ACTAS DEL VIII CONGRESO
DR. ANTONIO A. R. MONTEIRO
(2005), Páginas 131–150

LECTURES ON THE BRAUER GROUP AND THE PROJECTIVE SCHUR SUBGROUP OF A FIELD

ELI ALJADEFF

1. INTRODUCTION

Representations of finite groups over the field of complex numbers is one of the most studied subjects in finite group theory. It has many applications to different areas of mathematics. It has also important applications to physics and chemistry. Given a finite group G we can construct the group algebra $A = kG$ over the field of complex numbers. By well known theorems of Maschke and Wedderburn, the algebra A is the direct sum of matrix algebras over the field k. For instance, if $G = D_6$ is the dihedral group of order 6, the decomposition of the algebra A is as follows:

$$kG \simeq k \oplus k \oplus M_2(k).$$

If the group G is the quaternion group of order 8 (Q_8) then the decomposition is

$$kG \simeq k \oplus k \oplus k \oplus k \oplus M_2(k).$$

The direct summands in such decompositions correspond to the irreducible representations of the group G. Both examples have irreducible representations of dimension 2. Let us analyze these (two) representations in more detail. If the dihedral group is given by $G = D_6 = \langle \sigma, \tau : \sigma^3 = \tau^2 = e, \sigma\tau = \tau\sigma^2 \rangle$ the irreducible representation of dimension 2 is given by

$$\sigma \longmapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\tau \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For the quaternion group $Q_8 = \langle \sigma, \tau : \sigma^4 = e, \tau^2 = \sigma^2, \sigma\tau = \tau\sigma^3 \rangle$ the representation of dimension 2 is given by

$$\sigma \longmapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

$$\tau \longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

It should be noted that in the dihedral case all the entries in the matrices are real whereas in the quaternion case some of the entries are complex numbers. Of course, it is possible to change the map (following a base change) in the dihedral case in such a way that some of the entries will be complex and not real but it is impossible to change the base of the

2-dimensional vector space k^2 in such a way that the matrices of the 2-dimensional representation of the quaternion group will have only real entries. We say that the two dimensional representation of Q_8 cannot be realized over the real numbers. Another way to see this phenomenon is by taking the group algebra RQ_8. Again, this algebra is semisimple and it decomposes into simple components. One of the components is the quaternion algebra of dimension 4 over the real numbers (and not the algebra of 2×2 matrices over the reals). Extending the scalars to the complex numbers (i.e. tensoring with the field of complex numbers over the reals) we "recover" the algebra of 2×2 matrices over the complex numbers. We would like to view the quaternion algebra of dimension 4 over the reals as an obstruction to the realization of the 2-dimensional irreducible representation of the quaternion group over the real numbers. If we tensor by the complex numbers we split the quaternion algebra and hence we split the obstruction.

An important question in the theory of representations of finite groups is over what fields one can realize the representations of a given group G. Another question which is intimately related to that question is what are the possible obstructions or more precisely, what are the division algebras that appear in the Wedderburn decomposition of a group algebra kG for a given group G and given field k. An easier question (but still highly non trivial) is if we fix the field k what are all the division algebras that can appear in such decomposition when we run over all finite groups. In this series of lectures I would like to consider that question and also the analogous question for projective representations (with $PGL_n(k)$ instead of $GL_n(k)$). But before we consider these problems we should study some basics in the theory of division algebras, cohomology and Brauer groups.

2. Group extensions and $H^2(G,A)$

Let Γ be a group (not necessarily finite), A an abelian, normal subgroup, and let $G=\Gamma/A$. We have a short exact sequence of groups

$$1\longrightarrow A\longrightarrow \Gamma\longrightarrow G\longrightarrow 1.$$

Such a sequence defines an action of G on A. This is defined as follows: for each $\sigma\in G$ *choose* an element $u_\sigma\in\Gamma$ with $\pi(u_\sigma)=\sigma$ and consider the automorphism of A:

$$\begin{aligned}\eta_\sigma : A &\longrightarrow A\\ a &\longmapsto u_\sigma a u_\sigma^{-1}.\end{aligned}$$

Since A is abelian one checks that the map η_σ is well defined, namely is independent of the choice of the element $u_\sigma\in\Gamma$. So we have defined a map

$$\begin{aligned}\eta : G &\longrightarrow \mathrm{Aut}(A)\\ \sigma &\longmapsto \eta_\sigma.\end{aligned}$$

and it is easy to check that η is a group homomorphism.

Since the elements u_σ are representatives of the cosets of A in Γ, every element in Γ is written uniquely as au_σ, $a\in A$, $\sigma\in G$. The product of two such elements is given by

$$(au_\sigma)(bu_\tau)=au_\sigma bu_\sigma^{-1}u_\sigma u_\tau=a\eta_\sigma(b)u_\sigma u_\tau.$$

Since the element $u_\sigma u_\tau$ is mapped onto $\sigma\tau$ by π, there exists an element in A, denoted by $f(\sigma,\tau)$, such that

$$u_\sigma u_\tau=f(\sigma,\tau)u_{\sigma\tau}.$$

Furthermore, if we abuse notation and write $\sigma(b) = \eta_\sigma(b)$ for the action of σ on b we obtain

$$(au_\sigma)(bu_\tau) = a\sigma(b) f(\sigma,\tau)u_{\sigma\tau}.$$

The associativity of Γ forces a condition on the function $f : G\times G \longrightarrow A$, namely the "2-cocycle" condition. Indeed the equality

$$(u_\sigma u_\tau)u_\nu = u_\sigma(u_\tau u_\nu)$$

implies the equality

$$f(\sigma\tau,\nu) f(\sigma,\tau) = f(\sigma,\tau\nu) f(\tau,\nu)^\sigma,$$

where $f(\tau,\nu)^\sigma$ stands for $\sigma(f(\tau,\nu))$. We call such a function "2-cocycle".

The set of 2-cocycles $f : G\times G \longrightarrow A$ is a group with the pointwise multiplication, that is, $fg(\sigma,\tau) = f(\sigma,\tau)g(\sigma,\tau)$. The identity is $f \equiv 1 \in A$. The group is denoted by $Z^2(G,A)$.

Conversely: Fix a group G and an abelian group A. Fix an action of G on A (i.e. a map $G \longrightarrow \mathrm{Aut}(A)$). A 2-cocycle $f : G\times G \longrightarrow A$ defines an extension of groups

$$1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1,$$

where the elements of Γ are of the form $au_\sigma, a \in A, u_\sigma$ a symbol, one for each element σ of G. The multiplication in Γ is defined by

$$(au_\sigma)(bu_\tau) = a\sigma(b) f(\sigma,\tau)u_{\sigma\tau}.$$

It is easy to show that the extension obtained "gives back" the action of G on A. Now put an equivalence relation on the extensions of G by A. Let

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \Gamma_1 & \longrightarrow & G & \longrightarrow & 1 \\ & & {\scriptstyle id}\downarrow & & \downarrow & & {\scriptstyle id}\downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & \Gamma_2 & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

be two extensions. We say that they are equivalent if there is a homomorphism (hence an isomorphism, check!) $\Gamma_1 \longrightarrow \Gamma_2$ making the two squares commutative. Denote the set of equivalence classes by $E(G,A)$. We have defined a map

$$\phi : Z^2(G,A) \longrightarrow E(G,A).$$

Now on the set $E(G,A)$ one can define a natural group structure which makes the map ϕ a group homomorphism. Furthermore by our discussion ϕ is surjective onto $E(G,A)$. The kernel of ϕ (check!) consists of the 2-cocycles $f : G\times G \longrightarrow A$ for which there exists a 1-parameter family $\{\lambda_\sigma\}_{\sigma\in G}$ in A such that

$$f(\sigma,\tau) = \lambda_\sigma \sigma(\lambda_\tau)\lambda_{\sigma\tau}^{-1} \quad \text{for every } \sigma,\tau \in G.$$

Such f is called a coboundary and we denote $\ker\phi = B^2(G,A)$.

Thus we obtain $Z^2(G,A)/B^2(G,A) \simeq E(G,A)$. We denote the quotient $Z^2(G,A)/B^2(G,A) = H^2(G,A)$ and call it the second cohomology group of G with coefficients in A. (Note that A is a G-module.)

