j \cdot y_j \cdot y_i = \sum_i x_i \cdot y_i \Rightarrow \sum_i x_i \cdot y_i = 0 \quad \text{or} \quad \sum_i x_i \cdot y_i = 1 .$$

If S verifies (H), it has no idempotents other than 0 and 1. If S is commutative, (H) holds if and only if S has no non trivial idempotents, because μ is a ring homomorphism in this case.

An example, given below, shows that there exist non commutative rings verifying (H).

Theorem 2.2. *Let S be a ring that verifies (H), G a finite group of automorphisms of S and $R=S^G$. Then S is a Galois extension of R with group G, if and only if S is R-separable.*

Proof. If S is R-separable, there exist x_i, y_i in S such that:

$$\sum_i x_i \cdot y_i = 1 \quad \text{and} \quad \sum_i x \cdot x_i \otimes y_i = \sum_i x_i \otimes y_i \cdot x , \quad \forall x \in S , \quad \text{in} \quad S \otimes_R S .$$

Applying to the last relation the composition $\Phi \cdot (1 \otimes \sigma)$, where $\Phi : S \otimes_R S \to S$ is the multiplication, we obtain

$$(1) \qquad x \cdot \sum_i x_i \sigma(y_i) = \sum_i x_i \sigma(y_i) \sigma(x) , \quad \text{for all } x \in S \text{ and } \sigma \in G .$$

Let $e_\sigma = \sum_i x_i \otimes \sigma(y_i)^0 \in S \otimes_Z S^0$. Using (1) it is easy to prove that $\mu(e_\sigma) = \mu(e_\sigma^2)$. If $\sum_i x_i \sigma(y_i) = 1$, $\sigma(x) = \sum_i x_i \sigma(y_i) \sigma(x) = x \sum_i x_i \sigma(y_i) = x$ by (1). Therefore $\sum x_i \sigma(y_i) = \mu(e_\sigma) = \delta_{1,\sigma}$.

3. Galois theorem.

A part of the following proposition is the proposition 3.4 of [2]. The remainder one is an immediate generalization of that of the theorem 2.2 of [1].

Proposition 3.1. *Let S be a Galois extension of R with group G, H a subgroup of G and $T=S^H$. Then S is a Galois extension of T with group H and H is the set of* all *elements of G leaving T pointwise fixed.*

Let us suppose that $tr(S)=R$. Then T is R-separable and if H is normal in G, T is a Galois extension of R with groug G/H.

The above assumption on S enable us to prove the reciprocal theorem just by using the same technique employed by Chase, Harrison and Rosenberg (see 2.2 of [1]).

Proposition 3.2. *Let S be a Galois extension of R with group G. Let us suppose that S verifies (H) and* $\mathrm{tr}(S)=R$. *If T is a subring of S that contains R and it is R-separable, then there exists a subgroup H of G such that $T=S^H$.*

Proof. Let H be the set of the elements of G such that its restriction to T is the identity, and $\sum_i x_i \otimes y_i \in T \otimes_R T$ the element that satisfies the condition of separability. A similar reasoning to that of Theorem 2.2 allows us to conclude that:

$$(2) \qquad \sum_i x_i \sigma(y_i) = \begin{cases} 1 & \text{if } \sigma \in H \\ 0 & \text{if } \sigma \notin H \end{cases}$$

As in [1] we define an action of G on E by $\sigma(v)(\tau)=v(\tau, \sigma)$ for $\sigma \in G$, $\tau \in G$, $v \in E$. Then E^H is the set of the elements of E, which are constant on each right coset of H in G. Since S is projective as right R-module and $h: S \otimes_R S \to E$ is an isomorphism, we have the injections $S \otimes_R T \to S \otimes_R S^H \to S \otimes_R S \simeq E$, where the image of $S \otimes_R S^H$ is contained in E^H. Now we shall show that $S \otimes_R T \to E^H$ is onto. Let $v \in E^H$ and J be a family of indices such that $(\sigma_j)_{j \in J}$ contains one element, and only one, of each right coset of H in G. We write $z = \sum_{j \in J} \sum_i v(\sigma_j) \sigma_j(x_i) \otimes y_i \in S \otimes_R T$. By using (2) it is easy to obtain $h(z)(\sigma_k)=v(\sigma_k)$ for all $k \in I$. Since $h(z)$ and v are constant on each right coset, it follows that $h(z)=v$. Then $S \otimes_R T = S \otimes_R S^H$ and by applying $\mathrm{tr} \otimes 1$ we obtain $T=S^H$. This completes the proof.

