ALBRECHT FRÖHLICH
C. T. C. WALL

Equivariant brauergroups in algebraic number theory

Mémoires de la S. M. F., tome 25 (1971), p. 91-96
<http://www.numdam.org/item?id=MSMF_1971__25__91_0>

Colloque Th. Nombres [1969, Bordeaux]
Bull. Soc. math. France,
Mémoire 25, 1971, p. 91 à 96

EQUIVARIANT BRAUERGROUPS IN ALGEBRAIC NUMBER THEORY (*)

by

A. FRÖHLICH and C.T.C. WALL

-:-:-:-

1. - The Equivariant Brauergroup

This section contains the bare minimum of general theory required in the sequel. We shall avoid going into the categorical generalities which underlie a systematic treatment. (See however our paper in the Proceedings of the Hull conference on K-theory (Springer Notes 108) for the notion of a group graded category $\mathfrak{C}$. Those familiar with this paper will realize that what we are considering here are examples of categories $\mathrm{Rep}(\mathfrak{C})$.

We give ourselves a pair (R,Γ) , where Γ is a 2-graded group whose underlying group we shall denote by Γ_+ with grading map $\omega : \Gamma_+ \to \pm 1$ (units of Z) and where R is a commutative ring (always with 1) and a Γ_+-module , Γ_+ acting by ring automorphisms. We shall be interested specifically in two particular cases, namely (a) direct action when $\omega = \varepsilon : \Gamma_+ \to 1$ is the null map, i.e. , "$\Gamma = \Gamma_+$", and (b) involution when $\omega : \Gamma \cong \pm 1$ is an isomorphism.

Let M , N be R-modules. An additive map $f : M \to N$ is said to have grade $\gamma (\gamma \in \Gamma_+)$, if

$$f(r\,m) = {}^{\gamma}r\, f(m) \qquad , \qquad r \in R \ , \ m \in M \ .$$

In the case of direct action an (R,Γ)-module (M,g) consists of an R -module M and a homomorphism $g : \Gamma \to \mathrm{Aut}_Z(M)$ so that, for all γ , g_γ is of grade γ . In the case of involution an (R,Γ)-module (M,g) consists of an R-module M and a non-singular Hermitian form h_g on M over R , with respect to the involution on R induced by the generator γ of Γ . There is of course a general definition applying to all cases, but we shall not need this here. We shall however give the general definition of an (R,Γ)-algebra (A,g) . This is an (R,Γ_+)-module, with A as R-algebra, and so that the g_γ act on the ring A by automorphisms when γ is even (i.e., $\omega(\gamma) = 1$) and by antiautomorphisms when γ is odd (i.e., $\omega(\gamma) = -1$). Thus in case (b) A is just an R-algebra with involutory antiautomorphism compatible with the involution on R .

(*) This is a version of the talk given by Fröhlich at the Bordeaux Colloquium. A detailed account of the underlying theory and its applications will be published elsewhere. No proofs will be given here.

The (R,Γ)-modules (M,g) for which M is an R-progenerator form a category $\mathfrak{Gen}(R,\Gamma)$ with product $\otimes_R$ (diagonal action of Γ) and identity object given by R. The morphisms of $\mathfrak{Gen}(R,\Gamma)$ are to be just the isomorphisms of grade 1 (of course commuting with the Γ-action). Similarly the (R,Γ)-algebras (A,g) with A central separable, and their isomorphisms of grade 1 form a category $\mathfrak{A}_Z(R,\Gamma)$ with product $\otimes_R$ and identity object. The isomorphism classes in each of these two categories form an Abelian monoid, which we shall denote by $\mathrm{Gen}(R,\Gamma)$, and $A_Z(R,\Gamma)$ respectively. The classes in $\mathfrak{Gen}(R,\Gamma)$ with underlying modules of rank one form the maximal subgroup $C(R,\Gamma)$ of $\mathrm{Gen}(R,\Gamma)$, the <u>equivariant class-group</u> or Picard group. Moreover one can define in general a product preserving functor

$$\mathrm{End} : \mathfrak{Gen}(R,\Gamma) \to \mathfrak{A}_Z(R,\Gamma) .$$

We only describe it in our two special cases. When the action is direct, then $\mathrm{End}(M,g)$ is just $\mathrm{End}_R(M)$ with Γ acting by conjugation, and in the case of involution then it is $\mathrm{End}_R(M)$ with the adjoint involution of h_g. We now get a monoid map

$$\mathrm{End} : \mathrm{Gen}(R,\Gamma) \to A_Z(R,\Gamma) ,$$

whose cokernel is a group, the <u>equivariant Brauergroup</u> $B(R,\Gamma)$. To establisch the group property one has to generalize the known isomorphism

$$A \otimes_R A^{op} \cong \mathrm{End}_R(A) .$$

Finally forgetting the Γ-action one gets a map from $B(R,\Gamma)$ into the ordinary Brauergroup $B(R)$, and we shall write

$$B_o(R,\Gamma) = \mathrm{Ker}[\, B(R,\Gamma) \to B(R)\,] .$$

It is this group in which we shall be interested mainly.

