The Dissertation Committee for John Lockwood Hammond IV
certifies that this is the approved version of the following dissertation:

Regular Realizations of p-Groups

Committee:

David Saltman, Supervisor

Daniel Allcock

David Ben-Zvi

Murray Schacher

John Tate

Regular Realizations of p-Groups

by

John Lockwood Hammond IV, B.S.

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

May 2008

For Fritz and Heike

Acknowledgments

Thanks are due to my advisor David Saltman for his advice and support, to John Tate for several helpful conversations, and to Steve McAdam for providing an excellent introduction to abstract Algebra and for his frank but encouraging assessment of my progress early on. I also thank my fellow graduate students, for sharing their enthusiasm for mathematics and providing a collegial atmosphere, in particular; Eric Chesebro, Jason DeBlois, Jim Kelliher, Richard Kent, Chris Leininger, Kelly McKinnie, Ben McReynolds, Clay Petsche, Russell Schwab, and Spencer Stirling. Most importantly, I thank Anna Popova for her patience.

John Lockwood Hammond IV

The University of Texas at Austin
May 2008

Regular Realizations of p-Groups

Publication No. _____

John Lockwood Hammond IV, Ph.D.
The University of Texas at Austin, 2008

Supervisor: David Saltman

This thesis is concerned with the Regular Inverse Galois Problem for p-groups over fields of characteristic unequal to p. Building upon results of Saltman, Dentzer characterized a class of finite groups that are automatically realized over every field, and proceeded to show that every group of order dividing p^4 belongs to this class. We extend this result to include groups of order p^5, provided that the base field k contains the p^3-th roots of unity. The proof involves reducing to certain Brauer embedding problems defined over the rational function field $k(x)$. Through explicit computation, we describe the cohomological obstructions to these embedding problems. Then by applying results about the Brauer group of a Dedekind domain, we show that they all possess solutions.

Contents

Chapter 1

Introduction

A regular realization of a finite group G over a field k is a G-Galois extension of fields L/K such that, K is a rational function field over k, and L is a regular extension of k. If such an extension exists then we say that G is regular over k. The Regular Inverse Galois Problem for k is to determine which finite groups are regular over k. There are certain fields k for which this problem has a complete solution, but the general case remains quite open. This thesis is the result of an attempt to prove a regular analog of the theorem of Scholz-Reichardt [Se2, Theorem 2.1.1, p. 9] which asserts that every group of odd prime power order is realized as the group of some Galois extension of the field of rational numbers. We offer two theorems concerning regular realizations of odd p-groups over a field k of characteristic unequal to p. The first is that, if k contains the p^{n+1}-th roots of unity then every extension of the wreath product $\mathcal{C}_{p^n} \wr \mathcal{C}_{p^n}$ by the cyclic group $\mathcal{C}_p$ is regular over k. The second is that, if k contains the p^3-th roots of unity then every group of order p^5 is regular over k.

In the proof of the first main theorem, we construct a regular extension L of the rational field $K = k(x)$ with group isomorphic to the wreath product, and consider the obstruction associated to the embedding problem for a central extension E of $\mathrm{Gal}(L/K)$ by a cyclic group of order p. By exploiting the relationships among the Brauer groups of the field K, its completions, the polynomial ring $k[x]$, and its localizations, we show that the obstruction is trivial. From this it follows that E is regular over k. In the proof of the second main theorem, we show that each group of order p^5 is either, a group that can be realized over k by the method of reduction, or else a quotient of a group of the form considered in the first main theorem.

Chapter 1 contains various preliminary material, including a review of some well-known group theoretic constructions, the necessary results concerning p-groups, and the method of Dentzer for obtaining regular realizations of reducible groups. Chapter 2 presents the relevant cohomological prerequisites. In it we give an introduction to the cohomology of groups, followed by sections on Galois cohomology, group extensions, and Brauer embedding problems. In Chapter 3, we collect the necessary material related to the Brauer group of a commutative ring. We begin by introducing the notion of an Azumaya algebra, then we show how the classical crossed product construction generalizes to the Azumaya case. In the third section we offer a treatment of norm residue symbols over certain commutative rings. In the last section, we pay special attention to the case of Dedekind domains and discrete valuation rings. The formal statements and proofs of the main theorems, along with the relevant description of cohomology of the wreath product, are all given in Chapter 5.

Chapter 2

Preliminaries

2.1 Notation

Let X and Y be sets. Then $\mathrm{Map}(X, Y)$ denotes the set of all maps $m\colon X \to Y$. If Y is a group, then we will always view $\mathrm{Map}(X, Y)$ as a group under pointwise multiplication in Y. That is, for each pair $f, g \in \mathrm{Map}(X, Y)$ we define $f \cdot g \in \mathrm{Map}(X, Y)$ by setting $(f \cdot g)(x) = f(x) \cdot g(x)$ for all $x \in X$. Given a map $f\colon X \to \mathrm{Map}(Y, Z)$ we will often write f_x instead of $f(x)$ and hence $f_x(y)$ instead of $f(x)(y)$. The same convention will apply to maps $f\colon X \to \mathrm{Aut}(G)$, $f\colon X \to \mathrm{Gal}(L/K)$, $f\colon X \to \mathrm{End}_R(S)$ and so on. We denote by $\mathbf{1}_X$ the identity map $\mathbf{1}_X\colon X \to X$.

We write $H \leq G$ if H is a subgroup of G, and $H < G$ if H is a proper subgroup of G. We let $\mathbf{Z}(G)$ denote the center of G. For $H \leq G$, we let $\mathbf{N}_G(H)$ and $\mathbf{C}_G(H)$ denote the normalizer and the centralizer of H in G respectively. For each pair of elements $x, y \in G$, we define

$$[x, y] = x^{-1}y^{-1}xy$$

For each $n = 3, 4, 5, \ldots$, and $x_1, \ldots, x_n \in G$ we define inductively

$$[x_1, \ldots, x_{n-1}, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$$

For subgroups $H, K \leq G$, we denote by $[H, K]$ the subgroup of G generated by all commutators of the form $[h, k]$ with $h \in H$ and $k \in K$. For each $n = 1, 2, 3, \ldots$, we define the

n-th commutator subgroup of G, denoted $\mathbf{K}_n(G)$, by setting $\mathbf{K}_1(G) = G$ and

$$\mathbf{K}_n(G) = [\mathbf{K}_{n-1}(G), G] \qquad \text{for } n = 2, 3, 4, \ldots.$$

The group G is said to be *nilpotent of class* c if $\mathbf{K}_c(G) \neq 1$ but $\mathbf{K}_{c+1}(G) = 1$.

By a left *G-set*, we mean a set X endowed with a left G-action. A *G-group* is G-set X that is also a group, and is such that the transform by each element of G is an automorphism of X. A *G-module* is an abelian G-group. Let G and H be groups, and X a left G-set. We endow $\mathrm{Map}(X, H)$ with the structure of a G-group by setting

$$(f^\sigma)(x) = f(\sigma \cdot x) \qquad \text{for all } f \in \mathrm{Map}(X, H),\ \sigma \in G.$$

The *wreath product of H and G with respect to X*, denoted $H \wr_X G$, is defined to be the semidirect product $G \ltimes \mathrm{Map}(X, H)$. If m is a natural number then $\mathcal{C}_m$ denotes the cyclic group of order m. If p is a prime number then $\mathbb{F}_p$ denotes the field of p-elements.

If G is a group then the integral group ring of G, denoted $\mathbb{Z}G$, is by definition the $\mathbb{Z}$-algebra generated by the symbols e_σ $(\sigma \in G)$ which multiply according to the rules in G. If G is a group, and A is a multiplicative G-module then the G-norm, denoted $\mathbf{Nm}_G$, is the function

$$\mathbf{Nm}_G \colon A \to A \qquad \mathbf{Nm}_G(a) = \prod_{\sigma \in G} \sigma(a)$$

If A is written additively then we define the G-norm as the analogous sum.

All rings are assumed to have a nonzero unit element. For $\varphi \colon R \to S$ to be a homomorphism of rings we require that $\varphi(1) = 1$. If P is a prime ideal of R then R_P denotes the localization of R at P. If M is an R-module then we write M_P for the R_P-module $M \otimes_R R_P$. If M is projective then the rank of M over R, denoted $[M : R]$, is defined to be the integer valued function on the set of prime ideals of R that maps a prime ideal P to the dimension of the R/P-vector space $M/PM = M \otimes_R R/P$.

Let K be a field. When we assume that K contains a primitive m-th root of unity then we implicitly assume then the characteristic of K does not divide m. In this situation, we denote the group of m-th roots of unity in K by $\boldsymbol{\mu}(m)$. The symbol K_s will always denote a separable closure of K, and $\mathrm{G}_K = \mathrm{Gal}(K_s/K)$. If L is a finite extension of K then we denote by $\mathbf{Nm}_K^L$ and $\mathbf{Tr}_K^L$ the norm and trace from L to K, respectively.

2.2 Useful Constructions

Let $\gamma\colon G \to K$ and $\eta\colon H \to K$ be homomorphisms of the groups G, H, K. Let L denote the subset of the direct product $G \times H$ consisting of all pairs (σ, τ) such that $\gamma(\sigma) = \eta(\tau)$. Let $\gamma_*\colon L \to H$ and $\eta_*\colon L \to G$ denote the restrictions to L of the canonical projections

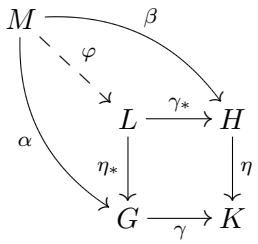
$$\gamma_*\colon L \to H \qquad \gamma_*(\sigma,\tau) = \tau \qquad\qquad \eta_*\colon L \to G \qquad \eta_*(\sigma,\tau) = \sigma$$

Then L is a subgroup of $G \times H$, and the maps γ^* and η^* are homomorphisms. We define the *pullback of γ and η* to be the triple (L, γ_*, η_*).

The pullback satisfies a useful universal mapping property, which we now describe. In the situation above, the compositions $\gamma \circ \eta_*$ and $\eta \circ \gamma_*$ are equal as maps from L to K. Moreover, given a group M and homomorphisms $\alpha\colon M \to G$ and $\beta\colon M \to H$ such that $\gamma \circ \alpha$ equals $\eta \circ \beta$, then the map

$$\varphi\colon M \to L \qquad \varphi(x) = (\alpha(x), \beta(x))$$

is the unique homomorphism from M to L that makes the following diagram commute



Concerning the pullback, we will have several opportunities to use the following lemma.

Lemma 2.1. *Let (L, γ_*, η_*) denote the pullback of the homomorphisms $\gamma\colon G \to K$ and $\eta\colon H \to K$. Then η_* restricts to an isomorphism from $\mathbf{ker}(\gamma_*)$ to $\mathbf{ker}(\gamma)$. If γ is monic (respectively epic) then so is γ_*.*

Proof. Since γ_* is the restriction of the canonical projection $G \times H \to H$, we have

$$\begin{aligned}\mathbf{ker}(\gamma_*) &= (G \times 1) \cap L \\ &= \{(\sigma, 1) : \sigma \in G, \gamma(\sigma) = \eta(1)\} \\ &= \{(\sigma, 1) : \sigma \in \mathbf{ker}(\gamma)\} \\ &= \mathbf{ker}(\gamma) \times 1\end{aligned}$$

which proves the first part. This also shows that γ is monic if and only if γ_* is. If γ is epic, then given $\tau \in H$ we can always find $\sigma \in G$ such that $\gamma(\sigma) = \eta(\tau)$. Equivalently, for each $\tau \in H$, there exists $\sigma \in G$ such that (σ, τ) belongs to L. Since γ_* sends (σ, τ) to τ this shows that γ_* is epic. □

Let G and H be groups. Every homomorphism $\theta\colon G \to \mathrm{Aut}(H)$ defines two action of G on H

$$^{\sigma}\tau = \theta_{\sigma}(\tau) \qquad \tau^{\sigma} = \theta_{\sigma^{-1}}(\tau) \qquad \text{for all } \sigma \in G,\, \tau \in H.$$

Under these two actions the compositions $^{\sigma}(\tau^{\sigma})$ and $(^{\sigma}\tau)^{\sigma}$ are both equal to τ. Accordingly the rules $(\sigma, \tau) \mapsto (^{\sigma}\tau, \sigma)$ and $(\tau, \sigma) \mapsto (\sigma, \tau^{\sigma})$ define mutually inverse isomorphisms between the semidirect products $G \ltimes H$ and $H \rtimes G$. Usually, we will omit θ and simply refer to H as a G-group, leaving the action implicitly specified. In the situation above, we will have several occasions to use the following lemma.

Lemma 2.2. *Let G, H and K be groups and let $\gamma\colon G \to K$ and $\eta\colon H \to K$ be homomorphisms. Assume that H is a G-group and that $\eta(\tau^{\sigma}) = \eta(\tau)^{\gamma(\sigma)}$ for all $\sigma \in G$ and $\tau \in H$. Then there exists a homomorphism $\varphi\colon G \ltimes H \to K$ that extends γ and η.*

Proof. Define $\varphi\colon G \ltimes H \to K$ by $\varphi(\sigma, \tau) = \gamma(\sigma) \cdot \eta(\tau)$. Then from the relation $\eta(\tau_1^{\sigma_2}) = \eta(\tau_1)^{\gamma(\sigma_2)}$ it is easy to see that

$$\varphi(\sigma_1\sigma_2, \tau_1^{\sigma_2}\tau_2) = \varphi(\sigma_1, \tau_1) \cdot \varphi(\sigma_2, \tau_2) \qquad \text{for all } \sigma_1, \sigma_2 \in G,\, \tau_1, \tau_2 \in H.$$

Thus φ is a homomorphism that extends γ and η. □

2.3 Finite p-Groups

Let G be a finite group. The *Frattini subgroup of* G, denoted $\mathbf{\Phi}(G)$, is defined to be the intersection of all maximal proper subgroups of G. If G is trivial then there are no maximal proper subgroups and so $\mathbf{\Phi}(G) = G$, otherwise $\mathbf{\Phi}(G)$ is a proper subgroup of G. In either case, $\mathbf{\Phi}(G)$ is a characteristic subgroup of G. The elements of $\mathbf{\Phi}(G)$ are sometimes termed *non-generators* because, as the following theorem shows, they can safely be removed from any generating set for G.

Theorem 2.3. *Let G be a finite group.*

(a) *Let $X \subseteq G$. Then $G = \langle X \rangle$ if and only if $G = \langle X, \mathbf{\Phi}(G) \rangle$.*

(b) *Let $N \trianglelefteq G$ be a normal subgroup. There exists a proper subgroup $H < G$ such that $G = HN$ if and only if $N \not\leq \mathbf{\Phi}(G)$.*

Proof. In part (a), if X generates a proper subgroup of G then there exists a maximal proper subgroup $M < G$ such that $X \subseteq M$. Since $\mathbf{\Phi}(G) \leq M$ we also have $\langle X, \mathbf{\Phi}(G) \rangle \leq M$ and thus $\langle X, \mathbf{\Phi}(G) \rangle$ cannot equal G. Therefore if G equals $\langle X, \mathbf{\Phi}(G) \rangle$ then X must generate G. The converse is obvious.

