Central Simple Algebras

Uzi Vishne

Department of Mathematics

Ph.D. Thesis

Submitted to the Senate of Bar-Ilan University

Ramat-Gan, Israel Jul. 2000

This work was carried under the supervision of Prof. Louis H. Rowen (Department of Mathematics), Bar-Ilan University.

Dedicated to my wife Tali,
and to Gal, Ariel, Hadar and Rotem,
who didn't help much with the mathematics,
but are invaluable in any other aspect.

I deeply thank Professor L. Rowen for being a truly great teacher.
His support and guidance go way beyond the scope of this work.

Contents

Preface

Pick a finite dimensional algebra over a field F. Compute its (Jacobson) radical, and factor it out. What you get is a direct sum of ideals, each one a simple algebra. Each of these components is a full matrix ring over a division algebra, finite dimensional over F.

Finite dimensional division algebras are the building blocks of ring theory. Make a list of all the possible division rings, learn how to lift properties back from the semiprimitive case to the general case, and you can study Artinian rings in general.

Emerging from the general structure theory of rings, the study of division algebras started from isolated constructions (like that of the cyclic algebras by Dickson), and expanded during the thirties and forties to results like the structure theory of p-algebras, the description of division algebras of low degree (both by A. Albert), the connection to cohomology (E. Noether), and the Albert-Brauer-Hasse-Noether theorem, which had great influence on the development of field arithmetic.

The vivid activity nowadays studies division algebras in their own right, counting on the machinery of generic matrices, the connections to K-theory or field arithmetic, homology or algebraic geometry. There is a counter play between division algebras and many current branches of mathematics, such as involutions and quadratic forms, Galois theory, local fields, Azumaya algebras, field arithmetic and number theory, and many others.

If A is a simple algebra with center F, then F is a field, and we say that A is central over F. Let K/F be a field extension, then $A \otimes_F K$ is central simple over K.

Suppose A/F is finite, then we have the equality of dimensions $[A \otimes_F K : K] = [K : F]$. By Wedderburn's structure theorem, $A = M_m(D)$ where D is a central division algebra over F. Let $K = \overline{F}$, the algebraic closure of F. Since there are no non-trivial finite dimensional division algebras over $\overline{F}$, $A \otimes_F \overline{F}$ is a matrix algebra over $\overline{F}$, say $A \otimes_F \overline{F} = M_n(\overline{F})$. It follows that the dimension $[A : F] = [A \otimes_F \overline{F} : \overline{F}] = n^2$. The **degree** of A is defined by $\deg(A) = \sqrt{[A : F]}$. The **index** of A is the degree of the underlying division algebra, $\mathrm{ind}(A) = \deg(D)$.

The best way to hold all the information on finite central simple algebras over F in one object is by means of the the Brauer group. Identify two algebras if they have the same underlying division algebra, and define multiplication by $[A][B] = [A \otimes_F B]$. The Brauer group $\mathrm{Br}(F)$ is the set of all classes $[A]$ for A finite-dimensional central simple over F. Inversion of elements is by $[A]^{-1} = [A^{op}]$ (where A^{op} is the algebra with the same additive structure and reversed multiplication; then $A \otimes A^{op} = M_{[A:F]}(F)$). Moreover, by means of the so-called Brauer factor sets it can be shown that $A^{\otimes_F \mathrm{ind}(A)}$ is a matrix algebra, so that $\mathrm{Br}(F)$ is a torsion group.

Suppose A is a division algebra. If $B \subseteq A$ in an F-subalgebra, then $C_A(C_A(B)) = B$, and $[B:F] \cdot [C_A(B):F] = [A:F]$. As a result, the dimension of every subfield of A/F is bounded by the degree of A. Every subfield of A/F is contained in a maximal subfield, which has dimension $\deg(A)$ over F. L/F of dimension n splits A (i.e. $A \otimes L$ is matrices over L) iff L is a maximal subfield in an algebra B, similar to A in the Brauer group, with $\deg(B) = n$ [**1**, p. 60].

A is called a p-algebra if the underlying base field is of characteristic p, and the dimension of A over its center is a power of p. The basic structure theorems of p-algebras were discovered around 1940, mostly by Albert [**1**] and Jacobson, whereas in the harder case of prime-to-p degree the progress was much slower. The breakthrough came around 1980, with theorems of Amitsur (the construction of noncrossed products) and Merkurjev-Suslin (connecting the Brauer group to algebraic K-theory), with the use of geometric methods that was possible mainly in characteristic 0. While there was a lot of activity in the theory of Azumaya algebras over commutative rings in characteristic p (e.g. Saltman's thesis [**36**] or [**18**]), certain aspects in the study of the p-part of the Brauer group itself seem to have been left behind.

Undoubtedly, the main method in the study of central simple algebras is by means of their subfields.

Our contribution in this work is in several directions. The main subject in Chapter 1 is the p-part of the Brauer group of fields with characteristic p. We begin with field extensions of p-power dimension in characteristic p, starting from well-known facts, and going deeper into classifying and counting composite extensions, thus producing a new proof for Witt's theorem that the p-part of the absolute Galois group of F is a free pro-p group, for the finitely generated case. We then discuss standard couples of generators of cyclic algebras of degree p, and give a description by generators and relations for the exponent-p part of the Brauer group. In Section 4 we study various presentations

of a given cyclic algebra of degree p, and show that an isomorphism of two cyclic p-algebras of degree p becomes tame (in the sense defined there) if we tensor by $M_p(F)^{\otimes 2(p-2)}$. In Section 5 we show that if K/F is a finite separable extension, then the p-part of the Brauer group of K is generated by the classes of symbol algebras of the form $[a, \beta)$, where $a \in K$ and $\beta \in F$. Moreover, $[K:F] + 1$ symbols of this form are enough to express any symbol algebra of degree p over K. In the sixth section we study Hilbert's theorem 90 in a general context, and develop some elementary tools which apply to any Abelian group of exponent p equipped with an action of a cyclic group. Given any cyclic extension K/F, with arbitrary characteristic, these tools enable us to suggest two interesting filtrations of subgroups of ${}_p\mathrm{Br}(K)$, and study their connections. Special attention is given to the case $\mathrm{char}F = p$. We show that under very mild assumption, Hilbert's theorem 90 fails for ${}_p\mathrm{Br}(K)$. In Subsection 6.5 we study the invariant subgroup of ${}_p\mathrm{Br}(K)$, and discuss some generic examples. Some easy results on corestriction of cyclic algebras down odd dimension extensions are given in the last subsection, and used to give a counterexample to Hilbert's theorem 90 for groups of the form ${}_n\mathrm{Br}(K)$.

In Chapter 2 we closely study a class of cyclic algebras, suggested by Brauer as examples with arbitrary degree and exponent. We give a precise formulation for the technique of passing to the leading monomial, and discuss some suggested construction of a noncrossed product of exponent p (a problem which is still open).

The last Chapter discusses algebras with involution. We study the presentations of involutions in crossed products, and show that given enough roots of unity, a dihedral crossed product with involution has an Abelian maximal subfield.

CHAPTER 1

p-Algebras

Central simple algebras of degree a power of p over a field of characteristic p, are called **p-algebras**.

The theory of (finite-dimensional) central simple algebras naturally split into two parts. While the basic structure theory of p-algebras was derived, mainly by Albert, back in the 40s, the theory of algebras with prime to p index still contains some very difficult open questions. On the other hand, some deep theorems from the 80s, most notably the Merkurjev-Suslin theorem, hold only for characteristic not dividing the index (and in the presence of enough roots of unity).

The main theme of this chapter is to introduce some of the recent results on prime-to-p index to the theory of p-algebras.

In the first section we describe the well-known Galois theory in characteristic p, and continue to study composite extensions, with results on the number of subgroups of various types of the absolute Galois group. The construction and basic properties of p-algebras of degree p are given in section 2.

In the third section we give a presentation of ${}_p\mathrm{Br}(F)$ by generators (p-symbols) and relations. In the fourth section we define tame isomorphisms between cyclic p-algebras of degree p, following similar ideas from the theory of the automorphism groups of polynomial rings. This is generalized to tensor product of cyclics of degree p, and the main question is, given $[a,b)\cong[a',b')$, what is the minimal m such that $[a,b)\otimes M_p(F)^{\otimes m}\cong[a',b')\otimes M_p(F)^{\otimes m}$ is tame. We show that the $m\leq 2(p-2)$ is always enough. Some special results for the case $p=2$ are also given.

In section 5 we show that if K/F is separable, then every p-symbol over K can be expressed as a sum of no more than $[K:F]+1$ symbols of the form $[a,\beta\}$, where $a\in K$ and $\beta\in F$. This is used to define a trace map on ${}_p\mathrm{Br}(K)$ if K/F is Galois. Applications to the case of C_2 fields of characteristic 2 are also given.

Let K/F be a cyclic extension of fields. In section 6 we study to what extent does Hilbert's theorem 90 fail for the group ${}_p\mathrm{Br}(K)$. We develop some elementary but useful tools, and use them to show that

Hilbert's theorem 90 holds iff every invariant algebra of exponent p is the restriction from F of an algebra of the same exponent. If both statements fail, we can match the two failures in the sense explain there. We show that if $[K:F]$ is divisible by p, then under very weak assumptions Hilbert's theorem 90 does fail for ${}_p\mathrm{Br}(K)$. Elements of the invariant subgroup of ${}_p\mathrm{Br}(K)$ are studied in the subsection 6.5, and properties of the corestriction are used in the last subsection to show that Hilbert's theorem 90 does fail in some cases.

1. Field Extensions in Characteristic p

Let F be a field with $\mathrm{char}F = p > 0$. In this section we briefly describe the (well known) theory of field extensions of such fields, of dimension an exponent of p. In subsections 1.3 and 1.4 we study composite extensions, and use the results in subsections 1.5–1.6 to count extensions of various types, and bound the number of corresponding subgroups in the absolute Galois group. The results can be used to give a new proof of Witt's theorem that the p-part of the absolute Galois group of F is a free pro-p group.

In subsequent sections we only use the basic facts from the first two subsections, and the properties of $H_{K/F}$ defined in the third.

1.1. Inseparable Extensions. In every finite dimensional extension L/F, there is an intermediate subfield $F \subseteq K \subseteq L$ such that K/F is separable, and L/K is purely inseparable. $[L:K]$ is a power of p.

LEMMA 1.1. *Let $b \in F$. $g(\lambda) = \lambda^p - b$ is either irreducible over F, or splits in F.*

PROOF. Let y be a root of g in a splitting field, g_1 the minimal polynomial over F, and $d = \deg(g_1)$.

$g(\lambda) = \lambda^p - y^p = (\lambda - y)^p$, and since g_1 divides g (in $F[y][\lambda]$), it is a power of $(\lambda - y)$. Then $y^d \in F$ as the constant coefficient of g_1.

If $d = p$ we are done. Otherwise, write $\alpha d + \beta p = 1$, then $y = (y^d)^\alpha b^\beta \in F$. □

COROLLARY 1.2. *$F[\lambda]/\langle \lambda^p - b \rangle$ is either a field or a local ring of dimension p over its residue field.*

Every inseparable extension of dimension p of F is constructed in this way: let S/F be such an extension, then some $y \in S$ satisfies $y^p \in F$, $y \notin F$, so that $\lambda^p - b$ is the minimal polynomial of y. Then we let $S = F[\sqrt[p]{b}]$.

If b_1, b_2 belong to the same class in $F^*/(F^*)^p$, then obviously $F[\sqrt[p]{b_1}] \cong F[\sqrt[p]{b_2}]$. For a complete classification we need to introduce a certain subfield of F.

The p-power map $F \to F$, defined by $x \mapsto x^p$, is a homomorphism of fields (and thus monic). The image is denoted by $F^p = \{x^p : x \in F\}$, so that $F \cong F^p$.

For example, suppose $b_1, b_2 \in F$, and denote $S_i = F[y : y^p = b_i]$. Then $S_1 \cong S_2$ iff $F^p[b_1] \cong F^p[b_2]$, since $S_i^p = F^p[b_i]$.

The **exponent** of a purely inseparable extension S/F is the least q (a power of p), for which $S^q \subseteq F$.

The p-power map is used to define $F^{1/p} = F[x^{1/p} : x \in F]$, an extension of F which contains all the exponent-p extensions. This can be done over and over, to get

$$\cdots \subseteq F^{p^2} \subseteq F^p \subseteq F \subseteq F^{1/p} \subseteq F^{1/p^2} \subseteq \cdots$$

— a chain of isomorphic fields.

Let K/F be a finite separable extension. If $\{b_1, \ldots, b_m\}$ is a basis of K/F, then the p-power isomorphism carries it to a basis $\{b_1^p, \ldots, b_m^p\}$ of K^p/F^p. Writing $K = \sum F b_i$ and $K^p = \sum F^p b_i^p$, we get that the composite of the two subfields F, K^p is $FK^p = \sum F b_i^p = K$. It follows that $F \otimes_{F^p} K^p \cong K$, and similarly $F^{1/p} \otimes_F K \cong K^{1/p}$. In particular, $[F : F^p] = [K : K^p]$.

It also follows that $\{b_1, \ldots, b_m\}$ is a basis for $K^{1/p}/F^{1/p}$, so that $\{b_1^p, \ldots, b_m^p\}$ is a basis for K/F.

COROLLARY 1.3. *If $\gamma \in K$, then $F[\gamma] = F[\gamma^p]$.*

PROOF. $\{1, \gamma, \ldots, \gamma^{m-1}\}$ is a basis for $F[\gamma]/F$ for some m, so that

$$\{1, \gamma^p, \ldots, \gamma^{p(m-1)}\}$$

is a basis too. □

1.2. Cyclic Separable Extensions. Let $\wp(\lambda)$ denote the expression $\lambda^p - \lambda$. Note the following trivial properties.

REMARK 1.4. If u, v are elements of a field of characteristic p, then:
a. $\wp(u + v) = \wp(u) + \wp(v)$.
b. If j is an integer, $\wp(ju) = j\wp(u)$.
c. $\wp(u) = \wp(v)$ iff $u - v$ is an integer.

REMARK 1.5. Let $a \in F$. $f(\lambda) = \lambda^p - \lambda - a$ is either irreducible over F, or splits in F.

PROOF. $f(\lambda)$ is separable. Let x be a root of f in a splitting field, then the roots are $x, x + 1, \ldots, x + p - 1$. Let $f_1(\lambda)$ be the minimal

polynomial of x over F. If $\deg(f_1) = 1$ we are done; otherwise let $x+j$ be another root of f_1. If σ is an automorphism sending $x \mapsto x+j$ then $x+2j, x+3j, \ldots$ are roots of f_1, and $\deg(f_1) = p$. □

COROLLARY 1.6. *$F[\lambda]/\langle \lambda^p - \lambda - a\rangle$ is either a Galois extension of F of dimension p, or the split ring $F^{\times p}$.*

A full description of Galois extensions of dimension p of F is given by the following.

THEOREM 1.7 (Artin-Schreier). *Every cyclic extension of dimension p over F is of the form $K = F[\lambda]/\langle \lambda^p - \lambda - a\rangle$ for some $a \in F$.*

PROOF. Let σ be a generator of the Galois group $\mathrm{Gal}(K/F)$. Obviously $\mathrm{tr}_{K/F}(1) = p = 0$, so by the additive analogue of Hilbert's theorem 90, we have that $1 = \sigma(x) - x$ for some $x \in K$.

$K = F[x]$ since $x \notin F$. Note that $\sigma(x^p - x) = (x+1)^p - (x+1) = x^p - x$, so that x is a zero of $f(\lambda) = \lambda^p - \lambda - a$ for $a = x^p - x \in F$, and since $\deg(f) = p$ this is the minimal polynomial of x over F. □

LEMMA 1.8. *Let $a_1, a_2 \in F$, $f_i = \lambda^p - \lambda - a_i$, and $K_i = F[\lambda]/\langle f_i(\lambda)\rangle$ $(i = 1, 2)$.*

If $K_1 \cong K_2$, then $a_2 = ja_1 + u^p - u$ for some $0 < j < p$ and $u \in F$.

PROOF. If f_i are reducible, then a_i are both of the form $a_i = {u_i}^p - u_i$ for $u_i \in F$, and the result follows. Assume $K_1 \cong K_2$ are fields, and let $x_i \in K_1$ be a root of $f_i = \lambda^p - \lambda - a_i$. Let σ be an automorphism of K_1 such that $\sigma(x_1) = x_1 + 1$. Since the roots of f_2 are $x_2 + j, j = 0, \ldots, p-1$, it follows that $\sigma(x_2) = x_2 + j$ for some $0 \le j < p$ (but $j \neq 0$ for $x_2 \notin F$). Now $u = x_2 - jx_1 \in F$, and $a_2 = \wp(x_2) = \wp(jx_1 + u) = ja_1 + \wp(u)$. □

The set $\wp(F) = \{\wp(u)\} u \in F$ is a vector subspace of F over the prime field $\mathbb{Z}_p$, and so is the quotient group $F/\wp(F)$. For $a \in F$, let

$$\Lambda_F(a) = F[\lambda]/\langle \lambda^p - \lambda - a\rangle$$

be the corresponding extension of dimension p. By the above discussion, Λ_F maps $F/\wp(F)$ onto the set of cyclic extensions of dimension p of F, where the elements in the projective point $\mathbb{Z}_p^* a = \{a, 2a, \ldots, (p-1)a\}$ are mapped to the same extension.

More generally, there is a bijection from subspaces of dimension d of $F/\wp(F)$, to Galois extensions of F with Galois group $\mathbb{Z}_p^d$. Let $\overline{a}$ denote the image of a in $F/\wp(F)$. If $\overline{a_1}, \ldots, \overline{a_d}$ generate a d-dimensional subspace of $F/\wp(F)$, then $F[\lambda_1, \ldots, \lambda_d]/\langle {\lambda_1}^p - \lambda_1 - a_1, \ldots, {\lambda_d}^p - \lambda_d - a_d\rangle$ is in fact a Galois extension of F with Galois group $\mathbb{Z}_p^d$, and this is the general form of such an extension.

We now give an alternative description, using only one generator. Let $q = p^d$. $\mathbb{F}_q$ denotes the finite field with q elements.

THEOREM 1.9. *Suppose $\mathbb{F}_q \subseteq F$.*

a. Let $c \in F$. $\lambda^q - \lambda - c$ is either irreducible over F, or completely splits. If $\lambda^q - \lambda - c$ is irreducible, then $K = F[\lambda]/\langle \lambda^q - \lambda - c\rangle$ is Galois over F, with $\mathrm{Gal}(K/F) = \mathbb{Z}_p^d$.

b. Let K/F be a Galois extension, with Galois group $\mathrm{Gal}(K/F) = \mathbb{Z}_p^d$. Then $K = F[\lambda]/\langle \lambda^q - \lambda - c\rangle$ for some $c \in F$.

PROOF. a. Same as in 1.5 and 1.6. If α is a root of $\lambda^q - \lambda - c$, then so are $\alpha + r$ for every $r \in \mathbb{F}_q$. This implies $\mathrm{Gal}(K/F) \cong (\mathbb{F}_q, +)$.

b. Let $\sigma_1, \ldots, \sigma_d$ be generators for $\mathrm{Gal}(K/F)$, and let

$$F_i = K^{\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_d}.$$

F_i/F is cyclic of dimension p, so we can write $F_i = F[u_i]$, $u_i^p - u_i = c_i \in F$. Note that $\sigma_i(u_j) = u_j + \delta_{ij}$.

Let $r_1, \ldots, r_d$ be a basis for $\mathbb{F}_q$ over $\mathbb{Z}_p$. Consider $u = r_1 u_1 + \cdots + r_d u_d$. For any $r = k_1 r_1 + \cdots + k_d r_d$ ($k_i \in \mathbb{Z}_p$), let $\sigma = \sigma_1^{k_1} \ldots \sigma_d^{k_d}$ and compute that $\sigma(u) = u + r$.

Thus $u + r$ ($r \in \mathbb{F}_q$) are all roots of the minimal polynomial of u. It follows that $[F[u] : F] \geq q$, so that $F[u] = K$. Since $u^q - u$ is invariant, the minimal polynomial of u is $\lambda^q - \lambda - c$ for $c = u^q - u \in F$, as asserted. □

REMARK 1.10. The splitting field of $\lambda^q - \lambda - c$ over F always contains $\mathbb{F}_q$. Suppose $F \cap \mathbb{F}_q = \mathbb{F}_{q_0}$, then the splitting field over F is $K = F[u] \otimes_{\mathbb{F}_{q_0}} \mathbb{F}_q$, where u is a root of the polynomial. $\mathrm{Gal}(K/F)$ is a semidirect product of $(\mathbb{F}_q, +) \cong \mathbb{Z}_p^d$ and $\langle \sigma_{FR} \rangle = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q_0}) \cong \mathbb{Z}_{q/q_0}$, where σ_{FR} is the Frobenius automorphism acting on $(\mathbb{F}_q, +)$ as exponentiation by q_0.

1.3. Composite Extensions. We now address the following question. Given a cyclic extension K/F, which cyclic extensions of dimension p over K are cyclic over F as well? Recall that if $a \in K$, $\overline{a}$ is the class of a in $K/\wp(K)$, and $\Lambda_K(\overline{a}) = K[\lambda]/\langle \lambda^p - \lambda - a\rangle$ (note that this field indeed depends on $\overline{a}$ only).

PROPOSITION 1.11. *Let $a \in K$, where K/F is Galois. $L = \Lambda_K(\overline{a})$ is Galois over F iff $\mathrm{Gal}(K/F)$ acts on $\mathbb{Z}_p^* \overline{a} = \{k\overline{a} : 0 < k < p\}$, that is, for every $\tau \in \mathrm{Gal}(K/F)$, $\tau(\overline{a}) \in \mathbb{Z}_p^* \overline{a}$.*

PROOF. First observe that in general, if L is the splitting field of $f(\lambda) \in K[\lambda]$, then L/F is Galois iff for every $\tau \in \mathrm{Gal}(K/F)$, $\tau(f(\lambda))$

splits in L (here $\mathrm{Gal}(K/F)$ acts on $K[\lambda]$ by the action on the coefficients).

Now, $L = \Lambda_K(\overline{a})$ is Galois iff $\lambda^p - \lambda - \tau(a)$ splits for $\tau \in \mathrm{Gal}(K/F)$, and we are done by Lemma 1.8. □

Fix $a \in K$, and let $L = \Lambda_K(\overline{a})$. Assume that L is indeed Galois over F. Then $\mathrm{Gal}(L/F)$ has a normal subgroup $\mathrm{Gal}(L/K) \cong \mathbb{Z}_p$, with quotient group $\mathrm{Gal}(K/F)$.

DEFINITION 1.12. A Galois extension L/F is said to be *central* over K/F, if $K \subseteq L$ and $\mathrm{Gal}(L/K)$ is central in $\mathrm{Gal}(L/F)$.

PROPOSITION 1.13. *Suppose L/F is Galois.*
L/F is central Galois over K/F iff the action of $\mathrm{Gal}(K/F)$ *on $\mathbb{Z}_p^* \overline{a}$ is trivial.*

PROOF. Write $L = K[\alpha]$, where $\wp(\alpha) = \alpha^p - \alpha = a$. Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator, such that $\sigma(\alpha) = \alpha + 1$. Given $\mu \in \mathrm{Gal}(L/F)$, we have that $\mu(\overline{a}) = i\overline{a}$ for some $i \in \mathbb{Z}_p^*$. Write $\mu(a) = ia + x^p - x$ for some $x \in K$, and take $\wp^{-1}$ on both sides to get $\mu(\alpha) = i\alpha + x'$, where $x' - x \in \mathbb{Z}_p$. Now, $\mu^{-1}\sigma\mu(\alpha) = \mu^{-1}\sigma(i\alpha + x') = \mu^{-1}(i\alpha + i + x') = \alpha + i$. It follows that the centralizer $C_{\mathrm{Gal}(L/F)}(\sigma)$ is the stabilizer of $\overline{a}$, so σ is central iff the action is trivial. □

It is clear that for $\mathrm{Gal}(L/F)$ to be cyclic, $\mathrm{Gal}(K/F)$ must be cyclic too, and from now on we assume this is the case. Let τ be a generator for $\mathrm{Gal}(K/F)$, and $q = [K:F]$ the order of τ.

The following object is very important in the classification of p-extensions of K over F.

DEFINITION 1.14. $H_{K/F}$ is the lift of the τ-invariant subgroup of $K/\wp(K)$ to K:

$$H_{K/F} = \{a \in K : \tau(a) - a \in \wp(K)\}.$$

Note that $H_{K/F}/\wp(K)$ is a subgroup of $K/\wp(K)$.

COROLLARY 1.15. *In this language, $\Lambda_K(\overline{a})$ is central Galois over K/F iff $a \in H_{K/F}$.*

Let $a \in H_{K/F}$. Then we have that

$$\tau(a) - a = x^p - x \tag{1}$$

for some $x \in K$.

Taking $\mathrm{tr}_{K/F}$ on both sides, we see that $\mathrm{tr}_{K/F}(x)$ is a root of $\lambda^p - \lambda = 0$, and is thus an integer.

REMARK 1.16. If $\mathrm{tr}_{K/F}(x) = 0$, then a can be adjusted (leaving $L = \Lambda_K(\overline{a})$ unchanged) to satisfy $a \in F$.

PROOF. By Hilbert's Theorem 90, $x = \tau(y) - y$ for some $y \in K$, and then $\tau(a) - a = x^p - x = (\tau(y)^p - \tau(y)) - (y^p - y)$. Thus $a - \wp(y) \in F$. □

Suppose $q = [K:F]$ is prime to p.

The only central extension of $\mathbb{Z}_p$ by $\mathbb{Z}_q$ is $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$, so that equation (1) is enough for L/F to be cyclic:

THEOREM 1.17. *Let K/F be a cyclic extension of order prime to p, and let $\overline{a} \in K/\wp(K)$.*

$L = \Lambda_K(\overline{a})$ is cyclic over F iff $\tau(\overline{a}) = \overline{a}$.

Moreover, if $\mathrm{tr}_{K/F}(x) = i$, we can replace x by $x - q^{-1}i$ and then apply Remark 1.16 to get $a \in F$. Thus we have proved

COROLLARY 1.18. *If $[K:F]$ is prime to p, then $H_{K/F} = F + \wp(K)$.*

Note that if q is prime to p there is a one-to-one correspondence between p-cyclic extensions of F and cyclic extensions of F which have dimension p over K, by $L_0 \mapsto L_0 \otimes_F K$, where the opposite direction is by taking the unique subfield of dimension p over F.

Now assume that p divides q.

The central extensions of $\mathbb{Z}_p$ by $\mathbb{Z}_q$ are $\mathbb{Z}_{pq}$ and $\mathbb{Z}_p \times \mathbb{Z}_q$.

As before, let $L = \Lambda_K(\overline{a}) = K[\alpha]$, $\alpha^p - \alpha = a$. From Equation (1) it follows that we can extend τ to L by $\tau : \alpha \to \alpha + x$. It is easily computed that $\tau^q(\alpha) = \alpha + \mathrm{tr}_{K/F}(x)$. $\mathrm{Gal}(L/F)$ is cyclic iff τ^q is a non-trivial element of $\mathrm{Gal}(L/F)$, that is if $\mathrm{tr}_{K/F}(x) \neq 0$.

Thus we have proved

THEOREM 1.19. *Let K/F be a cyclic extension of dimension divisible by p, and let $a \in H_{K/F}$. Then $\Lambda_K(\overline{a})$ is Galois over F.*

The Galois group is $\mathbb{Z}_p \times \mathbb{Z}_q$ if $a \in \wp(K) + F$, and $\mathbb{Z}_{pq}$ otherwise.

1.4. Relative H groups. In this subsection we study the groups $\wp(K) = \{a^p - a\}$ and $H_{K/F}$ (defined in 1.14). This will be used in the next subsection to count extensions of various types.

We first compute $F \cap \wp(K)$ where K/F is a cyclic extension of dimension p.

Set $\delta_{p|q} = 1$ if $p \,|\, q$, and $\delta_{p|q} = 0$ otherwise. If $U \subseteq V$ are groups, $[V:U]$ denotes the index of U in V (we use the same notation for dimension over subfields, but no confusion should result of that).

PROPOSITION 1.20. *If q is prime to p then $F \cap \wp(K) = \wp(F)$. Otherwise, let $a \in F$ be an element such that $K^{\tau^p} = F[\lambda]/\langle \lambda^p - \lambda - a\rangle$ (so that $a \notin \wp(F)$); then $F \cap \wp(K) = \wp(F) + \mathbb{Z}_p a$. To summarize,*

$$[F \cap \wp(K) : \wp(F)] = p^{\delta_{p|q}}.$$

PROOF. Define $\phi' : \wp(K) \cap F \to \mathbb{Z}_p$ as follows. Let $u \in K$ such that $\wp(u) \in F$. Then $\wp(\tau(u) - u) = \tau(\wp(u)) - \wp(u) = 0$, so that $j = \tau(u) - u$ is an integer. Set $\phi'(\wp(u)) = j$. If $\wp(u) = \wp(u')$ then $u - u' \in \mathbb{Z}_p$, and so ϕ' is well defined. If q is prime to p then $\tau(u) = u$ for $u = \tau^q(u) = u + qj$, so $\phi' = 0$. Otherwise, let α be a root of $\lambda^p - \lambda - a$; then $\tau(\alpha) - \alpha$ is a non-zero integer, and $u - i\alpha = f$ for some $i \in \mathbb{Z}_p$ and $f \in F$ (thus ϕ' is onto). It follows that $\wp(u) = ia + \wp(f)$, as asserted. □

This can be generalized.

PROPOSITION 1.21. *Let T/F be finite Galois extension, with an arbitrary finite Galois group G. Then $(F \cap \wp(T))/\wp(F) \cong G/G'G^p$*

PROOF. Let $N = G'G^p$, so that G/N is the maximal Abelian quotient of exponent p of G. Let $u \in T$, and suppose $\wp(u) \in F$. For every $\sigma \in G$ we have that $\wp(\sigma(u) - u) = \sigma(\wp(u)) - \wp(u) = 0$, so that $\sigma(u) = u + j_\sigma$ for some $j_\sigma \in \mathbb{Z}_p$. Note that the map $\sigma \mapsto j_\sigma$ is a group homomorphism from G to $\mathbb{Z}_p$, so that N is in the kernel of this map, and we have that $u \in T^N$.

