Revista de la
Unión Matemática Argentina
Volumen 25, 1971.

GRADED ALGEBRAS AND GALOIS EXTENSIONS

by D. J. Picco and M. I. Platzeck

Dedicado al profesor Alberto González Domínguez

We establish in this paper a connection between Galois extensions of a commutative ring and algebras graded over the Galois group. As in the case of Galois extensions whose group is Z_2, we introduce a Brauer group associated to central separable algebras that are graded over a group G; for our purpose, graded tensor products are not needed. The methods of [8], where Galois extensions appear as centralizers of the homogeneous component of degree 0 of algebras graded over Z_2, do not work for arbitrary G; here Galois extensions appear as centralizers of the full graded algebra in a new algebra, the construction of which from the given graduation is similar to the construction of a twisted group ring from an action of a group.

After this, we use graduations to obtain the results of [9], [4] on the cohomological description of Galois extensions that have normal basis.

1. **THE GRADED BRAUER GROUP.** Let R be a commutative ring and G a finite abelian group; we shall consider R-algebras graded over G, that is R-algebras A with a decomposition $A = \oplus_{\sigma\in G} A_\sigma$ where the A_σ's are R-submodules such that $A_\sigma . A_\eta \subset A_{\sigma\eta}$; if $a \in A$ we write $a = \sum a_{(\sigma)}$ to denote the homogeneous components $a_{(\sigma)}$ of a. If A and B are G-graded we consider $A \otimes_R B$ as G-graded by $A \otimes B = \oplus_\sigma (A \otimes B)_\sigma$ with $(A \otimes B)_\sigma = \oplus_{\alpha.\beta=\sigma} A_\alpha \otimes B_\beta$.

If A is G-graded, we denote with AE the R-algebra defined as follows: AE is the free left A-module generated by $\{e_\sigma : \sigma \in G\}$ with multiplication given by $ae_\sigma.be_\eta = a.b_{(\sigma^{-1}\eta)}e_\eta$; then AE is an associative R-algebra with unit $1 = \sum_\sigma e_\sigma$. We consider $A \subset AE$ via the R-algebra monomorphism $a \in A \longrightarrow a.1 = \sum_\sigma ae_\sigma$; then $e_\sigma.a = \sum_\eta a_{(\sigma^{-1}\eta)}e_\eta$.

LEMMA 1. *Let* A *be a* G-*graded* R-*algebra. If* A *is separable over* R *then* AE *is separable over* R.

Proof. Let $m: A \otimes A^\circ \longrightarrow A$ be the multiplication map and $e \in A \otimes A^\circ$ such that $m(e) = 1$ and $(1 \otimes a^\circ - a \otimes 1^\circ).e = 0$ for every $a \in A$. If we write $e = \sum_\sigma f_\sigma$ with $f_\sigma \in (A \otimes A^\circ)_\sigma$ then $m(f_1)=$ and $(1 \otimes a^\circ - a \otimes 1^\circ).f_1 = 0$ for every $a \in A$; thus we assume e=f (i.e. that we have a homogeneous splitting of $m: A \otimes A^\circ \longrightarrow A$) If $\bar{e} = e . \sum e_\sigma \otimes e^\circ_\sigma \in AE \otimes AE^\circ$, then $\bar{e}$ splits $AE \otimes AE^\circ \longrightarrow AE$

If A is a G-graded R-algebra, we consider G as a group of automophisms of AE by the action given by $\sigma(ae_\eta) = ae_{\sigma\eta}$. Then G acts trivially on $A \subset AE$ and if $Z(A)$ is the centralizer of A in AE th action of G in AE induces an action of G in $Z(A)$.

Let us recall the following facts from ([4], Def. 4.5). If R is a commutative ring, A a faithful R-algebra and G is a group of automorphisms of A, then A is said to be a Galois extension of R with group G if the following equivalent properties hold:

a) $A^G = R$, A is finitely generated and projective over R and the map $AG \longrightarrow End_R(A)$ is an isomorphism.

b) $A^G = R$; if F is the ring of functions from G to A then $f: A \otimes A \longrightarrow F$ defined by $f(a \otimes b)(\sigma) = a\sigma(b)$ is bijective.

Clearly b) is equivalent to b') $A^G = R$ and $f: A \otimes A \longrightarrow AG$ defined by $f(a \otimes b) = \sum_\sigma a\sigma(b)\sigma$ is bijective.

Moreover a) is equivalent to a') $A^G = R$ and AG is central separable over R. Indeed, if a) holds $AG \cong End_R(A)$ is central separable over R; conversely, assume AG is central separable, then A is finitely generated faithful projective over R and therefore

$AG \longrightarrow End_R(A)$ is injective (since it is the identity over R) ; now it follows from [1] that the map is onto since the centralizer of its image is $A^G = R$.

If G is a fixed finite abelian group and A , B are Galois extensions of R with group G, then $A \otimes B$ is a Galois extension of R with group $G \times G$; as in [3] , we see that if $H = \{(\sigma,\sigma^{-1}) \in G \times G\}$, the $(A \otimes B)^H$ is a Galois extension of R with group $G \times G/H = G$. Clearly, if $E_R(G)$ denotes the set of G-isomorphisms classes of Galois extensions of R with group G, then the above construction defines a product under which $E_R(G)$ becomes an abelian group (see [3]) whose identity element is $E = \oplus_{\sigma\in G} R\, e_\sigma$ with $e_\sigma . e_\eta = \delta_{\sigma\eta} e_\sigma$, $\sigma e_\eta = e_{\sigma\eta}$, the trivial Galois extension of R with group G (the algebra of functions from G to R).

PROPOSITION 2. *Let* A *be a* G*-graded central separable* R*-algebra. Then the centralizer* Z(A) *of* A *in* AE *is a Galois extension of* R *with group* G.