For (b), if $N \leq \mathbf{\Phi}(G)$ and $G = HN$ then $G = H$ by part (a). Therefore if $H < G$ is a proper subgroup and $G = HN$ then $N \not\leq \mathbf{\Phi}(G)$. For the converse, if $N \not\leq \mathbf{\Phi}(G)$, then there exists a maximal proper subgroup $M < G$ such that $N \not\leq M$. It follows that M is a proper subgroup of MN. By the maximality of M, this implies that MN equals G. □

Theorem 2.4. *Let G be a finite group and $N \trianglelefteq G$ a normal subgroup.*

(a) *We have $\mathbf{\Phi}(G)N/N \leq \mathbf{\Phi}(G/N)$.*

(b) *If $N \leq \mathbf{\Phi}(G)$ then $\mathbf{\Phi}(G)/N = \mathbf{\Phi}(G/N)$.*

Proof. See [Hu, Hilfssatz 3.4, p. 269]. □

Theorem 2.5 is [Hu, Satz 3.17, p. 274]. We include a proof for the convenience of the reader.

Theorem 2.5 (P. Hall)**.** *Let G be a finite group. If G can be generated by d elements then the order of* $\mathrm{Aut}(G)$ *divides* $|\mathrm{Aut}(G/\mathbf{\Phi}(G))| \cdot |\mathbf{\Phi}(G)|^d$.

Proof. As $\mathbf{\Phi}(G)$ is a characteristic subgroup of G, every automorphism of G acts by automorphism on the quotient $G/\mathbf{\Phi}(G)$. Let K denote the kernel of the resulting homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(G/\mathbf{\Phi}(G))$. Then to prove the theorem, it is enough to show that the order of K divides $|\mathbf{\Phi}(G)|^d$. To see this fix a d-element generating set $\{x_1, \ldots, x_d\}$ for G and let B denote the subset of the cartesian product $\prod_{i=1}^{d} G$ consisting of all d-tuples of the form

$$(x_1 \cdot f_1, \ldots, x_d \cdot f_d) \qquad \text{with } f_1, \ldots, f_d \in \mathbf{\Phi}(G).$$

Since K acts trivially on the quotient $G/\mathbf{\Phi}(G)$, the diagonal action of $\mathrm{Aut}(G)$ on the product $\prod_{i=1}^{d} G$ defines by restriction an action of K on B. We claim that B acts freely on K. As the components of each $b \in B$ comprise a generating set for G, the only automorphism of G that fixes b is the identity. Thus for each $b \in B$, the stabilizer of b in K is trivial, which proves the claim. Thus the length of each K-orbit in B is equal to the order of K. Therefore $|B| = |K| \cdot n$, where n is the number of orbits of K in B. In particular $|K|$ divides $|B|$. Since $|B| = |\mathbf{\Phi}(G)|^d$ this proves the theorem. □

For the rest of this section, we turn our attention to the class of finite p-groups. We begin with a theorem that collects the most useful properties of this class.

Theorem 2.6. *Let G be a finite p-group.*

(a) *The group G is nilpotent.*

(b) *If $H < G$ is a proper subgroup then $H < \mathbf{N}_G(H)$.*

(c) *If $N \trianglelefteq G$ is nontrivial normal subgroup then the intersection $N \cap \mathbf{Z}(G)$ is again nontrivial and commutator subgroup $[N, G]$ is a proper subgroup of N.*

(d) *We have $\mathbf{\Phi}(G) = \langle G^p, \mathbf{K}_2(G) \rangle$. For each subgroup $H \leq G$, we have $\mathbf{\Phi}(G) \leq H$ if and only if H is normal in G and the quotient G/N is elementary abelian.*

Proof. Parts (a) and (b) can be found in [Hu, Hauptsatz 2.3, p. 260]. For part (c), see [Hu, Satz 2.6, p. 262]. For the first half of part (d), see [Hu, Satz 3.14, p. 272]. The second is immediate from the first. □

By part (d) of Theorem 2.6, if G is a finite p-group then the quotient $G/\mathbf{\Phi}(G)$ is a $\mathbb{F}_p$-vector space. We define the *rank of G* to be its dimension.

Theorem 2.7 (Burnside Basis Theorem)**.** *Let G be a finite p-group of rank d. Then every minimal set of generators for G has exactly d elements and every element of G that does not belong to $\mathbf{\Phi}(G)$ occurs in a generating set with d elements.*

Proof. With Theorem 2.6, this is an immediate consequence of the analogous statement for vector spaces. See [Hu, Satz 3.15, p. 273]. □

Recall that a group G is said to be *metacyclic* if it has a cyclic normal subgroup $N \trianglelefteq G$ such that the quotient G/N is also cyclic. As Lemma 2.9 will show, metacyclic p-groups are of a relatively simple structure. By exploiting this structure, we will be able to simplify the proof of the second main theorem. Theorem 2.8 below is a simplified version of a characterization of metacyclic p-groups due to N. Blackburn [Hu, Hilfssatz 11.3, p. 336].

Theorem 2.8. *If G is a finite p-group then G is metacyclic if and only if $G/\mathbf{K}_3(G)$ is.*

Before proving Theorem 2.8, we need the lemma promised above.

Lemma 2.9. *Let G be a finite p-group and $T \trianglelefteq G$ a normal subgroup. If T and G/T are both cyclic then there exist $\sigma, \tau \in G$ such that*

$$G = \langle \sigma, T \rangle \qquad T = \langle \tau \rangle \qquad [\tau, \sigma] \in T^p$$

Proof. If T is trivial then the lemma is obvious. Otherwise, part (c) of Theorem 2.6 implies that $[T, G]$ is a proper subgroup of T. Since T is a cyclic p-group, every proper subgroup of T is contained in the subgroup of p-th powers T^p. Hence the commutator $[t, s]$ belongs to T^p for all $s \in G$ and $t \in T$. Thus any pair of elements $\sigma \in G$ and $\tau \in T$ such that $G/T = \langle \sigma T \rangle$ and $T = \langle \tau \rangle$ will suffice. □

Proof of Theorem 2.8. If G is metacyclic then clearly so is G/N for every normal subgroup $N \trianglelefteq G$. In particular if G is metacyclic then so is $G/\mathbf{K}_3(G)$. To prove the converse we proceed inductively. If G is trivial then the theorem is obvious. Thus we assume that G is nontrivial, the theorem holds for every proper quotient of G, and that $G/\mathbf{K}_3(G)$ is metacyclic. If $\mathbf{K}_3(G)$ is trivial then there is also nothing to show. Assuming this is not the case, $\mathbf{K}_3(G)$ must intersect $\mathbf{Z}(G)$ nontrivially. Hence there exists $U \leq \mathbf{K}_3(G)$ such that $U \leq \mathbf{Z}(G)$ and U is cyclic of order p.

As $U \leq \mathbf{K}_3(G)$, we have $\mathbf{K}_3(G/U) = \mathbf{K}_3(G)/U$ and thus

$$\frac{G/U}{\mathbf{K}_3(G/U)} = \frac{G/U}{\mathbf{K}_3(G)/U} = \frac{G}{\mathbf{K}_3(G)}$$

Hence $(G/U)/\mathbf{K}_3(G/U)$ is metacyclic. Therefore the inductive hypothesis implies the same for G/U. Hence there exists a normal subgroup $N \trianglelefteq G$ that contains U and is such that the quotients G/N and N/U are both cyclic. If N is cyclic then it follows that G is metacyclic, which proves the theorem.

To show that N is cyclic, we apply Lemma 2.9 to the quotient G/U. There exist elements $s, t \in G$ such that

$$G = \langle s, N \rangle \qquad N = \langle t, U \rangle \qquad [t, s] \in \langle t^p, U \rangle$$

Since the images of s and t generate G/U and we have $U \leq \mathbf{K}_3(G) \leq \mathbf{\Phi}(G)$, it follows that s and t generate G. Let $T = \langle t \rangle$. Thus we have $N = \langle T, U \rangle$ and we claim that $U \leq T$. If this is so, then N equals T and therefore N is cyclic.

Let u be a generator for U. Since $U \leq \mathbf{Z}(N)$ and N/U is cyclic, it follows that N is abelian. Therefore since $[t, s]$ belongs to $\langle T^p, U \rangle$, there are integers q and r such that $p \mid q$ and

$$[t, s] = t^q \cdot u^r$$

Since $[t, s]$ commutes with t we have $[t^k, s] = [t, s]^k$ for every integer k. Consequently

$$[t^q, s] = (t^q \cdot u^r)^q = t^{q^2}$$

As s and t generate G, this implies that T^q is normal in G. By [Hu, Hilfssatz 1.11, p. 258], $\mathbf{K}_3(G)$ is the smallest normal subgroup of G that contains the triple commutators $[t, s, t]$ and $[t, s, s]$. Since N is abelian, we see that $[t, s, t]$ is trivial. And from the equation above, we have

$$[t, s, s] = [t^q \cdot u^r, s] = [t^q, s] = t^{q^2}$$

Since $[t, s, t]$ and $[t, s, s]$ both belong to the normal subgroup T^q, it follows that $\mathbf{K}_3(G) \leq T$. But this implies that $U \leq T$. Thus T is cyclic and therefore G is metacyclic. □

The last theorem of this section is the promised application of Theorem 2.5. The theorem gives a useful upper bound on the index of a maximal abelian normal subgroup in a p-group. In particular, the theorem guarantees that for each $n = 1, 2, 3, 4$, every group of order p^n has an abelian normal subgroup of index p. This fact will be used to show that every such group has a regular realization over every field.

Theorem 2.10. *Let G be a finite p-group and assume that A is maximal among the abelian normal subgroups of G. If $|G| = p^n$ and $|A| = p^m$ then*

$$2n \leq m(m+1)$$

Proof. We claim that A equals its own centralizer in G. Since A is abelian, we have $A \leq \mathbf{Z}(\mathbf{C}_G(A))$. As A is normal in G, so is $\mathbf{C}_G(A)$. Assume for a contradiction, that A is a proper subgroup of $\mathbf{C}_G(A)$. Then by a repeated application of part (c) of Theorem 2.6, or by [Hu, Satz 7.2, p. 310], there exists a normal subgroup $N \trianglelefteq G$ that contains A as a central subgroup of index p. But then $N/\mathbf{Z}(N)$ is cyclic and therefore N is abelian. As we are assuming that A is maximal among the abelian normal subgroups of G, this is a contradiction.

Let d denote the rank of $A/\mathbf{\Phi}(A)$. Then the automorphism group of $A/\mathbf{\Phi}(A)$ is isomorphic to the general linear group $\mathbf{GL}_d(\mathbb{F}_p)$ and therefore the order of $\mathrm{Aut}(A/\mathbf{\Phi}(A))$ is of the form $p^{d(d-1)/2} \cdot q$ where $p \nmid q$. By the Burnside Basis Theorem, A is minimally generated by d elements and with Theorem 2.5 this implies that the order of $\mathrm{Aut}(A)$ divides

$$|\mathrm{Aut}(A/\mathbf{\Phi}(A))| \cdot |\mathbf{\Phi}(A)|^d = p^{d(d-1)/2} \cdot q \cdot p^{(m-d)d}$$

Since A is normal in G and equal to its own centralizer, the NC-Lemma [Hu, Satz 4.5, p. 20] implies that the quotient G/A is isomorphic to a subgroup of $\mathrm{Aut}(A)$. Since G/A has order p^{n-m} and $p \nmid q$, we must have

$$n - m \leq d(d-1)/2 + (m-d)d$$

Letting $r = m - d$, the inequality above is equivalent to

$$2n \leq m(m+1) - r(r-1)$$

As r is an integer, it is easy to see that $r(r-1)$ is nonnegative. Therefore we have $2n \leq m(m+1)$ as desired. □

2.4 Regular Extensions of Fields

Let F/k be an extension of fields. We call F a *rational extension of* k if F is a finitely generated, purely transcendental extension of k. We call F a *regular extension of* k if F is a separable extension of k, and k is algebraically closed in F. If k is a field and G a finite group then by a *regular realization of* G *over* k, we mean a finite Galois extension of fields L/K, such that K/k is rational, L/k is regular, and $\mathrm{Gal}(L/K)$ is isomorphic to G. If such an extension exists then we say that G *is regular over* k.

The Regular Inverse Galois Problem for the field k is to determine which finite groups are regular over k. Although we are interested in this problem for its own sake, one source of motivation is the Inverse Galois Problem for Hilbertian fields. Recall that k is said to be Hilbertian if, given finitely many irreducible polynomials $f_1(x,y),\ldots,f_n(x,y) \in k(x)[y]$, there are infinitely many values $a \in k$ for which $f_1(a,y),\ldots,f_n(a,y)$ are all defined and irreducible in $k[y]$. Hilbert's Irreducibility Theorem [Se2, p. 25] asserts that every algebraic number field is Hilbertian. By combining [Se2, Corollary 3.3.4, p. 23] with the results of this section one can show that, if G is regular over k then every Hilbertian field that contains k has infinitely many linearly disjoint G-Galois extensions. The main goal of this section is to show that a large class of finite groups are regular over every field. We begin by recording some useful and well-known facts concerning regular extensions.

First of all, every rational extension of fields is regular [Bo2, Proposition 5, V.141]. Also, every subextension of a regular extension is again regular, and regularity is transitive in towers [La1, Proposition 4.11, p. 367]. More precisely, if F/k is regular then so is E/k for each extension E of k contained in F, and if E/k and F/E are both regular then so is F/k. In what follows, we will often consider pairs of extensions L/K and K/k, in which L/K is a finite Galois extension, and K/k is rational. We note that in this situation, the extension L/k is regular if and only if k is algebraically closed in L. The next theorem gives two alternative characterizations of regularity.

Theorem 2.11. *Let E/k be an extension of fields, E_a an algebraic closure of E, and k_a the algebraic closure of k contained in E_a. The following conditions are equivalent.*

(a) *The extension E/k is regular.*

(b) *The fields E and k_a are linearly disjoint over k.*

(c) *For each extension F of k, the tensor product $E \otimes_k F$ is an integral domain and its field of fractions is a regular extension of F.*

Proof. See [Bo2, Chapter V, Propositions 8 & 9, p .142]. □

Assume E/k is regular, and that E_a and k_a are defined as in the theorem. Then we say that a polynomial $f(x) \in E[x]$ is *absolutely irreducible* if $f(x)$ is irreducible over the compositum Ek_a. The next theorem contains a slight generalization of the well-known fact that, if E is a regular extension of k and $\alpha \in E_a$ is a zero of an absolutely irreducible polynomial $f(x) \in E[x]$ then $E(\alpha)$ is also a regular extension of k. For our purposes, this and Theorem 3.19 in Section 3.4 will provide the most useful criteria for regularity.

Theorem 2.12. *Let E/k be a regular extension of fields, E_a an algebraic closure of E, and k_a the algebraic closure of k contained in E_a. An extension F of E contained in E_a is a regular extension of k if and only if F and Ek_a are linearly disjoint over E. If F/E is finite and $[F : E] = [Fk_a : Ek_a]$ then F is a regular extension of k.*

Proof. Since E and k_a are linearly disjoint over k, an application of [La1, Proposition 3.1, p. 361] shows that F and k_a are linearly disjoint over k if and only if F and Ek_a are linearly disjoint over E. This proves the first part. For the second, to show that F is linearly disjoint from Ek_a over E, it is enough to show that a E-basis for F remains linearly independent over Ek_a. If $[F : E] = [Fk_a : Ek_a]$ then this must be the case. □

Let E and F be two extensions of k at least one of which is regular. Then the field of fractions of the integral domain $E \otimes_k F$ is the compositum of its subfields $E \otimes 1$ and $1 \otimes F$. When no confusion can occur, we identify $E \otimes 1$ with E, $1 \otimes F$ with F, and the field of fractions of $E \otimes_k F$ with the compositum EF. The next theorem has an important consequence for the Regular Inverse Galois Problem. Namely, it implies that whenever G is regular over k, then G is also regular over every field that contains k.

