A NOTE ON GALOIS THEORY

MIGUEL FERRERO

Throughout the present note, $R \subset S$ will reprsent rings with common identity such that $R \subset Z(S)$ (the center of S). If G is a finite subgroup of $G(S/R)$ (the group of all R-automorphisms of S) with $S^G = R$ and there exist elements x_i, y_i ($i=1, \cdots, n$) in S such that $\sum_i x_i \sigma(y_i) = \delta_{1,\sigma}$ for every $\sigma \in G$, then we say that S is *strongly Galois* over R with Galois group G. On the other hand, if S is an R-separable algebra and finitely generated (abbr. f. g.) and projective as an R-module, and if there exists a finite subgroup G of $G(S/R)$ with $S^G = R$, then S is said to be *weakly Galois* over R (see [10]).

In §1, we prove that if S is weakly Galois over R then $C = Z(S)$ is weakly Galois over R, S is f. g. projective as a C-module and separable as a C-algebra and there exists a finite set $L \subset G(S/R)$ such that $S^L = C$. If R has no idempotents except 0 and 1, S is weakly Galois over C (see [7 ; Th. 3] and [4 ; Th. 1]). On the other hand, every R-automorphism of C can be extended to an automorphism of S. In §2, we obtain certain results on the quaternion algebra $Q(R)$ over a local ring R in which 2 is invertible. Although there can be a finite subgroup H of $G(Q(R)/R)$ such that $Q(R)^H$ is not R-separable, we have a 1-1 correspondence between R-separable proper subalgebras of $Q(R)$ and subgroups of $G(Q(R)/R)$ whose orders are 2.

The author wishes to thank Dr. M. Harada for the useful suggestions in the preparation of the manuscript.

1. Weakly Galois extension

The following generalizes [7 ; Th. 3] as well as [4 ; Th. 1] (the definitions of weakly Galois are slightly different).

Theorem 1.1. *Let R aud S be rings, where $R \subset C = Z(S)$ and S is weakly Galois over R. Then, C is weakly Galois over R, S is C-separable and f. g. projective as a C-module and there is a finite set $L \subset G(S/R)$ such that $S^L = C$. In particular, $S^{G(S/C)} = C$. Furthermore, for every $\sigma \in G(C/R)$ there exists $\tau \in G(S/R)$ such that $\tau | C = \sigma$. If every automorphism in $G(C/R)$ can be extended uniquely to an automorphism of S*

then S *is commutative. Finally, if* R *has no idempotents except* 0 *and* 1, *there is a finite subgroup* $F\subset G(S/R)$ *such that* $S^{F}=C$, *i.e.,* S *is weakly Galois over* C.

Proof. Since S is R-separable and f. g. projective as an R-module, S is C-separable and f. g. projective as a C-module and C is R-separable and f. g. projective as an R-module ([1; Prop. 1.2 and Th. 2.3] and [7; Lemma 2]). Let H be a finite subgroup of $G(S/R)$ with $S^{H}=R$, and $H'=H|C=\{\sigma|C:\sigma\in H\}$. Then, $C^{H'}=R$ and C is weakly Galois over R. Now, we shall consider the following three cases:

I) C has no idempotents except 0 and 1: In this case, C is H'-Galois over R. Let $F=\{\sigma\in H:\ \sigma|C=1\}$. Then, $C\subset S^{F}$ and F is a normal subgroup of H. Therefore, $H|S^{F}$ is a group of R-automorphisms of S^{F} isomorphic to $H|C$. Since $(S^{F})^{H}=R$, we obtain $S^{F}=C$ by [3; Cor. 5.6]. On the other hand, H' is the group of all R-automorphisms of C ([2; Cor. 3.3]), and so $G(C/R)=H|C\subset G(S/R)|C$.