Proof. Since A is central separable, we have ([1], Th. 3.1) $AE = A \otimes Z(A)$ and therefore Z(A) is separable over R. On the other side, if $e \in (A \otimes A^\circ)_1$ splits $m: A \otimes A^\circ \longrightarrow A$ and we write $e = \sum t_\sigma$ with $t_\sigma \in A_\sigma \otimes A_{\sigma^{-1}}$ then $1 = \sum_\sigma u_\sigma$ with $u_\sigma = m(t_\sigma) \in A_1$ such that $a_{(\theta)} . u_\sigma = u_{\sigma\theta} . a_{(\theta)}$, $\forall\, a_{(\theta)} \in A_\theta$. Then we can verify that $x = \sum_\sigma u_{\sigma^{-1}} e_\sigma$ belongs to the center of Z(A) and $\sum_{\sigma\in G} \sigma(x) = 1$. Therefore Z(A)G is separable over R (if $e = \sum_i a_i \otimes b_i^\circ$, then $\varphi: Z(A)G \longrightarrow Z(A)G \otimes Z(A)G$ given by $\varphi(a) = \sum_{i,\sigma} \sigma . x . a_i \otimes b_i \sigma^{-1} . a$ is a two sided Z(A)G-map that splits $Z(A)G \otimes Z(A)G \longrightarrow Z(A)G$) . On the other side, $Z(A)^G = R$ and since the automorphisms of Z(A) are easily seen to be linearly independent over Z(A), we conclude that the center of Z(A)G is R, i.e. Z(A)G is central separable over R.

We define now a Brauer group $B_G(R)$. If $M = \oplus_{\sigma\in G} M_\sigma$ is a G-graded module, we consider $End_R(M)$ as a G-graded algebra with the graduation given by $(End_R(M))_\sigma = \oplus_\eta Hom_R(M_\eta, M_{\sigma\eta})$. A G-graded central separable R-algebra is trivial if there exists a graded R-algebra isomorphism $A \cong End_R(M)$ with M a finitely generated, faithful projective G-graded module. If A and B are G-graded central separable over R, A is equivalent to B if $A \otimes T_1 \cong B \otimes T_2$ where T_1, T_2 are trivial; then $B_G(R)$ is the set of equivalence classes of G-graded central separable R-algebras under this equivalence; then $B_G(R)$ is an abelian group in which the inverse of A is $A°$, since the canonical isomorphism : $A \otimes A° \longrightarrow End_R(A)$ is graded. As in [1], Prop. 5.3 , we can see that the class of A in $B_G(R)$ is the identity if and only if A is trivial.

LEMMA 3. *If* $A \in B_G(R)$ *is trivial then* $Z(A) = E$ *in* $E_G(R)$.

Proof. $A = End_R(M)$ with $M = \oplus_\sigma M_\sigma$; let $u_\sigma : M \longrightarrow M_\sigma$ be the corresponding projection, then $u_\sigma . u_\eta = \delta_{\sigma,\eta}\, u_\sigma$, $\sum u_\sigma = 1$, $u_\sigma \in A_1$. Then $\varphi : E \longrightarrow AE$ defined by $\varphi(e_\eta) = \sum_\sigma u_{\sigma\eta} e_{\sigma^{-1}}$ is an R-algebra monomorphism such that $\varphi(E) \subset Z(A)$ and $\varphi : E \longrightarrow Z(A)$ is a G-monomorphism; therefore $\varphi(E) = Z(A)$ and $Z(A) = E$ in $E_G(R)$.

LEMMA 4. *If* $A, B \in B_G(R)$ *then* $Z(A \otimes B) = Z(A).Z(B)$ *in* $E_G(R)$.

Proof. Let $h : (A \otimes B)E \longrightarrow AE \otimes BE$ be the map defined by $h(e_\tau) = \sum_{\sigma\eta=\tau} e_\sigma \otimes e_\eta$; then h is an R-algebra homomorphism and $h(a \otimes b) = a \otimes b$; thus h maps $Z(A \otimes B)$ into the centralizer of $A \otimes B$ in $AE \otimes BE$, i.e., into $Z(A) \otimes Z(B)$. Since $\alpha \otimes \alpha^{-1} h(e_\tau) = \sum_{\sigma\eta=\tau} e_{\sigma\alpha} \otimes e_{\alpha^{-1}\eta} = h(e_\tau)$, we have

$h : Z(A \otimes B) \longrightarrow (Z(A) \otimes Z(B))^H = Z(A) . Z(B)$ and being h a G-map we conclude that $Z(A \otimes B) = Z(A) . Z(B)$.

LEMMA 5. *Let* L *be a Galois extension of* R *with group* G. *Then* *there exists* $A \in B_G(R)$ *such that* $L = Z(A)$.

Proof. Let $A = LG$ with $A_\sigma = L\sigma$. Then $LG \in B_G(R)$. Consider $Z(A) \subset AE$ and the map $\varphi: AE \longrightarrow L$ defined by $\varphi(\sum_\sigma a_\sigma e_\sigma) = a_1(1) \in L$ (if $a = \sum_\sigma h_\sigma \sigma \in LG$, $a(1) = \sum_\sigma h_\sigma$). We show that $\varphi \mid Z(A)$ is an antiautomorphism of Galois extensions.