Theorem 2.13. *Let L/K be a regular realization of the finite group G over the field k. For each extension E of k, the translated extension LE/KE is a regular realization of G over E.*

Proof. It is clear that KE is a rational extension of E, and Theorem 2.11 implies that LE is a regular extension of E. Since LE is equal to the compositum of L and KE, we know from elementary Galois theory [La1, Theorem 1.12, p. 266], that LE/KE is Galois, and that restriction of automorphisms from LE to L defines an isomorphism from $\mathrm{Gal}(LE/KE)$ to $\mathrm{Gal}(L/L \cap KE)$. Hence to show that $\mathrm{Gal}(LE/KE)$ is isomorphic to G, it is enough to show that $L \cap KE = K$. Since L and E are linearly disjoint over k, an application of [La1,

Proposition 3.1, p. 361] shows that the fields L and KE are linearly disjoint over K. Thus $L \cap KE = K$ and therefore the extension LE/KE is a regular realization of G over E. $\square$

We continue with an easy but important theorem which asserts that the class of finite groups that are regular over k is closed under formation of finite direct products and taking quotients by normal subgroups.

Theorem 2.14. *Let k be a field and G a finite group.*

(a) *Assume $G = G_1 \times \cdots \times G_n$ and that for each $i = 1, \ldots, n$, the extension L_i/K_i is a regular realization of G_i over k. Then $(L_1 \cdots L_n)/(K_1 \cdots K_n)$ is a regular realization of G over k.*

(b) *Let $N \trianglelefteq G$ be a normal subgroup. If L/K is a regular realization of G over k then L^N/K is a regular realization of G/N over k.*

Proof. In part (a), by an obvious inductive argument we are immediately reduced to the case that $n = 2$. The field $K = K_1K_2$ is clearly a rational extension of k, and the compositum $L = L_1L_2$ is a regular extension of k by [Bo2, Proposition 8 (b), V.142]. Theorem 2.13 implies that for $i = 1, 2$, the extension L_iK/K is Galois with group isomorphic to G_i. Since L is the compositum of L_1K and L_2K, by elementary Galois theory [La1, Theorem 1.14, p. 267], to show that L/K is Galois with group isomorphic to G, it is enough to show that $K = L_1K \cap L_2K$. To see this, we apply [La1, Proposition 3.1, p. 361] twice. First, since fields L_1 and L_2 are linearly disjoint over k, the proposition implies that L_1K and L_2 are linearly disjoint over K_2. Second, from the linear disjointness of L_1K and $L2$ over K_2, it implies the same for L_1K and L_2K over K. Thus $K = L_1K \cap L_2K$ which completes the proof of (a). Part (b) is obvious. $\square$

More complicated than Theorem 2.14, but just as important for out purposes, the next theorem shows that the class of groups regular over a given field is also closed under formation of wreath products.

Theorem 2.15. *Let k be a field, G and H finite groups, and I a finite G-set. If G and H are both regular over k then so is the generalized wreath product $H \wr_I G$.*

In the proof of Theorem 2.15 we will make use of the following lemma due to Miyata. The lemma is an application of Galois descent for vector spaces. Namely, let L/K be a

finite Galois extension of fields, $G = \mathrm{Gal}(L/K)$, and V an L-vector space. Assume there is a K-linear action of G on V such that

$$\sigma(x \cdot v) = \sigma(x) \cdot \sigma(v) \qquad \text{for all } \sigma \in G,\, x \in L,\, v \in V.$$

Then by Galois descent for vector spaces [KO, Theorem 5.1, p. 44], the natural homomorphism $L \otimes_K \left(V^G\right) \to V$ is an isomorphism of L-vector spaces.

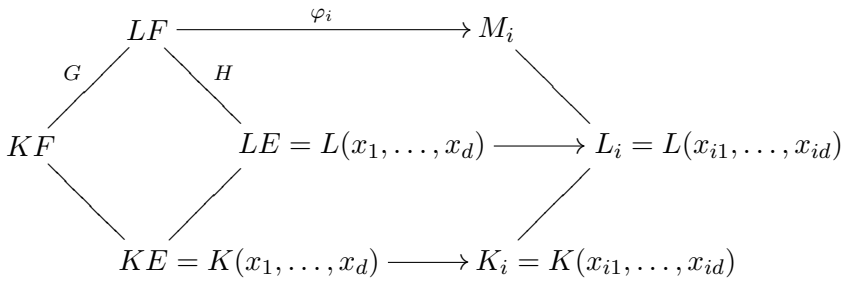
Lemma 2.16. *Let L/K be a finite G-Galois extension of fields, $E = L(x_1, \ldots, x_d)$ a rational extension of L, and V the L-subspace of E with basis $\{x_1, \ldots, x_d\}$. Assume the action of G on L extends to an action by automorphisms of E. If the extended action preserves V then the fixed field of G in E is a rational extension of K.*

Proof. Assume the action of G preserves V and let $U = V^G$ the K-subspace consisting of all G-fixed vectors in V. By Galois descent, the natural map $L \otimes_K U \to V$ is an isomorphism of L-vector spaces. In particular $[U : K] = [V : L]$ and every K-basis for U is also an L-basis for V. Let $\{u_1, \ldots, u_d\}$ be a K-basis for U and set $F = K(u_1, \ldots, u_d)$.

We claim that F is the fixed field of G in E. Clearly F is contained in E^G, and so it is enough to show that $[E : F] \leq [E : E^G]$. As $\{u_1, \ldots, u_d\}$ is an L-basis for V, the fields E and $L(u_1, \ldots, u_d)$ are equal. Thus $E = LF$ and hence $[E : F] \leq [L : K]$. But E/E^G and L/K are both G-Galois extensions and so their degrees are both equal to the order of G. It follows that $[E : F] \leq [E : E^G]$ and therefore $F = E^G$. Now because E/F is algebraic, the set $\{u_1, \ldots, u_d\}$ must comprise a transcendence basis for E/K. Therefore the elements $u_1, \ldots, u_d$ are algebraically independent over K and thus F is a rational extension of K. □

Proof of Theorem 2.15. Without loss of generality, we may assume that $I = \{1, \ldots, n\}$ for some natural number n. Let L/K and F/E be regular realizations of G and H over k. We note that by Theorem 2.14, the extension LF/KE is a regular realization of $G \times H$ over k. Suppose that $E = k(x_1, \ldots, x_d)$ where $x_1, \ldots, x_d$ are indeterminates, and for each $i \in I$, let $M_i/L_i/K_i$ denote the isomorphic copy of the tower $LF/LE/KE$ obtained by replacing $x_1, \ldots, x_d$ with new indeterminates $x_{i1}, \ldots, x_{id}$. Thus for each $i \in I$, there exists

an isomorphism of fields $\varphi_i \colon LF \to M_i$ that gives a commutative diagram



Let $M_I = M_1 \cdots M_n$ denote the external compositum of the fields $M_1, \ldots, M_n$ taken over k. Let $L_I = L_1 \cdots L_n$ and $K_I = K_1 \cdots K_n$ denote the composita taken in M_I.

Each $\sigma \in G$ extends uniquely to an automorphism of M_I/K_I such that, for each $i \in I$, the restriction of σ to M_i gives a commutative diagram

$$\begin{array}{ccc} LF & \xrightarrow{\sigma} & LF \\ \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_{\sigma(i)}} \\ M_i & \xrightarrow{\sigma} & M_{\sigma(i)} \end{array}$$

In particular, $\sigma(x_{ij}) = x_{\sigma(i)j}$ for all $i \in I$ and all $j = 1, \ldots, d$. Similarly, for each $\tau \in H$ and $i \in I$ there exists a unique automorphism τ_i of M_I/L_I that acts as the identity on the fields M_j for all $j \neq i$ and makes the following diagram commute

$$\begin{array}{ccc} LF & \xrightarrow{\tau} & LF \\ \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_i} \\ M_i & \xrightarrow{\tau_i} & M_i \end{array}$$

For each $i \in I$, let $H_i = \{\tau_i : \tau \in H\}$, and set $H_I = \prod_{i \in I} H_i$. Then the rule $\tau \mapsto \tau_i$ defines an isomorphism $H \to H_i$, and restriction of automorphisms from M_I to M_i an isomorphism $H_i \to \mathrm{Gal}(M_i/L_i)$. With Theorem 2.14 we see that M_I/L_I is a regular realization of H_I over L. As we are assuming that the extension L/k is regular, by the transitivity of regularity, so is M_I/k.

Let W denote the subgroup of $\mathrm{Aut}_{K_I}(M_I)$ generated by G and H_I. We claim that W is a split extension of G by H_I. Applying the definitions above, we have $\sigma \circ \tau_i = \tau_{\sigma(i)} \circ \sigma$ for all $\sigma \in G$, $\tau \in H$ and $i \in I$. Thus G normalizes H_I. Assume that $\omega \in G \cap H_I$.

Then since ω belongs to H_I, it fixes L_I and hence L. But each element of G is uniquely determined by its restriction to L and so ω is the identity. Therefore the intersection $G \cap H_I$ is trivial, and thus W is a split extension of G by H_I, which proves the claim. Now by considering the action of G on H_I, it is immediate that W is isomorphic to the generalized wreath product $H \wr_I G$.

To complete the proof of the theorem, it remains only to show that the fixed field of W in M_I is a rational extension of k. Since $G = W/H_I$ and the fixed field of H_I in M_I is L_I, it is enough to show that the fixed field of G in L_I is a rational extension of k. But L/K is G-Galois and L_I/L is rational with a transcendence basis permuted by the action of G. Hence Lemma 2.16 implies that L_I^G is a rational extension of K. Since K/k is rational by assumption, and rationality is clearly transitive, it follows that $(L_I)^G/k$ is also rational. □

The main result of this section is the next theorem. When combined with Theorem 2.14, without any hypothesis on k, it implies that the class of groups that are regular over k is fairly large, as it contains every finite abelian group and is closed under products, quotients, and split extensions by abelian groups. We will give further consideration to the groups that are automatically realized over every field in Theorems 2.18 and 2.19 below.

Theorem 2.17. *Let k be a field, G a finite group, and A a finite G-module. If G is regular over k then so is the semidirect product $G \ltimes A$.*

Proof. The group A is regular over k by [Sa1, Theorem 3.12 (a)]. With Theorem 2.15, we see that the wreath product $A \wr G$ is regular over k. Hence by Theorem 2.14, to prove the theorem, it is enough to show that the semidirect product $G \ltimes A$ is isomorphic to a quotient of the wreath product $A \wr G$.

As in Section 2.1, we represent the wreath product $A \wr G$ as the semidirect product $G \ltimes M$ where $M = \mathrm{Map}(G, A)$ is the set of maps from G to A under pointwise multiplication with G-action such that $(f^\sigma)(\tau) = f(\sigma\tau)$ for all $f \in M$ and $\sigma, \tau \in G$. Since G is finite and the groups A and M are both abelian, there is a homomorphism of abelian groups

$$\mu \colon M \to A \qquad \mu(f) = \prod_{\rho \in G} f(\rho^{-1})^\rho$$

By constructing suitable elements of M, it is easy to see that μ is epic. We claim that μ

is a homomorphism of G-modules. We need to show that for each $\sigma \in G$, the products

$$\mu(f^\sigma) = \prod_{\rho \in G} f(\sigma\rho^{-1})^\rho \qquad (\mu(f))^\sigma = \prod_{\rho \in G} f(\rho^{-1})^{\rho\sigma}$$

are equal. To see this define $g\colon G \to A$ by $g(\rho) = f(\sigma\rho^{-1})^\rho$. Then we have

$$\mu(f^\sigma) = \prod_{\rho \in G} g(\rho) \qquad (\mu(f))^\sigma = \prod_{\rho \in G} g(\rho\sigma)$$

As ρ ranges over the elements of G, so does $\rho\sigma$. Since A is abelian, it follows that the two products displayed above are equal. Therefore $\mu(f^\sigma) = \mu(f)^\sigma$ for all $\sigma \in G$, which proves the claim. Now by Lemma 2.2, there exists a homomorphism $\pi\colon G \ltimes M \to G \ltimes A$ that extends the identity on G and μ on M. As the semidirect product $G \ltimes A$ is generated by G and the image of μ, it follows that π is epic. □

Theorem 2.17 suggests the following relation on the category of finite groups. Let G and H be finite groups. We say that G *reduces to* H if there exists a sequence of groups $G_0, G_1, \ldots, G_n$ with $G = G_0$ and $H = G_n$, such that for each $i = 1, \ldots, n$, there exists a finite G_i-module A_i and an epimorphism $\pi_i\colon G_i \ltimes A_i \to G_{i-1}$. By an inductive application of Theorem 2.17, we have the next theorem. Loosely speaking it asserts that, if G reduces to H then proving that G is regular over k reduces to proving that H is.

Theorem 2.18. *Let G and H be finite groups and k a field. If H is regular over k, and G reduces to H, then G is also regular over k.*

Proof. The proof is immediate. □

We say that a finite group G is *reducible* if it reduces to one of its proper subgroups, otherwise we say that G is *irreducible*. The next theorem, a characterization of irreducible groups, is essentially [De, Corollary 2.4]. As irreducibility is defined slightly differently by Dentzer, we offer a proof of the theorem below.

Theorem 2.19 (Dentzer)**.** *Let G be a finite group. Then G is irreducible if and only if every abelian normal subgroup of G is contained in $\mathbf{\Phi}(G)$.*

Lemma 2.20. *The following conditions on a finite group G are equivalent.*

(a) *The group G reduces to one of its proper subgroups.*

(b) *The group G reduces to a group whose order properly divides that of G.*

(c) *The group G reduces to a group of smaller order.*

Proof. Clearly (a) implies (b) which in turn implies (c). To see that (c) implies (a), suppose that $G_0, G_1, \ldots, G_n$ is a sequence of finite groups such that for each $i = 1, \ldots, n$, there exists a finite G_i-module A_i and an epimorphism $\pi_i \colon G_i \ltimes A_i \to G_{i-1}$. Thus G_0 reduces to G_n and assuming that the order of G_0 is larger than that of G_n, we must show that G_0 reduces to one of its proper subgroups. In fact we will show that the sequence $G_0, G_1, \ldots, G_n$ may be replaced by an inductively defined sequence $H_0, H_1, \ldots, H_n$ where $H_0 = G_0$ and for each $i = 1, \ldots, n$ the group H_i is simultaneously a quotient of G_i and a subgroup of H_{i-1}.

Let $H_0 = G_0$ and for each $i = 1, \ldots, n$, let H_i and B_i denote the images of G_i and A_i under the composition

$$G_i \ltimes A_i \xrightarrow{\pi_i} G_{i-1} \to H_{i-1}.$$

It follows that the groups $B_1, \ldots, B_n$ are all abelian and since both of the arrows above are epic B_i is normal in H_{i-1}. By Lemma 2.2, for each $i = 1, \ldots, n$ there exists an epimorphism $\rho_i \colon H_i \ltimes B_i \to H_{i-1}$ that extends the inclusions of $H_i \to H_{i-1}$ and $B_i \to H_{i-1}$. Thus H_0 reduces to H_n. As we are assuming that the order of G_n is less than that of G_0, we see that H_n must be a proper subgroup of G_n. Therefore (c) implies (a). □

Proof of Theorem 2.19. Assume A is an abelian normal subgroup of G that is not contained in $\mathbf{\Phi}(G)$. Then by Theorem 2.3, there exists a proper subgroup $H < G$ such that $G = HA$. Now Lemma 2.2 implies the existence of an epimorphism $H \ltimes A \to G$. Therefore G reduces to its proper subgroup H. Conversely, assume that every abelian normal subgroup of G is contained in $\mathbf{\Phi}(G)$. Let G_1 be a finite group such that there exists an G_1-module A_1 and an epimorphism $\pi_1 \colon G_1 \ltimes A_1 \to G$. Then the image of A_1 is an abelian normal subgroup of G and so by assumption it must be contained in $\mathbf{\Phi}(G)$. Hence the restriction of π_1 to G_1 remains epic. It follows that, if G reduces to H then G is isomorphic to a quotient of H. In particular, the order of G is at most that of H. Therefore G is irreducible. □

Chapter 3

Cohomology of Groups

3.1 Generalities

This section contains a brief introduction to the cohomology of groups. The central object of the theory is a certain sequence of functors $\mathbf{H}_G$, defined for each group G, from the category of G-modules to the category of abelian groups. There are several equivalent ways of constructing the functors $\mathbf{H}_G$. We define them as the right-derived functors of the functor Fix_G which associates to each G-module A, the subgroup of all G-fixed elements A^G. We begin by recalling the notion of a right-derived functor and the encompassing notion of a δ-functor.