II) R has no idempotents except 0 and 1: Since C is weakly Galois over R, there exist mutually orthogonal minimal idempotents $e_1,\cdots,e_n$ in C such that $C=\bigoplus_{i=1}^{n}Ce_i$ where Ce_i has no idempotents except 0 and 1 and it is Galois over R ([9; Prop. 1.3]). Since every e_i is central, $S=\bigoplus_{i=1}^{n}Se_i$, where Se_i is R-separable and f. g. projective as an R-module. Let $H_i=\{\sigma|Se_i:\sigma\in H,\ \sigma(e_i)=e_i\}\subset G(Se_i/R)$. As in [9; Prop. 1.3], we can prove that H is transitive on $\{e_1,\cdots,e_n\}$. Now, let $s\in(Se_1)^{H_1}$ and let $\sigma_j\in H$ be such that $\sigma_j(e_1)=e_j$, where $\sigma_1=1$ by definition. We put $t=\sum_{j=1}^{n}\sigma_j(s)\in S^{H}=R$. Then, $s=te_1\in Re_1\simeq R$. Therefore, $(Se_1)^{H_1}=R$ and Se_1 is weakly Galois over R. Since $Z(Se_1)=Ce_1$ has no idempotents except 0 and 1, by I), there exists a finite group F_1 of automorphisms of Se_1 such that $Ce_1=(Se_1)^{F_1}$. Similarly, for every i we obtain a finite group F_i of automorphisms of Se_i such that $Ce_i=(Se_i)^{F_i}$. Putting $F=\prod_{i=1}^{n}F_i\subset G(S/R)$, F is a finite group and $S^{F}=C$.

Now, let $\sigma\in G(C/R)$, and $\sigma(e_i)=e_{\theta_i}$. Putting $\tau_{ij}=\sigma_j\circ\sigma_i^{-1}\in G(S/R)$, it is clear that $\tau_{\theta_j i}\circ\sigma\circ\tau_{ij}|Ce_i\in G(Ce_i/R)$. By I), we can find some $\tau_i\in G(Se_i/R)$ such that $\tau_{\theta_j i}\circ\sigma\circ\tau_{ij}|Ce_i=\tau_i|Ce_i$, or, $\tau_{i\theta_j}\circ\tau_i\circ\tau_{ij}|Ce_i=\sigma|Ce_i$. Let $\rho_{ji}=\tau_{i\theta_j}\circ\tau_i\circ\tau_{ji}:Se_j\rightarrow Se_{\theta_j}$, and let $\rho:S\rightarrow S$ be defined by $\rho(s)=\sum_{j=1}^{n}\rho_{ji}(se_j)$. Then, it is easy to verify that $\rho\in G(S/R)$ and $\rho|C=\sigma$.

III) General case: We use the same notation as in [10]. Let $x\in\operatorname{Spec}B(R)$. Then, S_x is R_x-separable and f. g. projective as an R_x-module. On the other hand, we have $(S_x)^{H_x}=R_x$. Furthermore, since S

is f. g. over R it is easy to see that $Z(S_x)=C_x$. Then, by II), there is a finite subgroup $H(x)$ of $G(S_x/R_x)$ such that $(S_x)^{H(x)}=C_x$. Since C is f. g. over R, by [10; (2.14)], there exists a finite subset H^x of $G(S/C)$ such that $(H^x)_x=H(x)$. Therefore, $(S_x)^{(H^x)_x}=C_x$ and there is a neighborhood $V(x)$ such that $(S_y)^{(H^x)_y}=C_y$ for every $y\in V(x)$. By the compactness of Spec$B(R)$, we can cover it with a finite number of these neighborhoods: Spec$B(R)=V(x_1)\cup\cdots\cup V(x_p)$. Since $L=H^{x_1}\cup\cdots\cup H^{x_p}$ is a finite subset of $G(S/C)$, $S^L=C$. But, for every $y\in$ Spec$B(R)$ there exists some i such that $y\in V(x_i)$. Then, $L_y\supset(H^{x_i})_y$ and $(S_y)^{L_y}\subset(S_y)^{(H^{x_i})_y}=C_y$, whence it follows $S^L=C$.