Observe that $\sum_\sigma u_\sigma e_\sigma \in Z(A)$ implies $h.u_\sigma = u_\sigma h$ and $\theta u_\sigma = u_{\sigma\theta^{-1}}\theta$, $h,\theta \in LG$. In particular, if $u_1 = \sum_\sigma h_\sigma \sigma$ with $h_\sigma \in L$ we have $\sum_\sigma h.h_\sigma\sigma = \sum_\sigma h_\sigma\sigma(h)\sigma$ and therefore $h_\sigma\sigma(h) = h.h_\sigma$ $\forall\ \sigma \in G$, $h \in L$ Let now $u = \sum_\sigma u_\sigma e_\sigma$, $v = \sum_\sigma v_\sigma e_\sigma \in Z(A)$, $u_1 = \sum_\sigma h_\sigma \sigma$, $v_1 = \sum_\sigma h'_\sigma \sigma$ then $u_1.v_1 = \sum_{\sigma,\eta} h_\sigma \sigma(h'_\eta)\sigma\eta = \sum_{\sigma,\eta} h'_\eta h_\sigma \sigma\eta$ and therefore $\varphi(u.v) = \sum_{\sigma,\eta} h'_\eta h_\sigma = \varphi(v)\ \varphi(u)$. On the other side, if $u = \sum_\sigma u_\sigma e_\sigma \in Z(A)$, $u_1 = \sum_\sigma h_\sigma \sigma$ then for $\eta \in G$ we have $\eta(u) = \sum_\sigma u_{\eta^{-1}\sigma} e_\sigma$ and since $u_{\eta^{-1}} = \eta u_1 \eta^{-1}$, $\varphi\eta(u) = u_{\eta^{-1}}(1) = \sum_\sigma \eta(h_\sigma)\sigma\eta^{-1}(1) = \sum_\sigma \eta(h_\sigma) = \eta\varphi(u)$, i.e. $\varphi: Z(A) \longrightarrow L$ is a G map, and since φ is also an R-algebra homomorphism it follows that φ is an isomorphism.

It follows from lemmas 3 and 4 that the correspondence $A \longrightarrow Z(A$ induces a group homomorphism $Z: B_G(R) \longrightarrow E_G(R)$. Consider now the map from the Brauer group $B(R)$ of R (see [1]), to the Brauer group $B_G(R)$ obtained by considering an ungraded central separable algebra as trivially graded. We clearly obtain a group homomorphism $B(R) \xrightarrow{i} B_G(R)$.

PROPOSITION 6. *Let* R *be a commutative ring and* G *a finite abelian group. Then*

$$0 \longrightarrow B(R) \xrightarrow{i} B_G(R) \xrightarrow{Z} E_G(R) \longrightarrow 0$$

is an split exact sequence.

Proof. If $A \in B(R)$ and we grade it trivially we have $a.e_\sigma = e_\sigma.a$

in AE for every $a \in A$; it follows that $Z(A) = E$. Let $\varphi: B_G(R) \longrightarrow B(R)$ be the group homomorphism obtained considering a graded algebra as ungraded. Since φi = identity, it suffices to show that $\varphi|\mathrm{Ker}(Z)$ is injective. Let then $A \in B_G(R)$ be such that $Z(A) = E$ and $A = \mathrm{End}_R(M)$. Since $Z(A) = E$, $Z(A) = \oplus_{\sigma\in G} Rv_\sigma$ with $v_\sigma . v_\eta = \delta_{\sigma,\eta} v_\sigma$, $\sum_\sigma v_\sigma = 1$, $v_\sigma = \sigma(v_1)$. If $v_1 = \sum u_\sigma e_{\sigma^{-1}}$ with $u_\sigma \in A$ we have $v_\eta = \sum_\sigma u_\sigma e_{\sigma^{-1}\eta} = \sum_\sigma u_{\sigma\eta^{-1}} e_\sigma$. Since $v_\sigma . v_\eta =$ $= \delta_{\sigma,\eta} v_\sigma$, it follows that $u_\sigma . u_\eta = \delta_{\sigma,\eta} u_\sigma$ and $\sum_\sigma v_\sigma = 1$ implies $\sum_\sigma u_\sigma = 1$. On the other side, since $v_\sigma \in Z(A)$ we have $f_\theta u_\sigma =$ $u_{\sigma\theta} f_\theta$ for every $f_\theta \in A_\theta$. Let now be $M_\sigma = u_\sigma(M)$. Then $M = \oplus_{\sigma\in G} M_\sigma$ and for $f_\theta \in A_\theta$ we have $f_\theta(u_\sigma(m)) = (f_\theta u_\sigma)(m) = (u_{\sigma\theta} f_\theta)(m) =$ $= u_{\sigma\theta}(f_\theta(m))$, i.e. $f_\theta(M_\sigma) \subset M_{\sigma\theta}$ and therefore the graduation of A is induced by the graduation $M = \oplus_{\sigma\in G} M_\sigma$ of M ; thus A is trivial in $B_G(R)$.

2. ABELIAN EXTENSIONS WITH NORMAL BASIS.

Let G be a finite abelian group and E the trivial Galois extension of a commutative ring R with group G. The map $EG \longrightarrow EG$ defined by $a\sigma \longrightarrow \sigma^{-1}(a)\sigma^{-1}$ is easily seen to be an R-algebra antiautomorphism of EG; thus from the usual structure of left $EG \otimes EG^\circ$-module on EG we obtain a structure of left $EG \otimes EG$-module on EG, which is explicitly given by $a\sigma \otimes b\eta . x = a\sigma . x . \eta^{-1}(b)\eta^{-1}$. Considering E as a left EG-module, we have that $E \otimes E$ is a left $EG \otimes EG$-module and the canonical map $\varphi: E \otimes E \longrightarrow EG$ (induced by $\varphi(e \otimes f) = \sum_{\sigma\in G} e\sigma(f)\sigma$) is an $EG \otimes EG$-isomorphism. Since $EG \otimes EG \cong \mathrm{End}_R(E) \otimes \mathrm{End}_R(E) \cong \mathrm{End}_R(E \otimes E)$, it follows that R-automorphisms of $E \otimes E$ and EG have the form $x \longrightarrow u.x$ with $u \in U(EG \otimes EG)$.