Remarks: 1) the trivial 2-cocycle yields the semidirect product $\Gamma = G \ltimes A$.
2) A trivial action of G on A is equivalent to the extension $1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$ being central ($A \hookrightarrow Z(\Gamma)$).

3. Other cohomology groups

Given a group G and a G-module A (written multiplicatively) we define $H^0(G,A) = A^G$, the G invariant elements in A.

$H^1(G,A) = Z^1(G,A)/B^1(G,A)$ where $Z^1(G,A) = f : G \longrightarrow A : f(\sigma\tau) = f(\sigma)\sigma(f(\tau))$. Such f is called 1-cocycle or crossed homomorphism.

$B^1(G,A) = f : G \longrightarrow A : \exists a \in A$ with $f(\sigma) = \sigma(a)a^{-1},$ for every $\sigma \in G$.

In general, $H^n(G,A)$ is defined as follows (for this description we let A have an additive structure).

Consider $\mathbb{Z}$ as a trivial G module $(ga = a,\ \forall g \in G,\ a \in \mathbb{Z})$. Let

$$\to P_n \to P_{n-1} \to \cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

be a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}G$. Delete $\mathbb{Z}$ from this exact sequence and to the deleted complex apply the contravariant functor $F = \mathrm{Hom}_{\mathbb{Z}G}(-,A)$. We get

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(P_0,A) \xrightarrow{d_0} \mathrm{Hom}_{\mathbb{Z}G}(P_1,A) \xrightarrow{d_1} \mathrm{Hom}_{\mathbb{Z}G}(P_2,A)$$
$$\to \cdots \to \mathrm{Hom}_{\mathbb{Z}G}(P_n,A) \xrightarrow{d_n} \mathrm{Hom}_{\mathbb{Z}G}(P_{n+1},A) \to$$

This is a complex, usually nonexact (since F is not exact). We “define”

$$H^n(G,A) = \frac{\mathrm{Ker}\, d_n}{\mathrm{Im}\, d_{n+1}}.$$

One shows that up to isomorphism, the group $H^n(G,A)$ does not depend on the resolution. To check that this definition coincides with the definition of the low dimension cohomology groups, one uses the standard resolution in its non-homogeneous form, also called the *bar resolution*.

Explicitly, let $F_n,\ n \geq 1$ be the free $\mathbb{Z}G$ module with a basis $\{[g_1|g_2|\ldots|g_n] : g_i \in G\}$, and for $n = 0$, we let $F_0 \simeq \mathbb{Z}G$, i.e., the free module with a unique basis element denoted by $[\ ]$. The differentials $\partial : F_n \to F_{n-1}$ are defined in terms of the G basis $[g_1|\ldots|g_n]$ by $\partial = \sum_{i=0}^{n} (-1)^i d_i$, where d_i is the $\mathbb{Z}G$-homomorphism given by

$$d_i[g_1|\ldots|g_n] = \begin{cases} g_1\left[g_2|\ldots|g_n\right] & i = 0 \\ \left[g_1|\ldots|g_{i-1}|g_ig_{i+2}|\ldots|g_n\right] & 0 < i < n \\ \left[g_1|\ldots|g_{n-1}\right] & i = n. \end{cases}$$

Let us check for example that it yields the above construction of $H^2(G,A)$. We write the resolution

$$\to F_3 \xrightarrow{\partial_3} F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

delete $\mathbb{Z}$ and apply the functor $F = \mathrm{Hom}_{\mathbb{Z}G}(-,A)$ (say, A with additive structure). We obtain

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(F_0,A) \xrightarrow{\partial_1^*} \mathrm{Hom}_{\mathbb{Z}G}(F_1,A) \xrightarrow{\partial_2^*} \mathrm{Hom}_{\mathbb{Z}G}(F_2,A) \xrightarrow{\partial_3^*} \mathrm{Hom}_{\mathbb{Z}G}(F_3,A)$$

$$H^2(G,A) = \frac{\mathrm{Ker}\,\partial_3^*}{\mathrm{Im}\,\partial_2^*}.$$

Take $f \in \mathrm{Hom}_{\mathbb{Z}G}(F_2, A)$ and require $\partial_3^* f = 0$, i.e., on the basis of F_3,

$$(\partial_3^* f)\big[\sigma|\tau|\nu\big] = 0 \quad \text{or} \quad f\big(\partial_3\big[\sigma|\tau|\nu\big]\big) = 0$$

for every $\sigma, \tau, \nu \in G$. This means that

$$f\left(\sum_{i=0}^{3}(-1)^i d_i\big[\sigma|\tau|\nu\big]\right) = f\Big(\sigma[\tau|\nu] - [\sigma\tau|\nu] + [\sigma|\tau\nu] - [\sigma|\tau]\Big) = 0.$$

Since f is a $\mathbb{Z}G$ linear map (denoting $f([*|*])$ by $f(*,*)$), we get

$$f(\sigma\tau,\nu) + f(\sigma,\tau) = f(\sigma,\tau\nu) + f(\tau,\nu)^{\sigma}.$$

If A has a multiplicative structure we get the required form.

The ∂-coboundaries are computed similarly.

4. Cohomology of cyclic groups

For our discussion on Brauer groups it is convenient to compute the cohomology groups of cyclic groups (finite).

Let G be a finite cyclic group of order n generated by σ ($G = \langle\sigma\rangle$). Instead of using the standard resolution, in this case, one can use a much simpler resolution which is periodic, namely,

$$\cdots \to \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{\Sigma} \mathbb{Z}G \xrightarrow{\sigma-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

where the maps Σ and $\sigma - 1$ are given by

$$\begin{aligned} \Sigma : \mathbb{Z}G &\longrightarrow \mathbb{Z}G \\ z &\longmapsto \big(1+\sigma+\sigma^2+\cdots+\sigma^{n-1}\big)z \\ (\sigma-1) : \mathbb{Z}G &\longrightarrow \mathbb{Z}G \\ z &\longmapsto (\sigma-1)z. \end{aligned}$$

One checks that this sequence is exact. Apply $\mathrm{Hom}_{\mathbb{Z}G}(-,A)$ to the deleted complex and get

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,A) \xrightarrow{(\sigma-1)^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,A) \xrightarrow{\Sigma^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,A) \xrightarrow{(\sigma-1)^*} \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G,A) \to$$

In order to compute $H^2(G,A)$ we have to compute

$$\frac{\mathrm{Ker}(\sigma-1)^*}{\mathrm{Im}\,\Sigma^*} \simeq \frac{A^G}{\mathrm{Im}\,\Sigma^*} = \frac{A^G}{\langle(1+\sigma+\sigma^2+\cdots+\sigma^{n-1})x\rangle}.$$

It follows that an element in $H^2(G,A)$ is represented by a single element in A^G. This simple fact will be important for some future discussions.

Explicitly, if $f : G \times G \to A$ is a 2-cocycle (G cyclic) then the class $\alpha = [f]$ may be represented by a 2-cocycle of the form

$$g(\sigma^i,\sigma^j) = \begin{cases} a \in A^G & i+j \geq n \ \ (= \mathrm{ord}\, G) \\ 1 & i+j < n. \end{cases}$$

The element $a \in A^G$ is obtained in terms of the given 2-cocycle f by (A with the multiplicative structure)

$$a = f(\sigma,\sigma)f(\sigma,\sigma^2)f(\sigma,\sigma^3)\dots f(\sigma,\sigma^{n-1}).$$

(Here we are assuming that $f(1,\sigma^i) = f(\sigma^i,1) = 1$.)

5. Restriction, inflation, corestriction

We will discuss briefly some maps in cohomology.

Let G be a group and H a subgroup. Given a G-module A, one has a map

$$\mathrm{res} : H^n(G,A) \to H^n(H,A),$$

which can be realized in terms of the n-cocycles arising from the bar resolution. More precisely, if $f : G\times G\times\cdots\times G \longrightarrow A$ is an n-cocycle representing an element $\alpha \in H^n(G,A)$, then $\mathrm{res}\,\alpha$ is the element in $H^n(H,A)$ represented by the restriction of f to $H\times H\times\cdots\times H$.