To fix ideas, let $\mathbf{M}$ be an abelian category, and $\mathbf{Ab}$ the category of abelian groups. In the initial applications we will take $\mathbf{M}$ to be $\mathbf{Mod}(G)$ the category of left modules over a group G. Readers who are allergic to abstract nonsense may assume that $\mathbf{M}$ is $\mathbf{Mod}(G)$ without losing the gist of the next few paragraphs. A *δ-functor* from $\mathbf{M}$ to $\mathbf{Ab}$ consists of a sequence of additive functors

$$\mathrm{F}^n \colon \mathbf{M} \to \mathbf{Ab} \qquad n = 0, 1, 2, \ldots$$

together with a rule that associates to each short exact sequence in $\mathbf{M}$

$$0 \to A \to B \to C \to 0$$

a sequence of homomorphisms, called *connecting homomorphisms*

$$\boldsymbol{\delta}^n \colon \mathrm{F}^n(C) \to \mathrm{F}^{n+1}(A) \qquad n = 0, 1, 2, \ldots$$

that make a long exact sequence of abelian groups

$$\begin{array}{l} 0 \longrightarrow \mathrm{F}^0(A) \longrightarrow \mathrm{F}^0(B) \longrightarrow \mathrm{F}^0(C) \xrightarrow{\boldsymbol{\delta}^0} \mathrm{F}^1(A) \\ \qquad\qquad \cdots \\ \longrightarrow \mathrm{F}^n(A) \longrightarrow \mathrm{F}^n(B) \longrightarrow \mathrm{F}^n(C) \xrightarrow{\boldsymbol{\delta}^n} \mathrm{F}^{n+1}(A) \longrightarrow \cdots \end{array}$$

and are such that for each morphism of short exact sequences in $\mathbf{M}$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0 \end{array}$$

and every $n = 0, 1, 2, \ldots$, there is a commutative diagram

$$\begin{array}{ccc} \mathrm{F}^n(C_1) & \xrightarrow{\boldsymbol{\delta}_1^n} & \mathrm{F}^{n+1}(A_1) \\ \downarrow & & \downarrow \\ \mathrm{F}^n(C_2) & \xrightarrow{\boldsymbol{\delta}_2^n} & \mathrm{F}^{n+1}(A_2) \end{array}$$

The conditions on the connecting homomorphisms imply that a δ-functor from $\mathbf{M}$ to $\mathbf{Ab}$ defines a functor from the category of short exact sequences in $\mathbf{M}$ to the category of long exact sequences of abelian groups. Let $\mathrm{F}, \mathrm{E} \colon \mathbf{M} \to \mathbf{Ab}$ be two δ-functors. A *morphism of δ-functors* $\varphi \colon \mathrm{F} \to \mathrm{E}$ is a sequence of morphisms $\varphi^n \colon \mathrm{F}^n \to \mathrm{E}^n$ defined for $n = 0, 1, 2, \ldots$ that commute with the associated connecting homomorphisms. The δ-functor F is said to be *universal* if every morphism $\varphi^0 \colon \mathrm{F}^0 \to \mathrm{E}^0$ has a unique extension to a morphism of δ-functors $\varphi \colon \mathrm{F} \to \mathrm{E}$.

The principal examples of δ-functors are right-derived functors. In order to define them we need to assume that the category $\mathbf{M}$ has *enough injectives*, meaning that for each object A of $\mathbf{M}$, there exists an injective object I of $\mathbf{M}$, and a monomorphism $\alpha \colon A \to I$. It follows by an obvious inductive argument that every object of $\mathbf{M}$ has an injective resolution

in $\mathbf{M}$. Thus for each object A of $\mathbf{M}$ there is an exact sequence

$$0 \to A \to I(A) \ : \ 0 \to A \to I^0 \xrightarrow{i^0} I^1 \xrightarrow{i^1} I^2 \xrightarrow{i^2} I^3 \to \cdots$$

where each I^n is an injective object in $\mathbf{M}$.

Let $\mathrm{F}\colon \mathbf{M} \to \mathbf{Ab}$ be a left-exact covariant additive functor. For each $n = 0, 1, 2, \ldots$, the *n-th right derived functor* of F is by definition the functor $\mathrm{RF}^n\colon \mathbf{M} \to \mathbf{Ab}$ that associates to each object A of $\mathbf{M}$ the n-th homology group of the complex

$$\mathrm{F}(I(A)) \ : \ 0 \to \mathrm{F}(I^0) \to \mathrm{F}(I^1) \to \mathrm{F}(I^2) \to \mathrm{F}(I^3) \to \cdots$$

Thus, with the convention that $i^{-1} = 0$, we have

$$\mathrm{RF}^n(A) = \mathbf{ker}(\mathrm{F}(i^n))/\mathbf{img}(\mathrm{F}(i^{n-1}))$$

In particular, $\mathrm{RF}^n(A)$ is a subquotient of the abelian group $\mathrm{F}(I^n)$. The functoriality of RF^n arises by the defining characteristic of injective objects. Namely, every morphism $\alpha\colon A \to B$ in $\mathbf{M}$ extends to a morphism of injective resolutions $\tilde{\alpha}\colon I(A) \to I(B)$, which defines a morphism of complexes $\mathrm{F}(\tilde{\alpha})\colon \mathrm{F}(I(A)) \to \mathrm{F}(I(B))$, which in turn induces a sequence of homomorphisms on homology

$$\mathrm{RF}^n(\alpha)\colon \mathrm{RF}^n(A) \to \mathrm{RF}^n(B) \qquad \text{for } n = 0, 1, 2, \ldots.$$

It follows by a standard argument of homological algebra [La1, Lemma 5.2, p. 788], that the sequence $\mathrm{RF}(\alpha)$ is independent of the choice of extension $\tilde{\alpha}$. Moreover, by [La1, Theorem 6.1, p. 793], the sequence of functors $\mathrm{RF}\colon \mathbf{M} \to \mathbf{Ab}$ forms a δ-functor which is independent of the choice of injective resolutions up to a unique isomorphism of δ-functors.

It is easy to see from the definition that the functor RF^0 is isomorphic to F. We claim also that RF^n vanishes on injectives for $n > 0$. Indeed, if I is an injective object of $\mathbf{M}$, then the sequence $0 \to I \to I \to 0$ is an injective resolution of I. Since RF does not depend on the choice of injective resolutions, we must have $\mathrm{RF}^n(I) = 0$ for all $n > 0$. From this it follows that the right-derived functors of a left-exact functor form a universal δ-functor, and in a sense which the next theorem makes precise they are the only examples of universal δ-functors on a category with enough injectives. Before we can state the theorem, we need a definition. An additive functor $\mathrm{E}\colon \mathbf{M} \to \mathbf{Ab}$ is said to be *effaceable* if

for each A in $\mathbf{M}$, there exists a monomorphism $\alpha\colon A \to B$ in $\mathbf{M}$ such that $\mathrm{E}(\alpha) = 0$.

Theorem 3.1. *Let* $\mathbf{M}$ *be an abelian category with enough injectives. Then the following conditions on a* δ*-functor* $\mathrm{F}\colon \mathbf{M} \to \mathbf{Ab}$ *are equivalent.*

(a) *The* δ*-functor* F *is isomorphic to the right-derived functor of* F^0*.*

(b) *For each* $n > 0$*, the functor* F^n *vanishes on injectives.*

(c) *For each* $n > 0$*, the functor* F^n *is effaceable.*

(d) *The* δ*-functor* F *is universal.*

Proof. That (a) implies (b) is just the claim of the last paragraph. Since every object of $\mathbf{M}$ has a monomorphism to a injective object, we see also that (b) implies (c). The assertions of [La1, Theorem 7.1 & Corollary 7.2, p. 801,804] are that (c) implies (d), and that (d) in turn implies (a). □

Now let G be a group and $\mathbf{Mod}(G)$ the abelian category of left G-modules. It will sometimes be convenient to regard $\mathbf{Mod}(G)$ as the category of left modules over the integral group ring $\mathbb{Z}G$ of G. By definition, $\mathbb{Z}G$ is the $\mathbb{Z}$-algebra generated by the symbols e_σ for $\sigma \in G$ which multiply according to the rules in G. Since $\mathbf{Mod}(G)$ is equivalent to the category of modules over a ring, [La1, Theorem 4.1, p. 784] implies that it has enough injectives.

For each G-module A, let A^G denote the subgroup of G-fixed elements in A. Thus A^G consists of every $a \in A$ such that $\sigma \cdot a = a$ for all $\sigma \in G$. The rule which associates to each G-module A the subgroup of G-fixed elements A^G defines a covariant additive functor $\mathrm{Fix}_G\colon \mathbf{Mod}(G) \to \mathbf{Ab}$. It is easy to show that Fix_G is left-exact. We denote by $\mathbf{H}^n_G$ the n-th right-derived functor of Fix_G. For a G-module A, it is customary to write $\mathbf{H}^n(G, A)$ instead of $\mathbf{H}^n_G(A)$. The abelian group $\mathbf{H}^n(G, A)$ is called the *n-th cohomology group of G in A*. At this point we can compute it in precisely one case. Namely, assume G is the trivial group. Since Fix_G is then exact, there is a universal δ-functor $\mathrm{F}\colon \mathbf{Mod}(G) \to \mathbf{Ab}$ such that $\mathrm{F}^0 = \mathrm{Fix}_G$, and $\mathrm{F}^n = 0$ for every $n > 0$. Since the theorem implies that F and $\mathbf{H}_G$ are isomorphic, we must have $\mathbf{H}^n(G, A) = 0$ for all $A \in \mathbf{Mod}(G)$ and $n > 0$.

In applications of groups cohomology it will be useful to understand how the cohomology functors $\mathbf{H}_G$ of a group G are related to those of it subgroups and quotients. In fact every homomorphism of groups defines a morphism of cohomology functors in the opposite

direction. These are the so-called *change of group* morphisms, which we now describe. Let $\eta\colon H \to G$ be a homomorphism of groups. Then η determines an action of H on each G-module A by setting

$$\tau \cdot a = \eta(\tau) \cdot a \qquad \text{for } \tau \in H,\ a \in A.$$

In this way η defines a covariant additive functor $\mathrm{T}(\eta)\colon \mathbf{Mod}(G) \to \mathbf{Mod}(H)$. It is immediate that $\mathrm{T}(\eta)$ is an exact functor, and it follows that the composition $\mathbf{H}_H \circ \mathrm{T}(\eta)$ is a δ-functor on $\mathbf{Mod}(G)$. For a given element of a G-module A, it is easy to see that being fixed by G is a stronger condition than being fixed by H. Hence $A^G \leq A^H$ for every A in $\mathbf{Mod}(G)$. Taken over all G-modules, these inclusions define a morphism of functors $\eta^*\colon \mathrm{Fix}_G \to \mathrm{Fix}_H \circ \mathrm{T}(\eta)$. Since $\mathbf{H}_G$ is universal, this extends uniquely to a morphism of δ-functors $\eta^*\colon \mathbf{H}_G \to \mathbf{H}_H \circ \mathrm{T}(\eta)$. We leave it to the reader to verify that the change of group morphisms are natural in the following sense. First of all, the identity on G induces the identity on $\mathbf{H}_G$, and second, if $\kappa\colon K \to H$ is another homomorphism of groups then $(\eta\kappa)^*$ and $\kappa^* \circ \eta^*$ are equal as morphisms of functors from $\mathbf{H}_G$ to $\mathbf{H}_K \circ \mathrm{T}(\eta\kappa)$.

Of change of groups morphisms there are three especially important cases to consider. The first is associated to the inclusion of a subgroup $\eta\colon H \leq G$. In this case, we write T_H instead of $\mathrm{T}(\eta)$, and we observe that the effect of T_H is to turn G-modules into H-modules by restriction of structure. The *restriction from G to H*, denoted $\mathbf{Res}^G_H$, is defined to be the associated morphism of δ-functors

$$\mathbf{Res}^G_H\colon \mathbf{H}_G \to \mathbf{H}_H \circ \mathrm{T}_H$$

Thus for each G-module A, the restriction from G to H yields a sequence of homomorphisms

$$\mathbf{Res}^G_H\colon \mathbf{H}^n(G, A) \to \mathbf{H}^n(H, A) \qquad n = 0, 1, 2, \ldots$$

which coincides for $n = 0$ with the inclusion $A^G \leq A^H$.

Since $\mathrm{Fix}_H \circ \mathrm{T}_H$ is a left-exact functor on $\mathbf{Mod}(G)$, one may form its right-derived functors, and ask how they are related to the δ-functor $\mathbf{H}_H \circ \mathrm{T}_H$. As Theorem 3.3 below will show, the two are isomorphic. In the proof of that theorem, we will make use of a functor from $\mathbf{Mod}(H)$ to $\mathbf{Mod}(G)$, called *induction from H to G*, denoted $\mathbf{Ind}^G_H$, which is right adjoint to T_H. If A is an H-module then $\mathbf{Ind}^G_H(A)$ is defined to be the abelian group

$\mathrm{Hom}_H(\mathbb{Z}G, A)$ given the structure of a left G-module by setting

$$(\sigma \cdot f)(x) = f(x \cdot \sigma) \qquad \text{for all } \sigma \in G,\ f \in \mathrm{Hom}_H(\mathbb{Z}G, A)$$

If $\alpha\colon A \to B$ is a homomorphism of H-modules then the naturally induced homomorphism of abelian groups $\mathbf{Ind}_H^G(A) \to \mathbf{Ind}_H^G(B)$ under which $f \mapsto \alpha \circ f$ is readily seen to be a homomorphism of G-modules, which we denote by $\mathbf{Ind}_H^G(\alpha)$. It is also easy to see that the rule which evaluates each $f \in \mathbf{Ind}_H^G(A)$ at the identity element $e_1 \in \mathbb{Z}G$ defines an epimorphism of H-modules

$$\epsilon\colon \mathbf{Ind}_H^G(A) \to A \qquad \epsilon(f) = f(e_1)$$

Above we claimed that induction from H to G is right adjoint to restriction of structure from G to H. The precise formulation of this claim is the isomorphism in the first part of the next lemma. But the essential point it that, every homomorphism of G-modules $A \to \mathbf{Ind}_H^G(B)$, is uniquely determined by a homomorphism of H-modules $A \to B$, and conversely.

Lemma 3.2. *Let G be a group and $H \leq G$ a subgroup.*

(a) *For each G-module A, and each H-module B, the induced homomorphism*

$$\epsilon_*\colon \mathrm{Hom}_G(A, \mathbf{Ind}_H^G(B)) \to \mathrm{Hom}_H(A, B) \qquad \epsilon_*(\alpha) = \epsilon \circ \alpha$$

is an isomorphism of abelian groups.