The cohomology groups of the graded group Γ with coefficients in $U(R)$ (group of units) and in $C(R)$ (ordinary Picard group) are defined via the obvious action of Γ_+ twisted by the grading ω. Thus if $(\gamma, u) \to {}^{\gamma}u$ is the originally given action of Γ_+ on R, then the twisted action of Γ on $U(R)$ used to define $H^i(\Gamma, U(R))$ is $(\gamma,u) \to ({}^{\gamma}u)^{\omega(\gamma)}$. Thus in case (a) $H^i(\Gamma, U(R)) = H^i(\Gamma_+, U(R))$, in case (b) $H^i(\Gamma, U(R)) = H^{i+1}(\Gamma_+, U(R))$ $(i \geq 1)$. Similarly for $C(R)$.

From now on assume Γ finite.

THEOREM 1. <u>There is an exact sequence</u>

$$(1)\qquad 0 \to H^1(\Gamma, U(R)) \to C(R,\Gamma) \to H^0(\Gamma, C(R)) \to H^2(\Gamma, U(R)) \to$$
$$\to B_0(R,\Gamma) \to H^1(\Gamma, C(R)) \to H^3(\Gamma, U(R)) .$$

<u>Remarks</u> 1) This is the top row of a larger diagram involving $B(R,\Gamma)$ and other versions of the Brauergroup.

2) The sequence (1) is derived from an infinite exact sequence

$$0 \to H^1(\Gamma, U(R)) \to \dots \to H^i(\Gamma, U(R)) \to H^i(\mathfrak{C}(R,\Gamma)) \to$$
$$\to H^{i-1}(\Gamma, C(R)) \to H^{i+1}(\Gamma, U(R)) \to \dots$$

where the $H^i(\mathfrak{C}(R,\Gamma))$ are cohomology groups of a certain complex. One gets (1) via suitable isomorphisms for the lowest terms. We shall describe one example of this (cf. (2)). The only property of the $H^i(\mathfrak{C}(R,\Gamma))$ we shall need is

THEOREM 2. <u>The groups</u> $H^i(\mathfrak{C}(R,\Gamma))$ <u>are annihilated by</u> card Γ .

This result is of interest in connection with

THEOREM 3. <u>Every class in</u> $B_0(R,\Gamma)$ <u>is represented by an</u> (R,Γ)-<u>algebra</u> $(\mathrm{End}_R(M),g)$ <u>with rank</u> $(M) = \mathrm{card}\ \Gamma$. <u>If</u> R <u>is connected then the class in</u> $B_0(R,\Gamma)$ <u>of any</u> (R,Γ)-<u>algebra</u> $(\mathrm{End}_R(M),g)$ <u>is annihilated by</u> rank (M) .

<u>Examples</u> (i) - If ω is null , R/R^Γ Galois with group Γ then

$$C(R^\Gamma) \cong C(R,\Gamma) \quad , \quad B(R^\Gamma) \cong B(R,\Gamma)$$

$$\mathrm{Ker}\,[B(R^\Gamma) \to B(R)] \cong B_0(R,\Gamma)$$

and our sequence (1) yields one which looks like that of Chase-Harrison-Rosenberg.

(ii) - When R is a field then (1) yields an isomorphism

$$H^2(\Gamma, U(R)) \cong B_0(R,\Gamma) .$$

It is instructive to interpret this explicitly in the well known cases

(a) Γ acts directly as Galois group , (b) Γ acts trivially on R with direct action , (c) $\Gamma \cong \pm 1$ with non-trivial involution, (d) $\Gamma \cong \pm 1$ with trivial involution.

2. - Algebraic integers with involution

To begin with R can still be an arbitrary commutative ring, $\omega : \Gamma \cong \pm 1$, and γ denotes the generator of Γ.

Consider pairs (P,f), P a rank 1 projective, f an automorphism of P of grade γ with $f^2 = 1$. If Q is any rank 1-projective and ${}^{\gamma}Q$ its image under some bijection $q \mapsto {}^{\gamma}q$ of grade γ then for $P = {}^{\gamma}Q \otimes_R Q$ we may take $f({}^{\gamma}q_1 \otimes q_2) = {}^{\gamma}q_2 \otimes q_1$. Call this a trivial pair. The isomorphism classes of pairs (P,f) modulo those of trivial pairs form an Abelian group under $\otimes_R$ an this is $H^2(\mathfrak{C}(R,\Gamma))$ in our simple case. The general construction is really quite analogous. (There is also a special feature of the quadratic case tying up equivariant classgroups and Brauergroups for opposite gradings).