The two above propositions give the following version of the Galois theorem:

Theorem 3.3. *Let S be a Galois extension of R with group G. If S verifies (H) and $\mathrm{tr}(S)=R$, there is a one to one correspondence between subgroups of G and subrings of S that contain R and are R-separables, such that the subgroup H corresponds to the subring T if and only if $T=S^H$.*

4. An example

Let A be a commutative ring of characteristic 2 which has no non trivial idempotents; $A[X, Y]$ the non-commutative ring of polynomials; I the two-sided ideal of $A[X, Y]$ generated by $\{X^2, Y^2, XYX, YXY\}$. We write $A[X, Y]/I = A[u, v] = S$, where u and v denote the classes of X and Y in the quotient, respectively.

Since S is a free A-module with basis $\{1, u, v, uv, vu\}$, the equation $\mu(z) = \mu(z^2)$ for $z \in S \otimes_Z S^0$ is translated into a system of equations, which shows that $\mu(z)=0$ or $\mu(z)=1$ (we omitt here the resolution of this system but we want to emphasize that the assumption on the characteristic of S reduces the system). Therefore S verifies (H)(*).

(*) At the moment, the author is able to prove that every graded ring $A = \bigoplus_{i=0}^{\infty} A_i$ where A_0 has no non trivial idempotents and it is contained in the center of A, verifies condition (H).

Now let A be a Galois extension of B with group G (A as before). It is clear that $S=A[u, v]=A\otimes_{Z_2}Z_2[u, v]$ where $Z_2=Z/2Z$. Therefore G is a group of automorphisms of S (looking to each σ as $\sigma\otimes 1$) and the fixed subring is $R=B\otimes_{Z_2}Z_2[u, v]=B[u, v]$.

If a_i, b_i are the elements of A such that $\sum_i a_i\sigma(b_i)=\delta_{1,\sigma}$, then $a_i\otimes 1$, $b_i\otimes 1$, satisfy the same relation. Hence it follows that S is a Galois extension of R with group G.

Besides, by [1], there exists $c\in S$ such that $tr(c)=1$. Then $c\otimes 1$ satisfies the same relation in S, and hence $tr: S\to R$ is onto.

The theorem 3.3 shows that every subring of S that contains R and is separable on R, is of the form $C[u, v]=C\otimes_{Z_2}Z_2[u, v]$, where C is a subring of A, which is B-separable.

5. Endomorphisms, automorphisms and homomorphisms

An automorphism σ of S is called *outer* if $x\sigma(s)=s\cdot x$, $\forall s\in S\Rightarrow x=0$.

Proposition 5.1. *Let S be a Galois extension of R with group G. We suppose that every non outer R-automorphism of S is in G. Then G is the group of all R-automorphisms of S.*

Proof. Let x_i, y_i be the elements of S such that $\sum_i x_i\sigma(y_i)=\delta_{1,\sigma}$. The proof of Proposition 3.3 of [2] shows that the element $\sum_i x_i\otimes y_i\in S\otimes_R S$ satisfies the condition of separability. From relation (1) of Proposition 2.2 it follows that $\sum_i x_i\tau(y_i)=0$ for every outer R-automorphism of S.

Now let ρ be an R-automorphism of S which does not belong to G. We have that $h(\sum_i x_i\otimes\rho(y_i))=\sum_\sigma s_\sigma v_\sigma$, with $s_\sigma=\sum_i x_i\sigma\rho(y_i)\in S$. As $\sigma\rho$ is not in G for each $\sigma\in G$, it must be outer, hence $s_\sigma=0$. Therefore $\sum_i x_i\otimes\rho(y_i)=0$ and applying $1\otimes\rho^{-1}$ we obtain $\sum_i x_i\otimes y_i=0$, which contradicts $\sum_i x_i\cdot y_i=1$.

If we denote by s the application of S into S, defined by $x\mapsto sx$, for each $s\in S$, we have that $s\in\mathrm{Hom}_R(S^*, S^*)$.