Now, let $\sigma\in G(C/R)$. By II), for every $x\in$Spec$B(R)$ we have $\sigma_x\in G(C_x/R_x)\subset G(S_x/R_x)|C_x$, and so $\sigma_x=(\tau^x)_x|C_x$ with some $\tau^x\in G(S/R)$. There holds then $(\tau^x(c)-\sigma(c))_x=0$ for every $c\in C$. Therefore, there exists a neighborhood U_{e^x} (e^x is an idempotent in x) such that $(\tau^x(c)-\sigma(c))_y=0$ for every $y\in U_{e^x}$. We cover Spec$B(R)$ by $\{U_{e_1},\cdots,U_{e_n}\}$ where $e_i=e^{x_i}$, and put $\tau_i=\tau^{x_i}$. Then, for every $y\in$ Spec$B(R)$ there exists i such that $y\in U_{e_i}(e_i\in y)$ and furthermore $(\tau_i(c)-\sigma(c))(1-e_i)=0$. We set here $f_1=e_1$ and $f_2=1-(1-e_2)e_1$. Then, $1-f_1$ and $1-f_2$ are mutually orthogonal idempotents, $(\tau_i(c)-\sigma(c))(1-f_i)=0$ $(c\in C, i=1, 2)$, and $U_{e_1}\cup U_{e_2}=U_{f_1}\cup U_{f_2}$ where U_{f_1} and U_{f_2} are disjoint. By induction, we can prove that if $h\leqslant n$ then there exists a family of idempotents $\{f_1,\cdots,f_h\}$ such that $1-f_1,\cdots,1-f_h$ are pairwise orthogonal, $(\tau_i(c)-\sigma(c))(1-f_i)=0$ $(c\in C, i=1,\cdots,h)$ and $U_{e_1}\cup\cdots\cup U_{e_h}=U_{f_1}\cup\cdots\cup U_{f_h}$ where U_{f_i}'s are pairwise disjoint. In fact, if $f_1,\cdots,f_{h-1}$ have been defined, it is enough to put $f_h=1-(1-e_h)f_1\cdots f_{h-1}$. Eventually, we obtain idempotents $f_1,\cdots,f_n$ in R such that $1-f_1,\cdots,1-f_n$ are pairwise orthogonal, $(\tau_i(c)-\sigma(c))(1-f_i)=0$ $(c\in C, i=1,\cdots,n)$ and Spec$B(R)=U_{f_1}\cup\cdots\cup U_{f_n}$ where U_{f_i}'s are pairwise disjoint. For every $x\in$ Spec$B(R)$, there exists some i such that $x\in U_{f_i}$ and $x\notin U_{f_j}$ for each $j\neq i$. Then, we have $f_{i_x}=0$ and $(1-f_j)_x=0$ for each $j\neq i$, which implies $(\sum_{i=1}^n(1-f_i))_x=1_x$. It follows therefore $\sum_{i=1}^n(1-f_i)=1$. Now, we define $\tau:S\to S$ by $\tau(s)=\sum_{i=1}^n\tau_i(s)(1-f_i)$. Recalling that $1=\sum_{i=1}^n(1-f_i)$ is a decomposition of 1 into pairwise orthogonal idempotens, we readily see that $\tau\in G(S/R)$. If $c\in C$ then we have $(\tau(c)-\sigma(c))(1-f_i)=0$ $(i=1,\cdots,n)$. Let $y\in$Spec$B(R)$. Then, there exists a unique j such that $y\in U_{f_j}$ $(f_j\in y)$ and we have $(\tau(c)-\sigma(c))_y=0$. It follows therfore $\tau|C=\sigma$.

Finally, if every R-automorphism of S can be extended uniquely to an automorphism of S, then $G(S/C)=1$, which implies $S=S^{G(S/C)}=C$.

Remark. If S is commutative, then $G(S/R)$ is locally finite ([10; (2.16)]. However, in the present stage, $G(S/R)$ is not so and we can not prove that S is weakly Galois over C (see §2).

Corollary 1.2. *Let $R\subset S$ be rings such that $R\subset C$, and let $G(S/R)$ be locally finite. If S is weakly Galois over R then S is weakly Galois over C and C is weakly Galois over R.*

Proof. It is enough to consider the finite group generated by $H^{x_1}\cup\cdots\cup H^{x_p}$ (under the notation in the case III) of Th. 1.1).

2. Quaternion algebra

Let R be a commutative ring, and $Q(R)$ the *quaternion algebra* over R: $Q(R)$ is a free R-module with basis $\{1, i, j, k\}$ and the multiplication in $Q(R)$ is defined by $i^2=j^2=k^2=-1$, $ij=-ji=k$, $jk=-kj=i$ and $ki=-ik=j$.