Next we describe the isomorphism

$$\psi : H^2(\mathfrak{C}(R,\Gamma) \cong B_o(R,\Gamma) . \tag{2}$$

Let a pair (P,f), as above, be given. The associated Brauer class is then that of the pair $(\mathrm{End}_R(M), i_h)$ where (i) M is an R-progenerator, (ii) $h : M \times M \to P$ is a non-singular pairing which is R-linear in the first argument and so that $h(m_2,m_1) = fh(m_1,m_2)$ (in other words h is a "non-singular Hermitian from over (P,f)") (iii) i_h is the adjoint involution of h in $\mathrm{End}_R(M)$ (this exists !). Note that by Theorems 2 and 3 we could manage with an M of rank 2 and, except for the trivial class, not with M of rank 1. In fact we can choose

$$M = R \oplus P , \quad h((r_1,p_1), (r_2,p_2)) = r_1 \cdot fp_2 + {}^{\gamma}r_2 \cdot p_1 . \tag{3}$$

Viewing ψ as an identification the relevant maps of (1) have now an obvious description. Namely $B_o(R,\Gamma) \to H^1(\Gamma, C(R)) = \hat{H}^o(\Gamma_+, C(R))$ (Tate cohomology) takes $\mathrm{cl}(P,f)$ into $\mathrm{cl}(P)$. On the other hand let $u \in U(R)$, ${}^{\gamma}u \cdot u = 1$. Then under $H^1(\Gamma_+, U(R)) = H^2(\Gamma, U(R)) \to B_o(R,\Gamma)$ the class of u goes into the class of (R,f_u), $f_u(r) = u.{}^{\gamma}r$. The module M in (3) is now free, $\mathrm{End}_R(M)$ is the 2×2 matrix ring over R and

$$i_u \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} {}^{\gamma}a_{22} & {}^{\gamma}a_{12} \cdot {}^{\gamma}u \\ {}^{\gamma}a_{21} \cdot u & {}^{\gamma}a_{11} \end{pmatrix} .$$

Every full matrix ring over R with involution is Brauer equivalent to one of this type and criteria for equivalence can be derived from (1).

From now let R be the ring of integers in a finite algebraic number field L. If first the involution on R is trivial then (1) reduces to

$$(4)\qquad \begin{cases} C(R,\Gamma) \cong (U(R)/U(R)^2) \times C(R)_2 \\ B_o(R,\Gamma) \cong \{\pm 1\} \times (C(R)/C(R)^2) \end{cases},$$

where the subscript 2 denotes the kernel of multiplication by 2. If the involution is non-trivial then (2) yields

$$(5)\qquad B_o(R,\Gamma) \cong \mathrm{Cok}\,[\hat{H}^o(\Gamma_+,L^*) \to \hat{H}^o(\Gamma_+,I(R))]\ ,$$

where $L^* = U(L)$, $I(R)$ = group of fractional ideals. Hence $B_o(R,\Gamma)$ is an elementary 2-group and

$$(6)\qquad \begin{cases} \mathrm{card}\ B_o(R,\Gamma) = \sup\ (2,2^d) \\ d = \text{number of ramified prime ideals in } R/R^\Gamma . \end{cases}$$

3. - Algebraic integers with direct action of a Galoisgroup

L is again a finite algebraic number field with subfield K, $\Gamma = \mathrm{Gal}(L/K)$, with null grading $\omega = \varepsilon$, R = integers in L, T = integers in K. The subscript $\mathfrak{p}$ denotes completion at $\mathfrak{p}$, with respect to a prime $\mathfrak{p}$ in the base field K. Thus if $\mathfrak{p}$ is finite then $R_\mathfrak{p} = \Pi\, R_\mathfrak{P}$ (all $\mathfrak{P}$ in L above $\mathfrak{p}$). One knows that $B(R_\mathfrak{p}) = 0$ whence $B(R_\mathfrak{p},\Gamma) = B_o(R_\mathfrak{p},\Gamma)$. Also $B(R) \to B(L)$ is injective, and we may identify $B(R)$ with the group of those Brauer classes over L which split at all finite primes. Moreover, as by (1) $H^2(\Gamma, U(R_\mathfrak{p})) = B_o(R_\mathfrak{p},\Gamma)$, these groups vanish at all non-ramified prime ideals. Beyond this one has