A different way to realize the restriction map is the following:

Let $\to P_n \to P_{n-1} \to \cdots \to \mathbb{Z} \to 0$ be a projective resolution of $\mathbb{Z}$ as a trivial $\mathbb{Z}G$-module. Since $\mathbb{Z}G$ is free over $\mathbb{Z}H$ (coset representatives form a basis), projective modules over $\mathbb{Z}G$ are projective as $\mathbb{Z}H$ modules and hence the above complex is also a projective resolution of $\mathbb{Z}$ as a trivial $\mathbb{Z}H$ module. In order to compute $H^n(G,A)$ and $H^n(H,A)$, we apply the functors $F_G = \mathrm{Hom}_{\mathbb{Z}G}(-,A)$ and $F_H = \mathrm{Hom}_{\mathbb{Z}H}(-,A)$ to the deleted complexes respectively. We get

$$0 \to \mathrm{Hom}_{\mathbb{Z}G}(F_0,A) \to \mathrm{Hom}_{\mathbb{Z}G}(F_1,A) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}G}(F_n,A) \to$$
$$0 \to \mathrm{Hom}_{\mathbb{Z}H}(F_0,A) \to \mathrm{Hom}_{\mathbb{Z}H}(F_1,A) \to \cdots \to \mathrm{Hom}_{\mathbb{Z}H}(F_n,A) \to$$

The restriction map $H^n(G,A) \to H^n(H,A)$ is the map in cohomology induced by the "identity" map

$$\mathrm{Hom}_{\mathbb{Z}G}(F_n,A) \to \mathrm{Hom}_{\mathbb{Z}H}(F_n,A).$$

The inflation map is well understood by means of n-cocycles arising from the bar resolution. Let N be a normal subgroup in G and G/N the quotient. Let A be a G-module ($\mathbb{Z}G$-module), and let A^N be the N-invariants in A. Then A^N is a G/N module. The inflation map $\mathrm{inf} : H^n(G/N,A^N) \to H^n(G,A)$ is given by $\mathrm{inf}(g)\,(\sigma_1,\dots,\sigma_n) = g(\bar{\sigma}_1,\dots,\bar{\sigma}_n)$, where $\bar{\sigma}$ denotes the coset in G/N represented by $\sigma \in G$.

Finally, we wish to define the corestriction map. Let G be a group and H a subgroup of finite index (say, n). Let us define

$$H^r(H,A) \to H^r(G,A).$$

In dimension zero the definition goes as follows: Pick a set of representatives for the left cosets of H in G. $G/H = \{s_1,\dots,s_n\}$.

$$\begin{aligned} \mathrm{cor} : H^0(H,A) = A^H \quad &\longrightarrow \quad A^G = H^0(G,A) \\ a \quad &\longrightarrow \quad \sum_{s\in G/H} s(a) \end{aligned}$$

Since a is H invariant, the definition does not depend on the set of representatives.

The extension of this map to higher dimension cohomology groups can be done by general theory. Let us give here a more down-to-earth approach, namely, using resolutions of $\mathbb{Z}$ as a trivial $\mathbb{Z}G$ and $\mathbb{Z}H$ module. Let

$$\cdots \to P_m \to P_{m-1} \to \cdots \to P_0 \to \mathbb{Z} \to 0$$

be a projective resolution of $\mathbb{Z}$ as a trivial $\mathbb{Z}G$ module. As above, consider this resolution over $\mathbb{Z}H$, apply F_G and F_H to the deleted complexes and get

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_0,A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_1,A) & \longrightarrow & \dots & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_n,A) \\ & & \downarrow & & \downarrow & & & & \downarrow{\scriptstyle \pi_n} \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_0,A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_1,A) & \longrightarrow & \dots & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_n,A) \end{array}$$

The map

$$\pi_n : \mathrm{Hom}_{\mathbb{Z}H}(P_n,A) \to \mathrm{Hom}_{\mathbb{Z}G}(P_n,A)$$

is defined by

$$\pi_n : f \longmapsto \sum_{s\in G/H} sf(s^{-1}-)$$

or $(\pi_n f)(x) = \sum_{s\in G/H} sf(s^{-1}x)$.

In order to show that this map induces a map in cohomology, one shows that the squares that appear in the diagram above are commutative, i.e., the map $\{\pi_n\}$ is a map of complexes.

Proposition 5.1. *Let G be a group, H a subgroup of finite index, $(G:H)=n$, A a G-module. Then the composition of the maps*

$$H^r(G,A) \xrightarrow{\text{res}} H^r(H,A) \xrightarrow{\text{cor}} H^r(G,A)$$

$\mathrm{cor}\circ\mathrm{res} = n$ *(multiplication by n). In particular, if G is finite of order n then (take $H=\{1\}$) n annihilates $H^r(G,A)$.*

Proof. Consider the diagram (P_* is a projective resolution of $\mathbb{Z}$ over $\mathbb{Z}G$)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_0,A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_1,A) & \longrightarrow & \dots & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}H}(P_n,A) \\ & & & & & & & & \downarrow{\scriptstyle \pi_n} \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_0,A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_1,A) & \longrightarrow & \dots & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}G}(P_n,A) \end{array}$$

Start with $f \in \mathrm{Hom}_{\mathbb{Z}G}(P_n,A)$. $\mathrm{res}(f)$ is the "same" function viewed as an H-linear function. Since it is G-linear, $sfs^{-1} = f$ and $\pi_n(\mathrm{res}(f)) = nf$. □

6. Crossed product algebras

Let K be a commutative ring with unit element 1. Let G be a finite group, and denote by $KG = \left\{\Sigma x_\sigma u_\sigma : x_\sigma \in K,\ u_\sigma \text{ a symbol, one for each element } \sigma \in G\right\}$ the group algebra where the multiplication is defined by $(x_\sigma u_\sigma)(y_\tau u_\tau) = x_\sigma y_\tau u_{\sigma\tau}$.

Now assume that G acts on K via a homomorphism t:

$$t : G \to \mathrm{Aut}(K).$$

On the "same" left free K-module KG we introduce a new multiplication using the action (as in semidirect product)

$$(xu_\sigma)(yu_\tau) = x\sigma(y)u_{\sigma\tau}$$

where $\sigma(y) = t(\sigma)(y)$. Now extend this multiplication by the distributive law. We obtain an associative ring and denote it by K_tG.

Now we can introduce another perturbation on the multiplication. Since G acts on K, the invertible elements K^* in K form a (multiplicative) G module (i.e., $r\sigma \in \mathbb{Z}G$ acts on x by $r\sigma(x) = \sigma(x)^r$) and therefore one can consider the second cohomology group $H^2(G,K^*)$ of G with coefficients in the G module K^*. As explained in Section 2, an element $\alpha \in H^2(G,K^*)$ is represented by a 2-cocycle $f : G \times G \to K^*$.

On the same underlying free K-module as K_tG (or KG) we define a new multiplication so that it satisfies the rule

$$(xu_\sigma)(yu_\tau) = x\sigma(y)f(\sigma,\tau)u_{\sigma\tau}.$$

We denote this ring by K_t^fG. The associativity follows from the 2-cocycle condition satisfied by f. It is easy to check that, up to a ring isomorphism, this construction does not depend on the representative f but only on the cohomology class $[f] = \alpha \in H^2(G,K^*)$. This explains the notation

$$K_t^\alpha G.$$

This ring is called the crossed product of K with G.

If α is trivial (i.e., represented by $f \equiv 1$) we recover K_tG, the skew group ring of K with G.

If the action of G on K is trivial one writes $K^\alpha G$ and calls it the twisted group ring of K with G.

It is time for some examples.

Let K/k be a finite Galois extension of fields and $G = \mathrm{Gal}(K/k)$ be the Galois group. Then we can form the skew group algebra (trivial 2-cocycle) K_tG (the action on K is the Galois action). Let $(K:k) = n$. Then the dimension of K_tG as a K vector space is n and as a k-vector space is n^2.

The next proposition shows that K_tG is a simple algebra. More generally we show

Proposition 6.1. *Let K be a field and G a group (not necessarily finite) acting on K faithfully (i.e., $\ker t = \{1\}$ where $t : G \to \mathrm{Aut}(K)$). Let $\alpha \in H^2(G,K^*)$ and $f : G \times G \to K^*$ be a 2-cocycle representing α. Then the crossed product $K_t^\alpha G$ is simple.*

Proof. We have to show that $K_t^\alpha G$ has no non-trivial 2-sided ideals. Let $I \neq 0$ be an ideal in $K_t^\alpha G$ (2-sided) and let $z = x_1u_{\sigma_1} + x_2u_{\sigma_2} + \cdots + x_ru_{\sigma_r}$ be an element in I of minimum length. If $r = 1$, then $z = x_1u_{\sigma_1}$ is invertible and $I = K_t^\alpha G$.