Suppose R is of characteristic 2 and has no idempotents except 0 and 1. Then, $Q(R)$ is commutative and has no idempotents except 0 and 1. If $Q(R)$ is Galois over R then $o(G(Q(R)/R))=4$ ([8; p. 165]). However, every permutation of $\{i, j, k\}$ defines an R-automnrphism of $Q(R)$, which forces a contradiction $o(G(Q(R)/R)\geqslant 6$. Therefore, $Q(R)$ can not be Galois over R.

We assume henceforth that 2 *is invertible in* R. The set of all invertible elements of $Q(R)$ will be denoted by $U(Q(R))$. Given $u\in U(Q(R))$, σ_u will denote the inner automorphism defined by u.

Lemma 2.1. *$Q(R)$ is strongly Galois over R with Galois group $H=\{1, \sigma_i, \sigma_j, \sigma_k\}$, and central separable over R. If R is a local ring then $G(Q(R)/R)=\mathrm{Int}\,(Q(R)/R)=\{\sigma_u : u\in U(Q(R))\}$.*

Proof. It is easy to see that $Q(R)^H=R=Z(Q(R))$. Putting $x_1=1/2$, $x_2=-i/2$, $x_3=-j/2$, $x_4=-k/2$, $y_1=1/2$, $y_2=i/2$, $y_3=j/2$, $y_4=k/2$, we obtain $\sum_{r=1}^4 x_r\sigma(y_r)=\delta_{1,\sigma}$ $(\sigma\in H)$. Therefore, $Q(R)$ is R-separable by [5; Prop. 3.3]. The final assertion is obvious by [1; Th. 3.6].

As was mentioned in §1, $G(S/R)$ is not necessarily locally finite. In fact, if R is the field of real numbers then it is well-known that $G(Q(R)/R)=\mathrm{Int}(Q(R)/R)\simeq U(Q(R))/U(R)$ contains an element of infinite order.

Now, let $z=z_0+z_1i+z_2j+z_3k\in Q(R)$. Then, the following results are easy, and will be used occasionally in our subsequent study.

(I) $z \in U(G(R))$ if and only if $z_0^2+z_1^2+z_2^2+z_3^2 \in U(R)$.

(II) Let one of z_1, z_2, z_3 be in $U(R)$. If $u \in Q(R)$ and $zu=uz$ then $u=a_0+a_1z$ with some $a_0, a_1 \in R$.

(III) Let $z \in U(Q(R))$. Then, $\sigma_z=1$ if and only if $z=z_0 \in R$.

(IV) Let $z \in U(Q(R))$. Then, σ_z is of order 2 if and only if $z_0z_1=z_0z_2=z_0z_3=0$. In case R is a local ring, σ_z is of order 2 if and only if $z_0=0$.

From now on, we assume further that R *is a local ring with maximal ideal* $\mathfrak{m}$.

Lemma 2.2. *Let* $u, v \in U(Q(R))$. *If* σ_u *and* σ_v *are of order* 2, *then the following conditions are equivalent*:

(a) $Q(R)^{(\sigma_u)}=Q(R)^{(\sigma_v)}$, *where* (σ_u) *is the subgroup generated by* σ_u.

(b) $v=au$ *with some* $a \in R$.

(c) $\sigma_u=\sigma_v$.

Proof. It is enough to prove that (a) implies (b). By (IV), $u=u_1i+u_2j+u_3k$ and $v=v_1i+v_2j+v_3k$ $(u_i, v_i \in R)$. Since $u_1^2+u_2^2+u_3^2 \notin \mathfrak{m}$, one of u_1, u_2, u_3 is not in $\mathfrak{m}$. Noting that $uv=vu$ by (a), (b) is obvious by (II).

Proposition 2.3. *Let* T *be a proper* R*-subalgebra of* $Q(R)$. *Then,* T *is* R*-separable if and only if there exists an element* $u \in U(Q(R))$ *such that* σ_u *is of order* 2 *and* $\{1, u\}$ *forms a free* R*-basis of* T.