Let us recall the definition of Harrison's complex: the correspondences $\sigma_1 \times \ldots \times \sigma_n \longrightarrow \sigma_1 \times \ldots \times \sigma_i \times \sigma_i \times \sigma_{i+1} \times \ldots \times \sigma_n$ induce R-algebra homomorphisms $\Delta_i : RG^n \longrightarrow RG^{n+1}$, $i = 1,\dots,n$. If Δ_o , Δ_{n+1} are induced by $\sigma_1\times\dots\times\sigma_n \longrightarrow 1\times\sigma_1\times\dots\times\sigma_n$, $\sigma_1\times\dots\times\sigma_n\times 1$ respectively, then Δ_i: $U(RG^n) \longrightarrow U(RG^{n+1})$ and Harrison's complex is $U(RG^n)$, $n \geqslant 1$ with δ: $U(RG^n) \longrightarrow U(RG^{n+1})$ defined by $\delta(x) = \prod \Delta_i(x)^{(-1)^i}$. We shall use the second cohomology group $H^2(R,G)$ of this complex; with the usual identifications, it is obtained from

$$U(RG) \longrightarrow U(RG \otimes RG) \longrightarrow U(RG \otimes RG \otimes RG)$$

with $\delta(x) = x \otimes x.\Delta_1(x^{-1})$, where $\Delta_1(\sum_\sigma r_\sigma \sigma) = \sum_\sigma r_\sigma \sigma \otimes \sigma$, if $x \in U(RG)$, $\delta(x) = 1 \otimes x.\Delta_2(x).\Delta_1(x^{-1})\, x^{-1} \otimes 1$ if $x \in U(RG \otimes RG)$, where $\Delta_1(\sum_{\sigma,\eta} r_{\sigma,\eta}\sigma \otimes \eta) = \sum_{\sigma,\eta} r_{\sigma,\eta}\sigma \otimes \sigma \otimes \eta$, $\Delta_2(\sum_{\sigma,\eta} r_{\sigma,\eta}\sigma \otimes \eta) = \sum_{\sigma,\eta} r_{\sigma,\eta}\sigma \otimes \eta \otimes \eta$

Let $\sim$: $RG \otimes RG \longrightarrow RG \otimes RG$ be the map induced by $\sigma \otimes \eta \longrightarrow \sigma \otimes \sigma\eta^{-1}$; clearly $\sim$ is an R-algebra isomorphism of $RG \otimes RG$, $\sim^2 = 1$. Since $RG \otimes RG \subset EG \otimes EG$, then $RG \otimes RG$ acts on $E \otimes E$ and EG. Let us write $u[x]$, $u(y)$ to denote the corresponding action of $u \in RG \otimes RG$ on $x \in E \otimes E$, $y \in EG$. Then it is straightforward to see that, for $u \in RG \otimes RG$, $\delta(u) = 1$ if and only if

(1) $$\tilde{u}(m\, u[e \otimes f]) = \tilde{u}(e).\tilde{u}(f) \quad \forall\, e,f \in E$$

where m: $E \otimes E \longrightarrow E$ is the multiplication and we consider $E \subset EG$ as $E.1$.

Let $u \in U(RG \otimes RG)$ with $\delta(u) = 1$ and let $X_\sigma = \tilde{u}(E.\sigma) \subset EG$; since $\tilde{u} \in U(RG \otimes RG)$, $x \longrightarrow \tilde{u}(x)$ is an R-automorphism of EG and therefore $EG = \oplus_{\sigma\in G} X_\sigma$; if $u = \sum_{\sigma,\eta} r_{\sigma,\eta}\sigma \otimes \eta$ then $u(E.\sigma) = \sum_{\alpha,\beta} r_{\alpha,\beta}\alpha E\sigma\beta^{-1} = \sum r_{\alpha,\beta}\alpha E\beta^{-1}\sigma = \tilde{u}(E)\sigma$, and $\sigma\tilde{u}(e\eta) = \sum r_{\alpha,\beta}\sigma\alpha e\eta\beta^{-1} = \sum r_{\alpha,\beta}\alpha\sigma e\eta\beta^{-1} = \tilde{u}(\sigma\ e\ \eta) = \tilde{u}(\sigma(e)\sigma\eta)$. Now relation (1) shows that $X_1.X_1 \subset X_1$ and it follows that $X_\sigma.X_\eta \subset X_{\sigma\eta}$, i.e. we have a graduation on EG; call $[EG]_u$ this graded algebra and $\psi(u)$ the image of

$[EG]_u \in B_G(R)$ in $E_G(R)$. We shall show that $u \longrightarrow \psi(u)$ induces a map $H^2(R,G) \longrightarrow E_G(R)$.

Observe first the following : u and v define the same graduation on EG if and only if $v = u.t \otimes 1$ with $t \in U(RG)$; in fact, if $\tilde{u}(E) = \tilde{v}(E)$ we have $\tilde{u}^{-1}.\tilde{v}(E) \subset E$; if $\tilde{u}^{-1}.\tilde{v} = \sum r_{\sigma,\eta}\sigma \otimes \eta$ then $\sum r_{\sigma,\eta}\sigma.e.\eta^{-1} \in E$ for every $e \in E$ implies $r_{\sigma,\eta} = 0$ if $\sigma \neq \eta$; thus $\tilde{u}^{-1}.\tilde{v} = \sum_\sigma r_{\sigma,\sigma}\sigma \otimes \sigma = \Delta_1(t)$, $t = \sum_\sigma r_{\sigma,\sigma}\sigma \in U(RG)$ and therefore $v = u . \tilde{\Delta}_1(t) = u.t \otimes 1$; the converse is clear.

Let now $u, v \in U(RG \otimes RG)$ be cocycles such that $v = \delta(t).u = t \otimes 1.1 \otimes t. \Delta_1(t^{-1}).u$; then $\tilde{v} = \Delta_1(t).1 \otimes t^*.t^{-1} \otimes 1.\tilde{u}$, where $t^* = \sum_\sigma r_\sigma \sigma^{-1}$ if $t = \sum r_\sigma \sigma$. Since $\Delta(t)(E\sigma) = E\sigma$ we have $v(E\sigma) = t^{-1} \otimes 1 . 1 \otimes t^*.\tilde{u}.\Delta_1(t)(E\sigma) = t^{-1} \otimes 1.1 \otimes t^*(\tilde{u}(E\sigma))$. On the other side, $t^{-1}, t^* \in U(RG) \subset RG \subset EG$ and it is clear that $(t^{-1} \otimes 1.1 \otimes t^*)(x) = t^{-1}.x.t^*$ for $x \in EG$; thus $\tilde{v}(E\sigma) = t^{-1}.\tilde{u}(E\sigma).t$, which shows that $[EG]_u$ and $[EG]_v$ are isomorphic as graded algebras and therefore that they have the same image in $E_G(R)$. It follows that we have a map $\Psi : H^2(R,G) \longrightarrow E_G(R)$.