So assume that $r \geq 2$. Multiplying by $u_{\sigma_1}^{-1}$ we can assume that

$$z = x_1u_e + x_2u_{\sigma_2} + x_3u_{\sigma_3} + \cdots + x_ru_{\sigma_r} \quad (e \text{ identity in } G).$$

Now, since the action of G on K is faithful, there exists $y \in K$ with $\sigma_2(y) \neq y$. We claim that the element $\omega = yz - zy$ has length that is shorter than the length of z, and also $0 \neq \omega \in I$.

This is a contradiction to the minimality of z. Indeed,

$$\begin{aligned}\omega &= yx_1u_e + yx_2u_{\sigma_2} + yx_3u_{\sigma_3} + \cdots + yx_ru_{\sigma_r}\\ &\quad -\big(x_1u_ey + x_2u_{\sigma_2}y + \cdots + x_ru_{\sigma_r}y\big)\\ &= x_2\big(y-\sigma_2(y)\big)u_{\sigma_2} + x_3\big(u-\sigma_3(y)\big)u_{\sigma_3} + \cdots + x_r\big(y-\sigma_r(y)\big)u_{\sigma_r}.\end{aligned}$$

Since $y-\sigma_2(y)\neq 0$, the claim is proved.

So, the skew group algebra K_tG, where $G=\mathrm{Gal}(K/k)$, is simple artinian of dimension n^2 over $k=K^G$. We claim that

$$K_tG \simeq M_n(k),$$

where $M_n(k)$ is the algebra of all $n\times n$ matrices with entries in k. This is proved as follows.

Consider $V=K$, the n-dimensional vector space over k. We define a map

$$\begin{array}{rcl}\eta : K_tG & \longrightarrow & \mathrm{End}_k(K) \quad (\simeq M_n(k))\\ xu_\sigma & \longmapsto & \eta_{xu_\sigma},\ \eta_{xu_\sigma}(y) = x\sigma(y).\end{array}$$

One checks that η is a homomorphism of rings. Since K_tG is simple, η is a monomorphism, and since the two algebras have the same dimension over k, η is an isomorphism.

Consider the particular case $(K/k)=(\mathbb{C}/\mathbb{R})$, $G=C_2=\{1,\sigma\}$. By the preceding paragraph, $\mathbb{C}_tC_2\simeq M_2(\mathbb{R})$ ($\sigma(z)=\overline{z}$ the complex conjugation). Now we introduce a 2-cocycle. By the discussion on cohomology of cyclic groups, we need to consider 2-cocycles of the form

$$f(1,1)=f(\sigma,1)=f(1,\sigma)=1,\quad f(\sigma,\sigma)=a\in\mathbb{R}^*.$$

Two 2-cocycles f,g are equivalent if they differ by a coboundary. Here, it simply says that if $g(\sigma,\sigma)=b$ and $1=g(1,1)=g(1,\sigma)=g(\sigma,1)$ then $f\sim g$ if and only if

$$ab^{-1}=z\sigma(z)\quad\text{for some}\quad z\in\mathbb{C}.$$

In other words, $a=z\overline{z}b=|z|^2b$. This means that $f\sim g$ if and only if $ab^{-1}>0$. So, in $H^2(C_2,\mathbb{C}^*)$ there are two elements, one represented by the trivial cocycle $f\equiv 1$ and another one represented by the cocycle $g(1,1)=g(1,\sigma)=g(\sigma,1)=1$, but $g(\sigma,\sigma)=-1$.

So let us check what is $\mathbb{C}_t^gC_2$. It is a simple algebra 4-dimensional over $\mathbb{R}$. We claim that $\mathbb{C}_t^gC_2\simeq\mathbb{H}$ is the quaternion algebra of dimension 4 over $\mathbb{R}$. This is a division algebra with center $\mathbb{R}$.

$$\mathbb{H}=\Big\{\mathbb{R}_1\oplus\mathbb{R}_i\oplus\mathbb{R}_j\oplus\mathbb{R}k : \quad \begin{aligned} &i^2=j^2=k^2=-1\\ &ij=k=-ji\\ &jk=i=-kj\\ &ki=j=-ik.\end{aligned}$$

The isomorphism $\mathbb{C}_t^gC_2\to\mathbb{H}$ is given by

$$\begin{array}{rcl}(a+ib)=(a+ib)u_e & \longmapsto & a+ib\\ u_\sigma & \longmapsto & j.\end{array}$$

As noted in the examples, the center of the algebra $K_t^\alpha G$, where $G=\mathrm{Gal}(K/k)$ and $\alpha\in H^2(G,K^*)$, is $k=K^G$. This is true in general.

To see this, note that after an easy manipulation with 2-cocycles one can get a normalized representative, namely a 2-cocycle f with

$$f(e,\sigma)=f(\sigma,e)=1 \quad \text{for every} \quad \sigma\in G.$$

This simply says that we may consider u_e as the identity element in $K_t^f G$. Having done so, we see immediately that the elements $xu_e,\ x\in k$ are in the center of $K_t^\alpha G$.

Let us show that ku_e is exactly the center. Take

$$p=x_1u_{\sigma_1}+x_2u_{\sigma_2}+\cdots+x_ru_{\sigma_r}\in Z(K_t^\alpha G)$$

and assume that the coefficient x_i of some $\sigma_i\neq e$ is not zero. For such σ_i there exists $y\in K$ such that $\sigma_i(y)\neq y$. So on the one hand, $py=yp$. On the other hand, the coefficients of u_{σ_i} in py and yp are $x_i\sigma_i(y)$ and x_iy, respectively. This is impossible since u_{σ_j} form a basis over K.

7. Brauer groups

Fix a field k. Consider the set $\mathscr{M}(k)$ of all finite dimensional, central simple algebras over k. By the Wedderburn theorem, such an algebra A is isomorphic to the algebra of all $n\times n$ matrices $M_n(D)$ with entries in a division algebra D and some n. The center of D is k, and D is finite dimensional over k (the center of $M_n(D)$ is the scalar matrices $k\cdot I$). Furthermore, D is determined uniquely (and hence n) up to an isomorphism of k-algebras.

The preceding remark on the uniqueness of D allows us to introduce an equivalence relation on the set of k-central simple algebras, namely $A,B\in\mathscr{M}(k)$, $A\sim B$ iff the division algebras D_A and D_B determined by the Wedderburn theorem are k-isomorphic:

$$\Big(A\simeq M_{n_1}(D_A),\ \ B\simeq M_{n_2}(D_B) \quad \text{then} \quad D_A\simeq D_B\Big).$$

The set of equivalence classes is denoted by $\mathrm{Br}(k)$.

An important reason for introducing this equivalence relation is the following: We wish to define an algebraic structure on the set of division algebras, central over k. The tensor product over k of two k-central (simple) finite dimensional division algebras is k-central simple but not necessarily a division algebra; in other words, the set of division algebras is not closed under $\otimes_k$. For example, $\mathbb{H}\otimes_{\mathbb{R}}\mathbb{H}\simeq M_4(\mathbb{R})$.

The quotient set $\mathrm{Br}(k)$ is in 1-1 correspondence with the set of finite-dimensional k-central division algebras. Furthermore, we define a multiplication on $\mathrm{Br}(k)$ making $\mathrm{Br}(k)$ an abelian group: Explicitly, for $[A],[B]\in\mathrm{Br}(k)$ (two classes represented by A and B), we let

$$[A][B]=[A\otimes_k B].$$

There are several things to check.