(b) *Induction from H to G is exact and preserves injectivity.*

Proof. For part (a), let $\alpha\colon A \to B$ be a homomorphism of H-modules. For each $a \in A$, define $\lambda_a\colon \mathbb{Z}G \to B$ by $\lambda_a(x) = \alpha(x \cdot a)$. Then λ_a belongs to $\mathbf{Ind}_H^G(A)$ for all $a \in A$, and the map $\lambda\colon A \to \mathbf{Ind}_H^G(B)$ such that $\lambda(a) = \lambda_a$ is a homomorphism of G-modules. For $a \in A$, we find that

$$(\epsilon \circ \lambda)(a) = \epsilon(\lambda_a) = \lambda_a(e_1) = \alpha(e_1 \cdot a) = \alpha(a)$$

which shows that λ lifts α. We leave it to the reader to check that the rule $\alpha \mapsto \lambda$ defines a homomorphism of abelian groups $\mathrm{Hom}_H(A, B) \to \mathrm{Hom}_G(A, \mathbf{Ind}_H^G(B))$ which supplies the required inverse of ϵ_*.

For part (b), to show that $\mathbf{Ind}_H^G$ is exact amounts to checking that the functor $\mathrm{Hom}_H(\mathbb{Z}G, *)\colon \mathbf{Mod}(H) \to \mathbf{Ab}$ is, or equivalently, that $\mathbb{Z}G$ is projective as an H-module. But this is clear, as the group ring $\mathbb{Z}G$ is a free left H-module with basis given by a system of representatives for the space of right cosets of H in G. To see that induction preserves injectivity, assume I is an injective H-module. Then $\mathrm{Hom}_H(*, I)$ is an exact functor on $\mathbf{Mod}(G)$ and by the first part of the lemma, so then is $\mathrm{Hom}_G(*, \mathbf{Ind}_H^G(I))$. □

Theorem 3.3. *For each subgroup $H \leq G$, the composition $\mathbf{H}_H \circ \mathrm{T}_H$ is a universal δ-functor on $\mathbf{Mod}(G)$ isomorphic to the right derived functors of $\mathrm{Fix}_H \circ \mathrm{T}_H$.*

Proof. By Theorem 3.1, it is enough to show that $\mathbf{H}_H^n \circ \mathrm{T}_H$ is effaceable for $n > 0$. Let A be a G-module. Then there exists an injective H-module I, and a monomorphism of H-modules $\alpha\colon A \to I$. By Lemma 3.2, there is a unique a homomorphism of G-modules $\lambda\colon A \to \mathbf{Ind}_H^G(I)$ such that $\alpha = \epsilon \circ \lambda$. Since α is monic, so is λ. This shows that every G-module is isomorphic to a submodule of the form $\mathbf{Ind}_H^G(I)$ with I an injective H-module.

Since $\mathbf{H}_H^n$ vanishes on injectives for $n > 0$, it is enough to show that the composition $\mathrm{T}_H \circ \mathbf{Ind}_H^G$ preserves injectivity. By the second part of Lemma 3.2, we know this to be true of induction, and so we are reduced to showing it for T_H. This follows from the observation that $\mathbb{Z}G$ is free, and hence flat, as an H-module. Indeed, let I be an injective G-module. By a standard property of base change [Bo1, p. 277], the functors $\mathrm{Hom}_H(*, I)$ and $\mathrm{Hom}_G(\mathbb{Z}G \otimes_{\mathbb{Z}H} *, I)$ on $\mathbf{Mod}(H)$ are isomorphic. As $\mathbb{Z}G$ is a flat H-module, and I is an injective G-module, we see that the second functor is exact. Therefore so is the first, which completes the proof of the theorem. □

By an *induced G-module* we mean a G-module of the form $\mathbf{Ind}_1^G(A)$ for some abelian group A. The next theorem has the important consequence that the cohomology of an induced G-module is zero for all $n > 0$. In the proof of the theorem, we make use of the observation that Fix_G is isomorphic to the functor $\mathrm{Hom}_G(\mathbb{Z}, *)$, where G acts trivially on $\mathbb{Z}$. That $\mathrm{Hom}_G(\mathbb{Z}, A)$ and A^G are isomorphic is seen by noting that if $f\colon \mathbb{Z} \to A$ is a homomorphism of G-modules then $f(1)$ must belong to A^G, and that for each $a \in A^G$, there is a unique homomorphism of G-modules $f\colon \mathbb{Z} \to A$ such that $f(1) = a$.

Theorem 3.4 (Shapiro's Lemma)**.** *Let G be a group and $H \leq G$ a subgroup. Then the composition*

$$\epsilon_* \circ \mathbf{Res}_H^G\colon \mathbf{H}_G \circ \mathbf{Ind}_H^G \to \mathbf{H}_H$$

is an isomorphism of δ-functors on $\mathbf{Mod}(H)$.

Proof. Since $\mathbf{Ind}_H^G$ preserves injectivity, an argument similar to that given in the proof of Theorem 3.3 shows that $\mathbf{H}_G \circ \mathbf{Ind}_H^G$ is universal on $\mathbf{Mod}(H)$. Since $\mathbf{H}_H$ is also universal, it is enough to show that $\epsilon_* \circ \mathbf{Res}_H^G$ is an isomorphism for $n = 0$. This amounts to checking that for each H-module A, the homomorphism ϵ restricts to an isomorphism from $\mathbf{Ind}_H^G(A)^G$ to A^H. We leave it for the reader to check that the composition of the isomorphisms

$$\mathbf{Ind}_H^G(A)^G \to \mathrm{Hom}_G(\mathbb{Z}, \mathbf{Ind}_H^G(A)) \xrightarrow{\epsilon_*} \mathrm{Hom}_H(\mathbb{Z}, A) \to A^H$$

coincides with ϵ. □

Now let $N \trianglelefteq G$ be a normal subgroup. The canonical epimorphism $\pi\colon G \to G/N$ defines a morphism of the functors $\pi^*\colon \mathbf{H}_{G/N} \to \mathbf{H}_G \circ \mathrm{T}(\pi)$ on $\mathbf{Mod}(G/N)$. But by itself, this turns out to be less useful than the morphism defined by composing π^* with Fix_N. More precisely, for each G-module A, the subgroup A^N is both a G-submodule of A, and a G/N-module under the quotient action. Hence we may regard Fix_N as a functor from $\mathbf{Mod}(G)$ to itself, or as a functor from $\mathbf{Mod}(G)$ to $\mathbf{Mod}(G/N)$. In the next lemma, we observe that the second functor is right adjoint to $\mathrm{T}(\pi)$. This has the notable consequence that Fix_N preserves injectivity.

Lemma 3.5. *Let G be a group, and $N \trianglelefteq G$ a normal subgroup.*

(a) *For each G/N-module A, and each G-module B, the natural homomorphism*

$$\mathrm{Hom}_{G/N}(A, B^N) \to \mathrm{Hom}_G(A, B)$$

is an isomorphism of abelian groups.

(b) *If I is an injective G-module then I^N is injective as a G/N-module*

Proof. In part (a), the homomorphism given is monic by the left-exactness of Hom. To see that it is epic, note that N acts trivially on A. Thus if $\alpha\colon A \to B$ is a homomorphism of G-modules, then the image of α must be fixed by N. It follows that $\mathrm{Hom}_{G/N}(*, I^N)$ and $\mathrm{Hom}_G(*, I)$ are isomorphic as functors on $\mathbf{Mod}(G/N)$. Since the second functor is exact, this proves part (b). □

By the previous paragraph we see that Fix_N defines two new functors on $\mathbf{Mod}(G)$, the compositions $\mathbf{H}_{G/N} \circ \mathrm{Fix}_N$ and $\mathbf{H}_G \circ \mathrm{Fix}_N$. Change of group with respect to π defines a

morphism between them $\pi^*\colon \mathbf{H}_{G/N} \circ \mathrm{Fix}_N \to \mathbf{H}_G \circ \mathrm{Fix}_N$. We connect these two functors to $\mathbf{H}_G$ as follows. Let A be a G-module. When regarded as a homomorphism of G-modules, the inclusion $A^N \leq A$ induces a sequence of homomorphisms $i_*\colon \mathbf{H}_G(A^N) \to \mathbf{H}_G(A)$. As A ranges over all G-modules, the homomorphisms so obtained comprise a morphism of functors $i_*\colon \mathbf{H}_G \circ \mathrm{Fix}_N \to \mathbf{H}_G$. The *inflation from G/N to G*, denoted $\mathbf{Inf}_G^{G/N}$, is defined to be the composition

$$\mathbf{H}_{G/N} \circ \mathrm{Fix}_N \xrightarrow{\pi^*} \mathbf{H}_G \circ \mathrm{Fix}_N \xrightarrow{i_*} \mathbf{H}_G$$

Thus for each G-module A, inflation from G/N to G, defines a sequence of homomorphisms

$$\mathbf{Inf}_G^{G/N}\colon \mathbf{H}^n(G/N, A^N) \to \mathbf{H}^n(G, A)$$

For $n = 0$, the inflation homomorphism corresponds to the identity $(A^N)^{G/N} = A^G$.

And last, let $H \leq G$ be a subgroup and A a G-module. For each $\sigma \in G$, the action of σ on A restricts to an isomorphism of abelian groups $\sigma\colon A^{H^\sigma} \to A^H$. In this way σ defines an isomorphism of functors $\sigma_*\colon \mathrm{Fix}_{H^\sigma} \circ \mathrm{T}_{H^\sigma} \to \mathrm{Fix}_H \circ \mathrm{T}_H$. With Theorem 3.3, we see that there is a unique extension of σ_* to an isomorphism of δ-functors $\sigma_*\colon \mathbf{H}_{H^\sigma} \to \mathbf{H}_H$. For lack of a better term, this isomorphism is called *conjugation by σ*. In the conventional notation, conjugation by σ defines for each G-module A, a sequence of isomorphisms

$$\sigma_*\colon \mathbf{H}^n(H^\sigma, A) \to \mathbf{H}^n(H, A) \qquad n = 0, 1, 2, \ldots$$

which corresponds for $n = 0$ with the isomorphism $\sigma\colon A^{H^\sigma} \to A^H$. Concerning the relationships among the restriction, inflation and conjugation morphisms, we have our next theorem.

Theorem 3.6. *Let G be a group and A a G-module. Inflation, restriction, and conjugation are all transitive; for each $n = 0, 1, 2, \ldots$, we have*

$$\begin{aligned} \mathbf{Inf}_G^{G/N} = \mathbf{Inf}_G^{G/M} \circ \mathbf{Inf}_{G/M}^{G/N} &: \mathbf{H}^n(G/N, A^N) \to \mathbf{H}^n(G, A) \\ \mathbf{Res}_K^G = \mathbf{Res}_K^H \circ \mathbf{Res}_H^G &: \mathbf{H}^n(G, A) \to \mathbf{H}^n(K, A) \\ (\sigma\tau)_* = \sigma_* \circ \tau_* &: \mathbf{H}^n(H^{\sigma\tau}, A) \to \mathbf{H}^n(H, A) \end{aligned}$$

for all $\sigma, \tau \in G$, subgroups $H, K \leq G$, and normal subgroups $M, N \trianglelefteq G$, $M \trianglelefteq N$. Inflation, restriction, and conjugation are also commuting morphisms in the sense that for each

$n = 0, 1, 2, \ldots$, *we have*

$$\begin{aligned} \mathbf{Inf}_H^{H/N} \circ \mathbf{Res}_{H/N}^{G/N} = \mathbf{Res}_H^G \circ \mathbf{Inf}_G^{G/N} &: \mathbf{H}^n(G/N, A^N) \to \mathbf{H}^n(H, A) \\ \mathbf{Inf}_H^{H/K} \circ \sigma_* = \sigma_* \circ \mathbf{Inf}_{H^\sigma}^{H^\sigma/K^\sigma} &: \mathbf{H}^n(H^\sigma/K^\sigma, A^{K^\sigma}) \to \mathbf{H}^n(H, A) \\ \mathbf{Res}_K^H \circ \sigma_* = \sigma_* \circ \mathbf{Res}_{K^\sigma}^{H^\sigma} &: \mathbf{H}^n(H^\sigma, A) \to \mathbf{H}^n(K, A) \end{aligned}$$

for all $\sigma \in G$ *and all suitable subgroups* H, K, N *of* G.

Proof. Each of the identities that does not involve the inflation is a relation between universal δ-functors on $\mathbf{Mod}(G)$ and can easily be verified for $n = 0$. To verify the remaining identities, one decomposes the inflation and applies functoriality. See [La2, pp. 37–42] for details. □

Let $N \trianglelefteq G$ be a normal subgroup and A a G-module. Theorem 3.6 shows that for each $n = 0, 1, 2, \ldots$, the n-th cohomology group $\mathbf{H}^n(N, A)$ has the structure of a left G-module by means of conjugation. Moreover, as each $\sigma \in N$ acts as the identity on A^N, we see that N acts trivially on $\mathbf{H}^0(N, A)$. Since a morphism of universal δ-functors is uniquely determined by its 0-th component, it follows that N acts trivially on $\mathbf{H}^n(N, A)$ for all $n = 0, 1, 2, \ldots$. Thus by passage to the quotient, the conjugation morphisms give the n-th cohomology group $\mathbf{H}^n(N, A)$ the structure of a G/N-module. For $n = 0$, we recover the natural action of G/N on A^N observed above. For $n > 0$, we have a complex

$$\mathbf{H}^n(G/N, A^N) \xrightarrow{\mathbf{Inf}} \mathbf{H}^n(G, A) \xrightarrow{\mathbf{Res}} \mathbf{H}^n(N, A)^{G/N}$$

To see this, let $\pi\colon G \to G/N$ be the canonical epimorphism, and $i\colon A^N \to A$ the inclusion. Then we have a commutative diagram

$$\begin{array}{ccccc} \mathbf{H}^n(G/N, A^N) & \xrightarrow{\pi^*} & \mathbf{H}^n(G, A^N) & \xrightarrow{i_*} & \mathbf{H}^n(G, A) \\ \downarrow{\scriptstyle \mathbf{Res}} & & \downarrow{\scriptstyle \mathbf{Res}} & & \downarrow{\scriptstyle \mathbf{Res}} \\ \mathbf{H}^n(N/N, A^N) & \xrightarrow{\pi^*} & \mathbf{H}^n(N, A^N) & \xrightarrow{i_*} & \mathbf{H}^n(N, A) \end{array}$$

in which the compositions of the horizontal arrows are by definition the inflations $\mathbf{Inf}_G^{G/N}$ and $\mathbf{Inf}_N^{N/N}$. Since $N/N = 1$, the group $\mathbf{H}^n(N/N, A^N)$ is trivial for every $n > 0$. Therefore commutativity requires that $\mathbf{Res}_N^G \circ \mathbf{Inf}_G^{G/N} = 0$ for the same n. Since G fixes $\mathbf{H}^n(G, A)$ and the last theorem shows that conjugation commutes with restriction, we see that G/N

fixes the image of $\mathbf{Res}_N^G$. This proves the claim. The next theorem gives a useful condition for exactness of the complex just considered.

Theorem 3.7. *Let G be a group, $N \trianglelefteq G$ a normal subgroup, and A a G-module. Let n be a positive integer and assume that $\mathbf{H}^m(N, A) = 0$ for all $m = 1, \ldots, n-1$. Then the inflation-restriction sequence*

$$0 \to \mathbf{H}^n(G/N, A^N) \xrightarrow{\mathbf{Inf}} \mathbf{H}^n(G, A) \xrightarrow{\mathbf{Res}} \mathbf{H}^n(N, A)^{G/N}$$

is exact.