Let $u \in U(RG \otimes RG)$ be a cocycle. Since $EG = \oplus_\sigma \tilde{u}(E\sigma)$ is a graduation on EG, $\tilde{u}(E)$ is an R-subalgebra of EG; note that $\tilde{u}(E\sigma) = \tilde{u}(E)\sigma$ implies $\sigma \in \tilde{u}(E)$ and therefore $\sigma.\tilde{u}(E).\sigma^{-1} \subset \tilde{u}(E)$; this relation allows us to define an action of G on $\tilde{u}(E)$; since $\tilde{u}(\sigma(e)) = \sigma\tilde{u}(e)\sigma^{-1}$, $\tilde{u}(E)$ is RG-isomorphic to E; moreover, if we consider the twisted group ring of u(E) with respect to that action of G, we have a map $\tilde{u}(E)G \longrightarrow EG$ and $\tilde{u}(e)\sigma . \tilde{u}(f)\eta = \tilde{u}(e)\sigma\tilde{u}(f)\sigma^{-1}\sigma\eta = \tilde{u}(e)\sigma(\tilde{u}(f))\sigma\eta$ shows that $\tilde{u}(E)G \cong EG$ and by lemma 5 we have $\Psi(u) = \tilde{u}(E)$; in particular this shows that $\Psi(u)$ has a normal basis, i.e., $\Psi: H^2(R,G) \longrightarrow A_G(R)$, the subgroup of $E_G(R)$ formed by algebras with normal basis. Moreover, it follows from relation (1) that $\Psi(u) = E$ with the usual action of G and product defined by $(e,f) \longrightarrow m\, u\, [e \otimes f]$. This remark can be used to show that $\Psi : H^2(R,G) \longrightarrow A_G(R)$ is a group homomorphism; indeed, if $H = \{(\sigma,\sigma^{-1}) : \sigma \in G\}$ then $j : E \longrightarrow E \otimes E$ defined by $j(e_\sigma) = \sum_\alpha e_{\sigma\alpha} \otimes e_{\alpha^{-1}}$ maps E isomorphically onto $E \otimes E^H$, and $j\sigma = \sigma \otimes 1.j$. Then we can verify that j is an isomophism from $\Psi(uv)$ onto $\Psi(u)\Psi(v)$.

Let us finally show that $\Psi : H^2(R,G) \longrightarrow A_G(R)$ is an isomorphism. If $\Psi(u)$ is trivial, from $EG \cong \tilde{u}(E)G \cong [EG]_u$, it follows that there exist an R-algebra isomorphism $\omega : EG \longrightarrow EG$ such that $\omega(\sigma) = \sigma$ and $\omega(E) = \tilde{u}(E)$; we know that ω must be of the form $x \longrightarrow w(x)$ with $w \in U(EG \otimes EG)$ and since $\omega(\sigma) = \sigma$ we have $w \in U(RG \otimes RG)$; then $\tilde{u}^{-1}w(E) \subset E$ and we have $\tilde{u}^{-1}w = \Delta_1(t)$ with $t \in U(RG)$.

Let us show that $u = \Delta_1(t^{-1})$; to this end, we can assume R to be local ; then ω is an inner automorphism of EG, i.e. $w(x) = p.x.p^{-1}$ with $p \in U(EG)$; but $w(\sigma) = \sigma$ implies $p \in U(RG)$. Then $w = p \otimes p^{*-1}$ and $u = \tilde{w}(\Delta_1(\tilde{t}^{-1})) = \Delta_1(p).1 \otimes p^{-1}.t^{-1} \otimes 1$; now $1 = \delta(u) = \delta(\Delta_1(p).1 \otimes p^{-1})\ \delta(t^{-1} \otimes 1) = \delta(p \otimes 1)\delta(t^{-1} \otimes 1)$ implies $1 \otimes p.\Delta_1(p^{-1}) = 1 \otimes t.\Delta_1(t^{-1})$ and therefore $u = \Delta_1(t).t^{-1} \otimes t^{-1}$. Thus Ψ is injective.

Let now $L \in E_G(R)$, then there exists an RG-isomorphism $j : E \longrightarrow L$ and if we denote with J the R-algebra isomorphism defined by $LG \cong End_R(L) \cong End_R(E) \cong EG$, then $J : LG \longrightarrow EG$ is such that $J(\sigma) = \sigma$; then setting $X_\sigma = J(A\sigma)$ we obtain a graduation on EG, $EG = \oplus_\sigma X_\sigma$ whose image in $E_G(R)$ is L. Let now $f : EG \longrightarrow EG$ be the map defined by $f(e) = J(j(e)\ \sigma)$; then f is an R-automorphism of EG such that $f(E_\sigma) = X_\sigma$; thus there exists $z \in U(EG \otimes EG)$ such that $z(E_\sigma) = X_\sigma$; note that $f(\sigma.x.\eta) = \sigma f(x)\eta$ and therefore $z \in U(RG \otimes RG)$. If $z = \sum_{\sigma,\eta} r_{\sigma,\eta}\ \sigma \otimes \eta$, let $t = \sum_\sigma (\sum_\eta r_{\sigma,\eta})\sigma \in U(RG)$ and set $v = \Delta_1(t^{-1}) \cdot 1 \otimes t . \tilde{z}$. From the relation $X_1.X_1 \subset X_1$ we have $z(E).z(E) \subset z(E)$, i.e. $z^{-1}(z(E)z(E)) \subset E$ and it follows that