In particular, $\wp(T) \cap F = \wp(T^N) \cap F$. Let $\sigma_1 N, \ldots, \sigma_d N$ be a basis for G/N as a vector space over $\mathbb{Z}_p$, and $\alpha_1, \ldots, \alpha_d$ a standard set of generators for T^N/F, that is $\sigma_i(\alpha_j) = \alpha_j + \delta_{ij}$, $a_i = \wp(\alpha_i) \in F$.

Check that $f = u - \sum_{1 \le i \le d} j_{\sigma_i} \alpha_i \in F$, so that $\wp(T) \cap F = \wp(F) + \mathbb{Z}_p a_1 + \cdots + \mathbb{Z}_p a_d$. Factoring out $\wp(F)$ we get the result, since $a_1, \ldots, a_d$ are independent modulo $\wp(F)$. □

From now on we assume K/F is cyclic. Recall that if $[K:F]$ is prime to p, then $H_{K/F} = F + \wp(K)$ (Corollary 1.18). We now assume p divides $[K:F]$, and study $H_{K/F}$.

REMARK 1.22. If K/F is separable, then $\mathrm{tr}_{K/F}$ is onto. (This is a well known consequence of Artin's lemma).

THEOREM 1.23. *If p divides $q = [K:F]$, then*

$$H_{K/F}/(F + \wp(K)) \cong \mathbb{Z}_p.$$

PROOF. Given $a \in H_{K/F}$, write $\tau(a) - a = \wp(x)$ for $x \in K$, and consider the map $\phi : a \mapsto \mathrm{tr}_{K/F}(x)$. This is well defined since if $\tau(a) - a = \wp(x')$, then $x - x' \in \mathbb{Z}_p$ and $\mathrm{tr}(x) = \mathrm{tr}(x')$. Since $\wp(\mathrm{tr}_{K/F}(x)) = 0$, ϕ is into $\mathbb{Z}_p$. Note that if $a \in F + \wp(K)$, then $\mathrm{tr}_{K/F}(x) = 0$. By

Remark 1.16, $\mathrm{Ker}(\phi) = F + \wp(K)$. Finally, let $x \in K$ be an element with $\mathrm{tr}_{K/F}(x) = 1$, then $\mathrm{tr}_{K/F}(\wp(x)) = \wp(\mathrm{tr}_{K/F}(x)) = 0$, and there exist $a \in K$ such that $\sigma(a) - a = \wp(x)$. Obviously $a \in H_{K/F}$ and $a \mapsto 1$. □

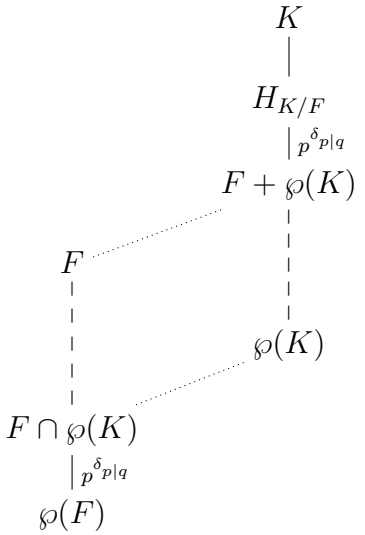
We have the following commutative diagram for the maps ϕ and ϕ' defined in the proofs of the last theorem and Proposition 1.20. The rows are exact if p divides $[K:F]$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F + \wp(K) & \longrightarrow & H_{K/F} & \xrightarrow{\phi} & \mathbb{Z}_p & \longrightarrow & O \\ & & \downarrow{\scriptstyle \mathrm{tr}} & & \downarrow{\scriptstyle \mathrm{tr}} & & \| & & \\ 0 & \longrightarrow & \wp(F) & \longrightarrow & \wp(K) \cap F & \xrightarrow{\phi'} & \mathbb{Z}_p & \longrightarrow & 0 \end{array}$$

The leftmost trace map is readily seen to be onto, so by the '5 lemma' we also have

COROLLARY 1.24. *The map* $\mathrm{tr} : H_{K/F} \to \wp(K) \cap F$ *is onto.*

Here is the lattice of the subspaces involved for K/F cyclic of dimension q, with the relative indices as computed above.



Consider a more complicated situation, where L/F is cyclic with an intermediate field K. We want to describe the lattice of $\mathbb{Z}_p$-vector spaces generated by F, K, L, their $\wp$-groups and the relative H groups. For this we need to compare some points on that lattice.

Recall that the lattice of subspaces of a given space is *modular*, i.e., for every three subspaces A, B, C, if $A \subseteq C$ then

$$A + (B \cap C) = (A + B) \cap C.$$

In this case we write $A + B \cap C$ and omit parenthesis.

THEOREM 1.25. *Let L/F be a cyclic extension, with $F \subseteq K \subseteq L$. Then the following equalities hold:*

a. $K \cap H_{L/F} = H_{K/F}$.

b. $H_{K/F} \cap \wp(L) = K \cap \wp(L)$.

c. $H_{L/F} + K = H_{L/K}$.

d. $\wp(L) + H_{K/F} = \wp(L) + K \cap H_{L/F}$.

e. $H_{K/F} + \wp(L) = F + \wp(L)$ *if* $p \mid [L:K]$ *or* $[K:F]$ *prime to* p, *and* $[H_{K/F} + \wp(L) : F + \wp(L)] = p$ *otherwise.*

f. $\wp(L) \cap K \subseteq H_{K/F}$.

g. $F + \wp(L) \cap H_{K/F} = F + \wp(L) \cap K$.

PROOF. Let $m = [K:F]$. Denote by τ a generator of $\mathrm{Gal}(L/F)$, and let $\theta : L \to L$ denote the map $\theta = 1 + \tau + \cdots + \tau^{m-1}$. Note that the restriction of θ to K is $\mathrm{tr}_{K/F}$, and that $\mathrm{tr}_{L/K} \circ \theta = \mathrm{tr}_{L/F}$. Also, $(\tau^m - 1) = \theta(\tau - 1)$.

a. The inclusion $K \cap H_{L/F} \supseteq H_{K/F}$ is trivial. Let $a \in K \cap H_{L/F}$. Then $\tau(a) - a = \wp(l)$ for some $l \in L$. Compute that $0 = \mathrm{tr}_{K/F}(\tau a - a) = \mathrm{tr}_{K/F}\wp(l) = \wp(\theta l)$, so that $\theta l \in \mathbb{Z}_p \subseteq F$. Now $\tau^m(l) - l = \tau(\theta l) - \theta l = 0$, so that $l \in K$ and $a \in H_{K/F}$.

b. By part a., $H_{K/F} \cap \wp(L) = H_{L/F} \cap K \cap \wp(L) = K \cap \wp(L)$ as $\wp(L) \subseteq H_{L/F}$.

c. The inclusion $H_{L/F} + K \subseteq H_{L/K}$ is trivial. Let $a \in H_{L/K}$, then $\tau^m(a) - a = \wp(l)$ for some $l \in L$. As before $\wp(\mathrm{tr}_{K/L}(l)) = \mathrm{tr}_{K/L}\wp(l) = \mathrm{tr}_{K/L}(\tau^m(a) - a) = 0$ so $\mathrm{tr}_{K/L}(l) \in \mathbb{Z}_p \subseteq F$. By Remark 1.22, we can find $l_1 \in L$ such that $\mathrm{tr}_{L/F}(l_1) = \mathrm{tr}_{L/K}(l)$. Since $\mathrm{tr}_{L/K}\theta = \mathrm{tr}_{L/F}$, we have that $\mathrm{tr}_{L/K}(l - \theta l_1) = \mathrm{tr}_{L/K} l - \mathrm{tr}_{L/F} l_1 = 0$, and there is some $r \in L$ such that $l - \theta l_1 = (\tau^m - 1)(r)$. Let $l_0 = l_1 + (\tau - 1)(r)$, then $\theta l_0 = \theta l_1 + \theta(\tau - 1)r = \theta l_1 + (\tau^m - 1)(r) = l$. Compute that $\mathrm{tr}_{L/F}\wp(l_0) = \wp(\mathrm{tr}_{L/F} l_1) = \wp(\mathrm{tr}_{L/K} l) = \mathrm{tr}_{L/K}(\tau^m a - a) = 0$. Thus there is some $b \in L$ such that $\tau(b) - b = \wp(l_0)$, so that $b \in H_{L/F}$. Now, $\tau^m(b) - b = \theta(\tau - 1)(b) = \theta\wp(l_0) = \wp(\theta l_0) = \wp(l) = \tau^m(a) - a$, so that $\tau^m(a - b) = a - b$, and $a - b \in K$. Thus $a \in K + H_{L/F}$, as asserted.

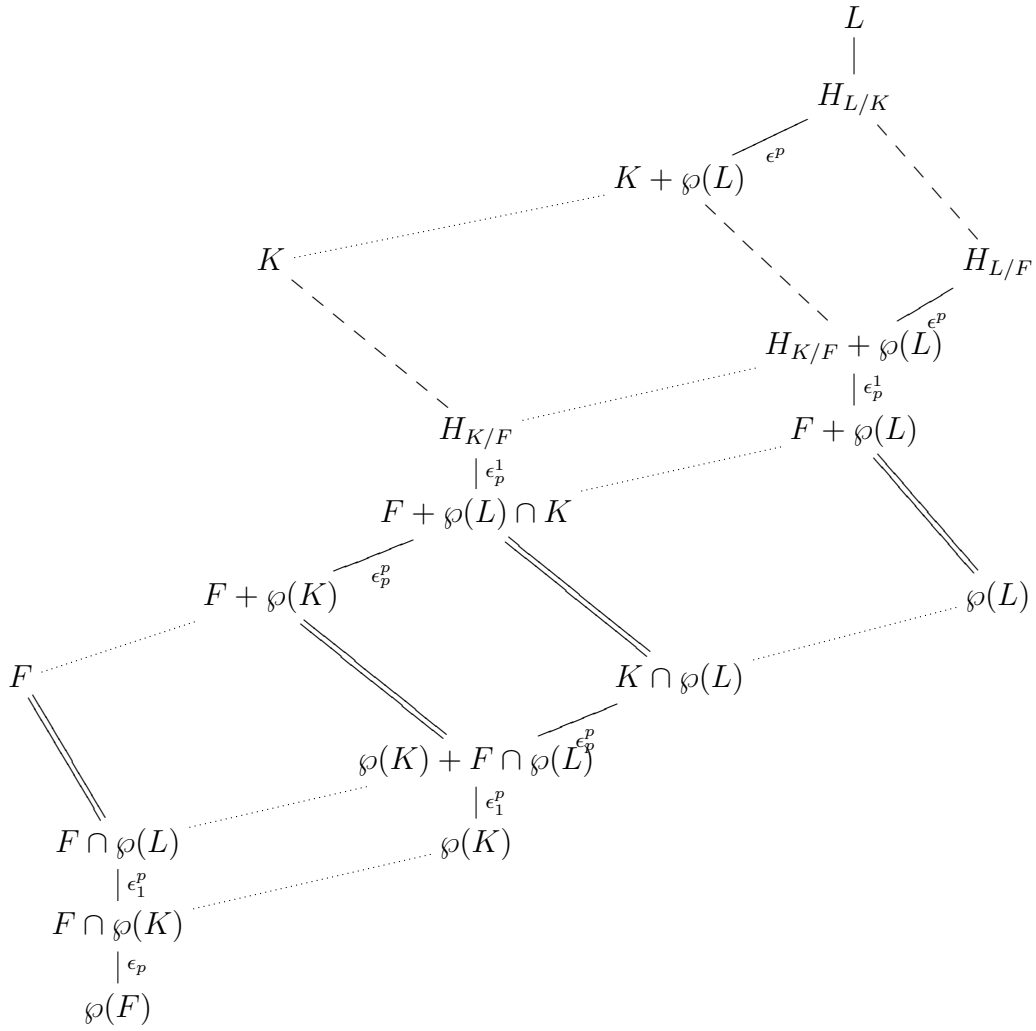
d. Immediate from part a.

e. Consider the spaces $K + \wp(L)$ and $H_{L/F}$. Their sum is, by part c., equal to $H_{L/K} + \wp(L) = H_{L/K}$. By part d., their intersection is $H_{K/F} + \wp(L)$. Thus $H_{L/F}/(H_{K/F} + \wp(L)) \cong H_{L/K}/(K + \wp(L))$. This quotient is of size $p^{\delta_{p|[L:K]}}$ by Corollary 1.18 and Theorem 1.23. From the same reasons $\left|H_{L/F}/(F + \wp(L))\right| = p^{\delta_{p|[L:F]}}$. Dividing, we find out that $[H_{K/F} + \wp(L) : F + \wp(L)]$ is as asserted.

f. Let $\wp(l) \in K$ for some $l \in L$. Then $0 = (\tau^m - 1)\wp(l) = \wp((\tau^m - 1)l)$, so that $(\tau^m - 1)l \in \mathbb{Z}_p \subseteq F$. Thus $(\tau^m - 1)(\tau - 1)l = (\tau - 1)(\tau^m - 1)l = 0$, and $(\tau - 1)l \in K$. Now, $\tau\wp(l) - \wp(l) = \wp((\tau - 1)l) \in \wp(K)$, so that $\wp(l) \in H_{K/F}$.

g. The inclusion $F + \wp(L) \cap H_{K/F} \cap F + \wp(L) \cap K$ is obvious, and the other direction follows from part f. □

With all these facts put together, we get the following lattice (in which the intersection and sum of spaces always appears in its proper place). We set ϵ_p^1 to be p if $[L:K]$ is prime to p and $[K:F]$ is divisible by p, and 1 otherwise. Similarly $\epsilon_1^p = p$ if $[L:K]$ is divisible by p and $[K:F]$ prime to p, and 1 otherwise. Also, $\epsilon_p^p = p$ if $[L:K]$ and $[K:F]$ are both divisible by p, and 1 otherwise. Finally, we set $\epsilon^p = \epsilon_1^p \epsilon_p^p$, and $\epsilon_p = \epsilon_p^1 \epsilon_p^p$. The numbers in the diagram denote relative indices.



1.5. Counting Cyclic Extensions. In subsection 1.2 it was mentioned that Galois extensions of F with Galois group $\mathbb{Z}_p^d$ are parameterized by d-dimensional subspaces of $F/\wp(F)$. If

$$d_F = \dim_{\mathbb{Z}_p} F/\wp(F)$$

is finite, we can actually count the extensions. The simplest example is where F is finite — then $d_F = 1$. Note that by [**15**, Prop. 4.4.8], the p-part of the Brauer group $\mathrm{Br}(F)$ is trivial when d_F is finite.

Let K/F be a cyclic extension. The lines of $K/\wp(K)$ correspond to cyclic extensions of dimension p over K, and there are $\frac{p^{d_K}-1}{p-1}$ such extensions. Similarly, by Corollary 1.15 there are exactly $\frac{[H_{K/F}:\wp(K)]-1}{p-1} =$

$\frac{p^{d_F}-1}{p-1}$ central Galois extensions of F which are p-dimensional over K (the equality follows from Theorem 1.23).

The possible Galois groups for these extensions over F are $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_{pq}$ (the two types coincide if q is prime to p). By Theorem 1.19, extensions of the first type correspond to the classes $(F+\wp(K))/\wp(K)$.

The following follows from Proposition 1.20.

REMARK 1.26.

$$[F+\wp(K):\wp(K)] = p^{d_F-\delta_{p|q}}.$$

PROOF.

$$\begin{aligned}[F+\wp(K):\wp(K)] &= [F:F\cap\wp(K)] \\ &= [F:\wp(F)]/[F\cap\wp(K):\wp(F)] \\ &= p^{d_F-\delta_{p|q}}.\end{aligned}$$

□

COROLLARY 1.27. *Suppose K/F is a cyclic extension. From Remark 1.26 we have that*

$$[F+\wp(K):\wp(K)] = p^{d_F-\delta_{p|q}},$$

so that there are exactly $\frac{p^{d_F-\delta_{p|q}}-1}{p-1}$ Galois extensions L of F, containing K as a subfield, such that $\mathrm{Gal}(L/F)\cong\mathbb{Z}_p \times \mathbb{Z}_q$.

For example, if $d_F = 1$, let K be the only extension of dimension p. Then $F \subseteq \wp(K)$, and, as expected, there are no extensions of F with Galois group $\mathbb{Z}_p \times \mathbb{Z}_p$.

Now assume $p \mid q$, and count the extensions of the second type (those which are cyclic over F). From Theorem 1.23 we have

COROLLARY 1.28. *Suppose K/F is cyclic of dimension divisible by p.*

The number of extensions of K which are cyclic of dimension $p\cdot[K:F]$ over F, equals p^{d_F-1}.

PROOF. By Remark 1.26 and Theorem 1.23, we have that $[H_{K/F}:\wp(K)] = [H_{K/F}:F+\wp(K)]\cdot[F+\wp(K):\wp(K)] = p^{d_F}$. Now subtract the number of extensions with Galois group $\mathbb{Z}_p \times \mathbb{Z}_q$ (Corollary 1.27) from the number of central Galois extensions:

$$\frac{[H_{K/F}:\wp(K)]-1}{p-1} - \frac{p^{d_F-1}-1}{p-1} = \frac{p^{d_F}-p^{d_F-1}}{p-1} = p^{d_F-1}.$$

□

In particular, if F has at least one cyclic extension, then $p^{d_F-1} \geq 1$, and we can inductively define a chain of cyclic extensions of F,

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$$

and inspect $\hat{F} = \cup F_i$:

COROLLARY 1.29. *Every cyclic extension K/F of dimension a power of p is embedded in an extension $\hat{F}/F$ such that $\mathrm{Gal}(\hat{F}/F) = \lim_{\leftarrow} \mathbb{Z}_{p^n}$ is the Abelian pro-p group of rank 1 (i.e. the additive group of the p-adic integers).*

This last corollary is usually deduced by the construction of Witt vectors, e.g. [**14**].

In particular, if $d_F = 1$ then $p^{d_F-1} = 1$ and we have

COROLLARY 1.30. *Suppose F has a unique cyclic extension of order p.*

Then F has a unique *cyclic extension of any order p^n. Moreover, F has a unique extension $\hat{F}$ with $\mathrm{Gal}(\hat{F}/F) = \lim_{\leftarrow} \mathbb{Z}_{p^n}$.*

REMARK 1.31. In the case $d_F = 1$, the field $\hat{F}$ has no cyclic extensions of dimension p.

PROOF. Let $\theta \in \hat{F}$. Then $\theta \in F_i$ for some i, and $\lambda^p - \lambda - \theta$ has a solution in F_{i+1}, and thus in $\hat{F}$. □

COROLLARY 1.32. *Let K be a separably closed field of characteristic p. Then the absolute Galois group $\Lambda = \mathrm{Gal}(K/\mathbb{Z}_p)$ has no finite p-subgroups.*

PROOF. Otherwise, let $\sigma \in \Lambda$ be an element of order p. Then $F = K^\sigma$ has a cyclic extension, so that $d_F \geq 1$ and by the theorem $d_K \geq 1$. But $d_K = 0$ by assumption. □

The information in Corollary 1.28 can also be interpreted in terms of subgroup growth of the absolute Galois group of F, denoted by Γ_F. For a group G, let $C_n(G)$ denote the number of normal subgroups $N \trianglelefteq G$ of index n with cyclic quotient group.

THEOREM 1.33.

$$C_{p^n}(\Gamma_F) = \frac{p^{d_F} - 1}{p - 1} p^{(d_F-1)(n-1)}.$$

In particular, $\frac{\log C_{p^n}(\Gamma_F)}{\log p^n} \longrightarrow d_F - 1$.

PROOF. Every normal subgroup with quotient $\Gamma_F/N = \mathbb{Z}_{p^n}$ is contained in exactly one normal subgroup with quotient $\mathbb{Z}_{p^{n-1}}$, so that $C_{p^n}(\Gamma_F) = C_{p^{n-1}}(\Gamma_F) \cdot p^{d_F-1}$. But $C_p(\Gamma_F) = \frac{p^{d_F}-1}{p-1}$ by definition of d_F, so the result follows by induction. □

1.6. Going Up One Stage. We now discuss the number of p-cyclic extensions of F and K when $F \subseteq K$. We treat two easy cases (K/F Galois of dimension prime to p, or K/F purely inseparable), and a harder and more fruitful one, when K/F is itself cyclic of dimension p.

PROPOSITION 1.34. *If K/F is Galois and $[K:F]$ is prime to p, then $d_F \leq d_K$.*

PROOF. The map $L \mapsto L \otimes_F K$ (taking cyclic extensions of dimension p over F to cyclic extensions of the same dimension over K) is injective, since the (normal) subgroup of elements of prime-to-p order in $\mathbb{Z}_p \times \mathrm{Gal}(K/F)$ is unique. □

THEOREM 1.35. *Let K/F be a purely inseparable extension. Then*
a. $K = F + \wp(K)$.
b. $\wp(K) \cap F = \wp(F)$.
c. $d_K = d_F$.

PROOF. We may assume K/F is of exponent p (and then use induction).
a. For every $k \in K$, $k = k^p - (k^p - k) \in F + \wp(K)$.
b. If $k^p - k \in F$, then $k \in K^p + F = F$.
c. $K/\wp(K) = (F + \wp(K))/\wp(K) \cong F/(\wp(K) \cap F) = F/\wp(F)$. □

And now, the cyclic case. The result we give here follows from Witt's theorem that the Galois group of the maximal pro-p extension over F is a free pro-p group [**25**, Cor. 3.2]. Since our theorem counts subgroups of index p, it is equivalent to Witt's theorem for the finitely-generated case by a result of A. Lubotzky.

THEOREM 1.36. *Let $K = F[u]$, $u^p - u = \theta \in F$, be a cyclic extension of dimension p over F. Then*

$$d_K = p(d_F - 1) + 1.$$

PROOF. In order to compute $d_K = \log_p |K/\wp(K)|$ we construct a set of representatives for $K/\wp(K)$.

Since $\theta \notin \wp(F)$, $\Theta = (\mathbb{Z}_p\theta + \wp(F))/\wp(F)$ is a subgroup of order p of $F/\wp(F)$. Pick a set B_F of representatives for the quotient group $(F/\wp(F))/\Theta$, so that $B_F + \mathbb{Z}_p\theta$ is a complete set of representatives for $F/\wp(F)$. In particular, $p^{d_F} = |F/\wp(F)| = p|B_F|$.

Another way to put it: every element $f \in F$ is expressible in the form

$$f = g^p - g + b + i\theta \tag{2}$$

for $g \in F, b \in B_F, i \in \mathbb{Z}_p$, where b, i are unique (and g is unique up to adding integers). In a more graphic form, $F = \wp(F) \oplus B_F \oplus \mathbb{Z}_p\theta$.

Let $B_K = B_F + B_F u + \cdots + B_F u^{p-1} + \mathbb{Z}_p \theta u^{p-1}$. We claim that B_K is a complete set of representatives for $K/\wp(K)$. Let $f_K = \sum_{i=0}^{p-1} f_i u^i \in F[u]$ be an arbitrary element of K. We shall use reverse induction on the degree of f_K in order to show that f_K is expressible as

$$f_K = \wp(g_K) + b_K \tag{3}$$

for unique $b_K \in B_K$, and unique $g_K \in K$ up to adding integers.

Write $b_K = \sum_{i=0}^{p-1} b_i u^i + j\theta u^{p-1}$, $b_i \in B_F$, and $g_K = \sum_{i=0}^{p-1} g_i u^i$, $g_i \in F$. Note that in general, the upper monomial of $(u^i)^p = (u^p)^i = (u+\theta)^i$ (considered as a polynomial in u over F) is u^i. Hence, the coefficient of u^{p-1} in ${g_K}^p - g_K$ is ${g_{p-1}}^p - g_{p-1}$. Comparing coefficients of u^{p-1} in (3), we have the equation

$${f_{p-1}} = {g_{p-1}}^p - g_{p-1} + b_{p-1} + j\theta, \tag{4}$$

which by (2) has a solution with unique b_{p-1} and j, and g_{p-1} unique up to adding integers.

Now let $i \leq p-1$. Suppose $j \in \mathbb{Z}_p, b_{p-1}, \ldots, b_i \in B_F$, $g_{p-1}, \ldots, g_{i+1} \in F$ are fixed, and g_i is fixed up to adding integers. Write $g_i = g_{i0} + j_i$, where g_{i0} is already fixed and $j_i \in \mathbb{Z}_p$ is yet to be determined. We solve for b_{i-1},j_i, and g_{i-1} up to integers, by comparing coefficients of u^{i-1} after removing the fixed part from (3). If $h \in K = F[u]$, we denote by $[u^i]h$ the coefficient of u^i in h.

Let $f'_{i-1} = [u^{i-1}](f_K - \wp(\sum_{l=i+1}^{p-1} g_l u^l))$, and compute using (3):

$$\begin{aligned}
f'_{i-1} &= [u^{i-1}](f_K - \wp(\sum_{l=i+1}^{p-1} g_l u^l)) \\
&= [u^{i-1}](\wp(\sum_{l=0}^{i} g_l u^l) + \sum_{i=0}^{p-1} b_l u^l + j\theta u^{p-1}) \\
&= [u^{i-1}](\sum_{l=0}^{i} (g_l^p u^{lp} - g_l u^l)) + b_{i-1} \\
&= [u^{i-1}](\sum_{l=0}^{i} g_l^p (u+\theta)^l - \sum_{l=0}^{i} g_l u^l) + b_{i-1} \\
&= [u^{i-1}](\sum_{l=i-1}^{i} g_l^p (u+\theta)^l - \sum_{l=i-1}^{i} g_l u^l) + b_{i-1} \\
&= [u^{i-1}](g_i^p (u+\theta)^i - g_i u^i + g_{i-1}^p (u+\theta)^{i-1} - g_{i-1} u^{i-1}) + b_{i-1} \\
&= [u^{i-1}](i g_i^p \theta u^{i-1} + (g_{i-1}^p - g_{i-1}) u^{i-1}) + b_{i-1} \\
&= (g_{i-1}^p - g_{i-1}) + i({g_{i0}}^p + j_i)\theta + b_{i-1}
\end{aligned}$$

Subtracting $i g_{i0}^p \theta$, we get the equation

$$f'_{i-1} - i g_{i0}\theta = g_{i-1}^p - g_{i-1} + b_{i-1} + i j_i \theta. \tag{5}$$

By the choice of B_F this equation has a solution, with unique $b_{i-1} \in B_F$ and $j_i \in \mathbb{Z}_p$, and g_{i-1} unique up to adding integers. After fixing j_i we know g_i, and the next induction step can be performed.

We have shown that B_K is indeed a basis for $K/\wp K$, so that $p^{d_K} = |K/\wp(K)| = |B_K| = |B_F|^p p = p^{p(d_F-1)+1}$, and we are done. □

Corollary 1.37. *If $F = F_0 \subset \cdots \subset F_n$ is a chain of cyclic extensions of dimension p, then $d_{F_n} = p^n(d_F - 1) + 1$.*

This result too is related to subgroup growth of $\Gamma = \Gamma_F$, the absolute Galois group of F. Let $S_n(G)$ denote the number of subnormal subgroups of index n in G.

Theorem 1.38.

$$S_{p^n}(\Gamma) < \left(\frac{p}{p-1}\right)^n p^{\frac{p^n-1}{p-1}(d_F-1)}.$$

In particular, $\frac{\log\log S_{p^n}(\Gamma)}{\log p^n} < 1 + o(1)$ whenever d_F is finite.

PROOF. Note that if $N \leq G$ is a subnormal group of p-power index, then $N = N_t \trianglelefteq N_{t-1} \trianglelefteq \ldots \trianglelefteq N_1 \trianglelefteq N_0 = G$, where N_i/N_{i-1} is of order p. In particular, $S_{p^n}(G)$ is bounded by the sum of numbers of normal subgroups of index p of all the subnormal subgroups of index p^{n-1} in G. By the last corollary we have that $S_{p^n}(\Gamma) \leq S_{p^{n-1}}(\Gamma)^{\frac{p^{p^n(d_F-1)+1}-1}{p-1}}$, and by induction

$$\begin{aligned} S_{p^n}(\Gamma) &\leq \Pi_{i=0}^{n-1} \frac{p^{p^i(d_F-1)+1}-1}{p-1} \\ &< \Pi_{i=0}^{n-1} \frac{p^{p^i(d_F-1)+1}}{p-1} \\ &= (p-1)^{-n} p^{n+(d_F-1)(1+p+\cdots+p^{n-1})}. \end{aligned}$$

□

REMARK 1.39. In the special case where F has no prime-to-p extensions, Γ is a pro-p group and every subgroup is subnormal. In this case $S_{p^n}(\Gamma)$ is the number of subgroups of index p^n.

2. Cyclic p-Algebras

A simple algebra A/F is **cyclic** if it contains a maximal subfield K which is cyclic over F. See [**22**] for a survey of the history of cyclic algebras.

The main structure theorem on p-algebras (algebras over F with $\deg(A)$ a power of $char(F) = p$) is that every p-algebra is similar (in the Brauer group) to a cyclic algebra ([**1**, VII.31], [**15**, 4.5.7]). Non-cyclic p-algebras (with degree $\geq p^2$) were first constructed by Amitsur and Saltman [**4**].

If $\exp(A) = p$, then A is similar to a tensor product of cyclic algebras of degree p [**15**, 4.2.17]. It follows that the exponent-p part of $\mathrm{Br}(F)$ is generated by (the classes of) cyclic algebras of degree p. Whether or not every p-algebra of degree p is cyclic is still wide open.

Every p-algebra A has a finite dimensional purely inseparable subfield S/F [**15**, 4.1.10], and $\exp(A)$ equals the minimal exponent of such a field over F. If $S = S'[u]$ where $u^p \in S'$, and $[F[u]:F] = p^e$, and S' does not split A, then $A \otimes C$ is split by S' for C a cyclic p-algebra of degree p^e over F [**15**, 4.2.11].

This is used as an induction mechanism to show, for example, the following. If $[F^* : F^{*p}] = p^d$, then A is similar to a product of at most d cyclic algebras of degree p (since $F^{1/p}$ splits A, and is of dimension p^d over F). More generally we have

REMARK 2.1. Suppose $\exp(A) = p^e$, where $[F^* : F^{*p}] = p^d$. Then A is split by F^{1/p^e}, which has dimension p^{de} over F. It follows that A is similar to a product of at most de cyclic algebras, at most d of any degree p^i $(i = 1 \dots e)$. At least one cyclic algebra of degree p^e must be present.