Proof. First, we consider the case where R is a field. Assume that T is an R-separable proper subalgebra of $Q(R)$. Then, $\dim_R(T)=2$ or 3. Suppose $\dim_R(T)=3$ and $\{1, u, v\}$ is an R-basis of T, where $u=u_0+u_1i+u_2j+u_3k$ and $v=v_0+v_1i+v_2j+v_3k$. Evidently, one of u_1, u_2, u_3 and one of v_1, v_2, v_3 are in $U(R)$. If $z \in Q(R)^T$ then $uz=zu$ and $vz=zv$. Hence, by (II), $z=a_0+a_1u=b_0+b_1v$ with some $a_i, b_i \in R$. It follows then $a_1=b_1=0$ and $z \in R$. We have seen therefore $Z(T)=Q(R)^T=R$, which implies a contradiction $Q(R)=T \otimes_R Q(R)^T=T$. Hence, $\dim_R(T)=2$. Now, let $\{1, u\}$ be an R-basis of T, where we may assume that $u^2 \in R$. Since $T \simeq R[x]/(x^2-u^2)$ is separable and R is not of characteristic 2, we obtain $u^2 \neq 0$. Concerning the converse, there is nothing to prove.

Next, we shall consider the general case. If T is R-separable then T is a direct summand of $Q(R)$ as a T-right module (cf. [6; pp. 106—107]), and so T is f. g. projective over R. In the converse part too, T is f. g. projective over R. Then, recalling that T is R-separable if and only if $T/\mathfrak{m}T$ is $R/\mathfrak{m}$-separable and that by Nakayama's lemma every $R/\mathfrak{m}$-basis of $T/\mathfrak{m}T$ can be lifted to an R-basis of T, the first step enables us to readily see the equivalence asserted in the proposition.

Finally, the last assertion is easy by (II).

Corollary 2.4. *If $u\in U(Q(R))$ and σ_u is of order 2, then $Q(R)^{(\sigma_u)}$ is an R-separable proper subalgebra of $Q(R)$ with $\{1, u\}$ as a free R-basis.*

Proof. By (II) and (IV), $Q(R)^{(\sigma_u)}=R\oplus Ru$. Now, our assertion is clear by Prop. 2.3.

Combining Prop. 2.3 with Cor. 2.4, we readily obtain the following:

Theorem 2.5. *If R is a local ring in which 2 is iuvertible, then there exists a 1—1 correspondence between R-separable proper subalgebras of $Q(R)$ and subgroups of $G(Q(R)/R)$ whose orders are 2.*

Remark. There can be a finite subgroup F of $G(Q(R)/R)$ such that $Q(R)^F$ is not R-separable. In fact, if $R=Z/(5)$ and $u=1+i+2j$ then $(i+2j)^2=0$ and $Q(R)^{(\sigma_u)}=R\oplus R(i+2j)$ is not R-separable.

REFERENCES

[1] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative ring, Trans. Amer. Math. Soc. **97** (1960), 367—407.

[2] 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.

[3] M. FERRERO: On the Galois theory of non-commutative rings, Osaka J. Math. **7** (1970), 81—88.

[4] M. HARADA: Note on Galois extension over the center, Revista de la Unión Mat. Argentina **24** (1968), 91—96.

[5] K. HIRATA and K. SUGANO: On semisimple extensions and separable extensions over non-commutative rings, J. Math. Soc. Japan **18** (1966), 360—373.

[6] T. KANZAKI: On commutor rings and Galois theory of separable algebras, Osaka J. Math. **1** (1964), 103—115.

[7] T. KANZAKI: On Galois algebra over a commutative ring, Osaka J. Math. **2** (1965), 309—317.

[8] O. VILLAMAYOR: Separable algebras and Galois extensions, Osaka J. Math. **4** (1967), 161—171.

[9] O. VILLAMAYOR and D. ZELINSKY: Galois theory for rings with finitely many idempotents, Nagoya Math. J. **27** (1966), 721—731.

[10] O. VILLAMAYOR and D. ZELINSKY; Galois theory with infinitely many idempotents, Nagoya Math. J. **35** (1969), 83—98.

UNIVERSIDAD DE ROSARIO

(Recived May 8, 1972)