$$z(m\ v[e \otimes f]) = z(e).z(f)$$

Now $\tilde{v} = t^{-1} \otimes t^*. z$ and since $t^{-1} \otimes t^*(x) = t^{-1}.x.t$ if $x \in EG$, we have $\tilde{v}^{-1}(\tilde{v}(e).\tilde{v}(f)) = z^{-1}(z(e).z(f))$ and therefore $\tilde{v}(m\ v\ [e \otimes f])$ $=\tilde{v}(e).\tilde{v}(f)$, i.e. v is a cocycle. Moreover, $\tilde{v} = t^{-1} \otimes t^*. z$ implies $\tilde{v}(E\sigma) = t^{-1} \otimes t^*(z(E\sigma)) = t^{-1}.X_\sigma.t$, i.e. EG with the graduation $EG = \oplus_\sigma X_\sigma$ is isomorphic to $[EG]_v$ and therefore $L = \Psi(v)$. Thus, we have obtained the following:

PROPOSITION 7. *If* $u \in U(RG \otimes RG)$ *is a cocycle in the Harrison's complex, let* E_u *be the* R-*algebra obtained defining a product in* E *by* $(e,f) \longrightarrow m\ u[e \otimes f]$. *Then with respect to the standard action of* G *on* E, G *is a group of* R-*algebra automorphisms of* E_u *and* E_u *is a Galois extension of* R *with group* G. *Moreover,* $u \longrightarrow E_u$ *defines a group isomorphism* $H^2(R,G) \cong A_G(R)$.

3. ABELIAN EXTENSIONS OF FIELDS.

We shall show now that for certain fields Harrison's cohomology can be replaced by the usual cohomology in order to study Abelian extensions (note that Galois extensions of fields have normal basis). Let K be a field and G an arbitrary group. We shall consider now central separable algebras with a representation of G as a group of K-algebra automorphisms of A. If M is a KG-module then G acts on $End_K(M)$ by $\sigma(f) = \sigma f \sigma^{-1}$; call a G-algebra A trivial if there is a G-isomorphism of K-algebras $A \cong End_K(M)$ for M a KG-module. If A and B are G-algebras, let G act on $A \otimes B$ via $\sigma(a \otimes b) = \sigma(a) \otimes \sigma(b)$, $a \in A$, $b \in B$. If A and B are central separable G-algebras, then A is equivalent to B if there is a G-isomorphism $A \otimes T_1 \cong B \otimes T_2$ with T_1, T_2 trivial G-algebras ; we obtain in this way an equivalence relation in the set of G-isomorphism classes of central separable G-algebras; if $B'_G(K)$ is the quotient set then $B'_G(K)$ is an abelian group (note that the inverse of $A \in B'_G(K)$ is $A°$, since $A \otimes A° \longrightarrow End_K(A)$ is a G-isomorphism).

Let A be a central separable G-algebra. If $\sigma \in G$, then σ is an inner automorphism of A, i.e. $\sigma(x) = a_\sigma x\, a_\sigma^{-1}$ for some unit $a_\sigma \in A$. Since $\sigma\eta(x) = (a_\sigma a_\eta).x.(a_\sigma a_\eta)^{-1}$ for every $x \in A$, we have $a_\sigma a_\eta =$ $= k_{\sigma,\eta} a_{\sigma\eta}$ with $k_{\sigma,\eta} \in K^*$. If we consider G acting trivially on K, then $k_{\sigma,\eta}$ is a 2-cocycle of G with coefficients in K. If $\sigma(x) =$ $= b_\sigma x b_\sigma^{-1}$ and $b_\sigma b_\eta = k'_{\sigma,\eta} b_{\sigma\eta}$, then $k_{\sigma,\eta} = k'_{\sigma,\eta} k_\sigma k_\eta k_{\sigma\eta}^{-1}$ with $k_\sigma \in K$ such that $b_\sigma = k_\sigma a_\sigma$ and therefore the cohomology class of $k_{\sigma,\eta}$ in $H^2(G,K)$ is well defined by the action of G in A.
We can now verify that the product of the cocycles associated to algebras A and B is the cocycle associated to $A \otimes B$; if $A =$ $= End_K(M)$ with M a G-module then $\sigma(x) = a_\sigma x a_\sigma^{-1}$ with $a_\sigma \in End_K(M)$ such that $a_\sigma a_\eta = a_{\sigma\eta}$ and therefore the cohomology class associated to A is trivial. It follows that the correspondence $A \longrightarrow k_{\sigma,\eta}$ defines a group homomorphism $B'_G(K) \xrightarrow{\theta} H^2(G,K^*)$. Consider now $B(K) \longrightarrow B'_G(K)$ obtained by letting G act trivially on central separable algebras.

PROPOSITION 7. *Let* K *be a field and* G *a finite group. Then*

$$0 \longrightarrow B(K) \longrightarrow B'_G(K) \longrightarrow H^2(G,K^*) \longrightarrow 0$$

is an split exact sequence.

Proof. We first show $B'_G(K) \longrightarrow H^2(G,K^*)$ is onto. Given $\{k_{\sigma,\eta}\} \in H^2(G,K^*)$, let E be the trivial Galois extension of K with group G and let A be the cross product associated to E and $k_{\sigma,\eta}$; explicitely $A = \oplus_{\sigma\in G} Eu_\sigma$ with $u_\sigma u_\eta = k_{\sigma,\eta} u_{\sigma\eta}$, $u_\sigma e = \sigma(e)\, u_\sigma$;

then $A \in B(K)$ and G acts on A by $\sigma(x) = u_\sigma x u_\sigma^{-1}$; clearly the cocycle corresponding to this action is $\{k_{\sigma,\eta}\}$. Consider the homomorphism $B'_G(K) \longrightarrow B(K)$ obtained by forgetting the action of G. Clearly $B(K) \longrightarrow B'_G(K) \longrightarrow B(K)$ is the identity ; to complete the proof we need only show that the restriction of θ to $\mathrm{Ker}(B'_G(K) \longrightarrow B(K))$ is injective; let then $A \in B'_G(K)$ be such that $k_{\sigma,\eta}$ is trivial and $A = \mathrm{End}_K(M)$. If the action of G on A is given by $\sigma(x) = a_\sigma x a_\sigma^{-1}$ we can assume (since $k_{\sigma,\eta}$ is a coboundary) that $a_\sigma a_\eta = a_{\sigma\eta}$; since $a_\sigma \in \mathrm{End}_K(M)$ this means that M is a G-module and that the induced action of G on $\mathrm{End}_K(M)$ is the given one on A. Thus A is trivial in $B'_G(K)$.