If S/F is purely inseparable, then the map $[A] \mapsto [A \otimes S]$ from $\mathrm{Br}(F)$ to $\mathrm{Br}(S)$ is surjective [**15**, 4.1.5]. In particular for $S = F^{1/p}$, we have that the map $[A] \mapsto [A \otimes F^{1/p}] = [A]^p$ is surjective, so that $\mathrm{Br}(F)$ is p-divisible. This is an important step in showing that every p-algebra is similar to a product of cyclic algebras.

We now discuss the presentation of cyclic algebras of degree p by means of generators and relations. We give full details of this old construction, in order to make the computations more accessible in the sequel.

Let A be a cyclic p-algebra of degree p, with maximal subfield K, generated by $x \in K$ such that $x^p - x = a \in F$ (Theorem 1.7). The automorphism $\sigma \in \mathrm{Gal}(K/F)$ acts on K by $\sigma(x) = x + 1$. By Skolem-Noether, there exists an element $y \in A$ such that $yxy^{-1} = x + 1$.

LEMMA 2.2. *$F[y]$ is an inseparable extension of degree p over F, and as a maximal subfield, it splits A.*

PROOF. It is easy to compute that $y^j x y^{-j} = x + j$, so that for every $f(\lambda) \in F[\lambda]$, $xf(y) - f(y)x = -yf'(y)$, where f' denote the standard derivative of f.

Now let $g(\lambda) \in F[\lambda]$ be the minimal polynomial of y over F. Since $g(y) = 0$, we also have $g'(y) = 0$. But $\deg(g') < \deg(g)$, so we must have $g'(\lambda) = 0$, and $p \mid \deg(g)$. Thus $[F[y] : F] \geq p$, but since $F[y]$ is commutative, $[F[y] : F] \leq \sqrt{[A : F]} = p$, so that $[F[y] : F] = p$. $F[y]$ is inseparable since $g(\lambda) = \lambda^p - (y^p)$. □

We have seen that no element of $F[y] - F$ commutes with x, so that $F[x] \cap F[y] = F$. Counting dimensions we see that $F[x, y] = A$. Now y^p commutes with x and with y, so that $b = y^p \in F$.

The relations

$$x^p - x = a, \quad y^p = b, \quad yxy^{-1} = x + 1 \tag{6}$$

fully determine the multiplication in A, and we may use them to define the **symbol p-algebra**

$$[a, b) = F[x, y : x^p - x = a, y^p = b, yx = xy + y].$$

Note that it is always central simple over F.

As mentioned above, the classes of $[a,b)$, $a,b \in F$, generate ${}_p\mathrm{Br}(F)$ (the exponent-p part of $\mathrm{Br}(F)$). We now give a list of relations satisfied by these generators.

LEMMA 2.3. *If $a \in \wp(F) = \{u^p - u : u \in F\}$, or $b \in (F^*)^p$, then $[a,b)$ is split.*

PROOF. Since $[a,b)$ is of prime degree, it is either a division algebra or the split algebra $M_p(F)$.

Thus, it is enough to show that $[a,b)$ is not a division algebra. Indeed, if $\lambda^p - \lambda - a$ is reducible over F, let $\alpha \in F$ be a root (Proposition 1.5). Then $\Pi_{i=0}^{p-1}(x - \alpha - i) = \wp(x - \alpha) = a - a = 0$, and we have zero divisors. If $b = \beta^p$ for $\beta \in F$, then $(\beta^{-1}y - 1)^p = 0$ and again we have zero divisors. □

The next theorem is responsible for the other identities. Its proof will be used in section 4.

THEOREM 2.4. *a.* $[a_1,b_1) \otimes [a_2,b_2) \cong [a_1 + a_2, b_1) \otimes [a_2, b_1^{-1}b_2)$.
b. $[a_1,b_1) \otimes [a_2,b_2) \cong [a_1, b_1b_2) \otimes [a_2 - a_1, b_2)$.

PROOF. The left hand side R is generated in both cases by x_1, x_2, y_1, y_2, satisfying ${x_i}^p - x_i = a_i$, $y_i^p = b_i$, $x_1x_2 = x_2x_1$, $y_1y_2 = y_2y_1$, $y_ix_jy_i^{-1} = x_j + \delta_{ij}$.

a. It is easy to check that $R_1 = F[x_1 + x_2, y_1]$ and $R_2 = F[x_2, y_1^{-1}y_2]$ are commuting subalgebras which generate R, $R_1 \cong [a_1 + a_2, b_1)$, and $R_2 \cong [a_2, b_1^{-1}b_2)$.

b. The same argument, with $R_1 = F[x_1, y_1y_2]$, $R_2 = F[x_2 - x_1, y_2]$. □

COROLLARY 2.5. *a.* $[a_1,b) \otimes [a_2,b) \cong [a_1 + a_2, b) \otimes M_p(F)$.
b. $[a,b_1) \otimes [a,b_2) \cong [a, b_1b_2) \otimes M_p(F)$.

PROOF. Substitute $b_1 = b_2$ in Theorem 2.4.a, $a_1 = a_2$ in 2.4.b, and use 2.3. □

A final computation:

REMARK 2.6. $[a,a) \cong M_p(F)$.

PROOF. Consider the elements $x, x^{-1}y$ in $[a,a) = F[x,y : x^p - x = y^p = a, yxy^{-1} = x + 1]$. They satisfy $x^p - x = a$, $(x^{-1}y)x(x^{-1}y)^{-1} = x^{-1}(yxy^{-1})x = x^{-1}(x+1)x = x + 1$, and finally,

$$(x^{-1}y)^p = N_{F[x]/F}(x)^{-1}y^p = a^{-1}a = 1.$$

Thus $[a,a) \cong [a,1) \cong M_p(F)$. □

Did we miss an identity? In the next section it will be shown that the results 2.3,2.5 and 2.6 are enough to prove any relation satisfied by p-symbols.

3. Presentation for ${}_p\mathrm{Br}(F)$

3.1. The Merkurjev-Suslin Theorem. Let R be a ring, and let $GL(R)$ denote the direct limit of the groups $GL_n(R)$ of invertible $n \times n$ matrices, under the canonical injections $GL_n(R) \to GL_{n+1}(R)$ by $A \mapsto A \oplus 1$.

The generators $e_{ij}(r) = 1 + re_{ij}$ ($r \in R$, $i, j \geq 1$) of $GL(R)$ satisfy certain identities, e.g. $e_{ij}(r)e_{jk}(s) = e_{ik}(r+s)$. It is not surprising that some relations depend on the arithmetic of the ring R.

The Steinberg group $St(R)$ of R is defined by generators $x_{ij}(r)$, and certain relations which apply to $\{e_{ij}(r)\}$ over every ring R. $\mathrm{K}_2(R)$ is defined as the kernel of the map $x_{ij}(r) \mapsto e_{ij}(r)$ from $St(R)$ onto $GL(R)$, and is a measure of how 'general' is the ring from an arithmetical point of view. It turns out that $\mathrm{K}_2(R)$ is always an Abelian group, and that $\mathrm{K}_2 : R \mapsto \mathrm{K}_2(R)$ is a functor from the category of rings to the category of abelian groups.

Matsumoto has proved (*cf.* [**26**, Thm. 4.3.15]) that if F is a field (of arbitrary characteristic), then $\mathrm{K}_2(F)$ is the abelian group generated by the symbols $\{a, b\}$ ($a, b \in F^*$), subject to the relations

$$\{a, b_1\} + \{a, b_2\} = \{a, b_1 b_2\},$$
$$\{a_1, b\} + \{a_2, b\} = \{a_1 a_2, b\},$$
$$\{a, 1 - a\} = 0.$$

The connection to simple algebras is evident, since symbol algebras in characteristic 0 obey the same rules. For every n, if $\mathrm{char}F$ is prime to n and F has primitive n'th roots of unity, there is a canonical map from $\mathrm{K}_2(F)$ to ${}_n\mathrm{Br}(F)$, sending the symbol $\{a, b\}$ to the cyclic algebra $(a, b)_{n;F} = F[x, y | x^n = a, y^n = b, yxy^{-1} = \rho x]$.

The precise result has very far reaching consequences.

THEOREM 3.1 (Merkurjev-Suslin [**24**]). *Let n be an integer, and F a field with characteristic prime to n, containing n'th roots of unity.*

Then the natural map sending $\{a, b\}$ to the symbol algebra $(a, b)_n$ induces an isomorphism $\mathrm{K}_2(F)/n\mathrm{K}_2(F) \to {}_n\mathrm{Br}(F)$.

Essentially, this is a description of ${}_n\mathrm{Br}(F)$ in terms of generators (the cyclic algebras) and relations. As a result, if $\mathrm{char}F = 0$ and F has all the roots of unity, then $\mathrm{K}_2(F) \cong \mathrm{Br}(F)$ (since the above mentioned maps are coherent).

There are partial results for the case where F does not have roots of unity. Merkurjev [**23**] has proved that if q is a prime $\neq \mathrm{char}F$, then ${}_q\mathrm{Br}(F)$ is generated by the classes of algebras of index q. Also if $[F[\mu_q]:F] \leq 3$, then ${}_q\mathrm{Br}(F)$ is generated by the classes of cyclic algebras of degree q.

In connection with this result, it was proved by Merkurjev that in the case $[E:F] \leq 3$, $\mathrm{K}_2(E)$ is generated by the symbols $\{a, \beta\}$, $a \in E$, $\beta \in F$. The same is true if F has no prime-to-$[E:F]$ extensions [**7**].

Even today, after several simplifications of the proof have been made, the Merkurjev-Suslin theorem is still considered very hard. The most difficult part is a K_2 analog for Hilbert's theorem 90: if K/F is cyclic, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, and $r \in \mathrm{K}_2(K)$ satisfies $\sum \sigma^i r = 0$, then $r = \sigma s - s$ for some $s \in \mathrm{K}_2(K)$. The proofs of this result use heavy machinery from étale cohomology, including higher K functors, the Braun-Gerstein-Quillen spectral sequence, and analysis of Chern classes (*cf.* [**40**]). A proof can be found in [**38**]. We discuss Hilbert's theorem 90 for subgroups of prime exponent of $\mathrm{Br}(K)$ in Section 6.

Motivated by the description of ${}_n\mathrm{Br}(F)$ by generators and relations for the prime-to-p case, we give in this section a similar description for ${}_p\mathrm{Br}(F)$ where $p = \mathrm{char}F$. The presentation we describe below was first proved by Teichmüller. In a more modern language, it can be derived from the Cartier map $\Omega^1_F \to \Omega^1_F/d(\Omega^0_F)$ defined by $x\frac{dy}{y} \mapsto (x^p - x)\frac{dy}{y}$, *cf.* [**17**]. Our proof is rather similar to that of Teichmüller, and we include it for completeness.

3.2. Generators and Relations for ${}_p\mathrm{Br}(F)$. Let F be a field of characteristic p.

In this subsection we give a presentation of ${}_p\mathrm{Br}(F)$ in terms of generators and relations. As generators we use the p-cyclic algebras — they generate ${}_p\mathrm{Br}(F)$ by Albert's structure theory for p-algebras, proved back in the 40's.

Definition 3.2. $\mathcal{K}_2(F)$ is defined as the free abelian group generated by all formal p-symbols $[a, b\}$ ($a, b \in F$, $b \neq 0$), subject to the following relations ($a, a_1, a_2, b_1, b_2 \in F$, $b, b_1, b_2 \neq 0$):

$$[a_1 + a_2, b\} = [a_1, b\} + [a_2, b\} \tag{7}$$

$$[a, b_1 b_2\} = [a, b_1\} + [a, b_2\} \tag{8}$$

$$[b, b\} = 0 \tag{9}$$

$$[a^p - a, b\} = 0. \tag{10}$$

REMARK 3.3. From Equations (7) and (8), we see that $[a, b^p\} = p[a, b\} = [pa, b\} = [0, b\} = 0$.

Another useful computation is given by

REMARK 3.4. For every $a, b, c \in F$, $b, c \neq 0$,

$$[a^p bc, b\} = -[a^p bc, c\} \tag{11}$$

PROOF. If $a = 0$ we are done. Otherwise, compute that $[a^p bc, b\} = [a^p bc, b\} - [a^p bc, a^p bc\} = [a^p bc, \frac{1}{ca^p}\} = -[a^p bc, c\}$. □

It is evident that $(a, b) \to [a, b\}$ defines a map from $(F, +) \otimes_{\mathbb{Z}_p} F^*$ onto $\mathcal{K}_2(F)$. Actually, this induces a map of abelian groups,

$$F/\wp(F) \otimes_{\mathbb{Z}} F^*/F^{*p} \to \mathcal{K}_2(F),$$

whose kernel is generated by the couples (a, a) (*cf.* [**10**, Lemma 11.14]).

Define a map $R_F : \mathcal{K}_2(F) \to {}_p\mathrm{Br}(F)$ by $R_F : [a, b\} \mapsto [a, b)$, where $[a, b) = F[x, y : x^p - x = a, y^p = b, yx = (x+1)y]$ is the cyclic p-algebra. This map is a well defined homomorphism by the basic computational rules satisfied by cyclic p-algebras (Corollary 2.5 and Remark 2.6).

R_F is onto by Albert's structure theory, so it remains to show that R_F is one-to-one.

We start with an example for values of a for which $[a, b\} \mapsto 0$.

LEMMA 3.5. *If* $a = \gamma_0^p - \gamma_0 + \sum_{i=1}^{p-1} \gamma_i^p b^i$ *for* $\gamma_i \in F$, *then* $[a, b\} = 0$.

PROOF. $[u, v\} = [u, v\} - [u, u\} = [u, \frac{v}{u}\}$. Now compute:

$$\begin{aligned}
[a, b\} &= [\gamma_0^p - \gamma_0 + \sum_{i=1}^{p-1} \gamma_i^p b^i, b\} \\
&= [\gamma_0^p - \gamma_0, b\} + \sum_{i=1}^{p-1} [\gamma_i^p b^i, b\} \\
&= \sum_{i=1}^{p-1} [\gamma_i^p b^i, b\} \\
&= \sum_{i=1}^{p-1} [\frac{1}{i} \gamma_i^p b^i, b^i\} \\
&= 0.
\end{aligned}$$

where the last equality follows from Remark 3.4 (with $c = 1$). □

It turns out that this example is the most general one:

FACT 3.6. Let B be an C-algbera, and C a commutative subalgebra. Let $\delta : C \to C$ be the derivation induced by $z \in B$: $zf - fz = \delta(f)$ for all $f \in C$.

Then $(z+f)^p = z^p + f^p + \delta^{p-1}(f)$.

THEOREM 3.7 (Teichmüller [**39**]). *If $[a,b)$ splits then $a = \gamma_0^p - \gamma_0 + \sum_{i=1}^{p-1} \gamma_i^p b^i$ for some $\gamma_i \in F$.*

PROOF. By assumption $[a,b) \cong M_p(F) \cong [0,b)$, so there are $x, y \in M_p(F)$ such that $x^p - x = a$, $y^p = b$ and $yx = (x+1)y$, and $z', y' \in M_p(F)$ such that $y'^p = b, z'^p - z' = 0$ and $y'z' = (z'+1)y'$. But since $F[y] \cong F[y']$, there is some $t \in M_p(F)$ such that $y = ty't^{-1}$. Setting $z = tz't^{-1}$, we have that $z^p - z = 0$ and $yz = (z+1)y$.

Now $y(x-z) = ((x+1) - (z+1))y = (x-z)y$, so that $x - z$ commutes with y and $x - z \in C_{M_p(F)}F[y] = F[y]$. Thus, $x - z = f(y)$ for some polynomial $f(\lambda) \in F[\lambda]$. Write $f(y) = \sum_{i=0}^{p-1} \gamma_i y^i$.

In 3.6 take $B = M_p(F)$ and $C = F[y]$. The derivation δ induced by z satisfies $\delta(y) = -y$, and more generally $\delta(f(y)) = -yf'$ where $f \mapsto f'$ is the ordinary derivation of polynomials. $\delta^{p-1}(y^i) = (-i)^{p-1}y^i = y^i$ for every $i > 0$, so that $\delta^{p-1}(f(y)) = f(y) - f(0)$.

We can now compute: $a + z + f(y) = a + x = x^p = (z + f(y))^p = z^p + f(y)^p + f(y) - f(0)$, so that $a = f(y)^p - f(0) = \sum_{i=0}^{p-1} \gamma_i^p b^i - \gamma_0$. □

REMARK 3.8. Let $F^p \subseteq F$ be the subfield of all $p-$powers in F. If $a = \gamma_0^p - \gamma_0 + \sum_{i=1}^{p-1} \gamma_i^p b^i$ then $\gamma_0 \in F^p(a,b)$.

For the induction step we need the following lemma.

LEMMA 3.9. *If $[a_1,b_1) \otimes \cdots \otimes [a_n,b_n)$ splits, then $[a_1,b_1\} + \cdots + [a_n,b_n\}$ can be written as a sum of $n-1$ symbols in $\mathcal{K}_2(F)$.*

PROOF. Let $S = F[b_2^{1/p}, \ldots, b_n^{1/p}]$, a purely inseparable extension of F. Obviously S splits $[a_i,b_i)$ for all $i = 2, \ldots, n$, but since $[a_1,b_1) \otimes \cdots \otimes [a_n,b_n)$ is split, S splits $[a_1,b_1)$ too. By Theorem 3.7, there exist $\gamma_0, \ldots, \gamma_{p-1} \in S$ with $a_1 = \gamma_0^p - \gamma_0 + \sum_{i=1}^{p-1} \gamma_i^p b_1^i$, where by the above remark $\gamma_0 \in S^p(a_1,b_1)$=F.

Let $G = \mathbb{Z}_p^{n-1}$ be the split abelian group of exponent p. If $g \in G$, g_j is the j'th component of g $(j = 2, \ldots, n)$.

Define a function $\beta : G \to S$ by $\beta_g = (b_2^{g_2} \ldots b_n^{g_n})^{1/p}$. The elements $\{\beta_g : g \in G\}$ form a basis for S over F. Of course, $\beta_g^p = b_2^{g_2} \ldots b_n^{g_n} \in F$.

For $i = 1, \ldots, p-1$, write $\gamma_i = \sum_{g \in G} \gamma_{i,g}\beta_g$, $\gamma_{i,g} \in F$. Then $\gamma_i^p = \sum_{g \in G} \gamma_{i,g}^p \beta_g^p$. Now compute:

$$\begin{aligned}
[a_1,b_1\} &= [\gamma_0^p-\gamma_0+\sum_{i=1}^{p-1}\gamma_i^p b_1^i,b_1\} = \\
&= [\gamma_0^p-\gamma_0,b_1\}+\sum_{i=1}^{p-1}[\gamma_i^p b_1^i,b_1\} = \\
&= \sum_{i=1}^{p-1}\sum_{g\in G}[\gamma_{i,g}^p\beta_g^p b_1^i,b_1\} = \\
&= \sum_{i=1}^{p-1}\sum_{g\in G}[\frac{1}{i}\gamma_{i,g}^p\beta_g^p b_1^i,b_1^i\} = \\
&= -\sum_{i=1}^{p-1}\sum_{g\in G}[\frac{1}{i}\gamma_{i,g}^p\beta_g^p b_1^i,\beta_g^p\},
\end{aligned}$$

the last equality follows from Remark 3.4 with $c=\beta_g^p$.

Now compute that

$$\begin{aligned}
[a_1,b_1\} &+ [a_2,b_2\}+\cdots+[a_n,b_n\} = \\
&= -\sum_{i=1}^{p-1}\sum_{g\in G}[\frac{1}{i}\gamma_{i,g}^p\beta_g^p b_1^i,b_2^{g_2}\dots b_n^{g_n}\}+[a_2,b_2\}+\cdots+[a_n,b_n\} = \\
&= -\sum_{j=2}^{n}\sum_{i=1}^{p-1}\sum_{g\in G}[\frac{g_j}{i}\gamma_{i,g}^p\beta_g^p b_1^i,b_j\}+[a_2,b_2\}+\cdots+[a_n,b_n\} = \\
&= \sum_{j=2}^{n}[a_j-\sum_{i=1}^{p-1}\sum_{g\in G}\frac{g_j}{i}\gamma_{i,g}^p b_1^i\beta_g^p,b_j\}.
\end{aligned}$$

Thus $[a_1,b_1\}+\cdots+[a_n,b_n\}$ is the sum of $n-1$ symbols, as asserted. □

THEOREM 3.10. $\mathcal{K}_2(F)\cong{}_p\mathrm{Br}(F)$.

PROOF. We need to show that R_F is one-to-one, that is, that $[a_1,b_1)\otimes\cdots\otimes[a_n,b_n)\sim F$ implies $[a_1,b_1\}+\cdots+[a_n,b_n\}=0$. The case $n=1$ is Teichmüller's Theorem 3.7 (combined with Lemma 3.5).

Assume the assertion holds for sums of $n-1$ symbols, and suppose $[a_1,b_1\}+\cdots+[a_n,b_n\}\mapsto 0$, i.e. $[a_1,b_1)\otimes\cdots\otimes[a_n,b_n)$ splits. By Lemma 3.9, $[a_1,b_1\}+\cdots+[a_n,b_n\}$ is a sum of $n-1$ symbols with split image, so by the induction hypothesis $[a_1,b_1\}+\cdots+[a_n,b_n\}=0$. □

4. Generators of p-Algebras

Among the basic notions in the study of the automorphisms group of polynomial rings (e.g. over fields) are that of elementary automorphisms, which are those who stabilize all but one of the variables, and that of tame automorphisms, which are compositions of elementary ones.

In this section we suggest a similar notion as a tool to study the variety of sets of standard generators of a p-algebra, which is a tensor product of symbol p-algebras. Since the automorphisms group of a central simple algebra A is already known, we consider the possible presentation of an algebra by standard generators, and use isomorphisms as a device holding two presentations of an algebra at the same time.

This approach is motivated by the fact that axioms (7)–(10) are all we need to make computations in ${}_p\mathrm{Br}(F)$ (Theorem 3.10), and that the corresponding relations between p-algebras are proved (in 2.3–2.6) in terms of explicit generators. It follows that every equality in ${}_p\mathrm{Br}(F)$ can be explained in terms of simple changes of generators, if we add enough matrices in both sides. A natural question is how many matrices are needed in order to make room for the elementary changes. An answer (and precise formulation of the question) are given in Theorem 4.16.

The standard presentations of symbol p-algebras were described in Section 2. In subsection 4.1 we discuss the elementary switches between standard sets of generators of symbol p-algebras, define tame isomorphisms, and prove some basic facts about sets of generators. This is generalized later to tensor products of several symbol p-algebras.

In the second subsection we prove (Theorem 4.9) that if two p-symbols are equal in the Brauer group, then there is a way to rewrite every symbol as sum of at most $p-1$ symbols, such that the isomorphism becomes, in a sense, obvious.

This result is used in the third subsection to show that if $[a,b)\cong[a',b')$ are two presentations of the same algebra, then there is a chain of elementary switches of sets of generators which goes from the presentation $[a,b)\otimes M_p(F)^{\otimes 2(p-2)}$ to $[a',b')\otimes M_p(F)^{\otimes 2(p-2)}$.

4.1. Generators of Cyclic p-Algebras. Let A/F be a cyclic p-algebra of degree p.

Definition 4.1. $x,y\in A$ form a standard couple of generators (SCOG) of A if $F[x,y]=A$, and

$$yxy^{-1}=x+1. \tag{12}$$

It should be noted that (12) gives a presentation of A as a p-symbol, $A=[x^p-x,y^p)$, by the following easy computation.

LEMMA 4.2. *If x, y form a SCOG, then x satisfies*

$$x^p - x \in F \tag{13}$$

and y satisfies

$$y^p \in F \tag{14}$$

PROOF. From (12) compute that $y^p x y^{-p} = x$, and that $y(x^p - x)y^{-1} = x^p - x$. It follows that $x^p - x, y^p \in C_A(F[x, y]) = \mathrm{Cent}(A) = F$. □

Write $A = [a, b)$ where $a = x^p - x$ and $b = y^p$. Note that for any $t \in A$, the SCOG txt^{-1}, tyt^{-1} gives the same presentation. Since we are interested mainly in the symbols, we identify two SCOGs if they are conjugate.

REMARK 4.3. If x, y and x', y' are two SCOGs of A, with $x^p - x = x'^p - x'$ and $y^p = y'^p$, then by Skolem-Noether there is a conjugation that takes $x \to x'$ and $y \to y'$. In other words, there is a one-to-one correspondence between SCOGs-up-to-conjugation, and presentations of A as a symbol algebra.

For a symbol p-algebra A, let

$$X_A = \{x \in A : x^p - x \in F, x \notin F\},$$

$$Y_A = \{y \in A : y^p \in F, y \notin F\}.$$

Every SCOG of A consists of $x \in X_A$ and $y \in Y_A$. Going from a SCOG x, y to a SCOG x', y' is called an **elementary switch** if $x' = x$ or $y' = y$. This amounts to a change of presentation $[a, b) \cong [a, b')$ or $[a, b) \cong [a', b)$, and these are called **elementary isomorphisms**.

As a framework, we form the graph of SCOGs of A, with vertices the ordered couples $(x, y) \in X_A \times Y_A$ such that $yxy^{-1} = x + 1$, where we connect every two points $(x, y), (x, y')$ or $(x, y), (x', y)$. We work in the quotient graph, identifying (x, y) and (x', y') if they are conjugate in A.

Let $[a_0, b_0) \cong [a_n, b_n)$ be an isomorphism, with respective SCOGs x, y and x', y'.

THEOREM 4.4. *There is a path connecting the SCOGs x, y to x', y' in the graph, iff there is a chain of elementary isomorphisms*

$$[a_0, b_0) \cong [a_1, b_1) \cong \ldots \cong [a_n, b_n).$$

PROOF. A path in the graph corresponds to a chain of presentations, where each step is an elementary isomorphism, i.e. one of the defining constants remains the same.

For the other direction, start from x, y, and replace one generator at a time, until reaching a SCOG of $[a_n, b_n)$ (which is possibly different from the target x', y'). Now use Remark 4.3. □

An isomorphism $[a, b) \cong [a', b')$ is called **tame**, if it satisfies the conditions of the above theorem, i.e. it is a composition of elementary isomorphisms.

QUESTION 4.5. *Let A be a symbol p-algebra. Is the isomorphism between any two presentations of A tame? In other words, is the graph of SCOGs of A connected?*

REMARK 4.6. The graph of SCOGs of $M_p(F)$ is connected.

PROOF. Suppose $[a, b) \cong M_p(F) \cong [a', b')$ are two presentations of the split algebra. Use

$$[a, b) \cong [0, b) \cong [0, b') \cong [a', b').$$

□

It follows that if $A \cong A'$ is tame (where A, A' are presentations of a given algebra), then the isomorphism $A \otimes M_p(F) \cong A' \otimes M_p(F)$ is tame too, and there is no need to specify the presentations of $M_p(F)$ in both sides. This observation motivates the definition of stably-tame isomorphisms in the third subsection. In subsection 4.4 we answer affirmatively Question 4.5 for $p = 2$.

We end this subsection with a closer look on elementary switches.

First, we remark that for every $x \in X_A$ there is some $y \in Y_A$ such that x, y form a SCOG, and *vice versa*:

REMARK 4.7. a. If $x \in X_A$, then there is some $y \in A$ such that x, y form a SCOG of A.

b. If $y \in Y_A$, then there is some $x \in A$ such that x, y form a SCOG of A.

PROOF. a. By Remark 1.5, $F[x]$ is either a subfield of A, or the split ring $F^{\times p}$. In both cases the automorphism induced by $x \mapsto x + 1$ is inner (Skolem-Noether or the generalization to maximal separable commutative subalgebras in [**9**]), say induced by y. $y \notin F[x]$, so that $F[x, y] = A$.

b. This is [**1**, Theorem IV.17]. □

The following is a characterization of elementary switches for symbol p-algebras, in terms of elements of the subfields involved.

LEMMA 4.8. *Let x, y be a SCOG of A.*

a. x, y_1 is a SCOG iff $y_1 = ky$ for some $k \in F[x]$.

b. x_1, y is a SCOG iff $x_1 = x + u$ for some $u \in F[y]$.

PROOF. a. $y_1 x y_1^{-1} = x + 1$ iff $y_1 y^{-1} \in C_A(F[x]) = F[x]$.
b. $y x_1 y^{-1} = x_1 + 1$ iff $x_1 - x \in C_A(F[y]) = F[y]$. □

4.2. The Connection Theorem.
Suppose we have the equalities

$$[c_k, b_1\} = [kc_k, b_2\},$$

for $c_k \in F$ $(k = 1, \dots, p-1)$. Then obviously

$$[\sum_{k=1}^{p-1} c_k, b_1\} = [\sum_{k=1}^{p-1} kc_k, b_2\}.$$

It turns out that every equality of p-symbols can be explained by this observation.

THEOREM 4.9 (Connection Theorem). *Suppose* $[a_1, b_1\} = [a_2, b_2\}$, $a_1, b_1, a_2, b_2 \in F$.

Then there exist $c_1, \dots, c_{p-1} \in F$ *such that*

$$[c_k, b_1\} = [kc_k, b_2\} \tag{15}$$

and

$$[a_1, b_1\} = \sum_{k=1}^{p-1} [c_k, b_1\} = \sum_{k=1}^{p-1} [kc_k, b_2\} = [a_2, b_2\}. \tag{16}$$

PROOF. If b_2 is a p-power in F then we can take $c_k = 0$, so assume $L = F[b_2^{1/p}]$ is a field. Since $[a_1, b_1) \otimes L \cong [a_2, b_2) \otimes L \sim L$, we can apply Theorem 3.7 and write $a_1 = {\gamma_0}^p - \gamma_0 + \sum_{i=1}^{p-1} \gamma_i^p b_1^i$ for $\gamma_i \in L$. By Remark 3.8, $\gamma_0 \in F$. For every $i > 0$, write $\gamma_i = \sum_{j=0}^{p-1} \gamma_{ij} b_2^{j/p}$, $\gamma_{ij} \in F$. Now let $c_k = \sum_{-j/i \equiv k \pmod p} \gamma_{ij}^p b_1^i b_2^j$ $(k = 0, 1, \dots, p-1)$, and note that $[c_0, b_1\} = 0$. Then

$$[a_1, b_1\} = [{\gamma_0}^p - \gamma_0 + \sum_{k=0}^{p-1} c_k, b_1\} = \sum_{k=1}^{p-1} [c_k, b_1\}.$$

Since $c_k \in F^p \cdot (b_1 b_2^{-k}) + \dots + F^p \cdot (b_1 b_2^{-k})^{p-1}$, we have that $[c_k, b_1 b_2^{-k}\} = 0$, from which (15) follows. Finally,

$$[a_2, b_2\} = [a_1, b_1\} = \sum [c_k, b_1\} = \sum [kc_k, b_2\}$$

by assumption. □

4.3. Generators of Products of Symbols. Let A be a tensor product of symbol p-algebras.

DEFINITION 4.10. Elements $\begin{pmatrix} x_1 & x_2 & \dots & x_k \\ y_1 & y_2 & \dots & y_k \end{pmatrix} \in A$ form a standard vector of generators (SVOG) of A if $x_1, \dots, x_k$ commute, $y_1, \dots, y_k$ commute, $F[x_1, \dots, x_k, y_1, \dots, y_k] = A$, and

$$y_i x_j y_i^{-1} = x_j + \delta_{ij}. \tag{17}$$

The change $\begin{pmatrix} x_1 & x_2 & \dots & x_k \\ y_1 & y_2 & \dots & y_k \end{pmatrix} \to \begin{pmatrix} x'_1 & x'_2 & \dots & x'_k \\ y'_1 & y'_2 & \dots & y'_k \end{pmatrix}$ of SVOGs is called an **elementary switch** if, for some $1 \le i_0 \le k$, either $x_i = x'_i$ for all $i \ne i_0$ and $y_{i_0} = y'_{i_0}$, or $y_i = y'_i$ for all $i \ne i_0$ and $x_{i_0} = x'_{i_0}$ (i.e. we allow one change in each column, as long as one of the lines has only one change in it).