Let S be a Galois extension of R with group G. The isomorphism $d: D\to \mathrm{Hom}_R(S^*, S^*)$ allows us to write $\alpha=\sum_\sigma s_\sigma\cdot\sigma$, for every $\alpha\in\mathrm{Hom}_R(S^*, S^*)$, where $s_\sigma\cdot\sigma$ is the composition in $\mathrm{Hom}_R(S^*, S^*)$.

Similarly, if $s\in S$ we denote by s^* the map $x\mapsto xs$. Then $s^0\in\mathrm{Hom}_R({}^*S, {}^*S)$ and $s^0\in\mathrm{Hom}_R(S^*, S^*)$ if and only if s is in the centralizer of R in S. If $s\in S$ and $\alpha\in\mathrm{Hom}_R(S^*, S^*)$, with $s^*\cdot\alpha$ we denote the composition in $\mathrm{Hom}_Z(S, S)$.

Lemma 5.2. *Let S be a Galois extension of R with group G and $\alpha=\sum_{\sigma\in G} s_\sigma\cdot$*

$\sigma \in \mathrm{Hom}_R(S^*, S^*)$. *Then α is a ring homomorphism if and only if $s_\sigma^0 \cdot \alpha = s_\sigma \cdot \sigma$ for every σ in G and $\sum_{\sigma \in G} s_\sigma = 1$.*

Proof. From the following equivalences it follows trivially:

$$\alpha(x \cdot y) = \alpha(x) \cdot \alpha(y), \quad \forall x \in S, \ \forall y \in S, \quad \text{if and only if}$$
$$\sum_{\sigma \in G} s_\sigma \sigma(x) \sigma(y) = \sum_{\tau \in G} [\sum_{\sigma \in G} s_\sigma \sigma(x)] s_\tau \tau(y), \ \forall x \in S, \ \forall y \in S, \quad \text{if and only if}$$
$$\sum_{\sigma \in G} s_\sigma \sigma(x) u_\sigma = \sum_{\tau \in G} [\sum_{\sigma \in G} s_\sigma \sigma(x)] s_\tau \cdot u_\tau .$$

The following theorem is a generalization of Corollary 3.3 of [1].

Theorem 5.3. *Let S be a Galois extension of R with group G and $\alpha = \sum_{\sigma \in G} s_\sigma \cdot \sigma \in \mathrm{Hom}_R(S^*, S^*)$. If x_i, y_i $(i = 1, 2, \cdots, n)$ are the elements of S such that $\sum_i x_i \sigma(y_i) = \delta_{1,\sigma}$ and if $e_\sigma = \sum_i \alpha(x_i) \otimes \sigma(y_i)^0 \in S \otimes_Z S^0$, then $s_\sigma = \mu(e_\sigma)$. Furthermore if α is a ring homomorphism each s_σ is in the centralizer of R in S, $\mu(e_\sigma) = \mu(e_\sigma^2)$, $\mu(e_\sigma \cdot e_\tau) = 0$ if $\sigma \neq \tau$ and $\sum_{\sigma \in G} \mu(e_\sigma) = 1$.*

If S verifies (H), G is the set of all endomorphisms of the ring S which are R-homomorphisms.

Finally, if each s_σ is in the center of S and α is a ring homomorphism, $(s_\sigma)_{\sigma \in G}$ is a family of pairwise orthogonal idempotents with sum one.

Proof. Since from the relation $\sum_i x_i \sigma(y_i) = \delta_{1,\sigma}$ it follows that $\sum_i \tau(x_i) \sigma(y_i) = \delta_{\tau,\sigma}$, we have:

$$\mu(e_\sigma) = \sum_i \alpha(x_i) \sigma(y_i) = \sum_i \sum_{\tau \in G} s_\tau \tau(x_i) \sigma(y_i) = \sum_{\tau \in G} s_\tau \delta_{\tau,\sigma} = s_\sigma .$$

If α is a ring endomorphism, from lemma 5.2 we obtain that each s_σ commutes with R and

$$\sum_\sigma \mu(e_\sigma) = 1 . \tag{3}$$

Besides:

$$\mu(e_\sigma \cdot e_\tau) = \sum_{i,j} \alpha(x_i) \alpha(x_j) \tau(y_j) \sigma(y_i) = \sum_i \alpha(x_i) s_\tau \sigma(y_i) = s_\tau \sum \tau(x_i) \sigma(y_i)$$
$$= \mu(e_\tau) \cdot \delta_{\sigma,\tau} .$$