THEOREM 4. <u>The sequences</u>

$$0 \to \mathrm{Ker}\,[B(T) \to B(R)] \to B_o(R,\Gamma) \to \prod_{\mathfrak{p}\text{ finite}} B_o(R_\mathfrak{p},\Gamma)$$

$$0 \to B(T) \to B(R,\Gamma) \to \prod_{\mathfrak{p}\text{ infinite}} B_o(R_\mathfrak{p},\Gamma)$$

<u>are exact and</u>

$$B_o(R,\Gamma) \to B_o(L,\Gamma)\ ,\ B(R,\Gamma) \to B(L,\Gamma)$$

<u>are injective.</u>

Let J_L be the idele group of L and

$$U_L = \prod_{\mathfrak{p}\text{ finite}} U(R_\mathfrak{p}) \times \prod_{\mathfrak{p}\text{ finite}} U(L_\mathfrak{p})\ .$$

Then we have

THEOREM 5. <u>In the commutative diagram</u>

$$\begin{tikzcd}
0 \arrow[r] & B_o(R,\Gamma) \arrow[r] \arrow[d] & H^2(\Gamma,U_L) \arrow[r, "\mathrm{inv}"] \arrow[d] & H^2(\Gamma,J_L/L^*) \arrow[d] \\
0 \arrow[r] & H^2(\Gamma,L^*) \arrow[r] & H^2(\Gamma,J_L) \arrow[r, "\mathrm{inv}"] & H^2(\Gamma,J_L/L^*)
\end{tikzcd}$$

<u>the first row is exact</u> (and so is of course by classfield theory the second row).

Let for the moment $B_o(L/K)$ denote the subgroup of $B(K)$ of Brauer classes which split in L, as well as at all finite, non-ramified $\mathfrak{p}$ and which have at all finite ramified primes cocycles in the group of units. From the last theorem we have an isomorphism

$$(7) \qquad \theta : B_o(L/K) \cong B_o(R,\Gamma) .$$

We shall describe θ explicitly.

Let A be a central simple K-algebra whose class lies in $B_o(L/K)$. Then $A \otimes_K L \cong \mathrm{End}_L(V)$, V an L-vector space. The Γ-structure, given by the action on L, is reflected in a Γ-structure on $\mathrm{End}_L(V)$ given by conjugation with automorphisms f_γ of grade γ on V, so that $f_\gamma f_\delta \equiv f_{\gamma\delta} \pmod{L^*}$. One can then construct an R-lattice M spanning V and fractional R-ideals $\mathfrak{a}_\gamma$ so that $f_\gamma M = \mathfrak{a}_\gamma M$. This yields an R-algebra $\mathrm{End}_R(M) \subset \mathrm{End}_L(V)$ stable under the f_γ. Its class is the required image in $B_o(R,\Gamma)$. Moreover the ideal classes $\mathrm{cl}(\mathfrak{a}_\gamma)$ define its image under $B_o(R,\Gamma) \to H^1(\Gamma,C(R))$.

We shall finally compute the order of $B_o(R,\Gamma)$. Let $\mathfrak{P}$ be a finite prime in L, $L_\mathfrak{P}$ the completion, $U_\mathfrak{P}$ the group of units of $R_\mathfrak{P}$ and consider the exact valuation sequence

$$\theta \to U_\mathfrak{P} \to L_\mathfrak{P}^* \xrightarrow{v_\mathfrak{P}} Z \to 0 .$$

If $e_\mathfrak{P} = e_\mathfrak{p}$ is the ramification index over $K_\mathfrak{p}$ $(\mathfrak{P}|\mathfrak{p})$ then $v_\mathfrak{P}|K_\mathfrak{p} = e_\mathfrak{P} v_\mathfrak{p}$. It follows that effectively $H^2(\mathrm{Gal}\, L_\mathfrak{P}/K_\mathfrak{p}), L_\mathfrak{P}^*) \to H^2(\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}),Z)$ is multiplication by $e_\mathfrak{P}$ and hence that $H^2(\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}),U_\mathfrak{P})$ is cyclic of order $e_\mathfrak{P}$. Going over to the global field and taking into account the infinite primes we conclude that $H^2(\Gamma,U_L)$ id the direct product of cyclic groups of frder $e_\mathfrak{p}$, $\mathfrak{p}$ running through all primes of K, with the obvious meaning of $e_\mathfrak{p}$ for infinite $\mathfrak{p}$. On the other hand the image of inv from $H^2(\Gamma,U_L)$ clearly has order the least common multiple of the $e_\mathfrak{p}$. Hence finally

$$(8) \qquad \mathrm{card}\, B_o(R,\Gamma) = \frac{\Pi e_\mathfrak{p}}{\mathrm{LCM} e_\mathfrak{p}} .$$

University of London King's College
Department of Mathematics
Stand, W.C.2. (Grande-Bretagne)