DEFINITION 4.11. Let X, Y and X', Y' be SVOGs of A.

An isomorphism $F[X, Y] \cong F[X', Y']$ is **tame** if there is a sequence $(X, Y) = (X_0, Y_0), (X_1, Y_1), \dots, (X_m, Y_m) = (X', Y')$ of SVOGs, such that each change $(X_i, Y_i) \to (X_{i+1}, Y_{i+1})$ is elementary.

$A_1 \cong A_2$ is **stably-tame of level** $\le d$ if $A_1 \otimes M_p(F)^{\otimes d} \cong A_2 \otimes M_p(F)^{\otimes d}$ is tame.

The last definition needs a little clarification. Indeed, the notion of tameness refers to an isomorphism between two presentations of an algebra, and $M_p(F)$ is given without any specific presentation. But according to Remark 4.6, one can change generators of each of the split components inside itself, so the choice of SCOGs for them is irrelevant. Note that a stably-tame isomorphism of level 0 is tame.

REMARK 4.12. If $A = F[X, Y] \cong F[X', Y'] = A'$ is tame, then

$$A \otimes M_p(F) \cong A' \otimes M_p(F)$$

is tame too.

To be precise, if z, u and z', u' are SCOGs of $M_p(F)$, the statement is that $F[X, z, Y, u] \cong F[X', z', Y', u']$ is tame.

PROOF. Glue z, u to any SVOG in the chain going from A to A'. You get a chain of SVOGs from $F[X, z, Y, u] = A \otimes M_p(F)$ to $F[X', z, Y', u]$. Now make three more steps without touching X', Y' to go from z, u to z', u', as in Remark 4.6. □

LEMMA 4.13. *Suppose the isomorphisms $A_1 \cong A'_1$ and $A_2 \cong A'_2$ are stably-tame of levels m_1, m_2, respectively. Then $A_1 \otimes A_2 \cong A'_1 \otimes A'_2$ is stably-tame of level $\le \max\{m_1, m_2\}$.*

PROOF. Let $m = \max\{m_1, m_2\}$. Since $A_i \otimes M_p(F)^{\otimes m_i} \cong A_i' \otimes M_p(F)^{\otimes m_i}$ are tame, we may by the above remark assume that $m_1 = m_2 = m$.

Let U_1, U_1', U_2, U_2' be the corresponding SVOGs of A_1, A_1', A_2 and A_2'. By the assumption, there are SVOGs W_1, W_1', W_2, W_2' of $M_p(F)^{\otimes m}$ with chains of elementary switches from $U_i \cup W_i$ to $U_i' \cup W_i'$.

It is easily seen that the chain from $U_1 \cup U_2 \cup W_1$ to $U_1' \cup U_2 \cup W_1'$, then (using Remark 4.6) to $U_1' \cup U_2 \cup W_2$, and then to $U_1' \cup U_2' \cup W_2'$, is a chain of elementary switches, so that $A_1 \otimes A_2 \otimes M_p(F)^{\otimes m} \cong A_1' \otimes A_2' \otimes M_p(F)^{\otimes m}$ is tame. □

LEMMA 4.14. *Let $k \geq 1$, $a, b \in F$.*
a. $[a,b)^{\otimes k} \cong [a,b^k) \otimes M_p(F)^{\otimes(k-1)}$ *is tame.*
b. $[a,b)^{\otimes k} \cong [ka,b) \otimes M_p(F)^{\otimes(k-1)}$ *is tame.*
c. $[a,b^k) \cong [ka,b)$ *is stably-tame of level* $\leq k-1$.

PROOF. Note that by Remark 4.6 we do not need to specify the presentation of matrix components. Let $\begin{pmatrix} x_1 & \dots & x_k \\ y_1 & \dots & y_k \end{pmatrix}$ be a SVOG of $A = [a,b)^{\otimes k}$, where $x_j^p - x_j = a$, $y_j^p = b$, and $F[x_j, y_j], F[x_{j'}, y_{j'}]$ commute if $j \neq j'$.

a. Check that $\begin{pmatrix} x_1 & x_2 - x_1 & \dots & x_k - x_1 \\ y_1 y_2 \dots y_k & y_2 & \dots & y_k \end{pmatrix}$ is a SVOG of A, which gives the presentation $[a,b^k) \otimes [0,b)^{\otimes(k-1)} = [a,b^k) \otimes M_p(F)^{\otimes(k-1)}$.

b. Similarly, $\begin{pmatrix} x_1 + \dots + x_k & x_2 & \dots & x_k \\ y_1 & y_1^{-1} y_2 & \dots & y_1^{-1} y_k \end{pmatrix}$ is a SVOG which gives the presentation $[ka,b) \otimes [a,1)^{\otimes(k-1)} = [ka,b) \otimes M_p(F)^{\otimes(k-1)}$.

c. Immediate from parts a. and b. □

Taking $k = p$, we get the special case

COROLLARY 4.15. $[a,b)^{\otimes p} \cong M_p(F)^{\otimes p}$ *is tame.*

We are ready for the main result of this subsection.

THEOREM 4.16. *Every isomorphism of the form $[a,b) \cong [a',b')$ is stably-tame of level $\leq 2(p-2)$.*

PROOF. We use the Connection theorem 4.9, where (16) gives an isomorphism of p-algebras of degree $(p-1)p$:

$$\begin{aligned} [a_1,b_1) \otimes M_p(F)^{\otimes(p-2)} &\cong [c_1,b_1) \otimes \dots \otimes [c_{p-1},b_1) \\ &\cong [c_1,b_2) \otimes \dots \otimes [c_{p-1},b_2^{p-1}) \\ &\cong [c_1,b_2) \otimes \dots \otimes [(p-1)c_{p-1},b_2) \\ &\cong [a_2,b_2) \otimes M_p(F)^{\otimes(p-2)}. \end{aligned}$$

Let x_k, y_k by SCOGs for $[c_k, b_1)$, so that $\begin{pmatrix} x_1 & x_2 & \dots & x_{p-1} \\ y_1 & y_2 & \dots & y_{p-1} \end{pmatrix}$ is a SVOG for $[c_1, b_1) \otimes \dots \otimes [c_{p-1}, b_1)$.

By an inductive argument using Theorem 2.4,

$$\begin{pmatrix} x_1 + \dots + x_{p-1} & x_2 & \dots & x_{p-1} \\ y_1 & y_1^{-1}y_2 & \dots & y_1^{-1}y_{p-1} \end{pmatrix}$$

is a SVOG for $[a_1, b_1) \otimes M_p(F)^{\otimes p-2}$. It follows that the first isomorphism is tame. The last isomorphism is treated similarly.

The second isomorphism

$$[c_1, b_1) \otimes \dots \otimes [c_{p-1}, b_1) \cong [c_1, b_2) \otimes \dots \otimes [c_{p-1}, b_{p-1})$$

is easily seen to be tame.

In the third isomorphism, every $[c_k, b_2^k) \cong [kc_k, b_2)$ is stably-tame of level $\leq k-1$ by the last lemma, so by Lemma 4.13 the isomorphism is stably-tame of level $\leq p-2$.

It follows that the isomorphism $[a_1, b_1) \cong [a_2, b_2)$ is stably-tame of level $\leq 2(p-2)$. □

We can define a hierarchy of equivalence relations on the collection of SCOGs of a given symbol p-algebra A: two SCOGs of A are equivalent in level m if the isomorphism between the symbol algebras they generate is stably-tame of level $\leq m$. Obviously the relations become coarser as the level increases, and by the theorem all the classes unite eventually.

An isomorphism scheme which is not obviously tame appears in [**28**, Lemma 3.2]. If x, y form a SCOG of an algebra A, then x induces a derivation of $F[y]$, and for any $u \in F[y]$ we have that $v = ux - xu \in F[y]$. It follows that $xv^{-1}u, u$ form a SCOG of A. A natural question is of what level of tameness is the isomorphism $F[x, y] \cong F[xv^{-1}u, u]$.

4.4. Quaternions in Characteristic 2. We now apply and interpret the results of the previous subsections to the case $p = 2$.

By Theorem 4.16, every isomorphism of symbol 2-algebras is tame. Indeed, the connection theorem for $p = 2$ reads:

Suppose $[a_1, b_1\} = [a_2, b_2\}$. Then there exists $c \in F$ such that

$$[a_1, b_1\} = [c, b_1\} = [c, b_2\} = [a_2, b_2\}. \tag{18}$$

Note that [**3**, Lemma 6.3] is essentially the same result for quaternion algebras over a field k with $\mathrm{char} k \neq 2$: if $(a_1, b_1)_2 \cong (a_2, b_2)_2$, then

$$(a_1, b_1)_2 \cong (c, b_1)_2 \cong (c, b_2)_2 \cong (a_2, b_2)_2$$

for some $c \in k$.

We can explain Equation (18) in terms of generators. Recall that x, y is a standard couple of generators for $[a, b)_2$ if $x^2 - x = a$, $y^2 = b$, and $yx = xy + y$. Now suppose

$$[a_1, b_1) \cong [a_2, b_2).$$

By the usual argument, we can write $a_1 = \mu_0^2 - \mu_0 + \mu^2 b_1$ for $\mu_0 \in F$ and $\mu \in F[\sqrt{b_2}]$. Expressing $\mu = \mu_1 + \mu_2\sqrt{b_2}$ for $\mu_1, \mu_2 \in F$, we have

$$a_1 = \mu_0^2 + \mu_0 + \mu_1^2 b_1 + \mu_2^2 b_1 b_2. \tag{19}$$

By symmetry, one can also solve

$$a_2 = \eta_0^2 + \eta_0 + \eta_1^2 b_2 + \eta_2^2 b_1 b_2. \tag{20}$$

By the proof of the connection theorem, $[a_1, b_1) \cong [c, b_1) \cong [c, b_2) \cong [a_2, b_2)$ for $c = \mu_2^2 b_1 b_2$. Let x, y be a standard couple of generators for $[a_1, b_1)$, and set $x' = x + \mu_0 + \mu_1 y$, and $y' = \mu_2 b_2 c^{-1} x' y$.

One can check that x', y' is a SCOG for $[c, b_2)$. There is a SCOG $\tilde{x}, \tilde{y}$ for $[a_2, b_2)$, so by Skolem-Noether, $y' = z\tilde{y}z^{-1}$ for some $z \in R$. Set $x'' = z\tilde{x}z^{-1}$. This completes the chain of SCOGs:

x, y is a SCOG for $[a_1, b_1)$;
x', y is a SCOG for $[c, b_1)$;
x', y' is a SCOG for $[c, b_2)$;
x'', y' is a SCOG for $[a_2, b_2)$.

COROLLARY 4.17 (answer to Question 4.5 for $p = 2$). *The graph of SCOGs of a quaternion algebra is connected.*

Now write $x'' = q + rx' + sy' + tx'y'$, and solve $(x'')^2 - x'' = a_2, y'x'' + x''y' = y'$ for the variable q, r, s, t. One gets $r = 1, t = 0$, so that $x'' = q + x' + sy'$. Now computing $a_2 = (x'')^2 - x'' = q^2 + q + s^2 b_2 + c$, we proved

COROLLARY 4.18. *If $[a_1, b_1) \cong [a_2, b_2)$, then it is possible to solve (19),(20) with $\mu_2 = \eta_2$.*

5. Generators of ${}_p\mathrm{Br}(K)$

Let K/F be finite extension.

The subgroup of ${}_p\mathrm{Br}(K) \cong \mathcal{K}_2(K)$ (Definition 3.2) generated by symbols of the form $[a, \beta\}$ ($a \in K$, $\beta \in F$) is denoted by $[K, F\}$. The main result of this section is that if K/F is separable, then $\mathcal{K}_2(K) = [K, F\}$. Moreover, every symbol in $\mathcal{K}_2(K) = [K, K\}$ can be written as sum of no more than $[K : F] + 1$ symbols from $[K, F\}$.

The immediate application is that it is easy to compute the corestriction. More on that — in subsection 5.2.

It is known that if F is a C_2-field of characteristic 0, then every central simple algebra of exponent 2 over F is similar to a quaternion symbol algebra [**6**]. In subsection 5.3 we extend this result to characteristic 2, and show that if K/F is separable of dimension 2 and F is C_2, then every 2-algebra of exponent 2 over K is similar to a symbol $[a, \beta\}$ where $\beta \in F$.

The last subsection is just a quick reference for the translation between 'our' symbols and the so-called differential symbols.

5.1. The Subgroup $[K, F\}$.

LEMMA 5.1. *Let $b \in K$, and suppose $F[b]/F$ is separable. If $a \in F[b]$, then $[a, b\} \in [K, F\}$.*

PROOF. Let $n = [F[b]:F]$.

First show that it is possible to write a as a polynomial in b, without any monomials of the form $\alpha_i b^i$ with $p \,|\, i$. Indeed, since $F[b]/F$ is separable, $F[b^p] = F[b]$ (Corollary 1.3), and for every $0 \leq j < n$ we have that $b^{j-1} \in F[b^p] = \sum_{0 \leq i < n} F b^{ip}$. Multiplying by b, we get $b^j \in \sum_{0 \leq i < n} F b^{ip+1}$.

It follows that $F[b] = \sum_{0 \leq i < n} F b^{ip+1}$, and writing $a = \sum_{0 \leq i < n} \alpha_i b^{ip+1}$ we have that

$$\begin{aligned}
[a, b\} &= \sum_{0 \leq i < n} [\alpha_i b^{ip+1}, b\} \\
&= \sum_{0 \leq i < n} [\alpha_i b^{ip+1}, b^{ip+1}\} \\
&= \sum_{0 \leq i < n} [\alpha_i b^{ip+1}, \frac{1}{\alpha_i}\} \\
&= \sum_{0 \leq i < n} [-\alpha_i b^{ip+1}, \alpha_i\} \in [K, F\}.
\end{aligned}$$

□

REMARK 5.2. Under the conditions of the above lemma, $[a, b\}$ can be expressed as a sum of n symbols from $[K, F\}$.

QUESTION 5.3. *Suppose K/F is inseparable. Is it still true that $[K, K\} = [K, F\}$? Inspecting the monomials one finds that if $a \in F[b]$, then $[a, b\} \in [K, F\} + [F[b^p], K\}$.*

COROLLARY 5.4. *If $[K:F]$ is prime $\neq p$, then $\mathcal{K}_2(K) = [K, K\} = [K, F\}$.*

PROOF. Let $[a, b\} \in [K, K\}$. If $b \in F$, we are done. Otherwise $F[b] = K$ and $a \in F[b]$, so we are done by Lemma 5.1. □

REMARK 5.5. If K is a finite field, then $\mathcal{K}_2(K) = 0$.

PROOF. Since $|K^*|$ is prime to p, every $b \in K$ is a p-power, and every symbol $[a, b\}$ is trivial. □

THEOREM 5.6. *Suppose K/F is a finite separable extension. Then $\mathcal{K}_2(K) = [K, F\}$.*

PROOF. If F is finite then K is finite too, and $\mathcal{K}_2(K) = 0$ by Remark 5.5. Assume henceforth that F is infinite.

Let $[a, b\} \in [K, K\}$. The idea is to replace $[a, b\}$ by an equivalent symbol with the property $a \in F[b]$, where we can use Lemma 5.1.

Consider the collection of subfields $F[b(a+\alpha b)] \subseteq K$, where $\alpha \in F$. Since K has only finitely many subfields containing F, there are $\alpha_1 \neq \alpha_2 \in F$ such that $L = F[b(a + \alpha_1 b)] = F[b(a + \alpha_2 b)]$. Subtracting, we see that $ab, b^2 \in L$, and so $a^2 = (ab)^2 b^{-2} \in L$.

Now suppose $p = \mathrm{char} F = 2$. Then

$$[a + \alpha_1 b, b\} = [a + \alpha_1 b, b(a + \alpha_1 b)\} = [(a + \alpha_1 b)^2, b(a + \alpha_1 b)\},$$

but $(a + \alpha_1 b)^2 = a^2 + \alpha_1^2 b^2 \in L$, so by Lemma 5.1

$$[a, b\} = [a + \alpha_1 b, b\} - [\alpha_1 b, b\} = [a + \alpha_1 b, b\} + [\alpha_1 b, \alpha_1\} \in [K, F\}.$$

The same trick works for arbitrary p, inspecting the subfield $F[b(a+\alpha b)^{p-1}]$, but technically it is a little more complicated. We give a slightly simpler proof for the case $p \neq 2$.

There must be three scalars $\alpha_1, \alpha_2, \alpha_3 \in F$ such that the three fields $F[\frac{(a+\alpha_i b)^2}{b}] = F[\frac{a^2}{b} + 2\alpha_i a + \alpha_i^2 b]$ are equal. Since the Vandermonde matrix of $\alpha_1, \alpha_2, \alpha_3$ is invertible, this field contains $\frac{a^2}{b}, 2a, b$ (but $2 \neq 0$). Then $a + \alpha_1 b \in F[\frac{b}{(a+\alpha_1 b)^2}]$, and

$$\begin{aligned} [a, b\} &= [a + \alpha_1 b, b\} - [\alpha_1 b, b\} = \\ &= [a + \alpha_1 b, \frac{b}{(a + \alpha_1 b)^2}\} + [\alpha_1 b, \alpha_1\} \in [K, F\}. \end{aligned}$$

□

COROLLARY 5.7. *If K/F is separable of dimension n, then every symbol $[a, b\}$ can be expressed as a sum of at most $n + 1$ symbols from $[K, F\}$.*

PROOF. By the proof of the last theorem, one symbol is needed in order to reach a symbol $[a, b\}$ with $a \in F[b]$, and then by Remark 5.2, $[F[b] : F] \leq n$ symbols suffice. □

If K/F has no intermediate subfield, then Remark 5.2 applies directly, and we never need more than n symbols from $[K, F\}$. The following question is natural.

QUESTION 5.8. *For what extensions K/F are $[K:F]+1$ symbols really needed?*

5.2. The Trace Map. Fix some field extension K/F. By Theorem 3.10, $R_K : \mathcal{K}_2(K) \to {}_p\mathrm{Br}(K)$ defined by $R_K : [a,b\} \to [[a,b)]$ is an isomorphism. We define $\mathrm{res}_{F\to K} : \mathcal{K}_2(F) \to \mathcal{K}_2(K)$ by sending every symbol $[\alpha,\beta\}$ over F to the same symbol over K. Note that this is not necessarily injective, as illustrated by the case when K is the algebraic closure of F. It is easily seen that

$$\mathrm{res}_{F\to K} \circ R_F = R_K \circ \mathrm{res}_{F\to K}, \tag{21}$$

where the restriction in the left hand side is the usual restriction of Brauer groups, $[A] \mapsto [A \otimes_F K]$.

For any separable extension K/F, there is a homomorphism $\mathrm{cor} : \mathrm{Br}(K) \to \mathrm{Br}(F)$ called the **corestriction** (see, e.g., [**30**, Section 7.2]). For $[A] \in \mathrm{Br}(F)$, we have that $\mathrm{cor}(\mathrm{res}_{F\to K}A) \sim A^{\otimes [K:F]}$. Another important property is the **projection formula**, that $\mathrm{cor}[a,\beta)_K = [\mathrm{tr}a,\beta)_F$ and $\mathrm{cor}[\beta,a)_K = [\beta, \mathrm{N}_{K/F}a)_F$ for $a \in K$, $\beta \in F$, where $\mathrm{tr}_{K/F}$ denotes the usual trace map of fields..

We use the usual corestriction of the Brauer groups to define a corestriction map from $\mathcal{K}_2(K)$ to $\mathcal{K}_2(F)$ by

$$\mathrm{cor}_{K/F} = R_F^{-1} \circ \mathrm{cor}_{K/F} \circ R_K. \tag{22}$$

REMARK 5.9. By (21) and (22), $\mathrm{cor}_{K/F} \circ \mathrm{res}_{F\to K} : \mathcal{K}_2(F) \to \mathcal{K}_2(F)$ is multiplication by $[K:F]$.

REMARK 5.10. From Corollary 5.7 it follows that $\mathrm{cor}_{K/F}[a,b\}$ is a sum of no more than $[K:F]+1$ symbols in $\mathcal{K}_2(F)$. Note that P. Mammone [**19**] showed that $[K:F]$ symbols are enough.

Suppose K/F is Galois. For symbols of the form $[a,\beta\}$ ($\beta \in F$), we get from the projection formula (for corestriction of symbol algebras) that

$$\mathrm{cor}_{K/F}[a,\beta\} = R_F^{-1}\mathrm{cor}_{K/F}[a,\beta) = R_F^{-1}[\mathrm{tr}_{K/F}a,\beta) = [\mathrm{tr}_{K/F}a,\beta\}_F.$$

$\mathrm{Gal}(K/F)$ acts on $\mathcal{K}_2(K)$ by $\sigma : [a,b\} \to [\sigma a, \sigma b\}$. We define a trace map $\mathrm{Tr}_{K/F} : \mathcal{K}_2(K) \to \mathcal{K}_2(K)$ by

$$\mathrm{Tr}_{K/F}(u) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(u).$$

REMARK 5.11. Suppose K/F is Galois. Then

$$\mathrm{Tr}_{K/F} = \mathrm{res}_{F\to K} \circ \mathrm{cor}_{K/F}. \tag{23}$$

PROOF. Let $u \in \mathcal{K}_2(K)$. Use Theorem 5.6 to write $u = \sum [a_i, \beta_i\}$, $\beta_i \in F$. Now,

$$\begin{aligned}
\mathrm{res}_{F\to K}\mathrm{cor}_{K/F}(u) &= \mathrm{res}_{F\to K}\mathrm{cor}_{K/F}\sum [a_i,\beta_i\} \\
&= \mathrm{res}_{F\to K}\sum [\mathrm{tr}_{K/F}a_i,\beta_i\}_F \\
&= \sum_i [\mathrm{tr}_{K/F}a_i,\beta_i\}_K \\
&= \sum_i\sum_\sigma [\sigma a_i,\beta_i\}_K \\
&= \sum_\sigma \sigma\left(\sum_i [a_i,\beta_i\}_K\right) \\
&= \sum_\sigma \sigma u = \mathrm{Tr}_{K/F}(u).
\end{aligned}$$

□

THEOREM 5.12. *If K/F is finite Galois, then*

$$\mathrm{cor}_{K/F} : \mathcal{K}_2(K) \longrightarrow \mathcal{K}_2(F)$$

is onto.

PROOF. Let $v \in K$ be an element such that $\mathrm{tr}_{K/F}(v) = 1$ (such an element exists by Remark 1.22). Then for every $\alpha, \beta \in F$,

$$\mathrm{cor}_{K/F}[v\alpha,\beta\} = [\mathrm{tr}_{K/F}(v)\alpha,\beta\} = [\alpha,\beta\}.$$

□

5.3. Quaternions over C_2-fields of Characteristic 2. A field F is a C_n-field if any system of homogeneous equations, with the number of variables greater than the sum of n-powers of the total degrees of the equations, has a non-trivial solution [**12**, Chap. 19]. For example, a field which has transcendence degree n over an algebraically closed field is C_n.

In [**6**, section 6] it is proved that if F is a C_2 field of characteristic 0, then for every central simple algebra A of degree 2^a3^b, we have that $\exp(A) = \mathrm{ind}(A)$.

PROPOSITION 5.13. *Let $p = 2$ or 3. Assume F is a C_2 field with* $\mathrm{char}F = p$. *If A/F is a p-algebra, then* $\exp(A) = \mathrm{ind}(A)$.

PROOF. If $\exp(A) = p$, then $A \sim D_1 \otimes \cdots \otimes D_t$ where D_i are symbol p-algebras. By Step 3 in the Appendix of [**6**] (which is characteristic free), every D_i, D_j has a common splitting field of dimension p over F,

so that $\mathrm{ind}(A) = p$. The induction argument in [**6**] works here too, so the result apply for any exponent p^t. □

Some new cyclicity results for central simple algebras over C_2 fields appear in [**32**].

THEOREM 5.14. *Let K/F be a separable extension of dimension 2, where F is a C_2-field of characteristic 2.*

Every 2-symbol $R = [a, b)$ over K $(a, b \in K)$, can be written as $R \cong [c, \gamma)$, where $c \in K$ and $\gamma \in F$.

PROOF. Let x, y be the standard generators of the 2-symbol $R = F[x, y : x^2 - x = a, y^2 = b, yxy^{-1} = x + 1]$. Write $u = q + rx + sy + txy$. By direct computation, we see that $u^2 \in K$ iff $r = 0$. Note that if $u \notin F$, then $u^2 \in F$ ensures $u \notin K$, since K/F is separable. Let θ be a generator of K/F, and write $q = q_0 + q_1\theta$, $s = s_0 + s_1\theta$, $t = t_0 + t_1\theta$, for $q_0, q_1, s_0, s_1, t_0, t_1 \in F$. Set $q_0 = 0$, so that $u \notin F$ unless $u = 0$. Now compute that

$$u^2 = (q + sy + txy)^2 = q^2 + bst + bs^2 + abt^2,$$

so substituting, the coefficient of θ in u^2 is immediately seen to be a homogeneous quadratic form in the five variables q_1, s_0, s_1, t_0, t_1 over F. Since F is C_2 and $5 > 2^2$, there is a non-trivial solution for $\gamma = u^2 \in F$.

By Remark 4.7.b, there is a $v \in R$ such that $uvu^{-1} = v + 1$, and $R = F[v, u] \cong [c, \gamma)$.

□

REMARK 5.15. Using similar arguments, the same result holds when $charF \neq 2$.

QUESTION 5.16. *Do we really need K/F to be separable?*

5.4. Two Types of Symbols. The special form of p-symbols we used to define cyclic p-algebras of degree p is, of course, a matter of convenience. Other authors (e.g. [**15**], [**36**]) prefer the so-called differential symbols. For example, Teichmüller's result was reproved by Jacobson [**16**] in the differential setting. This short subsection is intended to serve as a quick reference for the two languages and the translations between them.

DEFINITION 5.17.
$[a, b) = F[x, y| \quad x^p - x = a, y^p = b, yxy^{-1} = x + 1]$.
$(\alpha, \beta) = F[u, v| \quad u^p = \alpha, v^p = \beta, vu - uv = 1]$.

The transformation of defining generators is by $x = uv, y = v$ $(u = xy^{-1}, v = y)$, so that

$$[a, b) = (ab^{-1}, b),$$

$$(\alpha, \beta) = [\alpha\beta, \beta) = [\alpha\beta, \alpha^{-1}).$$

The defining relations for $\mathcal{K}_2(F)$ are listed in (7)-(10). The parallel relations for the differential symbols are

$$(a_1 + a_2, b) = (a_1, b) + (a_2, b) \tag{24}$$

$$(a, b_1 b_2) = (ab_1, b_2) + (ab_2, b_1) \tag{25}$$

$$(1, a) = 0 \tag{26}$$

$$(a^p b^{-1}, b) = (ab^{-1}, b) \tag{27}$$

Note that taking $a = 1$ in axiom (25) and using axiom (26), we get the antisymmetry relation

$$(b_1, b_2) = -(b_2, b_1). \tag{28}$$

Inducting on (25) and (24), we get $(a, b^p) = p(ab^{p-1}, b) = 0$. By antisymmetry, (26) is now obsolete.

Thus we can use (24),(25),(27) and (28) as defining relations. In particular, ${}_p\mathrm{Br}(F)$ is now seen to be a quotient group of $F \wedge F$, or even better, of $(F \wedge F)/(F^p \wedge F^p)$.

If $F \subseteq K$, then $[K, F\} = (K, F) = (F, K)$, so Theorem 5.6 reads $(K, K) = (K, F)$ (assuming K/F is separable). The trace of a symbol from $[K, F\}$ or $[F, K\}$ is a symbol. The same is true, of course, for (K, F). The differential symbols parallel to $[F, K\}$ are $\{(\alpha, \beta) : \alpha\beta \in F\}$, for which $\mathrm{cor}_{K/F}(\alpha, \beta) = (\alpha\beta N_{K/F}(\beta)^{-1}, N_{K/F}(\beta))$.

6. Hilbert's Theorem 90 for ${}_p\mathrm{Br}(K)$

Let K/F be a cyclic extension of fields, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Theorem 90 in Hilbert's classical book on Number theory [**13**] asserts that every $a \in K$ with $N_{K/F}(a) = 1$ is of the form $a = \sigma(u)u^{-1}$ $(u \in K)$.

Similarly, every element $a \in K$ with $\mathrm{tr}_{K/F}(a) = 0$ is of the form $a = \sigma(u) - u$ for some $u \in K$.

As mentioned in subsection 3.1, a similar result about the trace map of $\mathrm{K}_2(K)$ (where $\mathrm{char}F$ is prime to $[K:F]$) plays a key role in the proof of the Merkurjev-Suslin theorem.

It should be noted, however, that Hilbert's theorem 90 does not in general hold for relative K_2 groups $\mathrm{K}_2(F)/n\mathrm{K}_2(F) \cong {}_n\mathrm{Br}(F)$. This is discussed and demonstrated in Subsection 6.6.

The main purpose of this section is to study to what extent does Hilbert's theorem 90 apply to ${}_p\mathrm{Br}(K)$. It is trivial that the elements

of the form $(1-\sigma)(r)$ ($r \in {}_p\mathrm{Br}(K)$) are in the kernel of $\mathrm{Tr}_{K/F}$, so we focus on the quotient $\mathrm{Ker}(\mathrm{Tr}_{K/F})/\mathrm{Im}(1-\sigma)$.