1. If A and B are k-central simple algebras (let us agree that the word “algebra” already implies finite dimensional) then $A\otimes_k B$ is a k-central simple algebra and hence $[A\otimes_k B]\in\mathrm{Br}(k)$.
2. This multiplication is well defined. Let $A_1\sim A_2,\ B_1\sim B_2$. Write

$$\begin{aligned} A_1&\simeq M_{r_1}(D) \qquad & B_1&\simeq M_{s_1}(\widetilde{D})\\ A_2&\simeq M_{r_2}(D) \qquad & B_2&\simeq M_{s_2}(\widetilde{D})\end{aligned}$$

Then $A_1 \otimes_k B_1 \simeq M_{r_1 s_1}(D \otimes_k \widetilde{D})$ and $A_2 \otimes_k B_2 \simeq M_{r_2 s_2}(D \otimes_k \widetilde{D})$, and if $D \otimes_k \widetilde{D} \simeq M_t(\widehat{D})$ then

$$A_1 \otimes_k B_1 \simeq M_{r_1 s_1 t}(\widehat{D}),\ A_2 \otimes_k B_2 \simeq M_{r_2 s_2 t}(\widehat{D}),$$

so the algebras are equivalent.

3. The tensor product up to an isomorphism of k-algebras is associative and commutative.
4. The identity element is represented by k or, in general, by $M_n(k)$. Clearly, $[k][A] = [k \otimes_k A] = [A]$.
5. Given a class $[A] \in \mathrm{Br}(k)$, its inverse is given by an element $[B]$ with $[A][B] = [k]$. In other words, we need an algebra B such that

$$A \otimes_k B \simeq M_n(k) \quad \text{some } \ n.$$

Hence, we wish to find B such that $A \otimes_k B \simeq \mathrm{End}_k(V)$ $(n = \dim_k V)$.

So, we are looking for an algebra B such that $A \otimes_k B$ acts on a vector space V. Such algebra is given by A^{op}. As a k-vector space $A^{op} \simeq A$ but the multiplication is reversed ($\overline{a} * \overline{b} = \overline{ba}$).

The algebra $A \otimes_k A^{op}$ acts on A by $x \otimes \overline{y}(z) = xzy$. This gives a map

$$\varphi : A \otimes_k A^{op} \longrightarrow \mathrm{End}_k(A).$$

If $\dim_k A = n^2$, then $\dim A \otimes_k A^{op} = n^4$, and also $\dim_k \mathrm{End}_k(A) = n^4$. Finally, since $A \otimes_k A^{op}$ is central simple, φ is an isomorphism.

Thus we obtain that $\mathrm{Br}(k)$ is an abelian group.

8. Some basic examples

1. If $k = \overline{k}$ is algebraically closed, then $\mathrm{Br}(k) = 0$. This follows from the fact that there are no nontrivial k-central simple division algebras over $k = \overline{k}$. Note that the field $\mathbb{C}$ is embedded in the quaternion algebra $\mathbb{H} \simeq \mathbb{C}_t^g C_2$ but is not central!

Proof. If D is a k central division algebra, let $z \in D \setminus k$. Since k is central, the algebra generated by k and z in D is commutative and therefore a field (take all inverses that already exist in D). Since $k = \overline{k}$ we have $\langle k, z \rangle = k$, that is, $z \in k$. □

2. If k is a finite field then $\mathrm{Br}(k) = 0$. If D is k-central simple over k then D is finite dimensional over a finite field and hence a finite algebra.

A theorem of Wedderburn states that there are no noncommutative finite division algebras. So $\mathrm{Br}(k) = 0$.

3. If $k = \mathbb{R}$ it is known that the $\mathbb{R}$ central division algebras are $\mathbb{R}, \mathbb{H}$. So, $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}_2$. The generator is $[\mathbb{H}]$ and $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq M_4(\mathbb{R})$, i.e., $[\mathbb{H}][\mathbb{H}] = 1 = [\mathbb{R}]$.

9. The cohomological description

Let K/k be an n-dimensional Galois extension of fields. Let $G = \mathrm{Gal}(K/k)$ be the Galois group. We can define a map (called restriction)

$$\begin{aligned} \mathrm{res} : \mathrm{Br}(k) &\longrightarrow \mathrm{Br}(K) \\ [A] &\longmapsto [A \otimes_k K]. \end{aligned}$$

A is k-central simple and so $A \otimes_k K$ has $k \otimes_k K \simeq K$ in its center. It is not difficult to prove that $k \otimes_k K$ is exactly the center of $A \otimes_k K$, and therefore $[A \otimes_k K]$ defines an element in $\mathrm{Br}(K)$.

Furthermore, the map res is a homomorphism of groups. This follows from the isomorphism

$$(A \otimes_k B) \otimes_k K \simeq (A \otimes_k K) \otimes_K (B \otimes_k K).$$

Let us denote the kernel of res by

$$\mathrm{Br}(K/k).$$

It consists of classes in $\mathrm{Br}(k)$ such that $[A \otimes_k K] = [K]$, i.e.,

$$A \otimes_k K \simeq M_r(K) \quad (r = \dim_k A \quad \text{check!})$$

We say that a k-central simple algebra is split by K if $A \otimes_k K \simeq M_r(K)$. So, $\mathrm{Br}(K/k)$ is the subgroup that consists of all elements that are represented by algebras that are split by K.

We have an exact sequence

$$0 \to \mathrm{Br}(K/k) \to \mathrm{Br}(k) \xrightarrow{\text{res}} \mathrm{Br}(K).$$

We wish to describe the subgroup $\mathrm{Br}(K/k)$ (called the K/k relative Brauer group) but before that, we exhibit some results concerning splitting fields and some consequences.

If $A \simeq M_r(D)$ is a k-central simple algebra, D a k-central division algebra, it is easy to see that a field K splits A if and only if it splits D. This follows immediately from

$$A \otimes_k K \simeq M_r(D) \otimes_k K \simeq M_r(k) \otimes_k D \otimes_k K \simeq M_r(D \otimes_k K).$$

So if K splits $M_r(D)$, then $M_r(D) \otimes_k K \simeq M_{rs}(K)$ and by the uniqueness in Wedderburn's theorem, $D \otimes_k K \simeq M_s(K)$. The converse is clear.

Let D be k-central simple and let $K \simeq \tilde{k}$, the algebraic closure of k. Since there are no nontrivial division algebras over K, we have

$$D \otimes_k K \simeq M_r(K).$$

Computing dimensions we see that

$$\dim_k D = \dim_K D \otimes_k K = r^2.$$

In other words, the dimension of a division algebra over its center is always a square. The positive square root r is called the index of D denoted by $\mathrm{ind}(D)$.

In order to find a finite dimensional splitting field for D, take a maximal field K in D. Such a field is characterized by being equal to its centralizer in D (i.e., $C_D(K) = K$). Moreover, it is not difficult to show that its dimension over k is $n = \sqrt{\dim_k D}$.

The claim is that a maximal field in D splits D. In order to show that, we show that $D \otimes_k K \simeq \mathrm{End}_K(D) \simeq M_r(K)$. Here we view D as a right linear space over K. Consider the endomorphisms

$$D_\ell = \Big\{ L_a \,|\, a \in D,\ L_a : x \longmapsto ax \ \text{ for } \ x \in D \Big\}$$
$$K_r = \Big\{ R_u \,|\, u \in K,\ R_u : x \longmapsto xu \ \text{ for } \ x \in D \Big\}.$$

D_ℓ and K_r are in $\mathrm{End}(D)$ and they commute there. Thus we have a homomorphism

$$\begin{aligned} \varphi : D\otimes_k K &\longrightarrow \mathrm{End}_K(D) \quad \text{of rings} \\ a\otimes u &\longmapsto L_a R_u. \end{aligned}$$

Since $D\otimes_k K$ is simple, this is an isomorphism (possibly not surjective). But the image of φ in $\mathrm{End}(D)$ commutes with the action of $K_e \simeq K$ and therefore

$$\varphi : D\otimes_k K \longrightarrow \mathrm{End}_K(D).$$

A computation of the dimensions of these algebras as vector spaces over K shows that they are equal. Hence φ is an isomorphism onto $\mathrm{End}_K(D) \simeq M_r(K)$.

The extension K/k may not be Galois but, if $\mathrm{char}\, k = 0$, certainly K/k is separable and we can take $L \supset K \supset k$, the Galois closure. L/k is a finite extension and splits D. This follows from the simple but important fact that if K/k splits D, then every extension L of K also splits D. Indeed,

$$D\otimes_k L \simeq D\otimes_k K\otimes_K L \simeq M_r(K)\otimes_K L \simeq M_r(L).$$

So in characteristic zero we have found a finite Galois splitting field for every division algebra D. In characteristic $p > 0$ it is not difficult to show the existence of a finite separable extension of k that splits D. For many years it was not known whether every division algebra *contains* a maximal field which is Galois. This was shown to be false by Amitsur in 1972 using generic constructions.

