Remark: For any prime p the cohomology groups of the elementary abelian group E_{p^m} with coefficients in the finite field $\mathbb{F}_p$ may be determined by relating them to the cohomology groups of the factors in the direct product as mentioned at the end of Section 2. In general, $H^2(E_{p^m}, \mathbb{F}_p)$ is a vector space over $\mathbb{F}_p$ of dimension $\frac{1}{2}m(m+1)$. When $p = 2$ and $m = 2$ this is the result $H^2(Z_2 \times Z_2, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^3$ above.

Crossed Product Algebras and the Brauer Group

Suppose F is a field. Recall that an F-algebra B is a ring containing the field F in its center and the identity of B is the identity of F, cf. Section 10.1.

Definition. An F-algebra A is said to be *simple* if A contains no nontrivial proper (two sided) ideals. A *central simple F-algebra* A is a simple F-algebra whose center is F.

Among the easiest central simple F-algebras are the matrix algebras $M_n(F)$ of $n \times n$ matrices with coefficients in F.

If K/F is a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(K/F)$, then we can use the normalized 2-cocycles in $Z^2(G, K^\times)$ to construct certain central simple K-algebras. The construction of these algebras from 2-cocycles and their classification in terms of $H^2(G, K^\times)$ (cf. Theorem 42 below) are important applications of cohomological methods in number theory. Their construction in the case when G is cyclic was one of the precursors leading to the development of abstract cohomology.

Suppose $f = \{a_{\sigma,\tau}\}_{\sigma,\tau \in G}$ is a normalized 2-cocycle in $Z^2(G, K^\times)$. Let B_f be the vector space over L having basis u_σ for $\sigma \in G$:

$$B_f = \left\{ \sum_{\sigma \in G} \alpha_\sigma \, u_\sigma \mid \alpha_\sigma \in K \right\}. \tag{17.39}$$

Define a multiplication on B_f by

$$u_\sigma \, \alpha = \sigma(\alpha) \, u_\sigma \qquad u_\sigma \, u_\tau = a_{\sigma,\tau} \, u_{\sigma\tau} \tag{17.40}$$

for $\alpha \in L$ and $\sigma, \tau \in G$. The second equation shows that the $a_{\sigma,\tau}$ give a "factor set" for the elements u_σ in B_f and is one reason this terminology is used. Using this multiplication we find

$$(u_\sigma u_\tau) u_\rho = a_{\sigma,\tau} a_{\sigma\tau,\rho} u_{\sigma\tau\rho} \qquad \text{and} \qquad u_\sigma \, (u_\tau \, u_\rho) = \sigma(a_{\tau,\rho}) \, a_{\sigma.\tau\rho} \, u_{\sigma\tau\rho}.$$

Since $a_{\sigma,\tau} \, a_{\sigma\tau,\rho} = \sigma(a_{\tau,\rho}) \, a_{\sigma,\tau\rho}$ is the multiplicative form of the cocycle condition (26), it follows that the multiplication defined in (40) is associative.

Since the cocycle is normalized we have $a_{1.\sigma} = a_{\sigma,1} = 1$ for all $\sigma \in G$ and it follows from (40) that the element u_1 is an identity in B_f. Identifying K with the elements αu_1 in B_f, we see that B_f is an F-algebra containing the field K and having dimension n^2 over F if $n = [K : F] = |G|$.

Proposition 40. The F-algebra B_f with K-vector space basis u_σ in (39) and multiplication defined by (40) is a central simple F-algebra.

Proof: It remains to show that the center of B_f is F and that B_f contains no nonzero proper ideals. Suppose $x = \sum_{\sigma \in G} \alpha_\sigma u_\sigma$ is an element in the center of B_f. Then $x\beta = \beta x$ for $\beta \in K$ shows that $\sigma(\beta) = \beta$ if $\alpha_\sigma \neq 0$. Since there is an element $\beta \in K$ not fixed by σ for any $\sigma \neq 1$, this shows that $a_\sigma = 0$ for all $\sigma \neq 1$, so $x = \alpha_1 u_1$. Then $x u_\tau = u_\tau x$ if and only if $\tau(\alpha_1) = \alpha_1$, so if this is true for all τ then we must have $\alpha_1 = a \in K$. Hence $x = a u_1$ and the center of B_f is F.