In the first subsection we give a very simple computation, which, assuming $[K:F]$ is coprime to p, gives for every $u \in \mathcal{K}_2(K) \cong {}_p\mathrm{Br}(K)$ with $\mathrm{Tr}_{K/F}(u) = 0$, an explicit $v \in \mathcal{K}_2(K)$ such that $u = v - \sigma(v)$.

In the second subsection we rephrase Hilbert's theorem 90 in the context of modules, and give some general elementary results, which show that Hilbert's theorem 90 holds iff the invariant submodule is the image of the trace. Then we dissect the modules in question into pieces, and get a quantitative connection between the 'Hilbert defect' and 'Galois defect' of the module.

The results are applied in the fourth subsection to the group ${}_p\mathrm{Br}(K)$. We discuss the quotient modules defined in the general case, and give some more details for the p-power dimension case. We also show that under very weak hypothesis, Hilbert's theorem 90 does fail for ${}_p\mathrm{Br}(K)$. In Subsection 6.5 we study the invariant subgroup ${}_p\mathrm{Br}(K)^\sigma$, and show that in some cases, invariant p-symbol algebras have special structure. The relations to the Eilenberg-MacLane description of the invariant subgroup of the Brauer group are also discussed.

In the last subsection we use properties of the corestriction to give examples of failures of Hilbert's theorem 90 in ${}_n\mathrm{Br}(K)$ in characteristic prime to n.

6.1. Hilbert's Theorem 90 in the Prime-to-p Case. Suppose $d = [K:F]$ is prime to p.

Let $r \in \mathcal{K}_2(K)$ be an element such that $\mathrm{Tr}_{K/F}(r) = 0$. Since $\mathcal{K}_2(K) = [K, F\}$ (Theorem 5.6), we can write $r = \sum_{i=1}^m [a_i, \beta_i\}$ for $a_i \in K$ and $\beta_i \in F$.

Now note that for every $a \in K$, $\mathrm{tr}_{K/F}(a - d^{-1} \cdot \mathrm{tr}_{K/F}(a)) = 0$, so that for every i, there is some $c_i \in K$ such that $a_i - d^{-1} \cdot \mathrm{tr}_{K/F}(a_i) = \sigma(c_i) - c_i$. An explicit formula for elements in $\mathrm{Ker}(\mathrm{Tr}_{K/F})$ follows. It is probably not new, but we include the short proof here for completeness.

THEOREM 6.1. *Let $r \in \mathcal{K}_2(K)$ satisfy $\mathrm{Tr}_{K/F}(r) = 0$. Write $r = \sum_{i=1}^m [a_i, \beta_i\}$, let c_i be as above, and $u = \sum_{i=1}^m [c_i, \beta_i\}$.*

Then $r = \sigma(u) - u$.

PROOF. Compute

$$\begin{aligned}\sigma(u)-u &= \sigma\left(\sum_{i=1}^{m}[c_i,\beta_i\}\right)-\sum_{i=1}^{m}[c_i,\beta_i\} = \\ &= \sum[\sigma(c_i)-c_i,\beta_i\} = \\ &= \sum[a_i-d^{-1}\cdot\mathrm{tr}_{K/F}(a_i),\beta_i\} = \\ &= \sum[a_i,\beta_i\}-d^{-1}\cdot\sum[\mathrm{tr}_{K/F}(a_i),\beta_i\} = \\ &= r-d^{-1}\cdot\mathrm{Tr}_{K/F}(r)=r.\end{aligned}$$

□

6.2. Elementary Results. Let R be an arbitrary commutative ring, and M an R-module. The idea is to use knowledge of the structure of R to get information on the submodules of M. We identify elements of R with the module homomorphism of multiplication from the left. We are mainly interested in results of the form $\mathrm{Ker}(\phi)\subseteq\mathrm{Im}(\psi)$, where $\pi,\psi\in R$, and the main result will be used later to give necessary and sufficient conditions for the validity of Hilbert's theorem 90 in $\mathcal{K}_2(K)$ where K/F is a cyclic extension.

Let $\pi\in R$ be an element. Trivially,

$$\mathrm{Ker}(\pi)\subseteq\mathrm{Ker}(\pi^2)\subseteq\cdots\subseteq\mathrm{Ker}(\pi^m),$$

and

$$\mathrm{Im}(\pi^m)\subseteq\mathrm{Im}(\pi^{m-1})\subseteq\cdots\subseteq\mathrm{Im}(\pi).$$

PROPOSITION 6.2. *Let* $0<k<m$. *Then* $\mathrm{Ker}(\pi^{k+1})\subseteq\mathrm{Im}(\pi^{m-k})$ *iff* $\mathrm{Ker}(\pi^k)\subseteq\mathrm{Im}(\pi^{m-k+1})$.

PROOF. Suppose $\mathrm{Ker}(\pi^{k+1})\subseteq\mathrm{Im}(\pi^{m-k})$. Let $v\in M$ such that $\pi^k v=0$. Then $\pi^{k+1}v=0$, so by the assumption $v=\pi^{m-k}u$ for some $u\in M$. Compute that $0=\pi^k v=\pi^m u=\pi^{k+1}(\pi^{m-k-1}u)$, so again by the assumption $\pi^{m-k-1}u=\pi^{m-k}w$ for some $w\in M$, and $v=\pi\pi^{m-k-1}u=\pi\pi^{m-k}w\in\mathrm{Im}(\pi^{m-k+1})$.

Now assume $\mathrm{Ker}(\pi^k)\subseteq\mathrm{Im}(\pi^{m-k+1})$, and let $v\in M$ such that $\pi^{k+1}v=0$. Then $\pi v\in\mathrm{Ker}(\pi^k)\subseteq\mathrm{Im}(\pi^{m-k+1})$; write $\pi v=\pi^{m-k+1}u$. It follows that $\pi^k(v-\pi^{m-k}u)=0$, so that $v-\pi^{m-k}u=\pi^{m-k+1}w$ for some $w\in M$, and $v=\pi^{m-k}(u+\pi w)$. □

By induction, we have

COROLLARY 6.3. *The relations*

$$\mathrm{Ker}(\pi^k)\subseteq\mathrm{Im}(\pi^{m+1-k})\qquad(0<k\leq m)$$

are all equivalent. In particular, $\mathrm{Ker}(\pi) \subseteq \mathrm{Im}(\pi^m)$ *iff* $\mathrm{Ker}(\pi^m) \subseteq \mathrm{Im}(\pi)$.

We say that $\phi, \psi \in R$ are coprime if $R\phi + R\psi = R$, that is, there are $\alpha, \beta \in R$ such that $\alpha\phi + \beta\psi = 1$.

LEMMA 6.4. *If* $\phi, \psi \in R$ *are co-prime, then*
a. $M = \mathrm{Im}(\phi) + \mathrm{Im}(\psi)$,
b. $\mathrm{Ker}(\phi) \cap \mathrm{Ker}(\psi) = 0$, *and*
c. $\mathrm{Ker}(\phi) \subseteq \mathrm{Im}(\psi)$ *and* $\mathrm{Ker}(\psi) \subseteq \mathrm{Im}(\phi)$.

PROOF. Write $\alpha\phi + \beta\psi = 1$.
a. Every $x \in M$ can be written as $x = (\alpha\phi+\beta\psi)x = \phi(\alpha x)+\psi(\beta x)$.
b. If $\phi x = \psi x = 0$, then $x = (\alpha\phi + \beta\psi)x = \alpha(\phi x) + \beta(\psi x) = 0$.
c. If $\phi x = 0$, then $x = (\alpha\phi + \beta\psi)x = \psi(\beta x) \in \mathrm{Im}(\psi)$; similarly $\mathrm{Ker}(\psi) \subseteq \mathrm{Im}(\phi)$. □

LEMMA 6.5. *If* $\phi, \psi \in R$ *are co-prime, then*
a. $\mathrm{Im}(\phi\psi) = \mathrm{Im}(\phi) \cap \mathrm{Im}(\psi)$, *and*
b. $\mathrm{Ker}(\phi\psi) = \mathrm{Ker}(\phi) + \mathrm{Ker}(\psi)$.

PROOF. Write $\alpha\phi + \beta\psi = 1$.
a. The inclusion $\mathrm{Im}(\phi\psi) \subseteq \mathrm{Im}(\phi) \cap \mathrm{Im}(\psi)$ is trivial. Let $v = \phi x = \psi y$ for $x, y \in M$. Then $x = (\alpha\phi + \beta\psi)x = \alpha(\phi x) + \beta\psi x = \alpha(\psi y) + \beta\psi x = \psi(\alpha y + \beta x)$, and $v = \phi x = \phi\psi(\alpha y + \beta x) \in \mathrm{Im}(\phi\psi)$.
b. Again $\mathrm{Ker}(\phi\psi) \supseteq \mathrm{Ker}(\phi) + \mathrm{Ker}(\psi)$ is trivial. Let $x \in M$ satisfy $\phi\psi x = 0$. Then $x = (\alpha\phi + \beta\psi)x = (\alpha\phi x) + (\beta\psi x) \in \mathrm{Ker}(\psi) + \mathrm{Ker}(\phi)$ since $\psi(\alpha\phi x) = \alpha(\phi\psi x) = 0$ and $\phi(\beta\psi x) = \beta(\phi\psi x) = 0$. □

REMARK 6.6. The last lemma can be generalized as follows. Say that ϕ, ψ have greatest common divisor if there is some $\chi \in R$ such that $\phi = \chi\phi'$, $\psi = \chi\psi'$, and ϕ', ψ' are co-prime (when R is a domain, ϕ, ψ have greatest common divisor iff $R\phi + R\psi$ is principal).
Suppose ϕ, ψ have greatest common divisor and let $[\phi, \psi] = \chi\phi'\psi'$. It can be shown that
a. $\mathrm{Im}([\phi, \psi]) = \mathrm{Im}(\phi) \cap \mathrm{Im}(\psi)$, and
b. $\mathrm{Ker}([\phi, \psi]) = \mathrm{Ker}(\phi) + \mathrm{Ker}(\psi)$.

The motivation for the following result comes from Proposition 6.20 in subsection 6.4, describing the trace element in some suitable ring R.

COROLLARY 6.7. *Suppose* $\phi, \pi \in R$ *are co-prime, and* $\theta = \pi^m\phi$.
Then $\mathrm{Ker}(\pi) \subseteq \mathrm{Im}(\theta)$ *iff* $\mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi)$.

PROOF. Note that ϕ is coprime to π^m. By Lemma 6.4.c, $\mathrm{Ker}(\pi) \subseteq \mathrm{Im}(\phi)$. Thus, $\mathrm{Ker}(\pi) \subseteq \mathrm{Im}(\theta) \overset{Lemma\ 6.5.a}{=} \mathrm{Im}(\pi^m) \cap \mathrm{Im}(\phi)$ iff $\mathrm{Ker}(\pi) \subseteq$

$\mathrm{Im}(\pi^m)$. This relation holds iff $\mathrm{Ker}(\pi^m) \subseteq \mathrm{Im}(\pi)$ (Corollary 6.3), but since $\mathrm{Ker}(\phi) \subseteq \mathrm{Im}(\pi)$ (again Lemma 6.4.c), it happens iff $\mathrm{Ker}(\pi^m) + \mathrm{Ker}(\phi) \overset{Lemma\ 6.5.b}{=} \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi)$. □

REMARK 6.8. If $\phi, \psi \in R$, $\phi\psi = 0$, then $\mathrm{Im}(\psi) \subseteq \mathrm{Ker}(\phi)$ and $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(\psi)$. If, moreover, ϕ, ψ are co-prime, then $\mathrm{Im}(\psi) = \mathrm{Ker}(\phi)$, $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$, and $M = \mathrm{Im}(\phi) \oplus \mathrm{Im}(\psi)$ (by Lemmas 6.4 and 6.5).

The following proposition shows that in the special case $\theta\pi = 0$ (which will be important in Subsection 6.4), the last corollary is a special case of Corollary 6.3.

PROPOSITION 6.9. *Suppose $\phi, \pi \in R$ are co-prime, $\theta = \pi^m\phi$, and $\theta\pi = 0$.*

Then $\mathrm{Im}(\theta) = \mathrm{Im}(\pi^m) \cap \mathrm{Ker}(\pi)$ *and* $\mathrm{Ker}(\theta) = \mathrm{Ker}(\pi^m) + \mathrm{Im}(\pi)$.

PROOF. Since ϕ is coprime to π^{m+1}, we get from Remarks 6.5 and 6.8 that $\mathrm{Im}(\theta) = \mathrm{Im}(\pi^m) \cap \mathrm{Im}(\phi) = \mathrm{Im}(\pi^m) \cap \mathrm{Ker}(\pi^{m+1})$. But $\mathrm{Im}(\theta) \subseteq \mathrm{Ker}(\pi) \cap \mathrm{Im}(\pi^m) \subseteq \mathrm{Ker}(\pi^{m+1}) \cap \mathrm{Im}(\pi^m)$, so we get an equality.

Similarly, $\mathrm{Ker}(\theta) = \mathrm{Ker}(\pi^m) + \mathrm{Ker}(\phi) = \mathrm{Ker}(\pi^m) + \mathrm{Im}(\pi^{m+1}) \subseteq \mathrm{Ker}(\pi^m) + \mathrm{Im}(\pi) \subseteq \mathrm{Ker}(\theta)$. □

It is comfortable to be able to lift properties of the submodules of given exponent, to the whole module, as in the following proposition. We adopt the notation ${}_eM$ for $\mathrm{Ker}(e)$ for every $e \in R$ (but usually $e \in \mathbb{Z}$).

PROPOSITION 6.10. *Let $\theta, \pi, e, m \in R$ be elements such that $\theta\pi = 0$, and M is e-divisible.*

If

$$ {}_eM \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi), \quad {}_mM \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi), $$

then

$$ {}_{me}M \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi). $$

PROOF. Let $x \in {}_{me}M$ satisfy $\theta x = 0$. Then $ex \in {}_mM \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi)$. Write $ex = \pi y$. By e-divisibility, $y = ey'$ for some $y' \in M$. Now $ex = \pi y = e\pi y'$, so that $e(x - \pi y') = 0$. But also $\theta(x - \pi y') = \theta x - \theta\pi y' = 0$, and thus $x - \pi y' \in {}_eM \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi)$.

It follows that $x \in \mathrm{Im}(\pi)$, as asserted. □

COROLLARY 6.11. *Let $\theta, \pi, e \in R$ be elements such that $\theta\pi = 0$, and M is e-divisible. Let $M_e = {}_eM \cup {}_{e^2}M \cup \ldots$.*

If

$$ {}_eM \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi), $$

then

$$ M_e \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi). $$

PROOF. Show that ${}_{e^i}M \cap \mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi)$ by induction on i. □

Suppose $M = M_1 + M_2$ where M_1, M_2 are submodules. The following result can be used to combine properties of submodules into result on M, even though the assumption on ϕ is very restrictive.

PROPOSITION 6.12. *Suppose $\phi, \psi \in R$ are co-prime, and $\phi\psi = 0$. Then* $\mathrm{Ker}(\phi) = (\mathrm{Ker}(\phi) \cap M_1) + (\mathrm{Ker}(\phi) \cap M_2)$.

PROOF. Write $\alpha\phi + \beta\psi = 1$.

Let $x_1 + x_2 \in M$ where $x_i \in M_i$, and suppose $\phi(x_1 + x_2) = 0$. Compute that $\phi(\beta\psi x_i) = \phi\psi(\beta x_i) = 0$, so that $\beta\psi x_i \in \mathrm{Ker}(\phi) \cap M_i$.

Now $x_1 + x_2 = (\alpha\phi + \beta\psi)(x_1 + x_2) = \alpha\phi(x_1 + x_2) + \beta\psi(x_1 + x_2) = \beta\psi x_1 + \beta\psi x_2 \in (\mathrm{Ker}(\phi) \cap M_1) + (\mathrm{Ker}(\phi) \cap M_2)$. □

6.3. A Quantitative Theory. One of the main results in the last subsection is Corollary 6.7, that if $\phi, \pi \in R$ are co-prime, and $\theta = \pi^m\phi$, then $\mathrm{Ker}(\pi) \subseteq \mathrm{Im}(\theta)$ iff $\mathrm{Ker}(\theta) \subseteq \mathrm{Im}(\pi)$.

In this subsection we add the assumption $\theta\pi = 0$, and strengthen the result to show that $|\mathrm{Ker}\theta/\mathrm{Im}\pi| = |\mathrm{Ker}\pi/\mathrm{Im}\theta|$.

Multiplication by $\phi \in R$ induces the isomorphism $M/\mathrm{Ker}\phi \cong \mathrm{Im}\phi$. Let us generalize this. We use the standard notation

$$\phi^{-1}D = \{v \in M : \phi v \in D\}.$$

REMARK 6.13. Let $B \subseteq A$, $D \subseteq C$ be submodules of M. Multiplication by ϕ induces an isomorphism $\phi : A/B \to C/D$ iff the following conditions hold:

(1) $\phi A \subseteq C$ (the map is into C/D)
(2) $\phi B \subseteq D$ (the map is well defined)
(3) $A \cap \phi^{-1}D \subseteq B$ (the map is one-to-one)
(4) $C \subseteq \phi A + D$ (the map is onto)

From the above assumptions it follows that

$$A \cap \phi^{-1}\phi B \subseteq A \cap \phi^{-1}D \subseteq B \subseteq A \cap \phi^{-1}\phi B$$

and

$$D + \phi A \subseteq C \subseteq D + \phi A.$$

Thus the most general isomorphism possible is

COROLLARY 6.14. *Multiplication by ϕ induces an isomorphism*

$$\phi : A/(A \cap \phi^{-1}D) \longrightarrow (\phi A + D)/D.$$

For convenience, set $\pi^0 = 1$.

Let

$$U_k = \mathrm{Ker}(\pi^k) + \mathrm{Im}\pi,$$
$$L_k = \mathrm{Im}(\pi^k) \cap \mathrm{Ker}\pi.$$

Then

$$\mathrm{Im}\pi = U_0 \subseteq U_1 \subseteq \ldots \subseteq U_m = \mathrm{Ker}(\pi^m) + \mathrm{Im}\pi,$$
$$\mathrm{Ker}\pi = L_0 \supseteq L_1 \supseteq \ldots \supseteq L_m = \mathrm{Im}(\pi^m) \cap \mathrm{Ker}\pi.$$

The following is useful:

REMARK 6.15. We have that

$$U_k = \pi^{-k}(\mathrm{Im}(\pi^{k+1}))$$

and

$$L_k = \pi^k(\mathrm{Ker}(\pi^{k+1})).$$

PROOF. Trivially $\mathrm{Ker}(\pi^k), \mathrm{Im}\pi \subseteq \pi^{-k}\mathrm{Im}(\pi^{k+1})$, so that we have $U_k \subseteq \pi^{-k}\mathrm{Im}(\pi^{k+1})$. Now let $x \in \pi^{-k}\mathrm{Im}(\pi^{k+1})$, then $\pi^k x = \pi^{k+1}y$ for some $y \in M$, and $x = (x - \pi y) + \pi y \in \mathrm{Ker}(\pi^k) + \mathrm{Im}\pi = U_k$.

Likewise, it is trivial that $\pi^k\mathrm{Ker}(\pi^{k+1}) \subseteq \mathrm{Im}(\pi^k), \mathrm{Ker}\pi$, so that $\pi^k\mathrm{Ker}(\pi^{k+1}) \subseteq L_k$. If $x \in L_k$, write $x = \pi^k y$ where $\pi^{k+1}y = \pi x = 0$. Thus $y \in \mathrm{Ker}(\pi^{k+1})$, and $x \in \pi^k\mathrm{Ker}(\pi^{k+1})$. □

THEOREM 6.16. *$U_k/U_{k-1} \cong L_{k-1}/L_k$ $(1 \leq k \leq m)$.*

PROOF. We check that $\pi^{k-1} : U_k/U_{k-1} \to (L_{k-1} + \mathrm{Im}(\pi^k))/\mathrm{Im}(\pi^k)$ is a (well defined) isomorphism. Then

$$\begin{aligned} U_k/U_{k-1} &\cong (L_{k-1} + \mathrm{Im}(\pi^k))/\mathrm{Im}(\pi^k) \\ &\cong L_{k-1}/(L_{k-1} \cap \mathrm{Im}(\pi^k)) \\ &= L_{k-1}/L_k, \end{aligned}$$

and we are done. Let $A = U_k = \mathrm{Ker}(\pi^k) + \mathrm{Im}\pi$ and $D = \mathrm{Im}(\pi^k)$.

By Corollary 6.14, we have to check that $A \cap \pi^{-(k-1)}D = U_{k-1}$, and that $\pi^{k-1}A + D = L_{k-1} + \mathrm{Im}(\pi^k)$.

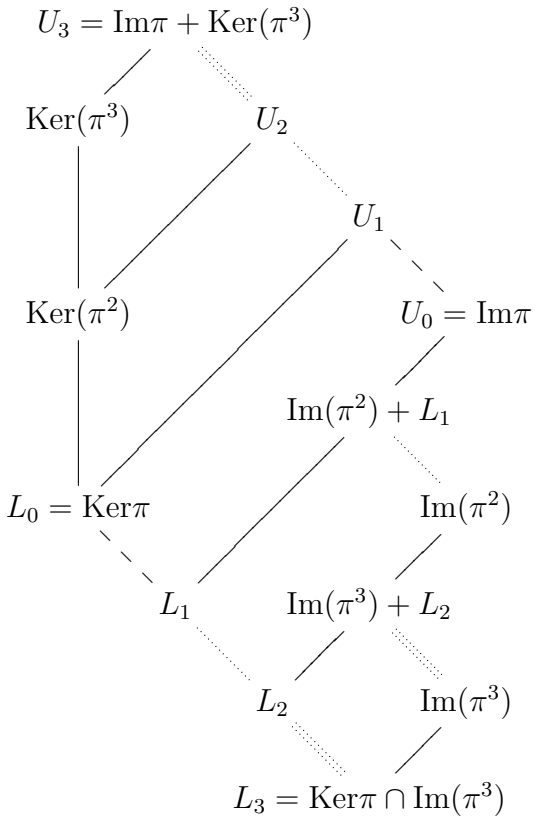
By the remark, $\pi^{k-1}D = U_{k-1} \subseteq A$, so that $A \cap \pi^{-(k-1)}D = U_k \cap U_{k-1} = U_{k-1}$.

Finally $D = \mathrm{Im}(\pi^k) = \pi^{k-1}\mathrm{Im}\pi \subseteq \pi^{k-1}A$, so that

$$\begin{aligned} \pi^{k-1}A + D &= \pi^{k-1}A \\ &= \pi^{k-1}(\mathrm{Ker}(\pi^k) + \mathrm{Im}\pi) = \\ &= \pi^{k-1}(\mathrm{Ker}(\pi^k)) + \pi^{k-1}\mathrm{Im}\pi = L_{k-1} + \mathrm{Im}(\pi^k). \end{aligned}$$

□

As an illustration, here is a very small portion of the lattice of submodules generated by $\mathrm{Ker}(\pi^k)$ and $\mathrm{Im}(\pi^k)$ for $1 \leq k \leq 3$.



COROLLARY 6.17. *The quotient modules U_m/U_0 and L_0/L_m have composition series, such that after reversing the order in one series, we get pairwise isomorphic quotients.*

Combining Proposition 6.9 with Theorem 6.16, we have proved the main result of this subsection, namely

COROLLARY 6.18. *Suppose $\phi, \pi \in R$ are co-prime, $\theta = \pi^m\phi$, and $\theta\pi = 0$. Then*

$$\mathrm{Im}\pi \subseteq \mathrm{Ker}\pi + \mathrm{Im}\pi \subseteq \ldots \subseteq \mathrm{Ker}(\pi^{m-1}) + \mathrm{Im}\pi \subseteq \mathrm{Ker}\theta,$$

$$\mathrm{Ker}\pi \supseteq \mathrm{Im}\pi \cap \mathrm{Ker}\pi \supseteq \ldots \supseteq \mathrm{Im}(\pi^{m-1}) \cap \mathrm{Ker}\pi \supseteq \mathrm{Im}\theta$$

form composition series with isomorphic quotients (in reverse order in which they appear).

In particular, $|\mathrm{Ker}\theta/\mathrm{Im}\pi| = |\mathrm{Ker}\pi/\mathrm{Im}\theta|$.

6.4. Hilbert's Theorem 90 for ${}_p\mathrm{Br}(K)$. Let K/F be a cyclic field extension of degree n, with σ a generator of $\mathrm{Gal}(K/F)$. We do not assume anything on $\mathrm{char}F$.

Abelian groups of exponent p with a σ-action can be viewed as modules over $R = \mathbb{Z}_p[\sigma|\sigma^n = 1]$. Let M be such a module. Later in this subsection we specialize to $M = {}_p\mathrm{Br}(K)$.

From now on, $\Sigma = 1 + \sigma + \cdots + \sigma^{n-1} \in R$ is the trace element, so that left multiplication by Σ induces $\mathrm{Tr}_{K/F} : M \to M$. Also let $\pi = 1 - \sigma$, so that $\Sigma \cdot \pi = 0$, and obviously $\mathrm{Im}(\pi) \subseteq \mathrm{Ker}(\Sigma)$. Hilbert's theorem 90 for M is precisely the statement $\mathrm{Ker}(\Sigma) = \mathrm{Im}(\pi)$.

In this general setup, Theorem 6.1 has the following proof:

PROPOSITION 6.19. *If n is prime to p, then Hilbert's theorem 90 holds for M:*

$$\mathrm{Ker}(\Sigma) = (1 - \sigma)M.$$

PROOF. $\Sigma, 1 - \sigma$ are co-prime since the image n of Σ in $R/\langle 1 - \sigma\rangle$ is invertible. We are done by Lemma 6.4. □

We now factor the trace element in R in the general case. Write $n = [K:F] = p^r d$, where $(p, d) = 1$.

PROPOSITION 6.20. *Let $\pi = 1-\sigma$. The trace element $\Sigma \in R$ factors as $\Sigma = \pi^{p^r-1}\phi$, where ϕ is coprime to π in R. Also $\Sigma \cdot \pi = 0$.*

PROOF. That $\Sigma\pi = \sigma^n - 1 = 0$ is obvious. Work in the preimage $R_1 = \mathbb{Z}_p[\lambda]$ of R: $1 - \lambda^n = (1 - \lambda^d)^{p^r} = (1 - \lambda)^{p^r}(1 + \lambda + \cdots + \lambda^{d-1})^{p^r}$, so that $1 + \lambda + \cdots + \lambda^{n-1} = (1 - \lambda)^{p^r-1}(1 + \lambda + \cdots + \lambda^{d-1})^{p^r}$. The image in R is $\Sigma = \pi^{p^r-1}(1 + \sigma + \cdots + \sigma^{d-1})^{p^r}$.

As before, $\phi = (1+\sigma+\cdots+\sigma^{d-1})^{p^r}$ is coprime to π since the image d^{p^r} in $R/\langle\pi\rangle = \mathbb{Z}_p$ is invertible. □

We define the 'Hilbert defect' of the R-module M as a measure of how badly does Hilbert's theorem 90 fail for M:

$$\mathrm{D_H}(M) = \mathrm{Ker}(\Sigma)/\mathrm{Im}(\pi).$$

The dual quotient (*cf.* Corollary 6.18) is $\mathrm{Ker}(\pi)/\mathrm{Im}(\Sigma)$. The kernel of $\pi = 1 - \sigma$ is simply the invariant subgroup M^σ. We define the 'Galois defect' as the quotient

$$\mathrm{D_G}(M) = M^\sigma/\mathrm{Im}(\Sigma).$$

Now apply Corollary 6.18 to get filtrations of $\mathrm{D_H}(K/F)$ and $\mathrm{D_G}(K/F)$. Recall that $n = [K:F] = p^r d$ where $(p, d) = 1$, and set $m = p^r - 1$. As in subsection 6.3, let

$$L_k = \pi^k(M) \cap M^\sigma,$$

$$U_k = \mathrm{Ker}(\pi^k) + \pi M$$

Then

$$M^\sigma = L_0 \supseteq L_1 \supseteq \ldots \supseteq L_m = \mathrm{Im}(\Sigma),$$
$$\pi M = U_0 \subseteq U_1 \subseteq \ldots \subseteq U_m = \mathrm{Ker}(\Sigma),$$

where the equalities in the right come from Proposition 6.9. Check that $\mathrm{D_H}(M) = U_m/U_0$, while $\mathrm{D_G}(M) = L_0/L_m$.

By Theorem 6.16, the quotients are isomorphic after reversing order: $U_k/U_{k-1} \cong L_{k-1}/L_k$ $(1 \leq k \leq m)$.

COROLLARY 6.21. *$\mathrm{D_H}(M)$ and $\mathrm{D_G}(M)$ have decomposition series with isomorphic quotients after reversing order in one of them.*

In particular, $\mathrm{D_H} = 1$ *iff* $\mathrm{D_G} = 1$.

If $[K:F]$ is prime to p, then by Proposition 6.19, $\mathrm{D_H}(M) = 1$ and $\mathrm{D_G}(M) = 1$. On the other extent we have that if $n = [K:F] = p^r$, then $\pi^n = 0$ and $\mathrm{Im}(\pi^{n-k}) \subseteq \mathrm{Ker}(\pi^k)$ always holds, so by Corollary 6.3 we have that $\mathrm{D_H}(M)$ and $\mathrm{D_G}(M)$ vanish iff $\mathrm{Ker}(\pi^k) = \mathrm{Im}(\pi^{n-k})$ for some $0 < k < n$.

REMARK 6.22. If $p = 2$ and $n = [K:F] = 2$, then $\mathrm{D_H}(M) = \mathrm{D_G}(M)$ since $\pi = \mathrm{Tr}_{K/F}$ (and the above filtration has only one level).

EXAMPLE 6.23. A possible application of the above results is for the module $M = {}_p\mathrm{Br}(K)$. Note that $\mathrm{Br}(K)$ is a module over $\mathbb{Z}[\sigma|\sigma^n = 1]$ (where σ acts on $\mathrm{Br}(K)$ by the action on the base field, and $\mathbb{Z}$ acts by exponentiation). The kernel of $p \in \mathbb{Z}[\sigma]$ is the subgroup of classes of exponent dividing p, i.e. $M = {}_p\mathrm{Br}(K)$. As required, this is a module over $R = \mathbb{Z}_p[\sigma|\sigma^n = 1]$.