Proof. See [La2, Theorem 2.4, p. 120]. □

Although theoretically expedient, the definition of $\mathbf{H}_G$ in terms of injective resolutions is too unwieldy for computations. There is an alternative definition of the cohomology groups using projective resolutions, which is derived from the observation that Fix_G is isomorphic to the functor $\mathrm{Hom}_G(\mathbb{Z}, *)\colon \mathbf{Mod}(G) \to \mathbf{Ab}$ that associates to each $A \in \mathbf{Mod}(G)$ the abelian group $\mathrm{Hom}_G(\mathbb{Z}, A)$. We will not explain this connection, instead we refer the reader to [La1, XX, §8]. However we will describe its most useful consequence which is to give the classical description of group cohomology in terms of inhomogeneous cocycles and coboundaries.

Let G be a group and A a G-module. For each $n = 0, 1, 2, \ldots$, let $\mathrm{C}^n(G, A) = \mathrm{Map}(G^n, A)$ the set of maps from the cartesian product of n-copies of G to A, given the structure of an abelian group under pointwise addition in A. We interpret the 0-fold cartesian product G^0 to mean the trivial group. Define $d^n\colon \mathrm{C}^n(G, A) \to \mathrm{C}^{n+1}(G, A)$ by

$$\begin{aligned}(d^n f)(\sigma_1, \ldots, \sigma_{n+1}) = {} & \sigma_1 \cdot f(\sigma_2, \ldots, \sigma_{n+1}) \\ & + \sum_{i=1}^{n} (-1)^i f(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1}) \\ & + (-1)^{n+1} f(\sigma_1, \ldots, \sigma_n)\end{aligned}$$

for all $\sigma_1, \ldots, \sigma_{n+1} \in G$. It will also be convenient to set $\mathrm{C}^{-1}(G, A) = 0$ and $d^{-1} = 0$. We leave it to the reader to check that d^n is a homomorphism and that $d^n \circ d^{n-1} = 0$ for every n. Furthermore, for each homomorphism of G-modules $\alpha\colon A \to B$, the naturally induced homomorphisms $\alpha\colon \mathrm{C}^n(G, A) \to \mathrm{C}^n(G, B)$ commute with the d^n. From here it is easy to

see that the rule which associates to each G-module A the complex

$$\mathrm{C}(G,A)\ :\ 0 \to \mathrm{C}^0(G,A) \xrightarrow{d^0} \mathrm{C}^1(G,A) \xrightarrow{d^1} \mathrm{C}^2(G,A) \xrightarrow{d^2} \mathrm{C}^3(G,A) \to \cdots$$

defines an exact functor from the category of G-modules to the category of complexes of abelian groups.

Since $\mathrm{C}(G,*)$ is exact, a standard theorem of homological algebra [La1, Theorem 2.1, p. 768] implies that the rule $\mathbf{H}(\mathrm{C}(G,*))$ which sends a G-module A to the homology $\mathbf{H}(\mathrm{C}(G,A))$ of the complex $\mathrm{C}(G,A)$ defines a δ-functor from $\mathbf{Mod}(G)$ to $\mathbf{Ab}$. In fact $\mathbf{H}(\mathrm{C}(G,*))$ is isomorphic to $\mathbf{H}_G$. To prove this, it would be sufficient by Theorem 3.1, to show that $\mathbf{H}^0(\mathrm{C}(G,*))$ is isomorphic to Fix_G, and that $\mathbf{H}^n(\mathrm{C}(G,*))$ vanishes on injectives for every $n > 0$. The first part is easy and will be shown below. For the second we refer the reader again to [La1, XX, §8].

By abuse of notation, we will write $\mathbf{H}^n(G,A)$ for the isomorphic groups $\mathbf{H}^n_G(A)$ and $\mathbf{H}^n(\mathrm{C}(G,A))$. Thus for $n = 0, 1, 2, \ldots$, we have $\mathbf{H}^n(G,A) = \mathrm{Z}^n(G,A)/\mathrm{B}^n(G,A)$ where

$$\mathrm{Z}^n(G,A) = \mathbf{ker}(d^n) \qquad \mathrm{B}^n(G,A) = \mathbf{img}(d^{n-1})$$

We call an element of $\mathrm{C}^n(G,A)$ an *n-cochain* of G in A. The elements of $\mathrm{Z}^n(G,A)$ are called *n-cocycles* and those of $\mathrm{B}^n(Z,A)$ are called *n-coboundaries*. We give special consideration to the cases $n = 0, 1, 2$. The rule which evaluates each $f \in \mathrm{C}^0(G,A)$ at the identity element of G^0 defines an isomorphism $\mathrm{C}^0(G,A) \to A$. Identifying $\mathrm{C}^0(G,A)$ with A thereby, the 0-th coboundary homomorphism takes the form

$$(d^0 a)(\sigma) = \sigma \cdot a - a \qquad \text{for all } a \in A,\ \sigma \in G.$$

Thus a belongs to $\mathbf{ker}(d^0)$ if and only if $\sigma \cdot a = a$ for all $\sigma \in G$, and so the 0-cocycles correspond to the elements of A^G. Since $d^{-1} = 0$, every 0-coboundary is trivial, and therefore $\mathbf{H}^0(G,A)$ is isomorphic to A^G. A similar computation reveals that a map $f\colon G \to A$ is a 1-cocycle if and only if

$$f(\sigma\tau) = f(\sigma) + \sigma \cdot f(\tau) \qquad \text{for all } \sigma, \tau \in G$$

and that f is a 1-coboundary precisely if there exists $a \in A$ such that $f(\sigma) = \sigma \cdot a - a$ for all $\sigma \in G$. In particular, if G acts trivially on A then the formula displayed above shows

that every 1-cocycle of G in A is a homomorphism and every 1-coboundary is trivial. In this case $\mathbf{H}^1(G, A)$ is isomorphic to $\mathrm{Hom}(G, A)$.

In the next section, it will be useful to have a cocyclic description of the 0-th connecting homomorphism. To this end, let G be a group, $0 \to A \to B \to C \to 0$ a short exact sequence of G-modules, and $\boldsymbol{\delta}^0 \colon C^G \to \mathbf{H}^1(G, A)$ the associated connecting homomorphism. For each $c \in C^G$, select $b \in B$ that maps to c, and define $f \colon G \to A$ by $f(\sigma) = \sigma \cdot b - b$. Then f is a 1-cocycle of G in A, and $\boldsymbol{\delta}^0(c) = [f]$. The derivation of the formula given is an easy application of the Snake Lemma and so we omit the argument.

An easy computation shows that a map $f \colon G^2 \to A$ is a 2-cocycle if and only if

$$f(\rho, \sigma) + f(\rho\sigma, \tau) = \rho \cdot f(\sigma, \tau) + f(\rho, \sigma\tau) \qquad \text{for all } \rho, \sigma, \tau \in G.$$

The map f is a 2-coboundary if there exists a map $b \colon G \to A$ such that

$$f(\sigma, \tau) = b(\sigma) + \sigma \cdot b(\tau) - b(\sigma\tau) \qquad \text{for all } \sigma, \tau \in G.$$

We say that a 2-cocycle f is *normalized* if $f(\sigma, \tau) = 0$ whenever σ or τ is 1. We claim that the normalized 2-cocycles comprise a subgroup of $\mathrm{Z}^2(G, A)$, and each 2-cocycle differs from a normalized 2-cocycle by a 2-coboundary. The first part is obvious. For the second, let f be a 2-cocycle and set $a = f(1, 1)$. The 2-cocycle condition implies that $f(\sigma, 1) = \sigma \cdot a$ and $f(1, \tau) = a$ for all $\sigma, \tau \in G$. Define $b \colon G \to A$ by setting $b(1) = a$ and $b(\sigma) = 0$ for $\sigma \neq 1$. Then the difference $f - d^1 b$ is a normalized 2-cocycle. The utility of normalized 2-cocycles will become apparent in Section 3.3.

The restriction homomorphism has the obvious expression in terms of cocycles. Similarly, for $f \in \mathrm{Z}^n(G/N, A^N)$, the inflation $\mathbf{Inf}_G^{G/N}[f]$ is the class $[g] \in \mathbf{H}^n(G, A)$ of the n-cocycle g of G in A obtained by composing f with the n-fold cartesian product of canonical epimorphism $\pi \colon G \to G/N$. That is

$$g(\sigma_1, \ldots, \sigma_n) = f(\sigma_1 N, \ldots, \sigma_n N) \qquad \text{for all } \sigma_1, \ldots, \sigma_n \in G.$$

For the conjugation morphism, fix $\sigma \in G$ and a subgroup $H \leq G$. For $f \in \mathrm{Z}^n(H^\sigma, A)$, define ${}^\sigma f \in \mathrm{Z}^n(H, A)$ by

$$({}^\sigma f)(\tau_1, \ldots, \tau_n) = \sigma \cdot f(\tau_1^\sigma, \ldots, \tau_n^\sigma) \qquad \text{for } \tau_1, \ldots, \tau_n \in H.$$

Then we claim that $\sigma_*[f] = [{}^\sigma f]$. In each case, the formula specified extends to a homomorphism of the relevant cochain complexes, and defines thereby a morphism of δ-functors. Therefore by universality, it is enough to check that the formulas are correct for $n = 0$. We leave this to the reader.

When G is a finite cyclic group the classical construction gives an especially simple description of the functor $\mathbf{H}_G$. The next theorem is stated only for $n = 1, 2$ by it can be extended to all $n > 0$ by the periodicity of the cohomology of a cyclic group, see [La2, pp. 32–36].

Theorem 3.8. *Let $G = \langle\sigma\rangle$ be a finite cyclic group of order n. For each G-module A, define $\mathrm{D}, \mathrm{T}\colon A \to A$ by $\mathrm{D}(a) = \sigma(a) - a$ and $\mathrm{T}(a) = a + \sigma(a) + \sigma^2(a) + \cdots + \sigma^{n-1}(a)$. Let A_T denote the kernel of T in A. Then there are functorial isomorphisms*

$$\varphi^1\colon \mathbf{H}^1(G, A) \to A_\mathrm{T}/\mathrm{D}(A) \qquad \varphi^1[f] = f(\sigma) + \mathrm{D}(A)$$

$$\varphi^2\colon \mathbf{H}^2(G, A) \to A^G/\mathrm{T}(A) \qquad \varphi^2[f] = \sum_{i=0}^{n-1} f(\sigma^i, \sigma) + \mathrm{T}(A)$$

Proof. See [La2, pp. 29–34]. □

3.2 Galois Cohomology

In this section we specialize the material of the last section to the case of the group of a Galois extension of fields. In the infinite case, this requires a slight reformulation of the definitions given in the last section. As much as the notation allows, we will abbreviate the expression $\mathrm{Gal}(L/K)$ by L/K. Thus $\mathbf{Mod}(L/K)$ denotes the category of $\mathrm{Gal}(L/K)$-modules, $\mathbf{H}^n(L/K, A)$ is an abbreviation for $\mathbf{H}^n(\mathrm{Gal}(L/K), A)$, and so on. The fundamental result of Galois cohomology is the next theorem, which is due as stated to Noether. It is often referred to as Hilbert's "Theorem 90" because the cyclic case of the theorem was Satz 90 of Hilbert's *Zahlbericht*.

Theorem 3.9. *If L/K is a finite Galois extension of fields then $\mathbf{H}^1(L/K, L^\times)$ is trivial.*

Proof. See [La1, Theorem 10.1, p. 302]. □

Let K be a field, and K_s a separable closure of K. For each extension L of K contained in K_s, we write G_L for the subgroup $\mathrm{Gal}(K_s/L)$ of $\mathrm{Gal}(K_s/K)$. By [La1, Theorem 14.1, p. 313], if L is a Galois extension of K in K_s then the action of G_K on L defines

an isomorphism $\mathrm{G}_K/\mathrm{G}_L \to \mathrm{Gal}(L/K)$, and as L ranges over all finite Galois extensions, the canonical epimorphisms $\mathrm{G}_K \to \mathrm{Gal}(L/K)$ define a isomorphism from the absolute Galois group G_K to the inverse limit of the $\mathrm{Gal}(L/K)$. Let A be a G_K-module. For each extension L of K in K_s, we write A_L for the subgroup of G_L-fixed elements in A. If L is a normal extension of K then A_L is a G_K-submodule of A, and the action by G_K gives it the structure of a $\mathrm{Gal}(L/K)$-module by passage to the quotient. We call A a *topological* G_K*-module* if A is the union of the submodules A_L as L ranges over the finite Galois extensions of K in K_s. This is equivalent to requiring that the stabilizer of each element of A be of finite index in G_K, or that the action of G_K on A is continuous for the profinite topology on G_K and the discrete topology on A. In particular, the additive and multiplicative groups of every extension of K in K_s are topological G_K-modules, as is every module with trivial G_K-action.

The topological G_K-modules form an abelian subcategory of $\mathbf{Mod}(\mathrm{G}_K)$, which we denote by $\mathbf{Mod}(K)$. By [La2, pp. 127,128], the category $\mathbf{Mod}(K)$ has enough injectives. We denote by $\mathbf{H}_K$ the right-derived functors of $\mathrm{Fix}_{\mathrm{G}_K}$ on $\mathbf{Mod}(K)$. If A is a topological G_K-module then, by abuse of notation, we write $\mathbf{H}^n(\mathrm{G}_K, A)$ for the group $\mathbf{H}^n_K(A)$, which is called the *n-th continuous cohomology group* of G_K in A.

Let A be a G_K-module. Then as L ranges over the finite Galois extensions of K contained in K_s, the cohomology groups $\mathbf{H}^n(L/K, A_L)$, together with the relevant inflation homomorphisms $\mathbf{Inf}\colon \mathbf{H}^n(L/K, A_L) \to \mathbf{H}^n(M/K, A_M)$, form a directed system of abelian groups. This follows from the fact that the compositum of each pair of finite Galois extensions of K in K_s is again a finite Galois extension, along with the transitivity of inflation. Moreover, the inflation homomorphisms $\mathbf{Inf}\colon \mathbf{H}^n(L/K, A_L) \to \mathbf{H}^n(\mathrm{G}_K, A)$ are seen to define a morphism from this directed system. This is just the observation that, for every extension M of L Galois over K, inflation from $\mathbf{H}^n(L/K, A_L)$ to $\mathbf{H}^n(\mathrm{G}_K, A)$ has the obvious factorization through $\mathbf{H}^n(M/K, A_M)$.

Theorem 3.10. *If A is a topological G_K-module then the inflation homomorphisms induce an isomorphism from direct limit of the $\mathbf{H}^n(L/K, A_L)$ to $\mathbf{H}^n(\mathrm{G}_K, A)$.*

Proof. See [La2, Theorem 2.3, p. 130]. □

If L/K is a Galois subextension of a Galois extension M/K then we say that a class $\xi \in \mathbf{H}^n(L/K, A_L)$ has trivial inflation to M/K if it vanishes in the inflation homomorphism $\mathbf{Inf}\colon \mathbf{H}^n(L/K, A_L) \to \mathbf{H}^n(M/L, A_M)$.