To show that B_f is simple, suppose I is a nonzero ideal in B_f and let

$$x = \alpha_{\sigma_1} u_{\sigma_1} + \cdots + \alpha_{\sigma_m} u_{\sigma_m}$$

be a nonzero element of I with the minimal number m of nonzero terms. If $m > 1$ there is an element $\beta \in K^\times$ with $\sigma_m(\beta) \neq \sigma_{m-1}(\beta)$. Then the element $x - \sigma_m(\beta)\, x\, \beta^{-1}$ would be an element of the ideal I with the nonzero element $(1 - \sigma_m(\beta)\, \sigma_{m-1}(\beta)^{-1})\, \alpha_{\sigma_{m-1}}$ as coefficient of $u_{\sigma_{m-1}}$, and would have fewer nonzero terms than x since the coefficient of u_{σ_m} is 0. It follows that $m = 1$ and $x = \alpha\, u_\sigma$ for some $\alpha \in K$ and some σ. This element is a unit, with inverse $\sigma^{-1}(\alpha^{-1})\, u_{\sigma^{-1}}$, so $I = B_f$, completing the proof.

Definition. The central simple F-algebra B_f defined by (39) and (40) is called the *crossed product algebra* for the factor set $\{a_{\sigma,\tau}\}$.

If $f' = a'_{\sigma,\tau}$ is a normalized cocycle in the same cohomology class in $H^2(G, K^\times)$ as $a_{\sigma,\tau}$ then there are elements $b_\sigma \in K^\times$ with

$$a'_{\sigma,\tau} = a_{\sigma,\tau}(\sigma(b_\tau) b_{\sigma\tau}^{-1} b_\sigma)$$

(the multiplicative form of the coboundary condition (27)). If $B_{f'}$ is the F-algebra with K-basis v_σ defined from this cocycle as in (39) and (40), then the K-vector space homomorphism φ defined by mapping u'_σ to $b_\sigma u_\sigma$ satisfies

$$\begin{aligned}\varphi(u'_\sigma u'_\tau) &= \varphi(a'_{\sigma,\tau} u'_{\sigma\tau}) = a'_{\sigma,\tau} b_{\sigma\tau}\, u_{\sigma\tau} = b_\sigma\, \sigma(b_\tau)\, u_\sigma u_\tau \\ &= (b_\sigma u_\sigma)(b_\tau u_\tau) = \varphi(u'_\sigma)\varphi(u'_\tau).\end{aligned}$$

It follows that φ is an F-algebra isomorphism from $B_{f'}$ to B_f.

We have shown that every cohomology class c in $H^2(G, K^\times)$ defines an isomorphism class of central simple F-algebras, namely the isomorphism class of any crossed product algebra for a normalized cocycle $\{a_{\sigma,\tau}\}$ representing the class c. The next result shows that the trivial cohomology class corresponds to the isomorphism class containing $M_n(F)$.

Proposition 41. The crossed product algebra for the trivial cohomology class in $H^2(G, K^\times)$ is isomorphic to the matrix algebra $M_n(F)$ where $n = [K : F]$.

Proof: If $\alpha \in K$ then multiplication by α defines a linear transformation T_α of K viewed as an n-dimensional vector space over F. Similarly, every automorphism $\sigma \in G$ defines an F-linear transformation T_σ of K, and we may view both T_α and T_σ as elements of $M_n(F)$ by choosing a basis for K over F. If B_0 denotes the crossed product algebra for the trivial factor set ($a_{\sigma,\tau} = 1$ for all $\sigma, \tau \in G$), consider the additive map $\varphi : B_0 \to M_n(F)$ defined by $\varphi(\alpha u_\sigma) = T_\alpha T_\sigma$. Since $T_{a\alpha} = aT_\alpha$ for $a \in F$, the map φ is an F-vector space homomorphism. If $x \in K$, we have