As mentioned above, we wish to describe the relative Brauer group $\mathrm{Br}(K/k)$ via cohomology and, more precisely, to represent the elements in $\mathrm{Br}(K/k)$ by crossed products algebras. Since every element in $\mathrm{Br}(k)$ is split by a finite Galois extension, we will conclude that every element in $\mathrm{Br}(k)$ may be represented by a crossed product algebra.

So let K/k be a finite Galois extension of dimension n and $G = \mathrm{Gal}(K/k)$ be the Galois group. We consider the skew group algebra K_tG (t denotes the Galois action).

We have shown that $K_tG \simeq M_n(k)$ which "is" the identity element in $\mathrm{Br}(k)$ (or in $\mathrm{Br}(K/k)$). For every $\alpha \in H^2(G,K^*)$ construct the crossed product algebra $K_t^\alpha G$. We know that this is a k-central simple algebra of dimension n^2 over k. We claim that K splits $K_t^\alpha G$ (note that $K_t^\alpha G$ is not necessarily a division algebra). The argument here is the same as the one used for division algebras. Note that the field $K = Ku_e$ is a maximal field in $K_t^\alpha G$. Indeed, an element outside Ku_e must have a non-trivial component $xu_\sigma,\ \sigma \neq e$ and u_σ does not commute with K. To end the proof, we use the fact that the $\{u_\sigma\}$ form a basis of $K_t^\alpha G$ over K. Thus we have defined a map

$$\begin{aligned} \eta : H^2(G,K^*) &\longrightarrow \mathrm{Br}(K/k) \subset \mathrm{Br}(k) \\ \alpha &\longmapsto [K_t^\alpha G]. \end{aligned}$$

The main claim here is that this map is an isomorphism of groups. To show that η is a homomorphism, one shows that

$$K_t^\alpha G\otimes_k K_t^\beta G \simeq K_t^{\alpha\beta} G\otimes_k K_t G.$$

Since $K_tG \simeq M_n(k)$, this implies

$$[K_t^\alpha G][K_t^\beta G] = [K_t^{\alpha\beta} G].$$

Since the algebraic closure of k contains splitting fields for all elements in $\mathrm{Br}(k)$ one can show (taking limits) that

$$H^2(G_k, k_s^*) \simeq \mathrm{Br}(k),$$

where G_k is the absolute Galois group of the field k and k_s^* is the separable closure of k.

The cohomological description has many applications as we shall see. First we show that $\mathrm{Br}(k)$ is a torsion group (i.e., every element is of finite order). Indeed, consider the composition

$$H^2(G,K^*) \xrightarrow{\text{res}} H^2(\{e\},K^*) \xrightarrow{\text{cor}} H^2(G,K^*).$$

We have shown that $\mathrm{cor} \circ \mathrm{res} = n$ but here $\mathrm{cor} \circ \mathrm{res} = 0$ since $H^2(\{e\},K^*) = 0$, so $n = |G|$ annihilates every element in $H^2(G,K^*)$. The order of $\alpha \in \mathrm{Br}(k)$ is denoted by $\exp(\alpha)$.

10. The Schur and projective Schur subgroups of the Brauer group

Let k be a field of characteristic zero, and N be a finite group. kN denotes the group algebra. By Maschke's theorem it is semisimple Artinian. Then we can write the following (using the Wedderburn theorem):

$$kN \simeq k \oplus M_{r_2}(D_2) \oplus \cdots \oplus M_{r_n}(D_n).$$

The field $k \simeq ku_e$ is embedded in the center of each simple component, i.e., we have

$$k \subset k_i = z(M_{r_i}(D_i)) \simeq z(D_i).$$

Consider only the simple components with $k = z(M_r(D))$. These components are k-central simple algebras and therefore determine elements in $\mathrm{Br}(k)$.

Definition 10.1. A k-central simple algebra $B \simeq M_r(D)$ is called a Schur algebra over k iff B is the homomorphic image of a group algebra kN for some finite group N.

As mentioned above, such algebras determine elements in $\mathrm{Br}(k)$ and we consider the subgroup of $\mathrm{Br}(k)$ generated by elements in $\mathrm{Br}(k)$ that are represented by Schur algebras. We denote this subgroup by $S(k)$ and call it the Schur group of k. We claim that $S(k)$ is not only generated but rather consists of classes represented by Schur algebras. This follows from the fact that if A and B are Schur algebras over k and if they are assumed to appear in the decomposition of kN_1 and kN_2 respectively, then $A \otimes_k B$ is a homomorphic image (i.e., appears in the decomposition) of $kN_1 \times N_2$.

Remark 10.2. The statement above on $S(k)$ holds also in positive characteristic. For $p > 0$, kN is not necessarily semisimple. There one defines a Schur algebra over k as a k-central simple algebra which is a homomorphic image of a group algebra kN.

Sometimes it is good to have an "internal" definition.

Proposition 10.3. *A k-central simple algebra B is a Schur algebra over k if and only if B^*, the group of units in B, contains a finite subgroup Γ, which spans B over k. We write $B = k(\Gamma)$. (Warning: Do not confuse $k(\Gamma)$ with the group algebra $k\Gamma$. The notation $k(\Gamma)$ simply says that $k(\Gamma)$ is spanned over k by the elements of Γ.)*

The proof is very easy. If B is a Schur algebra over k, it is the homomorphic image of kN (some finite group N). Let $\varphi : kN \to B$ be the projection onto B. Then $\varphi(N) \subset B^*$ is a finite group, and since φ is k-linear and N spans kN over k, we see that $\Gamma = \varphi(N)$ spans B

over k. For the converse, if B is k-central simple and is spanned by a finite group $\Gamma \subset B^*$, then $B = k(\Gamma)$ is the homomorphic image of the group algebra $k\Gamma$ in the obvious way.

For example, consider the algebra of quaternions over $\mathbb{R}$:

$$\mathbb{H} = \left\{\mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k\right\}.$$

We take $\Gamma = \left\{\pm 1, \pm i, \pm j, \pm k\right\}$, which is a quaternion group of order 8. Clearly, Γ spans $\mathbb{H}$ over $\mathbb{R}$, but it is certainly not a basis. There is a surjective map

$$\begin{array}{rcll} \mathbb{R}\Gamma & \longrightarrow & \mathbb{H} & \\ u_s & \longmapsto & s & \text{where} \quad s \in \{\pm 1, \pm i, \pm j, \pm k\}. \end{array}$$

Although the characterization of Schur algebras given above has some advantages, still it does not give an "explicit" way to construct them. Let us exhibit here such a construction (called cyclotomic algebra). Let $K = k(\zeta)$ be a finite cyclotomic extension (ζ is an n-th root of unity). Then, clearly, the field K is spanned over k by the finite group $\langle \zeta \rangle$. Let $G = \mathrm{Gal}(K/k)$ and form the skew group algebra $K_t G$. To form a crossed product, we must twist the multiplication by a 2-cocycle $f : G \times G \to K^*$. Instead of taking an arbitrary 2-cocycle we take a cocycle with values in the finite group $\langle \zeta \rangle$, i.e.,

$$f : G \times G \longrightarrow \langle \zeta \rangle \subset K^*.$$

The crossed product algebra $K_t^\alpha G,\ \alpha = [f]$, is called a cyclotomic algebra. By general theory, we know that $K_t^\alpha G$ is a k-central simple algebra. We wish to show that $K_t^\alpha G$ is a Schur algebra, i.e., spanned over k by a finite group of units. Indeed, let

$$1 \longrightarrow \langle \zeta \rangle \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$$

be the extension of groups defined by the Galois action of G on K (and hence on $\langle \zeta \rangle$) and by the given 2-cocycle $f : G \times G \to \langle \zeta \rangle$. Since $\langle \zeta \rangle$ and G are finite, the extension Γ is also finite and we claim that it spans $K_t^\alpha G$ over k. Since Γ contains $\langle \zeta \rangle$, it spans K. Further, the elements $u_\sigma,\ \sigma \in G$ in Γ span $K_t^\alpha G$ over K proving the claim. We view cyclotomic algebras as a "natural" construction of Schur algebras.