Lemma 3.11. *Let A be a topological G_K-module, L a finite Galois extension of K contained in K_s, and $\xi \in \mathbf{H}^n(L/K, A_L)$. If ξ has trivial inflation to G_K then there is a finite Galois extension M of K in K_s, that has L as a subextension, and is such that ξ has trivial inflation to M/K.*

Proof. This is a general property of direct limits, see [La1, p. 170]. □

For the rest of the section, we fix a natural number m, and we assume that K contains a primitive m-th root of unity. The object of Kummer Theory [La1, Theorem 8.1, p. 294] is describe the Galois extensions L of K such that $\mathrm{Gal}(L/K)$ is abelian of exponent m. This is accomplished through the existence of perfect pairing

$$\mathrm{A}_K \times K^\times/(K^\times)^m \to \boldsymbol{\mu}(m) \qquad \langle \sigma, a \rangle = \sigma(a^{1/m})/a^{1/m}$$

where A_K is the largest quotient of G_K that is abelian of exponent dividing m. Our goal is to formulate a relative version of this isomorphism, which we will use to construct certain Galois extensions in Chapter 5.

Let L/K be a finite Galois extension, B a $\mathrm{Gal}(L/K)$-submodule of $L^\times$ that contains $(L^\times)^m$ as a subgroup of finite index, and $L_B = L(B^{1/m})$ the extension obtained by adjoining to L every $\beta \in K_s$ such that $\beta^m \in B$. We will show that L_B/K is finite Galois, $\mathrm{Gal}(L_B/L)$ is an abelian normal subgroup of $\mathrm{Gal}(L_B/K)$, and that the homomorphism induced by the Kummer pairing

$$\mathrm{Gal}(L_B/L) \to \mathrm{Hom}(B/(L^\times)^m, \boldsymbol{\mu}(m)) \qquad \sigma \mapsto \langle \sigma, * \rangle$$

is an isomorphism of right $\mathrm{Gal}(L/K)$-modules.

By assuming that K contains the m-th roots of unity, we are implicitly assuming that m is prime to the characteristic of K. Therefore there is a short exact sequence of G_K-modules

$$1 \to \boldsymbol{\mu}(m) \to K_s^\times \xrightarrow{m} K_s^\times \to 1$$

where m stands for the m-th power homomorphism $x \mapsto x^m$ on $K_s^\times$. By applying the functor $\mathbf{H}_L$, we obtain a long exact sequence of $\mathrm{Gal}(L/K)$-modules

$$\cdots \to L^\times \xrightarrow{m} L^\times \xrightarrow{\boldsymbol{\delta}^0} \mathbf{H}^1(\mathrm{G}_L, \boldsymbol{\mu}(m)) \to 1$$

which is right exact by Theorem 3.9. Since G_L acts trivially on $\boldsymbol{\mu}(m)$, we may identify $\mathbf{H}^1(\mathrm{G}_L, \boldsymbol{\mu}(m))$ with $\mathrm{Hom}(\mathrm{G}_L, \boldsymbol{\mu}(m))$, and the computations of the last section provide us with an explicit form for $\boldsymbol{\delta}^0$. Namely, we have

$$(\boldsymbol{\delta}^0(b))(\tau) = \tau(b^{1/m})/b^{1/m} \qquad \text{for all } b \in L^\times,\ \tau \in \mathrm{G}_L.$$

By restricting to $B/(L^\times)^m$, we obtain a pairing

$$B/(L^\times)^m \times \mathrm{G}_L \to \boldsymbol{\mu}(m) \qquad \langle b, \tau\rangle = \tau(b^{1/m})/b^{1/m}$$

which is nondegenerate on the left. Let N_B be the right kernel of $\langle *, *\rangle$. Thus N_B is the subgroup consisting of all $\tau \in \mathrm{G}_L$ such that $\langle b, \tau\rangle = 1$ for all $b \in B$. The formula for $\langle *, *\rangle$ given above shows that L_B is the fixed field of N_B in K_s.

The fact that the connecting homomorphism $\boldsymbol{\delta}^0$ is a homomorphism of $\mathrm{Gal}(L/K)$-modules amounts to having

$$\langle \sigma(b), \tau\rangle = \langle b, \tau^\sigma\rangle \qquad \text{for all } \sigma \in \mathrm{G}_K,\ \tau \in \mathrm{G}_L,\ b \in B.$$

Thus for $\sigma \in \mathrm{G}_K$ and $\tau \in \mathrm{G}_L$, we see that τ belongs to $N_{\sigma(B)}$ if and only if τ^σ belongs to N_B. As we are assuming that the action of $\mathrm{Gal}(L/K)$ preserves B, it follows that N_B is normal in G_K. We have already observed that L_B is the fixed field of N_B in K_s, and so this implies that L_B/K is Galois. Since the quotient $B/(L^\times)^m$ is finite, [La1, Theorem 9.2, p. 49] implies that G_L/N_B is also finite, and that the induced pairing

$$\mathrm{G}_L/N_B \times B/(L^\times)^m \to \boldsymbol{\mu}(m)$$

is perfect. By combining this with the canonical isomorphism $\mathrm{G}_L/N_B \to \mathrm{Gal}(L_B/L)$, we obtain an isomorphism of right G_K-modules

$$\mathrm{Gal}(L_B/L) \to \mathrm{Hom}(B/(L^\times)^m, \boldsymbol{\mu}(m))$$

As $\mathrm{Gal}(L_B/L)$ is an abelian normal subgroup of $\mathrm{Gal}(L_B/K)$, we see that G_L acts trivially on both sides, and that the above isomorphism is also an isomorphism of right $\mathrm{Gal}(L/K)$-modules.

3.3 Group Extensions

Let G be a group and A a left G-module. An *extension of G by A* is by definition a short exact sequence of groups

$$1 \to A \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1$$

such that the action of E on A defined by conjugation coincides with the action defined by π. That is, we require that

$$\pi(x)(a) = x \cdot a \cdot x^{-1} \qquad \text{for all } x \in E,\ a \in A.$$

To compactify notation, we will almost always assume that A is a subgroup of E. In this case, to describe an extension of E by A it suffices to specify the epimorphism $\pi\colon E \to G$. Thus when we refer to a pair (E, π) as an extension of G by A, we are assuming that A is a normal subgroup of E and $\pi\colon E \to G$ is an epimorphism whose kernel is A.

Let (E_1, π_1) and (E_2, π_2) be two extensions of G by A. An *equivalence from (E_1, π_1) to (E_2, π_2)* is a homomorphism $\varphi\colon E_1 \to E_2$ that makes the following diagram commute

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\alpha_1} & E_1 & \xrightarrow{\pi_1} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow{\alpha_2} & E_2 & \xrightarrow{\pi_2} & G & \longrightarrow & 1 \end{array}$$

We say that (E_1, π_1) *and* (E_2, π_2) *are equivalent* if there exists an equivalence from (E_1, π_1) to (E_2, π_2). As stated the definition of equivalence is unsymmetric and we remedy this situation with the following lemma.

Lemma 3.12. *Assume φ is an equivalence from (E_1, π_1) to (E_2, π_2). Then φ is an isomorphism from E_1 to E_2 and its inverse is an equivalence from (E_2, π_2) to (E_1, π_1).*

Proof. The proof is an easy diagram chase, and we leave it to the reader. □

Thus equivalence of extensions is an equivalence relation and a finer relation than isomorphism. We let $\mathbf{E}(G, A)$ denote the set of equivalence classes of extensions of G by A. The first goal of this section is to give a cohomological description of the classes of extensions of G by A. This goal is achieved by Theorem 3.15 below which gives a bijection between the set of equivalence classes $\mathbf{E}(G, A)$ and the second cohomology group $\mathbf{H}^2(G, A)$.

Let (E, π) be an extension of G by A. By a *section of* π, we mean a function $e\colon G \to E$ such that $\pi \circ e = \mathbf{1}_G$. We say that a section e is *normalized* if $e(1) = 1$. Let e be a normalized section of π. The *factor set associated to* e is the function f defined by setting

$$f(\sigma, \tau) = e(\sigma) \cdot e(\tau) \cdot e(\sigma\tau)^{-1} \qquad \text{for all } \sigma, \tau \in G.$$

Thus $f(\sigma, \tau)$ belongs to A and $e(\sigma) \cdot e(\tau) = f(\sigma, \tau) \cdot e(\sigma\tau)$ for all $\sigma, \tau \in G$. In this way the factor set f measures the extent to which the section e fails to be a homomorphism.

Lemma 3.13. *Let G be a group, A a G-module, and (E, π) an extension of G by A. Let e be a normalized section of π, and f the associated factor set. Then f is a normalized 2-cocycle of G in A.*

Proof. By the associativity of the multiplication in E, we have

$$(e(\rho) \cdot e(\sigma)) \cdot e(\tau) = e(\rho) \cdot (e(\sigma) \cdot e(\tau)) \qquad \text{for all } \rho, \sigma, \tau \in G.$$

Expanding both sides of the equation above, we have

$$f(\rho, \sigma) \cdot f(\rho\sigma, \tau) = \rho(f(\sigma, \tau)) \cdot f(\rho, \sigma\tau) \qquad \text{for all } \rho, \sigma, \tau \in G.$$

And since $e(1) = 1$, we see that $f(\sigma, \tau)$ is the identity whenever σ or τ is. Hence f is a normalized 2-cocycle of G in A. □

Lemma 3.14. *Assume φ is an equivalence from (E_1, π_1) to (E_2, π_2). For $i = 1, 2$, let e_i be a normalized section of π_i, and f_i the associated factor set. Define*

$$b(\sigma, \tau) = \varphi(f_1(\sigma, \tau)) \cdot f_2(\sigma, \tau)^{-1} \qquad \textit{for all } \sigma, \tau \in G.$$

Then b is a 2-coboundary.

Proof. Define $a\colon G \to A$ by $a(\sigma) = \varphi(x_1(\sigma)) \cdot x_2(\sigma)^{-1}$. Then an easy computation shows that

$$b(\sigma, \tau) = a(\sigma) \cdot \sigma(a(\tau)) \cdot a(\sigma\tau)^{-1} \qquad \text{for all } \sigma, \tau \in G.$$

Hence b belongs to $\mathrm{B}^2(G, A)$. □

Let (E, π) be an extension of G by A. By applying Lemma 3.14 to the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \| & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

we see that the factor sets associated to every pair of normalized sections of π are cohomologous 2-cocycles of G in A. The lemma also shows that equivalent extensions determine cohomologous factor sets. It follows that there exists a map $\mathrm{fac}\colon \mathbf{E}(G, A) \to \mathbf{H}^2(G, A)$ that sends the equivalence class of an extension (E, π) to the cohomology class of a factor set associated to a normalized section of π.

In the other direction, we construct a function $\mathrm{exn}\colon \mathbf{H}^2(G, A) \to \mathbf{E}(G, A)$ which, given a cohomology class $[f] \in \mathbf{H}^2(G, A)$, determines an equivalence class of extensions $\mathrm{exn}[f]$. Let E denote the cartesian product of A and G. Each normalized 2-cocycle f of G in A defines a binary operation $*$ on E by setting

$$(a, \sigma) * (b, \tau) = (a\sigma(b)f(\sigma, \tau), \sigma\tau) \qquad \text{for all } a, b \in A,\ \sigma, \tau \in G.$$

We claim that E is a group under $*$. A reversal of the argument given in the proof of Lemma 3.13 shows that $*$ is an associative operator of E precisely because f is a 2-cocycle of G in A. Since we are assuming that f is normalized, it is easy to see that the element $(1, 1)$ is a two-sided identity with respect to $*$, and that the inverse of (a, σ) is the element (b^{-1}, σ^{-1}), where $b = \sigma^{-1}(a \cdot f(\sigma, \sigma^{-1}))$. We identify A with the subgroup $A \times 1$ of E. Then the set-theoretic projection $\pi\colon E \to G$ is an epimorphism whose kernel is A. We define $\mathrm{exn}[f]$ to be the equivalence class of (E, π).

To prove that this construction is well-defined, we would need to show that if f is replaced with a cohomologous 2-cocycle then the resulting extension is equivalent to (E, π). We leave it to the reader to check that a reversal of the argument given in the proof of Lemma 3.14 yields such an equivalence. Now we are ready to state the first main theorem of the section.

Theorem 3.15 (Schreier, 1926)**.** *Let G be a group and A a G-module. The functions*

$$\mathrm{exn}\colon \mathbf{H}^2(G, A) \to \mathbf{E}(G, A) \qquad \mathrm{fac}\colon \mathbf{E}(G, A) \to \mathbf{H}^2(G, A)$$

are mutual inverses. The equivalence classes of extensions of G by A are in bijective correspondence with the elements of $\mathbf{H}^2(G, A)$.

Proof. See [La2, Theorem 1.1, p. 158], but the first part of the theorem should be fairly clear from the constructions given above. The second part of the theorem is just a restatement of the first. □

The correspondence of Theorem 3.15 endows $\mathbf{E}(G, A)$ with the structure of an abelian group. We will not consider this structure in terms of extension classes. But it will be useful to characterize the equivalence class in $\mathbf{E}(G, A)$ that corresponds to the identity element of $\mathbf{H}^2(G, A)$.

Theorem 3.16. *Let G be a group and A a G-module. Let $\xi \in \mathbf{E}(G, A)$ denote the equivalence class of the extension (E, π). Then the following conditions are equivalent.*

(a) *There exists a section of π that is a homomorphism from G to E.*

(b) *The extension (E, π) is equivalent to the split extension $1 \to A \to A \rtimes G \to G \to 1$.*

(c) *The associated cohomology class* $\mathrm{fac}(\xi)$ *is trivial.*

Proof. It is easy to see that (a) implies (b) and that (b) implies (c). So assume that $\mathrm{fac}(\xi)$ is trivial. Then there exists a normalized section $e\colon G \to E$ such that the associated factor set f is a 2-coboundary. Hence there exists a function $a\colon G \to A$ such that

$$f(\sigma, \tau) = a(\sigma) \cdot \sigma(a(\tau)) \cdot a(\sigma\tau)^{-1} \qquad \text{for all } \sigma, \tau \in G.$$

Define $\gamma\colon G \to E$ by $\gamma(\sigma) = a(\sigma)^{-1} \cdot e(\sigma)$. Then γ is also section of π and a direct computation shows that γ is a homomorphism. Therefore (c) implies (a). □

For each homomorphism of groups $\eta^*\colon H \to G$, there is a corresponding map on extension classes defined by the composition

$$\begin{array}{ccc} \mathbf{H}^2(G, A) & \xrightarrow{\eta^*} & \mathbf{H}^2(H, A) \\ \uparrow & & \downarrow \\ \mathbf{E}(G, A) & \xrightarrow{\eta^*} & \mathbf{E}(H, A) \end{array}$$

The behavior of η^* on extension classes will be a recurring theme in this thesis. Let (E, π) be an extension of G by A and let (E_H, π_*, η_*) be the pullback of π and η as defined in Section 2.2. Then we have a commutative diagram

$$\begin{array}{ccc} E_H & \xrightarrow{\pi_*} & H \\ \downarrow{\scriptstyle \eta_*} & & \downarrow{\scriptstyle \eta} \\ E & \xrightarrow{\pi} & G \end{array}$$

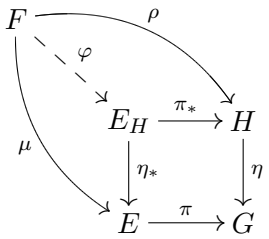
By Lemma 2.1, the homomorphism $\eta_* \colon E_H \to E$ defines by restriction an isomorphism from $\mathbf{ker}(\pi_*)$ to $\mathbf{ker}(\pi)$. Thus by taking its inverse, we obtain a monomorphism $A \to E_H$ whose image equals $\mathbf{ker}(\pi_*)$. Thus identifying $A = \mathbf{ker}(\pi_*)$ thereby, makes A an abelian normal subgroup of E_H. Moreover, we see that the H-module structures on A determined by η, and by conjugation in E_H, are equal. Accordingly we will regard the pair (E_H, π_*) as an extension of H by A.