Assume now that G is a finite abelian group of exponent e and K is a field of characteristic prime to e that contains the e-th roots of unity. If $\hat{G}$ is the group of characters from G to K, we know that $E \cong K\hat{G}$; indeed $T: K\hat{G} \longrightarrow E$ defined by $T(\chi) = \sum_{\sigma\in G} \chi(\sigma)e_\sigma$ is a K-algebra isomorphism with inverse $T^{-1}: E \longrightarrow K\hat{G}$ given by $T^{-1}(e_\sigma) = 1/n\ (\sum_{\chi\in\hat{G}} \chi\ (\sigma^{-1})\ \chi)$ (see [4]) . If A is a K-module, to say that $A = \oplus_{\sigma\in G} A_\sigma$ where the A_σ's are K-submodules of A is equivalent to say that A is a module over E, also equivalent to say that A is a $K\hat{G}$-module, as follows from $E \cong K\hat{G}$. If a decomposition $A = \oplus_{\sigma\in G} A_\sigma$ is related to an action of $\hat{G}$ on A by the isomorphism $E \cong K\hat{G}$ we can see that $\chi(a) = \sum_{\sigma\in G} \chi(\sigma^{-1})a_{(\sigma)}$ if $a = \sum a_{(\sigma)}$ with $a_{(\sigma)} \in A_\sigma$ and $A_\sigma = \{\ a \in A : \chi(a) = \chi(\sigma^{-1})a\ \forall\chi \in \hat{G}\}$; in particular, if A is a K-algebra then $A = \oplus_{\sigma\in G} A_\sigma$ defines a graduation on A if and only if the related action of $\hat{G}$ on A is an action by K-algebra automorphisms of A. Note that for a graduation $A = \oplus_{\sigma\in G} A_\sigma$ and an action of $\hat{G}$ on A related as above, the isomorphism $K\hat{G} \cong E$ can be extended to a K-algebra isomorphism $T : A\hat{G} \longrightarrow AE$ with $T(a) = a$ for $a \in A$.

Clearly trivial G-graded algebras are related to trivial $\hat{G}$-algebras; if A and B are K-algebras, the product graduation of $A \otimes B$ is related to the product $\hat{G}$-structure of $A \otimes B$ and it follows that $B_G(K) \cong B'_{\hat{G}}(K)$ canonically, which in turn implies that $E_G(K) \cong$ $\cong H^2(\hat{G},K^*)$.

Let us explicitate the isomorphism $H^2(\hat{G},K^*) \longrightarrow E_G(K)$: if $\{k_{\chi,\psi}\} \in H^2(\hat{G},K^*)$ let as in proposition 7, $A = \oplus_{\chi\in\hat{G}} Eu_\chi$ with $u_\chi u_\psi =$ $= k_{\chi,\psi}u_{\chi\psi}$, $u_\chi e = \chi(e)u_\chi$. Then $\hat{G}$ acts on A by $\chi(x) = u_\chi.x.u_\chi^{-1}$; for the G-graduation on A related to that action of $\hat{G}$ on A we have a K-algebra isomorphism $T: A\hat{G} \longrightarrow AE$ such that $T(a) = a$ and if we consider the action of G on AE, we obtain an action of G on $A\hat{G}$; thus Z(A) is isomorphic to the centralizer of A in $A\hat{G}$, which is easily seen to be $\oplus_{\chi\in\hat{G}} K.u_\chi^{-1}\chi$ with $\sigma(u_\chi^{-1}\chi) = \chi(\sigma^{-1})u_\chi^{-1}\chi$. Thus the Galois extension of K associated to $\{k_{\chi,\psi}\}$ is the K-vector space $L = \oplus_{\chi\in\hat{G}} K\, a_\chi$, with product given by $a_\chi.a_\psi = k_{\chi,\psi}^{-1}a_{\chi\psi}$ and G acting as $\sigma(a_\chi) = \chi(\sigma^{-1})\, a_\chi$.

Let G be a finite abelian group of exponent e and K a field whose characteristic is prime to e. Let $\bar{K}$ be the field obtained adjoining the e-th roots of unity to K and W the Galois group of $\bar{K}$ over K. If $\hat{G}$ is the group of characters from G to $\bar{K}$, we shall see that $E_G(K) \cong H_W^2(\hat{G},\bar{K}^*)$ (see [4] Cor. 4.8, Th. 2.2), where the cohomology groups $H_W(\hat{G},\bar{K}^*)$ are defined by W-invariant cochains, i.e. such that $wf(\chi_1,\dots,\chi_n) = f(w\chi_1,\dots,w\chi_n)$. Observe first that if $\bar{L}$ is a Galois extension of $\bar{K}$ such that W can be extended to a group of automorphisms of $\bar{L}$, then $\bar{L} = \bar{L}^W \otimes \bar{K}$; moreover, if the actions of G and W commute on $\bar{L}$, then G acts on $\bar{L}^W$ and $\bar{L}^W$ is a Galois extension of K with group G, as follows from $\bar{L}G = \bar{L}^WG \otimes \bar{K}$.