Theorem 10.4 (Brauer–Witt)**.** *Every element in the Schur group of k is represented by a cyclotomic algebra. (In other words, every Schur algebra is equivalent to a cyclotomic algebra.)*

The Schur group of a field k has been computed in some cases. For fields of positive characteristic $S(k) = 0$. Here is the idea of the proof:

If $k(\Gamma) \simeq M_r(D)$ is a Schur algebra, Γ is finite, one shows that $k(\Gamma)$ is of the form

$$k(\Gamma) = k \otimes_{k_0} k_0(\Gamma),$$

where $k_0(\Gamma)$ is k_0-central simple algebra, and k_0 is a finite extension of the prime field in k. Consequently, k_0 is finite and we know that $\mathrm{Br}(k_0) = 0$. So $k_0(\Gamma)$ is a matrix algebra $M_r(k_0)$, and therefore $k(\Gamma) \simeq M_r(k)$.

For a local field, $S(k)$ is rather small. It turns out to be finite (cyclic) where $\mathrm{Br}(k) \simeq Q/\mathbb{Z}$.

We wish now to study the projective analog of the Schur group. The group $S(k)$ is related to representations exactly as $PS(k)$, the projective Schur group, is related to projective representations of finite groups. Let kN be a group algebra as above. Let $\alpha \in H^2(N, k^*)$,

k^* a trivial N module, and let $f : N \times N \to k^*$ be a 2-cocycle representing α. We can form the twisted group algebra $k^\alpha N$ (recall the multiplication $xu_\sigma yu_\tau = xyf(\sigma,\tau)u_{\sigma\tau}$).

Let us explain how "projectivity" comes into the game. It is well known that a representation of the group N over the field k is a k-vector space V with a homomorphism of groups

$$N \longrightarrow GL_k(V).$$

This is equivalent to saying that V is a kN module. A projective representation of N is a vector space V over k and a map (not necessarily homomorphism)

$$\varphi : N \longrightarrow GL_k(V)$$

such that its composition $\nu \cdot \varphi$ with the natural homomorphism

$$\nu : GL(V) \longrightarrow PGL(V) \simeq GL(V)\big/k^*$$

is a homomorphism of groups. It is not difficult to see that this is equivalent to saying that V is a module over a twisted group algebra $k^\alpha N,\ \alpha \in H^2(N,k^*)$.

Let us build $\alpha \in H^2(N,k^*)$ for a given projective representation

$$\eta : N \longrightarrow PGL(V).$$

For every $\sigma \in N$, choose a representative $u_\sigma \in GL(V)$ of $\eta(\sigma) \in PGL(V)$. Since $\eta(\sigma)\eta(\tau)$ $= \eta(\sigma\tau)$ in $PGL(V)$, the elements $u_\sigma u_\tau$ and $u_{\sigma\tau}$ differ by an element in k^*:

$$u_\sigma u_\tau = f(\sigma,\tau)u_{\sigma\tau}.$$

It is easily checked that $f : N \times N \to k^*$ is a 2-cocycle and that V is a $k^\alpha N$ module where $\alpha = [f]$. Having a twisted group algebra $k^\alpha N$ we wish to define projective Schur algebras and the projective Schur group. This generalization was introduced by Lorenz and Opolka in 1976. As we shall see, the construction is much richer and many "natural" classes in $\mathrm{Br}(k)$ belong to the projective Schur group. Here are the definitions and some basic statements:

The twisted group algebra $k^\alpha N$ is semisimple (we are assuming that $\mathrm{char}(k) = 0$, and by Maschke's theorem, $k^\alpha N$ is semisimple) and so it decomposes into a direct sum of simple algebras. Again,

$$k^\alpha N \simeq M_{r_1}(D_1) \oplus M_{r_2}(D_2) \oplus \cdots \oplus M_{r_s}(D_s).$$

(Note that the trivial representation k is not necessarily a module over $k^\alpha N$. In fact, k is a $k^\alpha N$ module if and only if $\alpha = 0$ in $H^2(N,k^*)$.)

Again we choose the simple algebras $M_r(D)$ (in such decomposition) with center k. In general, k is contained in $k_i = Z(M_{r_i}(D_i))$. Thus we define a projective Schur algebra over k to be a k-central simple algebra which appears in the decomposition of a twisted group algebra $k^\alpha N$ for some finite group N and some $\alpha \in H^2(N,k^*)$.

The projective Schur group of k is the subgroup of $\mathrm{Br}(k)$ generated by (and again consisting of) the element in $\mathrm{Br}(k)$ that may be represented by projective Schur algebras. We denote this subgroup by $PS(k)$. We clearly have

$$S(k) \subset PS(k) \subset \mathrm{Br}(k).$$

As Schur algebras, also projective Schur algebras have an "internal" characterization. We claim that a k-central simple algebra B is a projective Schur algebra if and only if it is spanned over k by a group $\Gamma \subset B^*$ that is *finite modulo* k^*.

Let us show this. In $k^\alpha N$, consider the group of "trivial" units. It consists of the monomial elements

$$k^{*\alpha}N = \{xu_\sigma \in k^\alpha N\}.$$

This is a subgroup of $(k^\alpha N)^*$ and clearly it spans $k^\alpha N$ over k (in fact, even over $\mathbb{Z}$).

Now if B is a homomorphic image of $k^\alpha N$ (i.e., appears in the decomposition of $k^\alpha N$ into simples) under $\varphi : k^\alpha N \to M_r(D)$, the image $\Gamma = \varphi(k^{*\alpha}N) \subset B^*$ spans B over k, and Γ is finite modulo k^* (because $k^{*\alpha}N$ is finite modulo k^*). Conversely, if $B \simeq k(\Gamma)$, where Γ is finite modulo k^*, we consider the central extension

$$1 \longrightarrow k^* \longrightarrow \Gamma \longrightarrow \Gamma/k^* \simeq H \longrightarrow 1$$

(H finite). This extension determines an element β in $H^2(H,k^*)$ and one checks that B is the homomorphic image of $k^\beta H$ under the obvious map

$$\begin{array}{ccc} k^\alpha H & \longrightarrow & B \\ u_\sigma & \longmapsto & u_\sigma. \end{array}$$

The projective Schur group of a field k is much bigger than the Schur group. We will show that in two important cases it coincides with the full Brauer group. Let k be a number field that is a finite extension of Q (rationals). It follows from class field theory that every k-central simple algebra is split by a cyclic extension L of k which is contained in a cyclotomic extension of k (L/k is cyclic if it is Galois, and $\mathrm{Gal}(L/k)$ is cyclic).

So we have $k \subset L \subset F,\ F = k(\xi)$, where ξ is an r-th root of unity. Let $S = \mathrm{Gal}(F/k)$, $G = \mathrm{Gal}(L/k)$. Take $[B] \in \mathrm{Br}(k)$. We are to show that $[B] \in PS(k)$. Suppose first that the algebra B has a splitting field L that is a cyclic cyclotomic extension of k (rather than cyclic contained in a cyclotomic extension F of k). From Section 9 we know that $[B] \in \mathrm{Br}(L/k)$ and so $[B]$ is represented by a crossed product $L_t^\alpha G,\ G = \mathrm{Gal}(L/k),\ \alpha \in H^2(G,L^*)$. L is a cyclotomic extension of k, so spanned by a finite extension over k. By assumption, $G = \langle\sigma\rangle$ is cyclic, so we can find a representative

$$f(\sigma^i,\sigma^j) = \begin{cases} a \in k^* & i+j \geq \mathrm{ord}(G) \\ 1 & i+j < \mathrm{ord}(G). \end{cases}$$

Since f has value in k^* it defines an extension Γ

$$1 \longrightarrow k^* \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$$

which is clearly finite modulo k^*. Furthermore, the group Γ is contained in $L_t^\alpha G$ and spans $L_t^\alpha G$ over L. So the group generated by Γ and $\langle\zeta\rangle$ is finite modulo k^* (Γ normalizes $\langle\zeta\rangle$) and spans $L_t^\alpha G$ over k. So we have found a spanning group Γ over k such that $|\Gamma/k^*| < \infty$. This shows that $[L_t^\alpha G] \in PS(k)$.

Now drop the assumption that L is cyclotomic (L is cyclic contained in F, F/k is cyclotomic). Our algebra B is split by L and, since $F \supset L$, is split also by F.