In the special case $M = {}_p\mathrm{Br}(K)$ we write $\mathrm{D_H}(K/F)$ instead of $\mathrm{D_H}({}_p\mathrm{Br}(K))$, and similarly for $\mathrm{D_G}$.

Corollary 6.21 gives corresponding filtrations for the quotients

$$\mathrm{D_H}(K/F) = \mathrm{Ker}(\mathrm{Tr}_{K/F})/\pi\,{}_p\mathrm{Br}(K)$$

and

$$\mathrm{D_G}(K/F) = {}_p\mathrm{Br}(K)^\sigma/\mathrm{Im}(\mathrm{Tr}_{K/F}).$$

$\mathrm{D_G}(K/F)$ can be given a new form if $\mathrm{char}F = p$.

REMARK 6.24. If $\mathrm{char}F = p$, then $\mathrm{cor}_{K/F} : {}_p\mathrm{Br}(K) \to {}_p\mathrm{Br}(F)$ is onto by Corollary 5.12. Thus $\mathrm{Im}(\mathrm{Tr}_{K/F}) = \mathrm{Im}(\mathrm{res}_{F\to K} \circ \mathrm{cor}_{K/F}) = \mathrm{Im}(\mathrm{res}_{F\to K})$, and this group is denoted by $[F,F\} \subseteq \mathcal{K}_2(K) = [K,F\}$ (the last equality is Theorem 5.6).

In this case

$$\mathrm{D_H}(K/F) = \mathrm{Ker}(\mathrm{Tr}_{K/F})/[F,F\}.$$

We can show that very frequently $\mathrm{D_G}$, and thus also $\mathrm{D_H}$, are non-trivial. Recall that for an extension F_1/F, $\mathrm{Br}(F_1/F)$ denotes the kernel of $\mathrm{res}_{F\to[1}/F] : \mathrm{Br}(F) \to \mathrm{Br}(F_1)$, that is, the subgroup of $\mathrm{Br}(F)$ consisting of algebras split by F_1.

THEOREM 6.25. *Assume* $\mathrm{char}F = p$. *Let* K/F *be a cyclic extension, and* $F \subset F_1 \subseteq K$ *the subfield of dimension* p *over* F. *If* $\mathrm{Br}(F_1/F) \neq 1$, *then* $\mathrm{D_G}(K/F) \neq 1$, *that is, the map*

$$\mathrm{res}_{F\to K} : {}_p\mathrm{Br}(F) \to {}_p\mathrm{Br}(K)^\sigma$$

is not onto.

By Corollary 6.21, we also have $\mathrm{D_H}(K/F) \neq 1$, so that Hilbert's theorem 90 fails in this case. We need two lemmas before a proof of the theorem is given.

LEMMA 6.26. *Let* $A \in \mathrm{Br}(K)$. *For all the algebras* B *over* F *with* $\mathrm{res}_{F\to K}B = A$, *the number* $\mathrm{lcm}\{\exp(B), [K:F]\}$ *is a constant.*

PROOF. Let $n = [K:F]$. Suppose the algebras B_1, B_2 over F have the same restriction to K. Then $B' = B_2 \otimes {B_1}^{\mathrm{op}}$ is split by K, so that

$$\exp(B_2) = \exp(B_1 \otimes B') \,|\, \mathrm{lcm}\{\exp(B_1), \exp(B')\} \,|\, \mathrm{lcm}\{\exp(B_1), n\},$$

and also

$$\mathrm{lcm}\{\exp(B_2), n\} \,|\, \mathrm{lcm}\{\exp(B_1), n\}.$$

□

Note that the same result holds with $\exp(\mathrm{Br}(K/F))$ instead of $[K:F]$.

LEMMA 6.27. *Let* L/F *be a cyclic extension of degree* p^{t+1} *with* $\mathrm{Gal}(L/F) = \langle\sigma\rangle$, *and let* $b \in F$. *Set* $F_1 = L^{\sigma^p}$, *an intermediate subfield of dimension* p *over* F. *Then the cyclic algebra* $C = (L/F, \sigma, b)$ *satisfies*

$$C^{\otimes p^t} \sim (F_1/F, \sigma, b).$$

PROOF. Let $\omega = (\alpha_0, \ldots, \alpha_t)$ denote the Witt vector (over F) corresponding to L, so that $C = [\omega, b)$ — a symbol p-algebra of degree p^{t+1} (see [**20**] for some basic properties of such symbols). Then

$$\begin{aligned} C^{\otimes p^t} &= [(\alpha_0, \ldots, \alpha_t), b)^{\otimes p^t} \\ &\sim [p^t(\alpha_0, \ldots, \alpha_t), b) \\ &= [(0, \ldots, 0, \alpha_0), b) \\ &\sim [\alpha_0, b), \end{aligned}$$

the last symbol is of degree p over F, and contains $F_1 = F[x|x^p - x = \alpha_0]$. □

PROOF OF THEOREM 6.25. Let K_1 be a subfield of K such that $[K:K_1]$ is prime to p, and $n_1 = [K_1:F]$ is a power of p. Then $F \subset F_1 \subseteq K_1 \subseteq K$.

Let L/K_1 be an extension of dimension p over K_1, which is cyclic over F (such an extension always exist, by Corollary 1.29). Let σ be a generator of $\mathrm{Gal}(L/F)$. Pick some $1 \neq u \in \mathrm{Br}(F_1/F)$, then u is the class of an algebra containing F_1 as a maximal subfield, which is thus of the form $(F_1/F, \sigma, b)$ for some $b \in F$.

Consider the cyclic algebra $C = (L/F, \sigma, b)$. By Lemma 6.27, $C^{\otimes n_1} \sim (F_1/F, \sigma, b)$ which is non split by the choice of b. Thus $\exp(C) = pn_1$.

Let $A = \mathrm{res}_{F\to K}C$. Since C contains K_1 as a subfield and is of degree pn_1, we have that $\exp(A) \mid \mathrm{ind}(A)$ divides p, and so $[A] \in {}_p\mathrm{Br}(K)$, and is obviously invariant. Let $B \in \mathrm{Br}(F)$ such that $\mathrm{res}_{F\to K}B = A$. By Lemma 6.26, we have that $n_1 p = \exp(C)$ divides $(\exp(C), [K:F]) = (\exp(B), [K:F])$, but since $n_1 p$ does not divide $[K:F]$, we see that $\exp(B)$ cannot divide $[K:F]$, and so cannot be equal to p.

Thus A is not a restriction from ${}_p\mathrm{Br}(F)$, as asserted. □

We now move into a more complicated setting. The results below can be formulated for general modules of exponent p, but we prefer to specialize to $\mathrm{char}F = p$ and $M = \mathcal{K}_2(K)$.

The fact that Σ is a power of π when $n = p^r$ enables us to go a little deeper in that case. Let $F \subseteq L \subseteq K$ be an intermediate field, where $[L:F] = n_1$ and $[K:L] = n_2$ are powers of p. As before $\pi = 1-\sigma$ where $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, so that $\mathrm{Gal}(K/L) = \langle\sigma^{n_2}\rangle$.

Agree that $[L, F\} \subseteq \mathcal{K}_2(K)$ denotes the image of $\mathrm{res}_{L\to K} : \mathcal{K}_2(L) \to \mathcal{K}_2(K)$ (this is a different object than $\mathcal{K}_2(L)$). $\mathrm{D_H}(L/F)$ is a quotient of submodules of $\mathcal{K}_2(L)$. We can generalize it to measure the quotient of submodules of $[L, F\} \subseteq \mathcal{K}_2(K)$, by defining

$$\mathrm{D_H}(K, L/F) = \{u \in [L, F\} : \mathrm{Tr}_{L/F}u = 0\}/\pi[L, F\},$$

so that the usual Hilbert defect is $\mathrm{D_H}(K/F) = \mathrm{D_H}(K, K/F)$.

THEOREM 6.28. *If $[K:F]$ is a p power and $F \subseteq L \subseteq K$, then*

$$\mathrm{D_H}(K, L/F) = \frac{\mathrm{Ker}(\mathrm{Tr}_{L/F})}{\pi[L, F\}} \cong \frac{\mathrm{Ker}(\mathrm{Tr}_{K/F})}{\mathrm{Ker}(\mathrm{Tr}_{L/F}) + \pi[K, F\}}.$$

In particular, $\mathrm{D_H}(K, L/F)$ *is a quotient of* $\mathrm{D_H}(K/F)$.

PROOF. Similarly to the definition of U_k, we set

$$V_k = \{v \in [L, F\} : \pi^k v = 0\} + \pi[L, F\}.$$

Since $n_2 = [K:L]$ is a p power, $\Sigma_{K/L} = 1 + \sigma^{n_1} + \cdots + \sigma^{n_1(n_2-1)} = (1-\sigma^{n_1})^{n_2-1}$. But n_1 is a p power too, so that $(1-\sigma^{n_1}) = (1-\sigma)^{n_1}$ and $\Sigma_{K/L} = \pi^{n_1(n_2-1)}$. Thus multiplication by $\pi^{n_1(n_2-1)}$ induces the the trace map $\mathrm{Tr}_{K/L}$ from $\mathcal{K}_2(K)$, onto $[L,F\}$.

It follows that $\Sigma_{K/L} \cdot U_{n_1(n_2-1)+k} = V_k$ for $0 \le k < n_1$. Fortunately, $\mathrm{Ker}(\Sigma_{K/L}) \subseteq U_{n_1(n_2-1)}$ by definition of $U_{n_1(n_2-1)}$, so that multiplication by $\Sigma_{K/L}$ maps

$$U_{n_1n_2-1}/U_{n_1(n_2-1)} = \mathrm{Ker}(\mathrm{Tr}_{K/F})/(\mathrm{Ker}_{K/L} + \pi[K,F\})$$

(a quotient of $\mathrm{D_H}(K/F) = \mathrm{Ker}(\mathrm{Tr}_{K/F})/\pi[K,F\}$) bijectively to

$$V_{n_1-1}/V_0 = \mathrm{Ker}(\mathrm{Tr}_{L/F})/\pi[L,F\} = \mathrm{D_H}(K,L/F).$$

□

For the dual (and much easier) result on $\mathrm{D_G}$, define $\mathrm{D_G}(K,L/F)$ to be the Galois defect of $[L,F\}$ over $[F,F\}$ inside $\mathcal{K}_2(K)$:

$$\mathrm{D_G}(K,L/F) = [L,F\}^\sigma/[F,F\}.$$

PROPOSITION 6.29. $\mathrm{D_G}(K,L/F)$ *is a submodule of* $\mathrm{D_G}(K/F)$.

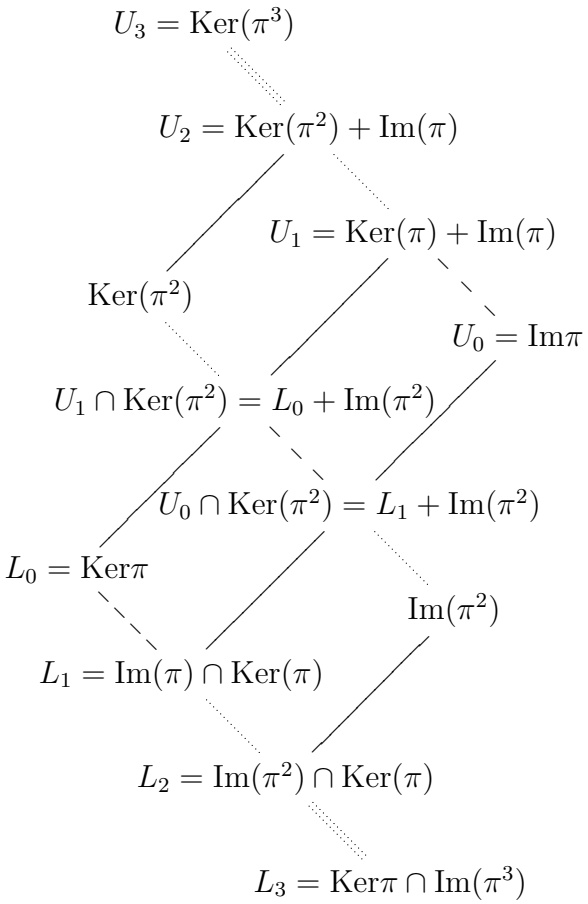
PROOF. By definition

$$\mathrm{D_G}(K,L/F) = [L,F\}^\sigma/[F,F\} \subseteq [K,F\}^\sigma/[F,F\}.$$

□

Note that in the decomposition series of length $n-1$ of $\mathrm{D_H}(K/F)$, the upper n_1-1 components correspond to $\mathrm{D_H}(K,L/F)$. Likewise, in the decomposition of $\mathrm{D_G}(K/F)$ to isomorphic (in reverse order) quotients, the lower n_1-1 components belong to $\mathrm{D_G}(K,L/F)$.

We end this subsection with a description of $\mathrm{D_H}(K,K/L)$ in the special case $[K:L] = [L:F] = 2$, $p = 2$. Letting $\pi = 1-\sigma$, we have that $\pi^4 = 0$, $\mathrm{Tr}_{K/F} = 1+\sigma+\sigma^2+\sigma^3 = \pi^3$, $\mathrm{Tr}_{L/F} = \pi$, and $\mathrm{Tr}_{K/L} = 1-\sigma^2 = \pi^2$. The (modular) lattice generated by the submodules $\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(\pi^2) \subseteq \mathrm{Ker}(\pi^3)$ and $\mathrm{Im}(\pi^3) \subseteq \mathrm{Im}(\pi^2) \subseteq \mathrm{Im}(\pi)$ of $\mathcal{K}_2(K)$ is similar to that of page 46:



Let $Q_k = L_k/L_{k+1}$, $k = 0, 1, 2$. $\mathrm{D_G}(K/F)$ has decomposition series with quotients Q_2, Q_1, Q_0, and the quotients in $\mathrm{D_H}(K/F)$ are Q_0, Q_1, Q_2. $\mathrm{D_G}(K/L) = \mathrm{Ker}(1-\sigma^2)/\mathrm{Im}(\mathrm{Tr}_{K/L}) = \mathrm{Ker}(\pi^2)/\mathrm{Im}(\pi^2) = \mathrm{D_H}(K/L)$, and this module has decomposition series with quotients Q_1, Q_0, Q_1.

By describing the lattice of submodules for general cyclic extension K/F with $[K\!:\!F] = p^r$, it can be shown that $\mathrm{D_H}(K/L)$ $(F \subseteq L \subseteq K)$ will always have a decomposition series whose quotients come from the standard quotients L_k/L_{k+1} of $\mathrm{D_H}(K/F)$.

6.5. The Invariant Subgroup ${}_p\mathrm{Br}(K)^\sigma$. Let K/F be a cyclic extension of fields, $n = [K\!:\!F]$, and σ a generator of $\mathrm{Gal}(K/F)$. Also let $R = \mathbb{Z}_p[\sigma|\sigma^n = 1]$, $\pi = 1 - \sigma$, and $\Sigma = 1 + \sigma + \cdots + \sigma^{n-1} \in R$. $[K, F\} = \mathcal{K}_2(K) \cong {}_p\mathrm{Br}(K)$ is a natural R-module, and multiplication by Σ induces the map $\mathrm{Tr}_{K/F}$.

As seen in the last subsection (Corollary 6.21), the R-module

$$\mathrm{D_H}(K/F) = \mathrm{Ker}(\mathrm{Tr}_{K/F})/\pi[K,F\}$$

which measures the failure of Hilbert's theorem 90 for $\mathcal{K}_2(K) \cong {}_p\mathrm{Br}(K)$ has a composition series which, after reversing the order of quotients, is the same as that of $\mathrm{D_G}(K/F) = \mathcal{K}_2(K)^\sigma/[F,F\}$.

In this subsection we study the invariant subgroup ${}_p\mathrm{Br}(K)^\sigma = \mathcal{K}_2(K)^\sigma$. We describe a special subgroup of $\mathcal{K}_2(K)^\sigma$, and study some generic examples.

It was proved by Eilenberg-MacLane [**11**] that for every Galois extension K/F (regardless of char$F$), the quotient $\mathrm{Br}(K)^\sigma/\mathrm{Im}(\mathrm{res}_{F\to K})$ embeds into $H^3(\mathrm{Gal}(K,F),K^*)$. If K/F is cyclic then $H^3 = 1$, and so every invariant class in $\mathrm{Br}(K)$ is a restriction from $\mathrm{Br}(F)$. It should be emphasized that the relation to the relative invariant groups ${}_n\mathrm{Br}(K)$ is not too tight: the fact that an invariant $[A] \in {}_n\mathrm{Br}(K)$ is a restriction, does not show that it is a restriction from ${}_n\mathrm{Br}(F)$. In general $A = \mathrm{res}_{F\to K}B$ with $\exp(A) \,|\, \exp(B)$, and, in view of Theorem 6.25, one should not expect to have an equality.

The situation in prime-to-p extensions do not reflect the general case:

Proposition 6.30. *If $n = [K:F]$ is prime to p, then $\mathcal{K}_2(K)^\sigma = [F,F\}$.*

Proof. By Theorem 6.1 we have that $\mathrm{D_H}(K/F) = 1$, so that $\mathrm{D_G}(K/F) = 1$ too. □

Recall that $H_{K/F} = \{a \in K : \sigma(a) - a \in \wp(K)\}$ (Subsection 1.3), where $\wp(K) = \{\alpha^p - \alpha : \alpha \in K\}$. $H_{K/F}/(F + \wp(K)) \cong \mathbb{Z}_p$ if p divides n (Theorem 1.23), and $H_{K/F} = F + \wp(K)$ otherwise (Corollary 1.18). We assume that p divides $[K:F]$.

Proposition 6.31. *We have that $[H_{K/F},F\} \subseteq \mathcal{K}_2(K)^\sigma$. Also, every class of $[H_{K/F},F\}/[F,F\}$ has a representative which is one symbol.*

Proof. Let $a \in H_{K/F}$, $\beta \in F$. Then $\sigma(a) - a = \wp(k)$ for some $k \in K$, and $\sigma([a,\beta)) = [a + \wp(k), \beta) = [a,\beta)$.

Recall that there is some $a_0 \in K$ such that $H_{K/F} = F + \wp(K) + \mathbb{Z}_p a_0$ (Proposition 1.23). Thus for every $a \in H_{K/F}$, we have that $a = ja_0 + \wp(k) + \alpha$ for some $j \in \mathbb{Z}_p$, $k \in K$ and $\alpha \in F$, so for every $\beta \in F$ we can write $[a,\beta\} = [ja_0 + \alpha, \beta\} \equiv [a_0, \beta^j\} \bmod [F,F\}$. Sum of such symbols can thus be given the same form. □

From the proof it follows that the map $\beta \mapsto [a_0,\beta\} + [F,F\}$ from F^* to $[H_{K/F},F\}$ is onto, so that $[H_{K/F},F\}/[F,F\}$ is a quotient group of F^*.

REMARK 6.32. By Corollary 1.15, if $a \in H_{K/F}$, then for every $x \in [a,\beta)$ such that $x^p - x = a$, we have that $K[x]$ is Galois over F.

By Theorem 5.6, ${}_p\mathrm{Br}(K)$ is generated by the symbol algebras $[a,\beta)$ where $a \in K$, $\beta \in F$. We now study an invariant algebra of this form. Again we emphasize that by the Eilenberg-MacLane result, $[a,\beta)$ is the restriction of some algebra B over F, which has exponent bounded by $p[K:F]$. Essentially we ask if it is a restriction of an algebra of exponent p (or even better — of index p).

Let $a \in K$, $\beta \in F$, and $R = [a,\beta) \in {}_p\mathrm{Br}(K)^\sigma$.

Let x, y be a SCOG (Definition 4.1) of $[a,\beta)$, and u', y' a SCOG of $[\sigma(a),\beta)$. We may assume this is the same algebra, so that $u', y' \in [a,\beta)$. Now, $F[y] \cong F[y']$, so there is a conjugation that carries y' to y; let u be the image of u' under this conjugation. Now extend σ (the generator of $\mathrm{Gal}(K/F)$) to an automorphism of R, by $\sigma(x) = u$ and $\sigma(y) = y$ (this can be done since the defining relations $x^p - x = a, y^p = \beta$ and $yxy^{-1} = x + 1$, are preserved). In this context it is worth mentioning that a central simple algebra over F is invariant iff the automorphisms of K over F can be extended to automorphisms of A ([**10**, Section 23, (12)]).

We assume henceforth that $p \mid n = [K:F]$.

PROPOSITION 6.33. *Suppose $a \notin \wp(K)$ (otherwise $[a,\beta)$ is split), and let $x, y, u \in R$ be as above.*

If $\sigma^n(x) \in K[x]$, then $[a,\beta\} \in [H_{K/F}, F\}$ (moreover, we can write $[a,\beta\} = [\alpha,\beta\}$ for $\alpha \in H_{K/F}$).

PROOF. From Lemma 4.8 it follows that $u = \sigma(x) = x + \gamma_0 + \gamma_1 y + \cdots + \gamma_{p-1} y^{p-1}$ for $\gamma_i \in K$. Now compute that $\sigma^n(x) = x + \mathrm{tr}_{K/F}(\gamma_0) + \cdots + \mathrm{tr}_{K/F}(\gamma_{p-1}) y^{p-1}$, but since σ^n acts trivially on K, we have that $\sigma^n(x)$ satisfies $\wp(\sigma^n(x)) = \sigma^n(\wp(x)) = a = \wp(x)$. By the assumption $\sigma^n(x)$ and x commute, so that $\wp(\sigma^n(x) - x) = 0$ and it follows that $\sigma^n(x) = x + j$ for some $j \in \mathbb{Z}_p$. Thus $\mathrm{tr}_{K/F}(\gamma_i) = 0$ for every $i > 0$. Use this to write $\gamma_i = \delta_i - \sigma\delta_i$ $(i > 0)$, and let $z = x + \delta_0 + \cdots + \delta_{p-1} y^{p-1}$ ($\delta_0 \in K$ can be arbitrary).

Compute that $\sigma(z) = z + (\gamma_0 + \sigma\delta_0 - \delta_0)$. (If $j = 0$, z could be made an element of R^σ). Set $\alpha = \wp(z) = a + \delta_0^p - \delta_0 + \delta_1^p \beta + \cdots + \delta_{p-1}^p \beta^{p-1}$, and compute that $\sigma(\alpha) - \alpha = \wp(\gamma_0 + \sigma\delta_0 - \delta_0)$. Thus $\alpha \in H_{K/F}$.

Since z, y form a SCOG of $[\alpha,\beta)$, we are done. □

REMARK 6.34. If, in the above setting, $\sigma^n(x) = x$, then $[a,\beta\} = [\alpha,\beta\}$ for $\alpha \in F$. In particular, $[a,\beta)_K = [\alpha,\beta)_F \otimes_F K$.

PROOF. In the above computations, we have $j = \sigma^n(x) - x = 0$, so that $\mathrm{tr}_{K/F}(\gamma_0) = 0$ and we can choose $\delta_0 \in K$ such that $\sigma(\alpha) = \alpha$ and $\alpha \in F$. This completes the proof.

The fact that σ extends to an automorphism of R *of the same order*, enables us to give another proof. The invariant subalgebra R^σ is an F-subalgebra of R, such that $R \cong R^\sigma \otimes_F K$ [**30**, 7.2.14]. Counting dimensions, $\deg(R^\sigma/F) = p$. Since $y \in R^\sigma$ satisfies $y^p \in F$, we can apply Albert's Theorem [**1**, VII.24], and find some $z \in R^\sigma$ such that $\alpha = z^p - z \in F$, $yz = zy + y$. Then $R^\sigma \cong [\alpha, \beta)_F$ and we have $[a, \beta) \cong [\alpha, \beta)_F \otimes_F K = [\alpha, \beta)_K$. □

We illustrate the method in the last remark by an example.

EXAMPLE 6.35. Let k be a field of characteristic 2, λ_1, λ_2 transcendental over k, $K = k(\lambda_1, \lambda_2)$, $\sigma : K \to K$ the automorphism defined by $\sigma : \lambda_1 \leftrightarrow \lambda_2$, and $F = K^\sigma$.

Then $r = [\lambda_1, \lambda_1 + \lambda_2\}$ is σ-invariant, for $[\lambda_1, \lambda_1 + \lambda_2\} = [\lambda_2, \lambda_1 + \lambda_2\}$. Taking a SCOG x, y for $R = [\lambda_1, \lambda_1 + \lambda_2)$ (so that $x^2 - x = \lambda_1, y^2 = \lambda_1 + \lambda_2$ and $yxy^{-1} = x + 1$), we look for $u \in R$ such that $yuy^{-1} = u + 1$ and $u^2 - u = \lambda_2$. Writing $u = x + \gamma_0 + \gamma_1 y$, it is easy to guess $u = x + y$.

Then σ is extended to an automorphism of R by $\sigma : x \mapsto u, y \mapsto y$, so we compute that $\sigma^2(x) = \sigma(u) = x$. Applying the zero-trace argument of Remark 6.34, we find out that $\lambda_1 = \frac{\lambda_1\lambda_2}{\lambda_1+\lambda_2} + \left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)^2 (\lambda_1 + \lambda_2)$, so that

$$[\lambda_1, \lambda_1 + \lambda_2\} = [\frac{\lambda_1\lambda_2}{\lambda_1 + \lambda_2}, \lambda_1 + \lambda_2\} \in [F, F\}.$$

Note that in this example $\mathrm{Gal}(K[x]/F) = \mathbb{Z}_2^2$ (by Theorem 1.19, as $x^2 - x \in F + \wp(K)$).

The next example is generic for $[H_{K/F}, F\}$, and we suspect it does not belong to $[F, F\}$.

EXAMPLE 6.36 (A generic element of $[H_{K/F}, F\}$). Let k be a field of characteristic 2, μ, η transcendental variables over k, and $K = k(\mu, \eta)$. Define $\sigma \in Aut(K)$ by $\sigma : \mu \mapsto \mu + 1$, $\sigma : \eta \mapsto \eta$, and let $F = K^\sigma$.

Let $a = \mu^2(1 - \mu)$. Then $a \in H_{K/F}$, since $\sigma(a) - a = \wp(\mu)$. And indeed, $r = [a, \eta\}$ is invariant: $\sigma(r) - r = [\sigma(a) - a, \eta\} = [\mu - \mu^2, \eta\} = 0$.

Note that $a \notin F + \wp(K)$ (for $\mathrm{tr}(\mu) = 1$, *cf.* Theorem 1.23). Thus if $x \in [a, \eta)$ satisfies $x^2 - x = a$, then $\mathrm{Gal}(K[x]/F) \cong \mathbb{Z}_4$.

6.6. Remarks on Corestriction. We make some remarks on the corestriction in Brauer groups for cyclic extensions, and use them to show that Hilbert's theorem 90 does fail for the Brauer groups.

PROPOSITION 6.37. *Let K/F be a cyclic extension of odd dimension n, such that F has n-roots of unity.*

Then $\mathrm{cor}_{K/F} : {}_n\mathrm{Br}(K) \to {}_n\mathrm{Br}(F)$ is onto $\mathrm{Br}(K/F)$.

PROOF. Let $u \in \mathrm{Br}(F)$ be a class split by K, then some algebra $A \in u$ has K as a maximal subfield. Writing $K = F[\alpha|\alpha^n = a]$, we see that A is a cyclic algebra $A = (a,b)_{n;F}$ for some $b \in F$. The cyclic algebra $(\alpha,b)_{n;K}$ over K satisfies $\mathrm{cor}_{K/F}(\alpha,b)_{n;K} = (N_\sigma(\alpha),b)_{n;F} = ((-1)^{n-1}a,b)_{n;F} = (a,b)_{n;F}$. □

If $[K:F] = 2$ and K/F is generated by $\alpha = \sqrt{1+t^2}$ for some $t \in F$, then $a = \alpha^2 = N_{K/F}(\alpha^2 + t\alpha)$ is a norm, so that $\mathrm{cor}_{K/F}$ covers $\mathrm{Br}(K/F)$ by the same argument.

However, this result is not true for $[K:F] = 2$ in general:

EXAMPLE 6.38. The class of the standard quaternions $[\mathbb{H}] \in \mathrm{Br}(\mathbb{C}/\mathbb{R})$ is not a corestriction from $\mathrm{Br}(\mathbb{C}) = 1$.

More can be said if $\mathrm{Br}(K) = 1$.

COROLLARY 6.39. *Let K/F be a (solvable) Galois extension of odd dimension $n = [K:F]$. Suppose F has n-roots of unity.*

If $\mathrm{Br}(K) = 1$, then $\mathrm{Br}(F) = 1$.

PROOF. By induction we may assume K/F is cyclic.

Let $u \in \mathrm{Br}(F)$, then $\mathrm{res}_{F\to K}(u) \in \mathrm{Br}(K) = 1$, so that $u \in \mathrm{Br}(K/F)$. By the proposition, u is a corestriction from $\mathrm{Br}(K) = 1$, so that $u = [F]$. □

Note that if $F_0 \subseteq F$, then $\mathrm{Br}(F_0) = \mathrm{Br}(F/F_0)$ since $\mathrm{Br}(F) = 1$.

Here is a diagram of the groups involved in the next setting.

$$\begin{array}{ccccccc} & & & & \mathrm{Br}(K) & & \\ & & & & \downarrow{\scriptstyle \mathrm{cor}_{K/F}} \quad \searrow{\scriptstyle \mathrm{Tr}_{K/F}} & & \\ 0 & \longrightarrow & \mathrm{Br}(K/F) & \longrightarrow & \mathrm{Br}(F) & \xrightarrow{\mathrm{res}_{F\to K}} & \mathrm{Br}(K)^\sigma \end{array}$$

PROPOSITION 6.40. *Let K/F be a cyclic extension of odd dimension n, $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, such that F has n-roots of unity.*

If $\mathrm{Br}(K/F) \neq 1$ then Hilbert's theorem 90 does not hold for ${}_n\mathrm{Br}(K)$ over ${}_n\mathrm{Br}(F)$, that is, there are $u \in {}_n\mathrm{Br}(K)$ with zero trace (where $\mathrm{Tr}_{K/F} = \mathrm{res}_{F\to K} \circ \mathrm{cor}_{K/F}$), which are not of the form $u = (1-\sigma)v$ for any $v \in \mathrm{Br}(K)$.