If S verifies (H) and α is a ring endomorphism of S which is an R-homomorphism, $\mu(e_\sigma)$ is 0 or 1. From (3) at least one of the s_σ has to be equal to one. If for $\sigma \neq \tau$, $s_\sigma = s_\tau = 1$ we have:

$0 = \mu(e_\sigma \cdot e_\tau) = \sum_i \alpha(x_i) s_\tau \sigma(y_i) = 1$. Therefore $\alpha = \rho$ for some $\rho \in G$.

Finally, if each s_σ is in the center of S, from the latter lemma we obtain:

$$s_\sigma\sigma(x)=s_\sigma\alpha(x)=\sum_{\tau\in G} s_\sigma s_\tau\tau(x),\ \forall x\in S,\ \forall\sigma\in G, \text{ hence } s_\sigma\cdot s_\tau=s_\sigma\delta_{\sigma,\tau}$$

which completes the proof.

The following corollary may be obtain as a particular case of Theorem 4.1 of [4].

As a consequence of the former proposition we have:

Corollary 5.4. *Let S be a Galois extension of R with group G and $\alpha=\sum_{\sigma\in G} s_\sigma\cdot\sigma\in Hom_R(S^*, S^*)$ a ring homomorphism. If G is a group of outer automorphisms, $(s_\sigma)_{\sigma\in G}$ is a family of pairwise orthogonal central idempotents with sum one. If furthermore the center of S has no non trivial idempotents, G is the set of all ring endormorphisms of S, which are R-homomorphisms.*

Proof. It is clear that G is a group of outer automorphisms if and only if, for every σ in G, $\sigma\neq 1$,

$$J_\sigma=\{x\in S: x\sigma(s)=sx,\ \forall s\in S\}=0\,.$$

Miyashita has observed in [4] that this is true if and only if S is outer G-Galois on R, that is if the centralizer of R in S is the center of S. The above theorem shows that, under these conditions, each s_σ is in the center of S and then, the last part of the same theorem completes the proof.

The following result is an immediate generalization of Theorem 3.4 of [1].

Proposition 5.5. *Let S and S' be rings, G a finite group of automorphisms of S and S', $f: S\to S'$ a ring homomorphism which is a G-homomorphism. If S is a Galois extension of R with group G, S' is a Galois extension of S'^G with group G. If furthermore $S'^G=R$ and f is a right R-homomorphism, then f is an isomor*phism.

Proof. If x_i, y_i are in S and satisfy $\sum_i x_i\sigma(y_i)=\delta_{1,\sigma}$, then $f(x_i), f(y_i)$ satisfy the same relation in S'. To prove the second part, it is enough to define $f':S'\to S$ by $f'(x')=\sum_i x_i\cdot tr(f(y_i)\cdot x')$, $\forall x'\in S'$. Then, it is easy to check that f' is the inverse of f.

Corollary 5.6. *Let S and S' be rings such that $S\subset S'$. Let us suppose that G is a finite group of automorphisms of S', whose restriction is a group of automorphisms of S isomorphic to G and let $R=S'^G$. Then if S is a Galois extension of R with group G, $S=S'$.*

Proof. It is enough to consider the inclusion $S\to S'$ and to apply the latter theorem.

Corollary 5.7. *Let S be a ring, C its center, G a finite group of automorphisms of S such that G restricted to C is isomorphic to itself and let us suppose that C is a Galois extension of C^G with group G. Then $S^G \subset C$ if and only if S is commutative.*

Proof. If $S^G \subset C$ then $S^G = C^G$ and from the latter corollary $S = C$.

UNIVERSIDAD DE ROSARIO

References

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

[2] K. Hirata and K. Sugano: *On semisimple extensions and separable extensions over non commutative rings*, J. Math. Soc. Japan **18** (1966), 360–373.

[3] T. Kanzaki: *On Galois extension rings*, Nagoya Math. J. **27** (1966), 43–49.

[4] Y. Miyashita: *Finite outer Galois theory of non commutative rings*, J. Fac. Sci. Hokkaido Univ. Ser. I, **19** (1966), 114–134.