If $\bar{k}_{\chi,\psi} \in \bar{K}^*$ is a W-invariant cocycle, let $\bar{L} = \oplus \bar{K} a_\chi$ the extension of K associated to it, that is, $a_\chi . a_\psi = \bar{k}^{-1}_{\chi,\psi} a_{\chi\psi}$, $\sigma(a_\chi) = \chi(\sigma^{-1}) a_\chi$; then the relation $w(k_{\chi,\psi}) = k_{w\chi,w\psi}$ implies that defining $w(a_\chi) = a_{w\chi}$ for $w \in W$, we extend W to a group of automorphisms of $\bar{L}$ which obviously commute with G and then $L = \bar{L}^W \in E_G(K)$. We can verify that the correspondence $k_{\chi,\psi} \longrightarrow L$ induces a group homomorphism $H^2_W(G,\bar{K}^*) \longrightarrow E_G(K)$. If L is trivial, then $L = \bar{L}^W$ has a normal basis generated by $\theta \in L$ such that $\sigma(\theta)\,\eta(\theta) = \delta_{\sigma,\eta}\sigma(\theta)$; writing $a_\chi = \sum_\sigma k^\sigma_\chi\, \sigma(\theta)$ with $k^\sigma_\chi \in \bar{K}$, we deduce that $w(k'_\chi) = k'_{w\chi}$ and $k'_{\chi\psi} = k_{\chi,\psi} k'_\chi\, k'_\psi$, which shows that $H^2_W(\hat{G},\bar{K}^*) \longrightarrow E_G(K)$ is injective.

Let $L \in E_G(K)$ and $\bar{L} = L \otimes \bar{K}$; if $A = LG$, $\bar{A} = \bar{L}G = A \otimes \bar{K}$ then L and $\bar{L}$ are the centralizers of A and $\bar{A}$ in AE and $\bar{A}E$ respectively. Consider the action of $\hat{G}$ on $\bar{A}$ related to the graduation of $\bar{A}$ and let $T\colon \bar{A}\hat{G} \longrightarrow \bar{A}E$ be the canonical isomorphism. Since $\bar{A}E = AE \otimes \bar{K}$, W acts on $\bar{A}E$; it is clear that $T\colon \bar{A}\hat{G} \longrightarrow \bar{A}E$ is a W-isomorphism if W acts on $\bar{A}\hat{G}$ by means of $w(\bar{a}\chi) = 1 \otimes w(\bar{a}).w\chi$. Then $L \cong T^{-1}(Z(A)) = T^{-1}(Z(\bar{A}))^W$. Let us determine a cocycle corresponding to $\bar{A}$ in $H^2(\hat{G},\bar{K}^*)$. Let $\theta = \sum u_\sigma e_\sigma \in Z(A)$ generate a normal basis of $Z(A)$ and $\bar{\theta} = T^{-1}(\theta) \in \bar{A}\hat{G}$; then $\bar{\theta} = \sum a_\chi \chi$ with $a_\chi = 1/n \sum_\sigma \chi(\sigma^{-1}) u_\sigma$; note that $\chi(\bar{a}).a_\chi = a_\chi.\bar{a}$; if b_χ is a unit of $\bar{A}$ such that $\chi(\bar{a}) = b_\chi\, \bar{a}\, b^{-1}_\chi$ we must have $a_\chi \in \bar{K}.b_\chi$ and since $\sum a_\chi \chi$ generates a normal basis, $a_\chi \neq 0$ and therefore a_χ is a unit of $\bar{A}$; then $\chi(\bar{a}) a_\chi = a_\chi\, \bar{a}$ shows that a cocycle corresponding to $\bar{A}$ can be defined by the relation $a_\chi a_\psi = \bar{k}_{\chi,\psi} a_{\chi\psi}$. Since $w(a_\chi) = a_{w\chi}$, and $a_{w\chi.w\psi} = a_{w\chi\psi}$, it follows that $w(\bar{k}_{\chi,\psi}) = \bar{k}_{w\chi,w\psi}$. Now $T^{-1}(Z(\bar{A}))$, the centralizer of $\bar{A}$ in $\bar{A}\hat{G}$, is $\oplus K a^{-1}_\chi \chi$. If $a^{-1}_\chi \chi = \bar{a}_\chi$, we have then $\bar{a}_\chi.\bar{a}_\psi = \bar{k}^{-1}_{\chi,\psi} \bar{a}_{\chi\psi}$ and $w(\bar{a}_\chi) = \bar{a}_{w\chi}$ and since $L = T^{-1}(Z(A)) = T^{-1}(Z(\bar{A}))^W$, we conclude that L is the image of $\{\bar{k}_{\chi,\psi}\} \in H^2_W(\hat{G},\bar{K}^*)$.

REFERENCES

[1] M. AUSLANDER and O. GOLDMAN, *The Brauer group of a commutative ring*, Transactions of the A.M.S., Vol. 97 (1960), p.p. 367-409.

[2] H. BASS, *Topics in algebraic K-theory*. Tata Institute of Fundamental Research, Bombay (1966).

[3] S. CHASE, D. HARRISON and A. ROSENBERG, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. N°. 52 (1965), p.p. 15-33.

[4] S. CHASE and A. ROSENBERG, *A theorem of Harrison, Kummer theory and Galois algebras*, Nagoya Math. Journal, Vol. 27 (1966), p.p. 663-685.

[5] M. ORZECH, *A cohomological description of abelian Galois extensions*, Transactions of the A.M.S., Vol. 137 (1969), p.p. 481-499.

[6] D.J. PICCO, *El grupo de Brauer graduado*, Notas (1967), Bahía Blanca.

[7] B. VAN DER WAERDEN, *Algebra*, Vol. 2, 5^{th} edition, Springer-Verlag.

[8] C.T.C. WALL, *Graded Brauer groups*, J. Crelle, Band 213 (1964), p.p. 187-199.

[9] P. WOLF, *Algebraische Theorie der Galoischen Algebren*, Deutschen Verlag der Wissenschaften, Berlin 1965.

Universidad Nacional del Sur
Argentina

Recibido en agosto de 1971.