PROOF. Let $1 \neq [A] \in \mathrm{Br}(F)$ be split by K. By proposition 6.37 one can write $[A] = [\mathrm{cor}_{K/F}(A_1)]$. Then

$$\mathrm{Tr}_{K/F}([A_1]) = \mathrm{res}_{F\to K}\mathrm{cor}_{K/F}[A_1] = \mathrm{res}_{F\to K}[A] = 0.$$

Assuming Hilbert's theorem 90 holds, we can write $[A_1] = (1-\sigma)[A_2]$ for some $[A_2] \in \mathrm{Br}(K)$; but then

$$[A] = [\mathrm{cor}_{K/F}(A_1)] = [\mathrm{cor}_{K/F}(A_2)] - [\mathrm{cor}_{K/F}(\sigma A_2)] = 0,$$

a contradiction. □

Suppose char$F = 0$ and F has all the roots of unity. By Merkurjev-Suslin theorem, ${}_n\mathrm{Br}(K) \cong \mathrm{K}_2(K)/n\mathrm{K}_2(K)$. Let u denote an element in $\mathrm{K}_2(K)$ corresponding to $[A]$ of the proposition; we have chosen A such that $Tr_{K/F}(u) \equiv 0$ in the relative K_2 group, that is $Tr_{K/F}(u) \in n\mathrm{K}_2(K)$. As we have seen, it does not follow that $u \equiv (1-\sigma)v \pmod{n\mathrm{K}_2(K)}$ for some $v \in \mathrm{K}_2(K)$.

CHAPTER 2

Brauer Algebras

1. Introduction

Let p be a prime number, F a field with $char(F) \neq p$. Building on Amitsur's famous example [**2**], Saltman [**34**] proved that the generic division algebra of degree p^ν and exponent p^μ is not a crossed product with respect to any group for $\nu \geq \mu \geq 3$ ($\mu = 2$ for p an odd prime, if F has no p-roots of unity). The situation for exponent p and degree p^ν, $\nu \geq 3$, remained open (except for degree 8 and exponent 2, where it is a crossed product with respect to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, [**29**]).

In this chapter we study Brauer algebras of degree p^ν and exponent p, making several reductions on possible sets of generators of a $\mathbb{Z}_p^\nu$-Galois extensions of the center.

The base fields in the examples we study contain finitely many roots of unity of p-power order. Using the ultraproduct argument at the end of [**33**], it is possible to produce an algebra with similar properties, such that the center contains the whole group μ_{p^∞}.

Once one produces a central simple algebra of the required degree and exponent which is not a $\mathbb{Z}_p^\nu$-crossed product, the generic division algebra would be a noncrossed product, for it is known that the generic division algebra of degree p^ν and arbitrary exponent is not a crossed product with respect to any other group. An example was presented in [**27**] and [**30**], but there were several major gaps. We continue the investigation of this example in a more general situation described in §4, closing some of the gaps. One gap remains, so the problem of producing a noncrossed product of exponent p is still open.

2. The Leading Monomial Technique

The technique of the leading monomial enables one to pass from good elements of a generic algebra to homogeneous good elements of a more concrete algebra. This was used numerous times, for example [**3**] or [**33**].

Let $\mathcal{M}$ be a commutative linearly ordered monoid, and T an $\mathcal{M}$-graded ring without zero divisors: $T = \oplus_{\alpha \in \mathcal{M}} T_\alpha$, with $T_\alpha T_\beta \subseteq T_{\alpha+\beta}$.

Let $\Phi = \{\phi\}$ be a set of grading-preserving automorphisms of T (that is $\phi(T_\alpha) \subseteq T_\alpha$ for all $\phi \in \Phi$, $\alpha \in \mathcal{M}$), such that the fixed subring $T^\Phi \subseteq \mathrm{Cent}(T)$.

For any element $r = \sum r_\alpha \in T$, the upper component of r is $\mu(r) = r_{\alpha_0}$, where α_0 is maximal in $\{\alpha : r_\alpha \neq 0\}$.

REMARK 2.1. a. If $f \in T^\Phi$ and $fg \in T^\Phi$, then $g \in T^\Phi$.
b. $\mu(fg) = \mu(f)\mu(g)$.
c. If $f \in T^\Phi$ then $\mu(f) \in T^\Phi$.
d. If f, g commute in T, then so do $\mu(f), \mu(g)$.

Let $\theta > 1$ be an integer, $\theta \neq 0$ in T. An element $f \in T$ is θ-invariant if $f^\theta \in T^\Phi$, but $f^i \notin T^\Phi$ for any $0 < i < \theta$.

PROPOSITION 2.2. *If $f \in T$ is θ-invariant, then so is $\mu(f)$.*

PROOF. $\mu(f)^\theta = \mu(f^\theta)$ is invariant since f^θ is.

We first show that if f is θ-invariant then $\mu(f) \notin T^\Phi$. Write $f = g + z$ where z is the sum of the invariant components in f, and g the sum of noninvariant components. In particular $z \in \mathrm{Cent}(T)$, so that z, g commute. By assumption, $g \neq 0$.

Assume $\mu(f)$ is a summand in z. The upper component of $f^\theta - z^\theta = (g+z)^\theta - z^\theta = \theta z^{\theta-1} g + \cdots + g^\theta$ is the upper component of $\theta z^{t-1} g$, so that $\mu(\theta z^{\theta-1} g) = \theta \mu(z)^{\theta-1} \mu(g)$ is invariant. Now $\mu(g)$ is invariant for $\mu(z)$ is, a contradiction to the definition of g.

Finally, suppose $\mu(f)^i \in T^\Phi$, then replacing i with (i, θ) we may assume $i \,|\, \theta$, and f^i is θ/i-invariant. By what we have just proved, $\mu(f^i) \notin T^\Phi$ unless $\theta/i = 1$, so that $i = \theta$. □

We call $\{f_1, \ldots, f_\nu\}$ a θ-set if $f_1, \ldots, f_\nu$ are pairwise commuting, $f_i^\theta \in T^\Phi$, and $f_1^{i_1} \cdots f_\nu^{i_\nu} \notin T^\Phi$ for all $0 \leq i_1, \ldots, i_\nu < \theta$, unless $i_1 = \cdots = i_\nu = 0$. Note that if f belongs to a θ-set then f is θ-invariant. If T^Φ is a field containing θ-roots of unity, then a θ-set is a standard set of generators for a $\mathbb{Z}_\theta^\nu$-Galois field extension of T^Φ.

PROPOSITION 2.3. *If the set $\{f_1, \ldots, f_\nu\}$ is a θ-set, then so is the set $\{\mu(f_1), \ldots, \mu(f_\nu)\}$.*

PROOF. In general, $f_1^{i_1} \cdots f_\nu^{i_\nu} \in T^\Phi$ iff every $i_j \equiv 0 \pmod{\theta}$.

Suppose $\mu(f_1)^{i_1} \cdots \mu(f_\nu)^{i_\nu} = \mu(f_1^{i_1} \cdots f_\nu^{i_\nu}) \in T^\Phi$, then $f_1^{i_1} \cdots f_\nu^{i_\nu}$ cannot be θ-invariant by the previous proposition, so that $i_1 \equiv \cdots \equiv i_\nu \equiv 0 \pmod{\theta}$. □

Let ρ_θ denote a (fixed) θ-root of unity in T.

PROPOSITION 2.4. *Let $\{f_1, \ldots, f_\nu\}$ be a θ-set, and g a θ-invariant element such that for every $i = 1, \ldots, \nu$, $g f_i g^{-1} = \rho_\theta^{\alpha_i} f_i$. Assume θ is*

a power of some prime p. Then T has a θ-set of the same size, with g as one of its elements.

PROOF. **Case 1:** $f_1, \ldots, f_\nu$ commute with g. The intersection of the subalgebras $L_i = T^\Phi[f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_\nu]$, $i = 1, \ldots, \nu$, is T^Φ, so that for some i we have $g^{\theta/p} \notin L_i$. Then $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_\nu, g$ form a θ-set of size ν, as asserted.

Case 2: Not every f_i commute with g; for example assume $\alpha_\nu \neq 0$. Then $\tilde{f}_i = f_i^{-1} f_\nu^{\alpha_i/\alpha_\nu \pmod\theta}$, $i = 1, \ldots, \nu - 1$, commute with g. Since $L = T^\Phi[\tilde{f}_1, \ldots, \tilde{f_{\nu-1}}] \subset T^\Phi[f_1, \ldots, f_\nu]$, g does not belong to L (for otherwise f_ν, g would commute). Thus, $\tilde{f}_1, \ldots, \tilde{f_{\nu-1}}, g$ form a θ-set. □

3. The Generic Elements Construction

We apply the leading monomial technique to an important special case.

Let $R = (K/F, \sigma, b)$ be a cyclic algebra of degree n and exponent θ, and let $z \in R$ be an element such that

$$(\forall k \in K) z k z^{-1} = \sigma(k), z^n = b.$$

Let λ be an indeterminate over K, and extend σ to $K(\lambda)$ by assigning $\sigma(\lambda) = \lambda$. $\tilde{R} = R \otimes_F F(\lambda) = K(\lambda)[z] = (K(\lambda)/F(\lambda), \sigma, b)$ is of course cyclic of the same degree and exponent as R. The idea is to mix λ with elements of R: take $K^\square = K(\lambda^\theta)$ and $R^\square = K(\lambda^\theta)[\lambda z] \subseteq \tilde{R}$. Also let $F^\square = \mathrm{Cent}(R^\square) = F(\lambda^\theta)$. Note that $R^\square \cong (K(\lambda^\theta)/F(\lambda^\theta), \sigma, \lambda^n b)$ is again cyclic of degree n.

THEOREM 3.1. $\exp(R^\square) = \theta$.

PROOF. By Wedderburn's criterion, $b^\theta \in N_{K/F}(K)$, but $b^i \notin N_{K/F}(K)$ for any $0 < i < \theta$.

We apply the same criterion for $\lambda^n b$ in the extension $K(\lambda^\theta)/F(\lambda^\theta)$. Write $b^\theta = N_{K/F}(\beta)$, then $N_{K(\lambda^\theta)/F(\lambda^\theta)}(\lambda^\theta \beta) = (\lambda^n b)^\theta$, so that $\exp(R^\square) \leq \theta$. On the other hand, suppose $(\lambda^n b)^i = N_{K(\lambda^\theta)/F(\lambda^\theta)}(f/g)$ where $f, g \in K[\lambda^\theta]$, $0 \leq i < \theta$. Multiplying by $N_{K(\lambda^\theta)/F(\lambda^\theta)}(g)$ and comparing degrees of λ, we see that $n\theta \mid ni$, so that $i = 0$. □

Note that $R^\square$ is the ring of central quotients of $T = K[\lambda^\theta][\lambda z]$, which is $\mathbb{N}$-graded as a ring of polynomials in λ. Let $k \in K$ be a generator of K/F. Conjugation by z or by k induce grading-preserving automorphisms, and the invariant subring under the conjugations is $F^\square$.

Note that for any $f \in K[\lambda^\theta][\lambda z] \subseteq R^\square$, $\mu(f) \in K[z^\theta] z^\alpha \cdot \lambda^u$ for some $0 \leq \alpha < \theta$.

Suppose F contains θ-root of unity, denoted by ρ_θ. Let k_1 be a generator for the field extension K^{σ^θ}/F, such that $\sigma(k_1) = \rho_\theta k_1$. In particular, $k_1^\theta \in F$.

Note that $K[z^\theta]$ is the centralizer of k_1 in R.

LEMMA 3.2 (Going down $R^\square \to R$). *If $R^\square$ contains a θ-set of size ν, then R has a θ-set $f_1, \ldots, f_\nu$ such that $f_1 = k_1$ and $f_2, \ldots, f_\nu \in K[z^\theta]$.*

PROOF. Let $g_1, \ldots, g_\nu \in R^\square$ be a θ-set. Multiplying by central elements, we may assume $g_i \in K[\lambda^\theta][\lambda z]$. The leading monomials of $g_1, \ldots, g_\nu$ (relatively to λ) form a θ-set by Proposition 2.3. We can thus assume $g_i \in K[z^\theta] \cdot (\lambda z)^{\alpha_i} \subseteq R^\square$. Moreover, dropping the appropriate powers of λ we have a θ-set $f_1, \ldots, f_\nu \in R$, $f_i \in K[z^\theta] \cdot z^{\alpha_i}$.

But now conjugation by k_1 multiplies each f_i by $\rho_\theta^{\alpha_i}$, so we can apply Proposition 2.4. □

REMARK 3.3 (Going up $R \to R^\square$). If $f_1, \ldots, f_\nu$ is a θ-set in R, such that $k_1 = f_1$, then it is a θ-set in $R^\square$ too.

PROOF. Since f_i commute with k_1, we have that $f_2, \ldots, f_\nu \in C_R(k_1) = K[z^\theta]$. Now $f_i = \sum_{j=0}^{n/\theta-1} k_i^{(j)} z^{j\theta} = \sum_{j=0}^{n/\theta-1} (k_i^{(j)} \lambda^{-j\theta})(\lambda z)^{j\theta} \in K(\lambda^\theta)[\lambda z] = R^\square$. □

4. Brauer's Example

We now focus on the Brauer algebra.

Recall the definition, following the notation in [**30**, Chap 7.3]. Fix a prime number p, and let t, θ be powers of p. Denote by ρ_θ a primitive θ-root of unity (over $\mathbb{Q}$), and let $\mu_0, ..., \mu_{t-1}$ be indeterminates over $\mathbb{Q}[\rho_\theta]$. The field $E_{\theta,t} = \mathbb{Q}[\rho_\theta](\mu_0, ..., \mu_{t-1})$ has an automorphism σ of order t defined by $\sigma : \mu_i \mapsto \mu_{i+1(mod\ t)}$, $\sigma : \rho_\theta \mapsto \rho_\theta$.

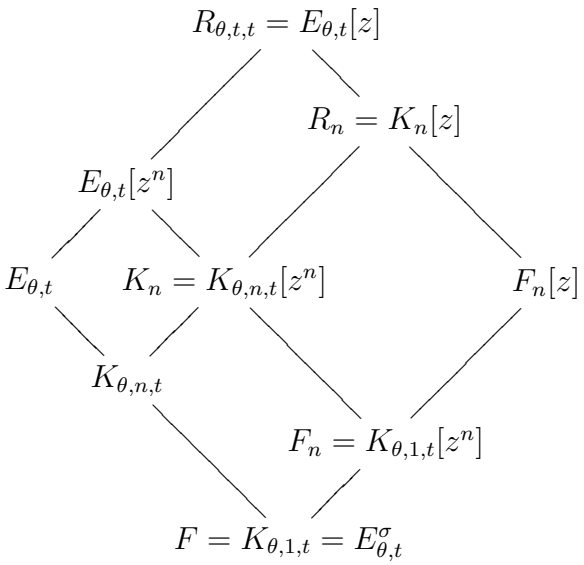
For any divisor n of t, let $K_{\theta,n,t}$ be the fixed subfield of $E_{\theta,t}$ under σ^n. The generalized Brauer example is the cyclic algebra $R_{\theta,n,t} = (K_{\theta,n,t}/K_{\theta,1,t}, \sigma, \rho_\theta)$, of degree n over its center $K_{\theta,1,t} = E_{\theta,t}^\sigma$. In what follows we work with subalgebras of $R_{\theta,t,t}$. Picking an element $z \in R_{\theta,t,t}$ such that conjugation by z induce σ on $E_{\theta,t}$ and $z^t = \rho_\theta$, we can write $R_{\theta,t,t} = E_{\theta,t}[z]$.

Note that z^n commutes with $K_{\theta,n,t}$, so that $K_n = K_{\theta,n,t}[z^n]$ is a field. This is a maximal subfield of $R_{\theta,t,t}$, of dimension t over the center F. Moreover, $(z^n)^{t/n} = \rho_\theta$ so that z^n is a $\theta t/n$-root of unity in K_n, and we sometimes denote $\rho_{\theta t/n} = z^n$. In particular, $K_n \cong K_{\theta t/n,n,t}$.

Let $R_n = K_n[z]$, a cyclic algebra of degree n, with center $F_n = K_n^\sigma = K_{\theta,1,t}[z^n] \cong K_{\theta t/n,1,t}$.

R_n is the centralizer of z^n in $R_{\theta,t,t}$, and it is isomorphic to $R_{\theta t/n,n,t}$ (*cf.* [**30**, Thm. 7.3.6(i)]). By [**30**, Thm. 7.3.8], R_n is a division algebra of exponent θ.

We add a picture of all that, for easy reference.



The reader is advised to add $F_{n/\theta}, K_{n/\theta}$ and $R_{n/\theta}$ in the diagram.

Let $H = \mathbb{Q}[\rho_\theta][\mu_0, \ldots, \mu_{t-1}]$ denote the subring of integers of $E_{\theta,t}$. Note that $H^{\sigma^n} = H \cap E^{\sigma^n}_{\theta,t}$, and that R_n, the centralizer of z^n in $R_{\theta,t,t}$, is the ring of central quotients of $H^{\sigma^n}[z]$. Let $q = \frac{t\theta}{n}$. Conjugation by $z^{n/\theta}$ induces a linear transformation of order $\frac{t}{n/\theta} = q$ on H.

THEOREM 4.1. *$H^{\sigma^n}[z]$ can be given an $\mathbb{N}^q$-grading, such that the components are eigenspaces of the action of $z^{n/\theta}$.*

PROOF. Let $V = \mathbb{Q}[\rho_\theta]\mu_0 + \cdots + \mathbb{Q}[\rho_\theta]\mu_{t-1}$, a generating linear subspace of H. H has the standard grading by total degree, inducing the decomposition to linear spaces over $\mathbb{Q}[\rho_\theta]$:

$$H = \mathbb{Q}[\rho_\theta] \oplus V \oplus V^2 \oplus \ldots \tag{29}$$

Conjugation by $z^{n/\theta}$ is a linear transformation of order q on V, but it has no eigenvalues in $\mathbb{Q}[\rho_\theta]$ (unless $n = t$). In order to use the $z^{n/\theta}$ action to decompose V, we take tensor products by $\mathbb{Q}[\rho_q]$ (over $\mathbb{Q}[\rho_\theta]$). $H \otimes \mathbb{Q}[\rho_q] = H[\rho_q]$ generates the commutative field $E_{\theta,t}[\rho_q]$, a different object from $E_{\theta,t}[z^n]$. But the two objects have the same subfield $K_n = K_{\theta,n,t}[z^n] \cong K_{\theta,n,t} \otimes \mathbb{Q}[\rho_q]$, which is the field we are really after.

Over $\mathbb{Q}[\rho_q]$, we have the decomposition

$$V = V_0 \oplus \cdots \oplus V_{q-1}, \tag{30}$$

where $z^{n/\theta}$ acts on V_j as multiplication by ρ_q^j.

Substituting (30) in (29), we see that $H[\rho_q]$ is a sum of all products $V_0^{n_0} \cdots V_{q-1}^{n_{q-1}}$. In order to see that this sum is direct, pick a basis $\{v_0^{(j)}, \ldots, v_{n/\theta-1}^{(j)}\}$ for V_j, then $\{v_u^{(j)}\}_{0\le j<q, 0\le u<n/\theta}$ generate H (as a ring). The transcendence degree of H is t, so that the $\{v_u^{(j)}\}$ must be algebraically independent. It is now obvious that every element is expressed in a unique way.

Let $e_0, \ldots, e_{q-1}$ be the standard basis of $\mathbb{Z}^q$. The degree function defined on monomials by $v_u^{(j)} \mapsto e_j$ makes $H[\rho_q]$ an $\mathbb{N}^q$-graded ring, with homogeneous components $V_0^{n_0} \cdots V_{q-1}^{n_{q-1}}$.

Consider the ring $H[\rho_q][u]$, subjected to the relations $uhu^{-1} = \sigma(h)$ ($h \in H$), $u^n = \rho_q$. It decomposes into a direct sum $H[\rho_q][u] = H[\rho_q] + H[\rho_q] \cdot u + \cdots + H[\rho_q] \cdot u^{n-1}$. Since conjugation by u preserves the linear components V_j, it preserves all the components, so that $H[\rho_q][u]$ is $(\mathbb{N}^q \times \mathbb{Z}_n)$-graded. The same is true for the subalgebra $H^{\sigma^n}[\rho_q][u]$ (and the only non-zero components are the products $V_0^{n_0} \cdots V_{q-1}^{n_{q-1}}$ with $n_1 + 2n_2 + \cdots + (q-1)n_{q-1} \equiv 0 \pmod{q/\theta}$).

Since $H^{\sigma^n}[\rho_q] \cong H^{\sigma^n}[z^n]$, we also have that $H^{\sigma^n}[\rho_q][u] \cong H^{\sigma^n}[z]$, so that $H^{\sigma^n}[z]$ is $(\mathbb{N}^q \times \mathbb{Z}_n)$-graded. In particular, $H^{\sigma^n}[z]$ is $\mathbb{N}^q$-graded with the components $V_0^{n_0} \cdots V_{q-1}^{n_{q-1}}[z]$. □

The reason we can't use the same proof to decompose into eigenspaces of $z^{n/k}$, $k > \theta$, is that $H^{\sigma^n}[\rho_{tk/n}] \ncong H^{\sigma^n}[z^{n\theta/k}]$: the leftmost ring is commutative, while the other is not.

NOTATION 4.2. *From now on we assume $\theta = p$. Also let $n = p^\nu$, $\nu \ge 2$.*

When $\nu = 2$, R_n is a crossed product, as shown by the following well known fact (also see Example 1.1 in Chapter 3):

REMARK 4.3. Let F be a field of characteristic $\neq p$, with p-roots of unity. Any cyclic algebra $R = (K/F, \sigma, b) = K[z]$ of degree p^2 over F is a $\mathbb{Z}^p \times \mathbb{Z}^p$-crossed product, by inspecting the subfield $K^{\sigma^p}[z^p]$.

A final remark before we dive into the reductions: we have the chains of inclusions

$$F_t \subset \cdots \subset F_n \subset F_{n/p} \subset \cdots \subset F_1,$$

$$R_t \supset \cdots \supset R_n \supset R_{n/p} \supset \cdots \supset R_1,$$

but the fields K_n $(n = 1, p, p^2, \dots, t)$ do not contain each other. It follows that the $R_n^{\square} = K_n(\lambda^p)[\lambda z]$ do not satisfy any natural inclusion relation among them.

PROPOSITION 4.4. *Suppose $R_n^{\square}$ has a p-set of size ν, then R_n has a p-set of the same size, with $k_1, z^{n/p}$ as two of the elements.*

PROOF. Recall that k_1 is a generator of the extension $K_{p,p,t}/K_{p,1,t}$, such that $\sigma(k_1) = \rho_p k_1$. In particular, $k_1^p \in K_{p,1,t}$. At the same time, $K_n^{\sigma^p} = F_n[k_1]$ and ${k_1}^p \in F_n$.

By Lemma 3.2, we have

REDUCTION 1. *R_n contains a p-set $f_1, \dots, f_\nu$ such that $f_1 = k_1$ and $f_2, \dots, f_\nu \in K_n[z^p]$.*

REDUCTION 2. *We may assume that $z^{n/p} f_i z^{-n/p} = \rho_p^{\alpha_i} f_i$ for some α_i.*

PROOF. Viewing f_i as elements of $R_{p,t,t}$, we may multiply by suitable central elements, and assume $f_i \in H[z^p] \cap R_n = H^{\sigma^n}[z^p] \subset H^{\sigma^n}[z]$.

We apply Theorem 4.1 to grade $H^{\sigma^n}[z]$ with components which are eigenspaces of $z^{n/p}$. Note that we may choose $k_1 = \sum_{i=0}^{t-1} \rho_p^{-i} \mu_i \in V_0$, so that $f_1 = k_1$ is homogeneous.

Let k_ν be a generator of $K_{\theta,n,t}/K_{\theta,n/p,t}$, such that $\sigma^{n/p}(k_\nu) = \rho_p k_\nu$. Since $R_n = F_n[k_\nu, z]$, central elements in R_n are exactly those invariant under conjugation by z and k_ν. Moreover, since z, k_ν are eigenvectors of $z^{n/p}$, conjugation by them takes V_j (of the grading) to itself, and so is grading-preserving. This is enough to apply Proposition 2.3.

Replacing $f_1, f_2, \dots, f_\nu$ by their upper homogeneous parts, we still have a p-set, where every f_i is an eigenvector of $z^{n/p}$. Finally, since f_i are p-central, the eigenvalues are powers of ρ_p, as required. □

REDUCTION 3. *We may assume that $f_2 = z^{n/p}$.*

PROOF. Note that $f_1 = k_1$ and $z^{n/p}$ commute.

By the previous reduction f_i are eigenvectors of $z^{n/p}$, so we can apply Proposition 2.4 with $g = z^{n/p}$. □

This finishes the proof of Proposition 4.4. □

COROLLARY 4.5. *Suppose $\nu \geq 3$. If $R_n^{\square} = K_n(\lambda^p)[\lambda z]$ is a $\mathbb{Z}_p^\nu$-crossed product, then $R_{n/p}^{\square}$ is a $\mathbb{Z}_p^{\nu-1}$-crossed product.*

PROOF. Suppose $R_n^{\square}$ has a p-set of size ν. By the last proposition, R_n has a homogeneous p-set of the same size, with one of the elements equals $z^{n/p}$ (and another equal k_1).

Then $C_{R_n}(z^{n/p}) = R_{n/p}$ has a p-set of size $\nu - 1$, and by Remark 3.3 so does $R^{\square}_{n/p}$. $\square$

As already mentioned in Remark 4.3, $R^{\square}_{p^2}$ contains the p-set k_1, z^p, so we are led to study the next case, $n = p^3$ (which we hope is not a $\mathbb{Z}_p^3$-crossed product for $p \neq 2$). This is done in Section 6.

Note that for $p = 2$, $k_1, z^4, z^2 + z^{-2}$ is a 2-set in $R^{\square}_8$.

5. Property $D(p)$ for Algebras of Degree p^2

A cyclic algebra $R = (K/F, \sigma, b) = K[z|zkz^{-1} = \sigma(k), z^n = b]$ of degree n is said to satisfy property $D(f)$, f a divisor of n, if it decomposes into a tensor product of cyclic subalgebras, one that contains K^{σ^f} and the other that contains $F[z^f]$. The property was introduced and studied in [**33**].

Suppose $\deg(R) = [K:F] = p^2$, and that F contains a p-root of unity. Choose a generator k_1 for K^{σ^p}/F such that $k_1^p \in F$. Consider the subfield $L = F[k_1, z^p]$, which is $\mathbb{Z}_p^2$-Galois over F. We use square brackets to denote the multiplicative commutator. By Skolem-Noether, there exist $u, v \in R$ such that

$$[u, k_1] = 1, \qquad [u, z^p] = \rho_p, \tag{31}$$

and

$$[v, k_1] = \rho_p, \qquad [v, z^p] = 1. \tag{32}$$

Note that letting k_2 be a cyclic generator for K/K^{σ^p}, $u = k_2$ and $v = z$ is a solution to (31)+(32).

We now add another constraint:

$$[u, v] = 1. \tag{33}$$

LEMMA 5.1. *Property $D(p)$ for R is equivalent to the existence of a solution for (31)+(32)+(33).*

PROOF. Assume property $D(p)$ is satisfied. Then there exist commuting central simple subalgebras $R_1, R_2 \subset R$ with $R_1 \cap R_2 = F$, $R_1R_2 = R$, $k_1 \in R_1$, $z^p \in R_2$. We can thus find $u \in R_1 = C_R(R_2)$ such that $[u, k_1] = \rho_p$ and $v \in R_2$ satisfying (32), and (33) is also clear.

Now suppose u, v commute, and satisfy (31),(32). We first show that $L[u, v] = R$. Indeed, $u \notin L$ (for it does not commute with z^p), so that $[L[u]:F] \geq p^3$. If $L[u] = R$, we are done. Otherwise, k_1 is in the center of $L[u]$, but does not commute with v — so that $v \notin L[u]$, and $L[u, v] = R$.

From (33) it now follows that u^p commutes with k_1, z^p, u, v, so that $u^p \in F$. Similarly $v^p \in F$, and $F[k_1, u]$, $F[z^p, v]$ are the commuting subalgebras we are looking for. □

We may look for a special kind of element: consider the constraint

$$u^p \in F. \tag{34}$$

PROPOSITION 5.2. *If equations (31)+(34) has a solution, then so do (31)+(32)+(33).*

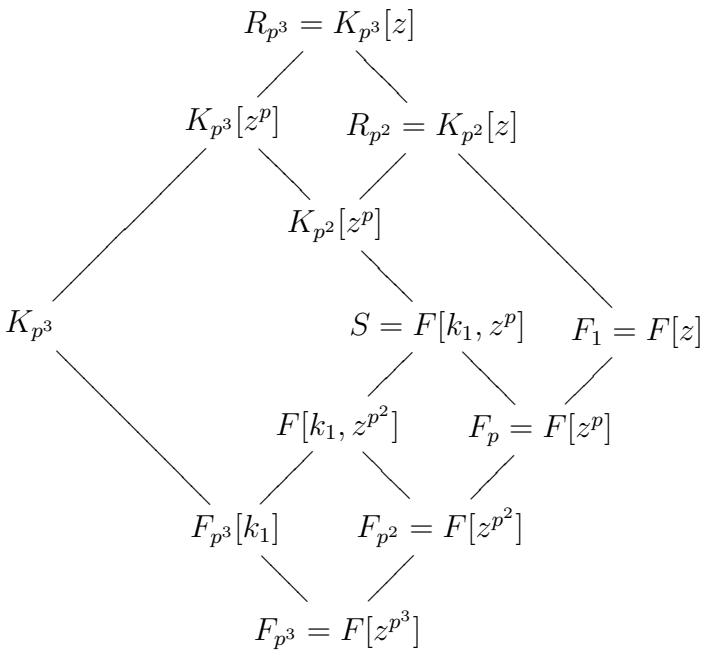
PROOF. By the assumption, $F[z^p, u]$ is a (cyclic) central subalgebra of R, of dimension p^2. Its centralizer is of dimension p^2, and contains the cyclic subfield $F[k_1]$. Applying Skolem-Noether to this centralizer we find $v \in C_R(F[z^p, u])$ such that $[v, k_1] = \rho_p$. u, v satisfy (31)+(32)+(33). □

6. Brauer's Example in Degree $n = p^3$

Suppose $R^{\square}_{p^3}$ has a p-set of size 3. By Proposition 4.4, R_{p^3} has the p-set z^{p^2}, k_1, f_3, where $f_3 \in R_{p^3}$. Actually by the choice of f_3 in Reduction 2, $f_3 \in H^{\sigma^{p^3}}[z^p]$.

LEMMA 6.1. *f_3 does not commute with z^p.*

PROOF. We draw a picture of the subalgebras of R_{p^3} appearing in the sequel (this is a zoom into the rightmost square in the previous diagram).