$$T_\sigma T_\alpha(x) = T_\sigma(\alpha x) = \sigma(\alpha x) = \sigma(\alpha)\sigma(x) = T_{\sigma(\alpha)}T_\sigma,$$

so $T_\sigma T_\alpha = T_{\sigma(\alpha)}T_\sigma$ as linear transformations on K. It then follows from $u_\sigma u_\tau = u_{\sigma\tau}$ that

$$\begin{aligned}\varphi((\alpha u_\sigma)(\beta u_\tau)) &= \varphi(\alpha\sigma(\beta)\, u_{\sigma\tau}) = T_{\alpha\sigma(\beta)}T_{\sigma\tau} = T_\alpha T_{\sigma(\beta)}T_\sigma T_\tau \\ &= T_\alpha T_\sigma T_\beta T_\tau = \varphi(\alpha u_\sigma)\,\varphi(\beta u_\tau)\end{aligned}$$

which shows that φ is an F-algebra homomorphism from B_0 to $M_n(F)$. Since $\ker\varphi$ is an ideal in B_0 and $\varphi \neq 0$, it follows from Proposition 40 that $\ker\varphi = 0$ and φ is an injection. Since both B_0 and $M_n(F)$ have dimension n^2 as vector spaces over F, it follows that φ is an F-algebra isomorphism, proving the proposition.

Example

If $K = \mathbb{C}$ and $F = \mathbb{R}$, then $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is of order 2 and generated by complex conjugation τ. We have $|H^2(G, \mathbb{C}^\times)| = 2$. The central simple $\mathbb{R}$-algebra B_0 corresponding to the trivial class is $\mathbb{C}u_1 \oplus \mathbb{C}u_\tau$ with $u_\tau(a + bi) = (a - bi)u_\tau$ and $u_\tau^2 = u_1$. This is isomorphic to the matrix algebra $M_2(\mathbb{R})$ under the map

$$\varphi((a + bi)u_1 + (c + di)u_\tau) = aI + bT_i + cT_\tau + dT_iT_\tau = \begin{pmatrix} a+c & -b+d \\ b+d & a-c \end{pmatrix}.$$

A normalized cocycle f representing the nontrivial cohomology class is defined by the values $a_{1,1} = a_{1,\tau} = a_{\tau,1} = 1$ and $a_{\tau,\tau} = -1$. The corresponding central simple $\mathbb{R}$-algebra B_f is given by $\mathbb{C}v_1 \oplus \mathbb{C}v_\tau$. The element v_1 is the identity of B_f, and we have the relations $v_\tau(a + bi) = (a - bi)v_\tau$ and $v_\tau^2 = -v_1$. Letting $v_1 = 1$ and $v_\tau = j$ we see that B_f is isomorphic as an $\mathbb{R}$-algebra to the real Hamilton Quaternions $\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$.

There is a rich theory of simple algebras and we mention without proof the following results. Let A be a central simple F-algebra of finite dimension over F.

I. If $F \subseteq B \subseteq A$ where B is a simple F-algebra define the *centralizer* B^c of B in A to be the elements of A that commute with all the elements of B. Define the *opposite algebra* B^{opp} to be the set B with opposite multiplication, i.e., the product b_1b_2 in B^{opp} is given by the product b_2b_1 in B. Both B^c and B^{opp} are simple F-algebras and we have
- **a.** $(\dim_F B)(\dim_F B^c) = \dim_F A$
- **b.** $A \otimes_F B^{opp} \cong M_r(B^c)$ as F-algebras, where $r = \dim_F B$
- **c.** $B \otimes_F B^c \cong A$ if B is a central simple F-algebra.

II. If A' is an Artinian (satisfies D.C.C. on left ideals) simple F-algebra, then $A \otimes_F A'$ is an Artinian simple F-algebra with center $(A')^c$.

III. We have $A \cong M_r(\Delta)$ for some division ring Δ whose center is F and some integer $r \geq 1$. The division ring Δ and r are uniquely determined by A. The same statement holds for any Artinian simple F-algebra.

The last result is part of Wedderburn's Theorem described in greater detail in the following chapter.