So B is similar to a crossed product $L_t^\alpha G,\ G$ cyclic. Thus we can choose a representative f of α with values in k^*. So the group Γ defined by $\alpha \in H^2(G,k^*)$,

$$1 \longrightarrow k^* \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$$

is finite modulo k^* and spans $L_t^\alpha G$ over L. We *cannot* say as before that L is spanned over k by a group that is finite modulo k^*.

By the Galois theory, $G = \mathrm{Gal}(L/k)$ is a quotient group of $S = \mathrm{Gal}(F/k),\ S/H \simeq G$, where $H = \mathrm{Gal}(F/L)$.

Recall the inflation map in cohomology

$$\begin{aligned} \inf : H^2\big(S/H, (F^*)^H\big) &\longrightarrow H^2(S,F^*) \\ \inf : H^2(G,L^*) &\longrightarrow H^2(S,F^*) \\ \alpha &\longmapsto \inf(\alpha) \end{aligned}$$

and if α is represented by g, we represent $\inf(\alpha)$ by $\inf(g)$, where $\inf(g)(\sigma,\tau) = g(\bar{\sigma},\bar{\tau})$ with $\bar{\sigma},\bar{\tau}$ in G. In particular, $\inf(\alpha)$ may be represented by a 2-cocycle which obtains exactly the same values as a chosen representative of α. G is cyclic, so choose a 2-cocycle g representing α with values in k^*. Represent $\inf(\alpha)$ by the corresponding 2-cocycle, i.e., also with values in k^*. Form the crossed product

$$F_t^{\inf(\alpha)}S.$$

Since the values of a representing 2-cocycle are in $k = F^S$ and F is a cyclotomic extension, it is clear that $\big[F_t^{\inf(\alpha)}S\big] \in PS(k)$. It remains to show that

$$[L_t^\alpha G] = \big[F_t^{\inf(\alpha)}S\big].$$

We define a map

$$\begin{aligned} \eta : F_t^{\inf(\alpha)}S &\longrightarrow M_q(k) \otimes_k L_t^\alpha G \simeq M_q(L_t^\alpha G) \\ &\simeq \mathrm{End}_{L_t^\alpha G}\big((L_t^\alpha G)^q\big), \end{aligned}$$

where $q = \mathrm{ord}(\mathrm{Gal}(F/L))$.

To this end, define an action of $F_t^{\inf(\alpha)}S$ on $F \otimes_L L_t^\alpha G$. (Note that $F \otimes_L L_t^\alpha G \simeq (L_t^\alpha G)^q$ as a right $L_t^\alpha G$ module.) For $xu_\sigma \in F_t^{\inf(\alpha)}S$ and $s \otimes \omega \in F \otimes_L L_t^\alpha G$ we define $xu_\sigma(s \otimes \omega) = x\sigma(s) \otimes u_{\bar{\sigma}}\omega$. This action commutes with the right action of $L_t^\alpha G$ and therefore defines a map of k-algebra

$$\eta : F_t^{\inf(\alpha)}S \longrightarrow \mathrm{End}_{L_t^\alpha G}\big((L_t^\alpha G)^q\big).$$

Since $F_t^{\inf(\alpha)}S$ is simple and the dimensions coincide, η must be an isomorphism. This completes the proof $PS(k) = \mathrm{Br}(k)$ for number fields.

Number fields (finite extensions of Q) contain only a finite number of roots of unity. We would like to show now that if k contains "enough" roots of unity, then again $PS(k) = \mathrm{Br}(k)$.

Theorem 10.5. *If k is a field that contains all roots of unity, then $PS(k) = \mathrm{Br}(k)$.*

Example 10.6. The field $\mathbb{C}$ contains all roots of unity but $\mathbb{C}$ is algebraically closed and therefore $\mathrm{Br}(\mathbb{C}) = PS(\mathbb{C}) = 0$.

The Brauer group of $\mathbb{C}(x)$ (rational function field on one indeterminate) is also trivial. But for $k = \mathbb{C}(x_1, x_2, \ldots, x_n),\ n \geq 2$, $\mathrm{Br}(k) \neq 0$, and by the theorem, $\mathrm{Br}(k) = PS(k)$.

In order to explain this result, we need some preparation.

11. SYMBOL ALGEBRAS

Let k be a field and assume that it contains a primitive n-th root of unity ω. For given elements $a,b \in k$ we define the symbol algebra (a,b) (or $(a,b)_n$) as follows. It is generated over k by x,y subject to the relations

$$x^n = a,\ y^n = b,\ yx = \omega xy.$$

It is clear that the elements $\{x^i y^i\}_{i,j=0}^{n-1}$ span $(a,b)_n$ over k and, in fact, form a base over k. By a shortest length argument one can show that $(a,b)_n$ is k-central simple.

The theory of symbols is of great importance in Brauer groups. On the one hand, their structure is well understood, and on the other hand, they may be regarded as the "building block" of the theory of Brauer groups. More precisely, Merkurjev and Suslin proved a very deep theorem which says:

Theorem 11.1. *Assume that k contains a primitive n-th root of unity. Then every element in* $\mathrm{Br}(k)$ *of exponent dividing n is (Brauer) similar to the tensor product (over k) of symbol algebras.*

In other words, if "enough" roots of unity are present in k the symbol algebras generate the Brauer group. More precisely (using this terminology), if μ_n, the n-th roots of unity, are contained in k, then $\mathrm{Br}(k)_n$, the subgroup of $\mathrm{Br}(k)$ which consists of classes annihilated by n, is generated by symbols. Recall that $\mathrm{Br}(k)$ is a torsion group, so if all roots of unity are contained in k, then $\mathrm{Br}(k)$ is generated by symbols (or rather by classes represented by symbols).

But now, from the structure of symbols, it is easy to see that a symbol algebra is a projective Schur algebra. Indeed, it is spanned by the group of units generated by x and y and modulo k^* is isomorphic to $\mathbb{Z}_n \times \mathbb{Z}_n$ $\left(x^n = a \in k^*,\ y^n = b \in k^*,\ yx = \omega xy,\ \omega \in k^*\right)$.

We conclude that if k contains all roots of unity, then $PS(k) = \mathrm{Br}(k)$.

If k contains μ_n, then $PS(k)_n = \mathrm{Br}(k)_n$. Thus we see in two different examples that $PS(k) = \mathrm{Br}(k)$. It was conjectured by Nelis and Van Oystaeyen that $PS(k) = \mathrm{Br}(k)$ for arbitrary fields. The purpose of this last part is to disprove this conjecture by analyzing the Brauer group of rational function fields on the one hand, and on the other hand by analyzing the structure of projective Schur algebras. It was shown by Aljadeff & Sonn (see ([AS1]) that every projective Schur algebra has an abelian splitting field, i.e., given a projective Schur algebra $A = k(\Gamma)$ over k, there exists a field extension K with $G = \mathrm{Gal}(K/k)$ abelian such that K splits A $\left(K \otimes_k A \simeq M_r(K)\right)$.

However, this result is not sufficient to show that $PS(k) \neq \mathrm{Br}(k)$ because it is a long standing open problem whether every element in $\mathrm{Br}(k)$ has an abelian splitting field. A year later this result was strengthened (by Aljadeff & Sonn) to the

Theorem 11.2. ([AS2]) *Every element in $PS(k)$ has an abelian splitting field which is contained in a radical extension of k. (L/k is radical if L is obtained from k by adding roots of elements of k, $L = k(z_1, z_2, \ldots, z_r)$, $z_i^{n_i} = a_i \in k^*$.)*

This stronger result implies that $PS(k) \neq \mathrm{Br}(k)$. This follows from the third

Theorem 11.3 (Aljadeff & Sonn)**.** ([AS2]) *If k is a number field and $k(x)$ denotes the rational function field in one indeterminate, then* $\mathrm{Br}(k(x))$ *contains elements which are not* *split by any abelian extension, that is contained in a radical extension of k. In particular,* $PS(k(x)) \neq \mathrm{Br}(k(x))$.

REFERENCES

[AS1] E. Aljadeff and J. Sonn, Projective Schur algebras have abelian splitting fields, *J. Algebra* **175** (1995), 179–187.

[AS2] E. Aljadeff and J. Sonn, On the projective Schur group of a field, *J. Algebra* **178** (1995), 530–540.

DEPARTMENT OF MATHEMATICS, TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA 32000, ISRAEL

E-mail: aljadeff@techunix.technion.ac.il