Note that $F_{p^3}[z^p]$ is Galois over $F_{p^3} = F[z^{p^3}]$.

k_1, z^{p^2} are elements of the field $S = F_{p^3}[k_1, z^p]$. Also, f_3 commutes with $F_{p^3}[k_1]$. Assume f_3, z^p commute. Then $f_3 \in C_R(S) = S$, so that $F_{p^3}[k_1, z^{p^2}, f_3] \subseteq S$, the two fields having the same dimension p^3 over F. It follows that the two fields are equal, but the Galois group of $S = F_{p^3}[k_1, z^p] = F_{p^3}[k_1] \otimes_{\mathbb{F}_{p^3}} F_{p^3}[z^p]$ over F_{p^3} is $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, a contradiction. □

Theorem 10 in [**33**] states that the Brauer algebra R_{pq,p^2,p^2q} does not satisfy $D(p)$. This algebra is isomorphic to our R_{p^2} by [**30**, 7.3.6(i)] (for $t = p^2q$).

Recall that in order to construct a noncrossed product of exponent p we need to get contradiction to the assumption that a p-central set of size 3 exists in $R^{\square}_{p^3}$. We discuss two possible approaches (one of which was suggested in [**27**]), and show why they fail.

One strategy is to try to use f_3 to solve (31)+(34) in R_{p^2}, thus showing that it satisfies property $D(p)$, a contradiction.

We look for an element $g \in R_{p^2}$, such that:

$$[g, k_1] = 1, \qquad [g, z^p] = \rho_p, \qquad g^p \in F_{p^2}. \tag{35}$$

Remark 6.2. Assuming such an element g exists, we have that $F_{p^2}[z^p, g]$ is a cyclic algebra of degree p over F_{p^2}, and its corestriction

down the extension F_{p^2}/F_{p^3} is

$$\mathrm{cor}_{F_{p^2}/F_{p^3}}(z^{p^2}, g) = (\rho_p, g).$$

Since f_3 commutes with k_1, z^{p^2}, it belongs to $H^{\sigma^{p^2}}[z^p]$. Apply theorem 4.1 with $n = p^2$ to grade $H^{\sigma^{p^2}}[z] \subset R_{p^2}$ with components which are eigenspaces of z^p.

It seems natural to continue as in Reduction 2, and replace f_3 by an eigenvector of z^p. Indeed, conjugation by z and by k_2 (a cyclic generator of $K_{p^3}^{\sigma^{p^2}}/K_{p^3}^{\sigma^p}$) preserve the grading (since z,k_2 are eigenvectors of z^{p^2}), so the p-power of an upper homogeneous component $\mu(f_3)$ of f_3 will be in $\mathrm{Cent}_{R_{p^3}}(F[z, k_2]) = F_{p^3}[z^{p^2}] = F_{p^2}$. But this is not enough, for we cannot exclude the possibility that $\mu(f_3)$,z^p commute (consider z^p itself as a candidate for $\mu(f_3)$; for $p = 2$ we do have $f_3 = z^2 + z^{-2}$).

This cannot be pursued further to show that $\mu(f_3)^p \in F_{p^3}$ since conjugation by k_3 does not preserve the grading (for example, $k_3 z k_3^{-1} \notin V_0 \cdot z$ in the above grading). Fortunately the condition (34) does not require $g^p \in F_{p^3}$.

We withdraw one step backwards and present a second approach. Apply Theorem 4.1 with $n = p^3$ and $q = t/p^2$, to get a decomposition $V = V_0 \oplus \cdots \oplus V_{q-1}$ to eigenspaces of z^{p^2} over $F[z^{p^3}]$. By Reduction 3 and the proof of Reduction 2, we can assume $f_3 \in V_0^{\alpha_0} \cdots V_{q-1}^{\alpha_{q-1}}[z^p]$ for some $\alpha_0, \ldots, \alpha_{q-1} \in \mathbb{N}$.

Let $W = V_0^{\alpha_0} \cdots V_{q-1}^{\alpha_{q-1}}$. Since W commutes with z^{p^2}, conjugation by z^p is a linear transformation of order p on W, so we have a decomposition $W = W_0 \oplus \cdots \oplus W_{p-1}$ over $\mathbb{Q}[\rho_p]$, where W_i is the eigenspace of the eigenvalue ρ_p^i. Consider the $\mathbb{N}^p$-graded algebra $A = \bigoplus_{\mathbb{Q}[\rho_p]} W_0^{\beta_0} \ldots W_{p-1}^{\beta_{p-1}}[z^p]$. Check that conjugation by z^p and by k_2 are grading-preserving (for $z^p W_i z^{-p} = W_i$, k_2 commutes with W_i, and $k_2 z^p k_2^{-1} = \rho_p^{-1} z^p$).

The invariant subalgebra under these conjugations in contained in the center $\mathrm{Cent}(A)$ (for $A \subseteq H^{\sigma^{p^2}}[z^p]$, and the invariant subalgebra is contained in the invariant subalgebra of $H^{\sigma^{p^2}}[z^p]$ under the same conjugations, which is the center $H^{\sigma^p}[z^{p^2}]$ of $H^{\sigma^{p^2}}[z^p]$).

This is enough to apply Proposition 2.2: since f_3 is p-invariant, so is any upper component of f_3. But since f_3 does not commute with z^p (Proposition 6.1), it has a non-zero component in some W_i ($i \neq 0$), and this component satisfies

$$[g, k_1] = 1, \qquad [g, z^p] = \rho_p, \qquad g^p \in F_{p^2}[k_1]. \tag{36}$$

Compare this to (35) — we need $g^p \in F_{p^2}$, but this could be achieved only if conjugation by z was grading preserving, and this is not the case.

Summarizing, we have that if $R^{\square}_{p^3}$ has a p-set of size 3, then R_{p^3} has a p-set consisting of k_1 (the cyclic generator of K^{σ^p}/F), z^{p^2} and f_3. We have that $f_3 \in W[z^p]$, $W = V_0^{\alpha_0} \cdots V_{q-1}^{\alpha_{q-1}}$ for some $\alpha_0, \ldots, \alpha_{q-1}$, where V_i are eigenspaces of z^{p^2}. We can decompose $W = W_0 \oplus \cdots \oplus W_{p-1}$ to eigenspaces of z^p, and f_3 has a component $g \in W_i[z^p]$ $(i \neq 0)$ such that g commutes with k_1, z^{p^2}, $z^p g z^{-p} = \rho_p^i g$, and $g^p \in F_{p^3}[k_1, z^{p^2}]$.

CHAPTER 3

Dihedral Crossed Products With Involution

1. Introduction

One of the best ways to understand central simple algebras is to study their maximal subfields. If an algebra happen to have a maximal subfield K Galois over the center F, it has an easy description via the second cohomology group $H^2(G, K^*)$, where $G = \mathrm{Gal}(K/F)$. Such an algebra is called a **crossed product** of G over K/F. For example, a cyclic algebra is a crossed product of a cyclic group.

In the early days every known division algebra was constructed as a crossed product, and by classical theorems of Wedderburn, Albert and Dickson, all division algebras of degree $2, 3, 4, 6$ or 12 are crossed products.

An interesting question concerning crossed products is to describe in what cases will every crossed product of a given group be a crossed product of some other group too. If all the Galois maximal subfields of a suitable central simple algebra have the same Galois group G, this group is termed **rigid**. Amitsur showed that the elementary abelian groups are rigid, and this was a key step in his construction of non-crossed products [**2**]. Since then it was shown by Saltman [**35**] and Amitsur-Tignol [**5**] that every noncyclic abelian group is rigid.

We use the notation $G \longrightarrow H$ to say that every crossed product of G is also a crossed product of H.

EXAMPLE 1.1. Let $n = m_1 m_2$ be integers and assume F has m_2-roots of unity. Then $\mathbb{Z}_n \longrightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, that is, every $\mathbb{Z}_n$-crossed product is also a $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$-crossed product.

PROOF. Let $R = (K/F, \sigma, b)$ be a cyclic algebra of degree n over F, $b \in F$, with $z \in R$ inducing σ on K. Obviously $K^{\sigma^{m_1}}[z^{m_1}] = K^{\sigma^{m_1}} \otimes_F F[z^{m_1}]$ is a maximal subfield of R, Galois over F with Galois group $\mathbb{Z}_m \times \mathbb{Z}_{n/m}$. □

It was shown by Rowen and Saltman [**31**] that if n is odd, then every D_n-crossed product is cyclic (assuming $\mathrm{char}F$ is prime to n, and F has n roots of unity). Their proof is constructive; a few years later Mammone and Tignol [**21**] gave another proof, using the corestriction.

If $\mathrm{char}(F)$ divides n, then any semidirect product of a cyclic group acting on $\mathbb{Z}_n$ is abelian. This is a result of Albert, proved by what is in modern language a relatively easy use of the corestriction.

Brussel [**8**] has shown that D_4, and more generally the dihedral-type groups of order p^3, are all rigid.

In this chapter we show that if one assumes the algebra has an involution, then a dihedral crossed product is also an abelian crossed product.

2. Involutions

Recall the standard description of crossed products. Let K/F be Galois extension of fields, with Galois group $G = \mathrm{Gal}(K/F)$. Let R be a central simple F-algebra, with a maximal subfield K. By Skolem-Noether, for every $g \in G$ there is an element $z_g \in R$ that induces g on K. We say that $\{z_g\}$ is a G-basis of R. Now, z_{gh} and $z_g z_h$ induce the same automorphism, so that $c_{g,h} = z_g z_h z_{gh}^{-1} \in C_R(K) = K$ defines a 2-cocycle $c \in H^2(G, K^*)$. Obviously $c_{g,h}$ determines the multiplication in $K[z_g]$, and we denote $(K, G, c) = K[\{z_g\} : z_g k z_g^{-1} = g(k), z_g z_h = c_{g,h} z_{gh}]$. The map $c \mapsto (K, G, c)$ induces an isomorphism $H^2(G, K^*) \cong \mathrm{Br}(K/F)$.

This construction can be refined for algebras with involution. Let R be a central simple F-algebra, with a maximal subfield $F \subseteq K \subseteq R$, and an automorphism $\tau \in G = \mathrm{Gal}(K/F)$ such that $\tau^2 = id_K$.

Proposition 2.1 ([**30**, Prop. 7.2.45]). *If R has an involution of the first kind, then there is an involution whose restriction to K is τ.*

Let $\{z_g : g \in G\}$ be a G-basis. Let $u \mapsto u^*$ be an involution of R whose restriction to K is τ. We denote $g^\tau = \tau g \tau^{-1}$, and $g^{-\tau} = (g^\tau)^{-1}$. Note that $g \mapsto g^\tau$ is an automorphism of order 2 of G.

Let $s_g = z_g^* z_{g^\tau}$.

Proposition 2.2. *The elements $\{s_g\}$ are in K.*

Proof. We show that $s_g \in C_R(K) = K$. Let $k \in K$.

$$\begin{aligned} s_g k {s_g}^{-1} &= z_g^* z_{g^\tau} k {z_{g^\tau}}^{-1} z_g^{*-1} \\ &= z_g^* \tau g \tau^{-1}(k) z_g^{*-1} \\ &= z_g^* (g\tau^{-1}k)^* (z_g^{-1})^* \\ &= (z_g^{-1}(g\tau^{-1}k) z_g)^* \\ &= (g^{-1} g \tau^{-1} k)^* \\ &= (\tau^{-1}k)^* = k. \end{aligned}$$

□

PROPOSITION 2.3. *The set* $\{s_g\} \subseteq K$ *satisfies*

$$s_{g^\tau} = \tau(s_g) \tag{37}$$

$$s_{gh} = s_h h^{-\tau}(s_g) \cdot \tau(gh)^{-1}(c_{g,h} \cdot \tau^{-1} c_{g^\tau,h^\tau})^{-1}. \tag{38}$$

PROOF. Compute.

$$\begin{aligned} \tau(s_g) &= \tau(z_g^* z_{g^\tau}) = \\ &= (z_g^* z_{g^\tau})^* = \\ &= z_{g^\tau}^* z_g = \\ &= s_{g^\tau}. \end{aligned}$$

$$\begin{aligned} s_{gh} &= z_{gh}^* z_{(gh)^\tau} = \\ &= (c_{g,h}^{-1} z_g z_h)^* z_{g^\tau h^\tau} = \\ &= z_h^* z_g^* \tau(c_{g,h}^{-1}) \cdot c_{g^\tau,h^\tau}^{-1} z_{g^\tau} z_{h^\tau} = \\ &= z_h^* z_g^* z_{g^\tau} z_{h^\tau} h^{-\tau} g^{-\tau} (\tau(c_{g,h}^{-1}) \cdot c_{g^\tau,h^\tau}^{-1}) = \\ &= z_h^* s_g z_{h^\tau} (gh)^{-\tau} (\tau(c_{g,h}^{-1}) \cdot c_{g^\tau,h^\tau}^{-1}) = \\ &= s_h h^{-\tau}(s_g) \tau(gh)^{-1} (c_{g,h} \cdot \tau^{-1} c_{g^\tau,h^\tau})^{-1}. \end{aligned}$$

□

By reversing the above computations, we have

PROPOSITION 2.4. *Let* R *be a crossed product of* G *over* K/F*, with a* G*-basis* $\{z_g\} \subseteq R$*, and multiplication defined by a* 2*-cocycle* $c_{g,h} \in H^2(G, K^*)$.

Then $z_g \mapsto s_g z_{g^\tau}^{-1}$ *defines an involution whose restriction to* K *is* τ*, iff* $\{s_g\} \subseteq K$ *satisfies Equations (37) and (38).*

PROOF. If $z_g \mapsto s_g z_{g^\tau}^{-1}$ defines an involution, then $\{s_g\}$ satisfy the conditions by Propositions 2.2 and 2.3.

Suppose $\{s_g\} \subseteq K$ satisfy (37) and (38). Define a map on $R = (K, G, c)$ by $(\sum a_g z_g)^* = \sum s_g \tau g^{-1}(a_g) z_{g^\tau}^{-1}$ (this definition extends $z_g^* = s_g z_{g^\tau}^{-1}$). Since additivity of $u \mapsto u^*$ is clear, it remains to check that $u \mapsto u^*$ is anticommutative and that $u^{**} = u$. Let $a, b \in K$, $g, h \in G$.

$$(ab)^* = \tau(ab) = \tau(a)\tau(b) = b^* a^*.$$

$$\begin{aligned}(az_g)^* &= s_g\tau g^{-1}(a)z_{g^\tau}^{-1}\\ &= s_g g^{-\tau}\tau(a)z_{g^\tau}^{-1}\\ &= s_g z_{g^\tau}^{-1}\tau(a)\\ &= z_g^* a^*.\end{aligned}$$

$$\begin{aligned}(z_g z_h)^* &= (c_{g,h}z_{gh})^*\\ &= s_{gh}\tau(gh)^{-1}(c_{g,h})z_{(gh)^\tau}^{-1}\\ &= s_h h^{-\tau}(s_g)\cdot\tau(gh)^{-1}(c_{g,h}\cdot\tau^{-1}c_{g^\tau,h^\tau})^{-1}\tau(gh)^{-1}(c_{g,h})z_{(gh)^\tau}^{-1}\\ &= s_h h^{-\tau}(s_g)\cdot(gh)^{-\tau}(c_{g^\tau,h^\tau}^{-1})z_{(gh)^\tau}^{-1}\\ &= s_h h^{-\tau}(s_g)\cdot(gh)^{-\tau}(c_{g^\tau,h^\tau}^{-1})(c_{g^\tau,h^\tau}^{-1}z_{g^\tau}z_{h^\tau})^{-1}\\ &= s_h h^{-\tau}(s_g)\cdot(gh)^{-\tau}(c_{g^\tau,h^\tau}^{-1})z_{h^\tau}^{-1}z_{g^\tau}^{-1}c_{g^\tau,h^\tau}\\ &= s_h h^{-\tau}(s_g)\cdot(gh)^{-\tau}(c_{g^\tau,h^\tau}^{-1})h^{-\tau}g^{-\tau}(c_{g^\tau,h^\tau})z_{h^\tau}^{-1}z_{g^\tau}^{-1}\\ &= s_h h^{-\tau}(s_g)z_{h^\tau}^{-1}z_{g^\tau}^{-1}\\ &= s_h z_{h^\tau}^{-1}\cdot s_g z_{g^\tau}^{-1}\\ &= z_h^* z_g^*.\end{aligned}$$

$$a^{**} = \tau^2(a) = a$$

Finally let $u = (z_{g^{-\tau}}z_{g^\tau})^{-1} \in K$, then

$$\begin{aligned}z_g^{**} &= (s_g z_{g^\tau}^{-1})^*\\ &= (s_g u z_{g^{-\tau}})^*\\ &= s_{g^{-\tau}}\tau g^\tau(s_g u)z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g u)z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)g(u^*)z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)g((z_{g^\tau}^{-1}z_{g^{-\tau}}^{-1})^*)z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)z_g(z_{g^\tau}^{-1}z_{g^{-\tau}}^{-1})^* z_g^{-1}z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)z_g(z_{g^{-\tau}}^*)^{-1}(z_{g^\tau}^*)^{-1}z_g^{-1}z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)z_g(s_{g^{-\tau}}z_{g^{-1}}^{-1})^{-1}(s_{g^\tau}z_g^{-1})^{-1}z_g^{-1}z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)z_g z_{g^{-1}}s_{g^{-\tau}}^{-1}z_g s_{g^\tau}^{-1}z_g^{-1}z_{g^{-1}}^{-1}\\ &= s_{g^{-\tau}}g\tau(s_g)z_g z_{g^{-1}}s_{g^{-\tau}}^{-1}g(s_{g^\tau}^{-1})z_{g^{-1}}^{-1}\end{aligned}$$

$$\begin{aligned} &= s_{g^{-\tau}} g\tau(s_g) z_g g^{-1}(s_{g^{-\tau}}^{-1} g(s_{g^\tau}^{-1})) \\ &= s_{g^{-\tau}} g\tau(s_g) s_{g^{-\tau}}^{-1} g(s_{g^\tau}^{-1}) z_g \\ &= g\tau(s_g) g(s_{g^\tau}^{-1}) z_g \\ &= g(\tau(s_g) s_{g^\tau}^{-1}) z_g \\ &= z_g. \end{aligned}$$

□

EXAMPLE 2.5. For cyclic algebras $G = \langle g | g^n = 1 \rangle$, and we can choose $z_{g^i} = z^i$ for $z = z_g$. Then the cocycle becomes $c_{g^i,g^j} = 1$ if $i + j < n$, $c_{g^i,g^j} = b^1$ otherwise, where $b = z^n \in F$

For $\tau = 1$, the conditions above translates to $N_{K/F}(\eta) = b^2$ where $\eta = s_g \in K$. If n is even and $\tau = g^{n/2}$, then $\eta = s_g \in K^\tau$ and again $N_{K/F}(\eta) = b^2$.

Proposition 2.4 is a generalization of the computations done by Albert [**1**, Theorems X.16–17] for the case $\tau = 1$, in his proof that R has an involution iff $\exp(R) \mid 2$.

Now let $r_g = z_g^* z_{g^{-\tau}}^{-1} = s_g (z_{g^{-\tau}} z_{g^\tau})^{-1} \in K$.

PROPOSITION 2.6.

$$r_{g^{-\tau}} = g\tau(r_g^{-1}) \tag{39}$$

PROOF. Compute:

$$\begin{aligned} g\tau(r_g) &= z_g (r_g)^* z_g^{-1} \\ &= z_g (z_g^* z_{g^{-\tau}}^{-1})^* z_g^{-1} \\ &= z_g (z_{g^{-\tau}}^*)^{-1} z_g z_g^{-1} \\ &= (z_{g^{-\tau}}^* z_g^{-1})^{-1} \\ &= (r_{g^{-ta}})^{-1} \end{aligned}$$

□

COROLLARY 2.7. $z_\tau^* = \pm z_\tau$.

PROOF. We have that $\tau^{-\tau} = \tau$, so by Equation (39), ${r_\tau}^2 = 1$, that is $z_\tau^* = \pm z_\tau$. □

Note that any element z_g of a G-basis can be replaced by another element kz_g, $k \in K$. If G has exponent 2, then every element of G satisfies $g^{-\tau} = g$. In [**3**, Theorem 2.1] it is shown that in this case z_g can be chosen such that $z_g^* = \pm z_g$. This can be slightly improved.

PROPOSITION 2.8. *If $g \in G$, $g \neq \tau$, satisfies $g^{-\tau} = g$, then we can choose z_g to satisfy $z_g^* = z_g$.*

PROOF. For every $k \in K$, we have that

$$(kz_g)^* = z_g^* k^* = r_g z_{g^{-\tau}} \tau(k) = r_g z_g \tau(k) = r_g g\tau(k) k^{-1} \cdot (kz_g).$$

By the assumption $(g\tau)^2 = gg^\tau = 1$, so using Equation (39) we have that $N_{g\tau}(r_g) = r_g \cdot g\tau(r_g) = 1$. Thus $r_g = g\tau(k)^{-1}k$ for some $k \in K$, and then $(kz_g)^* = kz_g$. □

3. Dihedral Crossed Products

Let $D_n = \langle g, t | g^n = 1, tgt^{-1} = g^{-1}, t^2 = 1 \rangle$ be the dihedral group of order $2n$.

As mentioned in the introduction, it is already known that if n is odd, then any crossed product of D_n is cyclic (given n roots of unity in the base field). Naturally, our interest is in the case where n is even.

Let K/F be a Galois extension with Galois group $\mathrm{Gal}(K/F) \cong D_n$. There are $\sigma, \tau \in \mathrm{Gal}(K/F)$ such that $\sigma^n = 1$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$.

Let R be a crossed product with center F and maximal subfield K, with an involution $(*)$. By Proposition 2.1 we can assume its restriction to K is τ. There is an element $z \in R$ that induces σ on K. By Proposition 2.8, we may assume $z^* = z$.

PROPOSITION 3.1. *$b = z^n \in F$.*

PROOF. $b \in K$ since $b = z^n$ acts trivially on K. $\sigma(b) = zbz^{-1} = zz^n z^{-1} = z^n = b$, and $\tau(b) = b^* = (z^n)^* = (z^*)^n = z^n = b$. Thus $b \in K^{\sigma,\tau} = F$. □

If F has n roots of unity, then $F[z]$ is cyclic over F. It commutes with K^σ, and obviously they intersect in F. Thus $K^\sigma[z]$ is a maximal subfield Galois over F, and we have proved

THEOREM 3.2. *Let R be a crossed product of D_n as above. If R has an involution and the center F has n roots of unity, then R is also a crossed product of the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_n$.*

COROLLARY 3.3. *Let R be central simple algebra of degree n with involution over F, with maximal subfield L, so that $[L:F] = n$. Assume F has n roots of unity. If the Galois closure of L/F has dihedral Galois group D_n, then R is Brauer equivalent to an abelian crossed product.*

PROOF. Denote the Galois closure of L/F by K. Since L splits R, K is a maximal subfield of $M_2(R)$. By the above theorem $M_2(R)$ has a maximal subfield whose Galois group over F is $\mathbb{Z}_2 \times \mathbb{Z}_n$. □

Let $m \,|\, n$. Then $\sigma^m \in D_n$ generates a normal subgroup of order n/m. K^{σ^m} is Galois with group $D_n/\langle\sigma^m\rangle \cong D_m$. The field $F[z^m]$ generated by z^m has dimension n/m, and the intersection with K is F. If F has n/m roots of unity, then $F[z^m]$ is cyclic over F.

COROLLARY 3.4. *If $m \,|\, n$ and F has n/m roots of unity, then a crossed product of D_n with involution is also a crossed product of the group $\mathbb{Z}_{n/m} \times D_m$ (viathe subfield $K^{\sigma^m}[z^m]$).*

Note that if $n/m = 2$ and m is odd, then $\mathbb{Z}_2 \times D_m = D_n$.

Here are the first few conclusions for crossed products with involution (assuming enough roots of unity):

$$
\begin{aligned}
D_4 &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2^3 \\
D_6 &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_6 \\
D_8 &\longrightarrow \mathbb{Z}_2 \times D_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_8 \\
D_{10} &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_{10} \\
D_{12} &\longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times S_3, \quad \mathbb{Z}_3 \times D_4, \quad \mathbb{Z}_4 \times S_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6, \quad \mathbb{Z}_2 \times \mathbb{Z}_{12}
\end{aligned}
$$

It would be interesting to know the relations between the other groups. For example, does $\mathbb{Z}_2 \times D_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ assuming involution?

Bibliography

[1] A. A. Albert, Structure of Algebras, Amer. Math. Soc. Coll. Publ., Vol. XXIV, Providence, 1961.

[2] S. Amitsur, *On Central Division Algebras*, Israel J. Math., **24**, 408–420, (1972).

[3] S. Amitsur, L. H. Rowen and J.-P. Tignol, *Division Algebras of Degree* 4 *and* 8 *with Involution*, Israel J. Math., **33**(2), 133–148, (1979).

[4] S. Amitsur and D. Saltman, *Generic Abelian Crossed Products and p-Algebras*, J. Algebra, **51**(1), 76–87, (1978).

[5] S. Amitsur and J.-P. Tignol, *Kummer subfields of Malcev-Neumann division algebras*, Israel J. Math., **50**, 114–144, (1985).

[6] M. Artin, *Brauer Severi Varieties*, in Brauer groups in ring theory and algebraic geometry (Wilrijk, 1981), LNM **917**, 194–210, 1982.

[7] H. Bass and J. Tate, *The Milnor Ring of a Global Field*, in Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Seattle, Wash., Battelle Memorial Inst., 1972), LNM **342**, 349–446, 1973.

[8] E. Brussel, *Noncrossed Products and Nonabelian crossed products over* $\mathbb{Q}(t)$ *and* $\mathbb{Q}((t))$, Amer. J. Math., **117**(2), 377–393, (1995).

[9] S. U. Chase, *Two Results on Central Simple Algebras*, Comm. Algebra, **12**, 2279–2289, (1984).

[10] P. K. Draxl, Skew Fields, London Math. Soc. Lec. Notes Ser. **81**, 1983.

[11] S. Eilenberg and S. MacLane, *Cohomology and Galois Theory,* I. *Normality of Algebras of Teichmüller's Cocycle*, Trans. Amer. Math. Soc., **64**, 1–20, (1948).

[12] M. D. Fried and M. Jarden, Field Arithmetic, Springer-Verlag, 1986.

[13] D. Hilbert, *Die Theorie der Algebraichen Zahlk orper*, Jahresb. Deut. Math. Ver., **4**, 175–546, (1897).

[14] N. Jacobson, Basic Algebra II, W. H. Freeman and Co., San Francisco, Calif., 1980.

[15] N. Jacobson, Finite Dimensional Division Algebras over Fields, Springer, 1996.

[16] N. Jacobson, *p-algebras of exponent p*, Bull. AMS, **43**, 667–670, (1937).

[17] K. Kato, *Galois Cohomology of Complete Discrete Valuation Fields*, in Algebraic K-theory, Part II (Oberwolfach, 1980), LNM **967**, 215–238, 1982.

[18] M. A. Knus, M. Ojanguren and D. J. Saltman, *On Brauer Groups in Characteristic p*, in Brauer groups (Proc. Conf., Northwestern Univ., Evanston, Ill., 1975), LNM **549**, 25–49, 1976.

[19] P. Mammone, *Sur la corestriction des p-symboles*, Comm. Alg., **14**(3), 517–529, (1986).

[20] P. Mammone and A. Merkurjev, *On the corestriction of* p^n*-symbol*, Israel J. Math., **76**(1–2), 73–79, (1991).

[21] P. Mammone and J.-P. Tignol, *Dihedral Algebras are Cyclic*, Proc. Amer. Math. Soc., **101**(2), 217–218, (1987).
[22] J. C. McConnel, *Division Algebras Beyond the Quaternions*, Amer. Math. Mont., **105**(1), 154–162, (1998).
[23] A. S. Merkurjev, *Brauer Groups of Fields*, Comm. Alg., **11**(22), 2611–2624, (1983).
[24] A. S. Merkurjev, A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk. SSSR ser. Mat., **46**(5), 1011–1046, 1135–1136. Trans. Math USSR Izv., **21**(2), 307–340, (1983).
[25] L. Ribes, Introduction to profinite groups and Galois cohomology, Queen's Papers in Pure and Applied Mathematics, 24. Queen's University, Kingston, ON, 1999.
[26] J. Rosenberg, Algebraic K-Theory and its Applications, Springer-Verlag, 1994.
[27] L. H. Rowen, *Cyclic Division Algebras*, Israel J. Math., **41**, 213–234, corr. ibid. **43**, 277–280, (1982).
[28] L. H. Rowen, *Are p-Algebras Having Cyclic Quadratic Extensions Necessarily Cyclic?*, J. Algebra, **215**, 205–228, (1999).
[29] L. H. Rowen, *Central Simple Algebras*, Israel J. Math., **29**(2–3), 285–301, (1978).
[30] L. H. Rowen, Ring Theory, Academic Press, 1988.
[31] L. H. Rowen and D. J. Saltman, *Dihedral Algebras are Cyclic*, Proc. Amer. Math. Soc., **84**(2), 162–164, (1982).
[32] L. H. Rowen and D. J. Saltman, *Division Algebras over C_2- and C_3-fields*, preprint, (2000).
[33] L. H. Rowen, J.-P. Tignol, *On the Decomposition of Cyclic Algebras*, Israel J. Math., **96**, 553–578, (1996).
[34] D. J. Saltman, *Noncrossed Products of Small Exponent*, Proc. Amer. Math. Soc., **68**, 165–168, (1978).
[35] D. J. Saltman, *Noncrossed product p-algebras and Galois p-extensions*, J. Algebra, **52**, 302–314, (1978).
[36] D. J. Saltman, Azumaya Algebras over Rings of Characteristic p,Doctoral Dissertation, Yale University, 1976.
[37] R. L. Snider, *Is the Brauer Group Generated by Cyclic Algebras?*, in Ring theory (Proc. Conf., Univ. Waterloo, Waterloo, 1978), LNM **734**, 279–301, 1979.
[38] A. A. Suslin, *Torsion in* K_2 *of fields*, K-Theory, **1**(1), 5–29, (1987).
[39] O. Teichmüller, *p-Algebren*, Deutsche Math., **1**, 362–388, (1936).
[40] W. van der Kallen, *The Merkurjev-Suslin Theorem*, in Orders and their Applications (Oberwolfach, 1984), LNM **1142**, 157–168, 1985.