Theorem 3.17. *Let $\eta \colon H \to G$ be a homomorphism of groups, A a G-module, (E, π) an extension of G by A, and $\xi \in \mathbf{E}(G, A)$ the equivalence class of (E, π).*

(a) *The map $\eta^* \colon \mathbf{E}(G, A) \to \mathbf{E}(H, A)$ sends ξ to the equivalence class of (E_H, π_*).*

(b) *If $\eta^*(\xi)$ is trivial then η lifts to a homomorphism from H to E.*

Proof. Let $e \colon G \to E$ be a section of π, and $g \in \mathrm{Z}^2(G, A)$ the associated factor set. Let f be the factor set of H in A that corresponds to g under η and (F, ρ) extension of H by A determined by f. To prove (a), we need to show that (E_H, π_*) and (F, ρ) are equivalent extensions of H by A. Define $\mu \colon F \to E$ by $\mu(a, \sigma) = a \cdot e(\eta(\sigma))$. Then μ is a homomorphism and $\pi \circ \mu$ equals $\eta \circ \rho$. By the universality of the pullback there exists a unique homomorphism $\varphi \colon F \to E_H$ that makes the following diagram commute



We claim that φ is an equivalence from F to E_H. Representing F as the cartesian product $A \times H$, and E_H as the fiber product $E \times_G H$, yields an expression for φ in terms of μ and

ρ. By applying the definitions of μ and ρ we see that

$$\varphi(a, \sigma) = (a \cdot e(\eta(\sigma)), \sigma) \qquad \text{for all } a \in A,\ \sigma \in G.$$

From here it is easy to check the following diagram commutes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & F & \xrightarrow{\rho} & H & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E_H & \xrightarrow{\pi_*} & H & \longrightarrow & 1 \end{array}$$

Thus (F, ρ) and (E_H, π_*) are equivalent extensions of H by A. This proves (a).

By the construction of the induced extension (E_H, π_*), we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E_H & \xrightarrow{\pi_*} & H & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \eta_*} & & \downarrow{\scriptstyle \eta} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

Assuming that $\eta^*(\xi)$ is trivial, by Theorem 3.16, there exists a homomorphism $\psi\colon H \to E_H$ such that $\pi_* \circ \psi$ is the identity on H. Let $\lambda = \eta_* \circ \psi$. Then $\lambda\colon H \to E$ is a homomorphism such that

$$\pi \circ \lambda = \pi \circ (\eta_* \circ \psi) = (\eta \circ \pi_*) \circ \psi = \eta.$$

Therefore λ gives the required lift of η. □

3.4 Brauer Embedding Problems

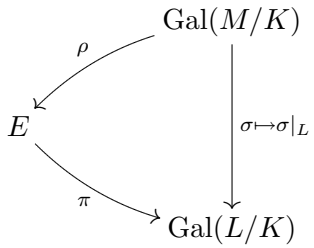
We close this chapter by introducing a method for obtaining regular realizations of certain finite groups that complements the constructions described in Section 2.4. Although we will define it more generally, this method is best suited for realizing finite p-groups as Galois groups over fields that contains the p-th roots of unity. Specifically, assume E is a nontrivial finite p-group and K a field that contains the p-th roots of unity. By part (c) of Theorem 2.6, there exists a central subgroup $U \leq \mathbf{Z}(E)$ which is cyclic of order p. Assume L/K is Galois with group isomorphic to E/U. The embedding problem for L/K and E is to determine if there exists an extension M/K that has L/K as a subextension and is Galois with group isomorphic to E. Identifying U with the group of p-th roots of unity in $L^\times$,

the epimorphism $E \to \mathrm{Gal}(L/K)$, defines a central extension of $\mathrm{Gal}(L/K)$ by $\boldsymbol{\mu}(p)$, which in turn, determines an element of $\mathbf{H}^2(L/K, L^\times)$. Under some additional assumptions, the vanishing of this cohomology class ensures the existence of a field extension that solves the embedding problem posed above.

A *Brauer embedding problem* is a quadruple $(L/K, E, \pi, \epsilon)$ where L/K is a finite Galois extension of fields, E a finite group, $\pi\colon E \to \mathrm{Gal}(L/K)$ an epimorphism, and $\epsilon\colon \mathbf{ker}(\pi) \to L^\times$ a monomorphism such that

$$\epsilon(xux^{-1}) = \pi(x)(\epsilon(u)) \qquad \text{for all } x \in E,\ u \in \mathbf{ker}(\pi).$$

A *solution to* $(L/K, E, \pi, \epsilon)$ is a pair $(M/K, \varphi)$ where M/K is a finite Galois extension that has L/K as a subextension, and $\varphi\colon \mathrm{Gal}(M/K) \to E$ is an isomorphism that makes the following diagram commute



Let $\xi \in \mathbf{H}^2(L/K, \mathbf{ker}(\pi))$ be the class determined by (E, π). The *obstruction* to the embedding problem $(L/K, E, \pi, \epsilon)$ is by definition the element $\epsilon_*(\xi)$ of $\mathbf{H}^2(L/K, L^\times)$.

Let $(L/K, E, \pi, \epsilon)$ be a Brauer embedding problem. Since the image of ϵ is a finite subgroup of $L^\times$ it must be the group of m-th roots of unity for some natural number m necessarily prime to the characteristic of L. In the situation described above, where $\mathbf{ker}(\pi)$ is a central subgroup of E, we see that the image of ϵ must be contained in $K^\times$. In this case we call $(L/K, E, \pi, \epsilon)$ a *central embedding problem.* The first theorem of this section gives a sufficient condition for the solvability of a Brauer embedding problem in terms of the vanishing of its obstruction.

Theorem 3.18. *Let $(L/K, E, \pi, \epsilon)$ be a Brauer embedding problem. If $\mathbf{ker}(\pi) \leq \mathbf{\Phi}(E)$ and $(L/K, E, \pi, \epsilon)$ has trivial obstruction then it has a solution.*

Proof. Let m denote the order of $\mathbf{ker}(\pi)$. Then the image of ϵ is $\boldsymbol{\mu}(m)$ the group of m-th

roots of unity in L. By identifying $\mathbf{ker}(\pi)$ with $\boldsymbol{\mu}(m)$, we obtain a short exact sequence

$$1 \to \boldsymbol{\mu}(m) \to E \xrightarrow{\pi} \mathrm{Gal}(L/K) \to 1.$$

Let $\xi \in \mathbf{H}^2(L/K, \boldsymbol{\mu}(m))$ correspond to the equivalence class of (E, π). Then the obstruction to $(L/K, E, \pi, \epsilon)$ is by definition the element $\epsilon_*(\xi) \in \mathbf{H}^2(L/K, L^\times)$. Assuming that $\epsilon_*(\xi)$ is trivial, we claim that ξ must have trivial inflation to G_K. From the commutativity of the diagram

$$\begin{array}{ccc} \mathbf{H}^2(L/K, \boldsymbol{\mu}(m)) & \xrightarrow{\mathbf{Inf}} & \mathbf{H}^2(\mathrm{G}_K, \boldsymbol{\mu}(m)) \\ \downarrow{\scriptstyle \epsilon_*} & & \downarrow{\scriptstyle \epsilon_*} \\ \mathbf{H}^2(L/K, L^\times) & \xrightarrow{\mathbf{Inf}} & \mathbf{H}^2(\mathrm{G}_K, K_s^\times) \end{array}$$

we see that the claim will follow, if we can show that the induced homomorphism from $\mathbf{H}^2(\mathrm{G}_K, \boldsymbol{\mu}(m))$ to $\mathbf{H}^2(\mathrm{G}_K, K_s^\times)$ is monic. To see this, consider the short exact sequence of G_K-modules

$$1 \to \boldsymbol{\mu}(m) \xrightarrow{\epsilon} K_s^\times \xrightarrow{m} K_s^\times \to 1$$

and the associated long exact sequence in cohomology

$$\cdots \to \mathbf{H}^1(\mathrm{G}_K, K_s^\times) \xrightarrow{\boldsymbol{\delta}^1} \mathbf{H}^2(\mathrm{G}_K, \boldsymbol{\mu}(m)) \xrightarrow{\epsilon_*} \mathbf{H}^2(\mathrm{G}_K, K_s^\times) \to \cdots$$

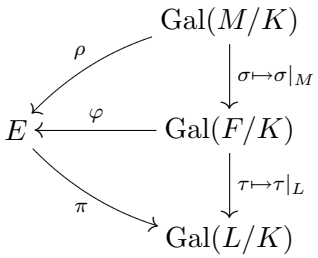
By Theorem 3.9, $\mathbf{H}^1(\mathrm{G}_K, K_s^\times)$ is trivial, and so ϵ_* is monic by exactness of the sequence above. This proves the claim.

Since ξ has trivial inflation to G_K, we see by Lemma 3.11 that there exists a finite Galois extension M of K in K_s, such that L is contained in M, and ξ has trivial inflation to M/K. Theorem 3.17 implies that the canonical epimorphism $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ lifts to E. That is, there exists a homomorphism $\rho\colon \mathrm{Gal}(M/K) \to E$ such that

$$\pi(\rho(\sigma)) = \sigma|_L \qquad \text{for all } \sigma \in \mathrm{Gal}(M/K).$$

As the canonical homomorphism $\mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ is epic, we see that E is generated by the image of ρ and the kernel of π. Since we are assuming that $\mathbf{ker}(\pi) \leq \mathbf{\Phi}(E)$, it follows by Theorem 2.3, that ρ is epic. Let F denote the fixed field of $\mathbf{ker}(\rho)$ in M. Then by elementary Galois theory, we see that F/K is Galois and that the epimorphism ρ

defines by passage to the quotient an isomorphism $\varphi\colon \mathrm{Gal}(F/K) \to E$. In the diagram



the upper and outer triangles are both commutative and the vertical arrows are epic. It follows that the lower triangle is also commutative and therefore that the pair $(F/K, \varphi)$ is a solution to the embedding problem $(L/K, E, \pi, \epsilon)$. □

In the situation of Theorem 3.18, if L/K is a regular realization of G over some field k, the last theorem says nothing about the regularity of solutions. As a remedy to this deficit in Theorem 3.18, we present the next theorem.

Theorem 3.19. *Let K/k be a regular extension of fields, L/K a finite G-Galois extension, and F the fixed field of $\mathbf{\Phi}(G)$ in L. Then L/k is regular if and only if F/k is.*

Proof. Since L/K and K/k are both separable extensions, so are L/k and F/k by [La1, Corollaries 4.2 & 4.3, p. 365]. Thus showing that either L or F is a regular extension of k amounts to checking that k is algebraically closed in the field of interest. Therefore if L/k is regular then so is F/k. For the converse, assume that F/k is regular. By [Bo2, Proposition 9, V.142], the field F is linearly disjoint from every algebraic extension of k in L. In particular, if $\alpha \in L$ is algebraic over k then F and $k(\alpha)$ are linearly disjoint over k. With [La1, Proposition 3.1, p. 361], this implies that F and $K(\alpha)$ are linearly disjoint extensions of K in L. Thus $F \cap K(\alpha) = K$. Let H denote the subgroup of G containing all automorphisms that fix $K(\alpha)$. Then since $K = K(\alpha) \cap F$ we have $G = \langle H, \mathbf{\Phi}(G)\rangle$ by elementary Galois theory. By Theorem 2.3, this implies that $G = H$. But then $K = K(\alpha)$ and therefore α belongs to K. Since we are assuming that K/k is regular, this implies that α belongs to k. Hence k is algebraically closed in L and therefore L is a regular extension of k. □

Chapter 4

The Brauer Group

4.1 Azumaya Algebras

In this section we introduce the class of Azumaya R-algebras. These algebras, which are defined for any commutative ring R, generalize the class of central simple algebras over a field K. A finite dimensional K-algebra $\mathfrak{A}$ is called a *central simple K-algebra* if $\mathfrak{A}$ has no nontrivial two-sided ideals and the center of $\mathfrak{A}$ equals K. Wedderburn's Main Theorem [Dr, p. 15] asserts that every central simple K-algebra is isomorphic to one of the form $\mathrm{End}_D(V)$ for some finite dimensional division algebra D over K and D-vector space V. It follows that a K-algebra $\mathfrak{A}$ is central simple if and only if there exists a finite extension L/K such that the extended algebra $\mathfrak{A} \otimes_K L$ is isomorphic to $\mathrm{End}_L(V)$ for some finite dimensional L-vector space V. These are all successful characterizations of central simple K-algebras, mainly for the reasons that, every K-module is free and every extension of fields L/K is faithfully flat. For an arbitrary commutative ring both are far from being the case, and so a more indirect approach is required.

Let R be a commutative ring and $A = (A, +, *)$ an R-algebra. The *opposite algebra of A*, denoted A°, is the R-algebra $(A, +, \diamond)$ where $a \diamond b = b * a$ for all $a, b \in A$. Thus $(A, +, *)$ and $(A, +, \diamond)$ are equal as R-modules but the order of multiplication in the second algebra is reversed. Since R is contained in the center of $(A, +, *)$, the same inclusion makes $(A, +, \diamond)$ into an R-algebra. Note that every left A-module M is naturally a right A°-module and

so on. Regarding A as a module over itself, we obtain homomorphisms of R-algebras

$$\lambda\colon A \to \mathrm{End}_R(A) \qquad \lambda_a(x) = a * x$$
$$\rho\colon A^\circ \to \mathrm{End}_R(A) \qquad \rho_b(x) = x * b$$

The associativity of multiplication in A implies the images of λ and ρ are commuting subalgebras of $\mathrm{End}_R(A)$. That is, we have $\lambda_a \circ \rho_b = \rho_b \circ \lambda_a$ for all $a \in A$ and $b \in A^\circ$. Consequently, λ and ρ define a homomorphism of R-algebras

$$\lambda \otimes \rho\colon A \otimes_R A^\circ \to \mathrm{End}_R(A).$$

We call A an *Azumaya R-algebra* if A is faithful, finitely generated, and projective as an R-module, and the above defined homomorphism $\lambda \otimes \rho\colon A \otimes_R A^\circ \to \mathrm{End}_R(A)$ is an isomorphism of R-algebras.

The first theorem of the section asserts that we have actually generalized the classical case.

Theorem 4.1. *Let K be a field and $\mathfrak{A}$ a K-algebra. Then $\mathfrak{A}$ is an Azumaya K-algebra if and only if $\mathfrak{A}$ is a central simple K-algebra.*

Proof. After one shows that the tensor product $\mathfrak{A} \otimes_K \mathfrak{A}^\circ$ is again a central simple K-algebra, the theorem follows by an easy dimension counting argument. See for example [Sa2, Lemma 2.1, p. 11]. □

In the next theorem, we collect three fundamental properties of Azumaya algebras. Namely that endomorphism rings of faithful, finitely generated, projective R-modules are Azumaya, the class of Azumaya R-algebras is closed under tensor product, and being Azumaya is preserved under base extension. In part (c) and below, we denote by A_S the S-algebra $A \otimes_R S$ and we call A_S the *algebra obtained by base extension from R to S*.

Theorem 4.2. *Let R be a commutative ring.*

(a) *Let P be an R-module. If P is a faithful, finitely generated, and projective then $\mathrm{End}_R(P)$ is an Azumaya R-algebra.*

(b) *If A and B are both Azumaya R-algebras then so is $A \otimes_R B$.*

(c) *If $\varphi\colon R \to S$ is a homomorphism of commutative rings and A is an Azumaya R-algebra then the extended algebra A_S is an Azumaya S-algebra.*

Proof. Part (a) and (b) are [DI, Proposition 3.3 & Proposition 4.1, pp. 52, 56]. For part (c), by [DI, Corollary 2.2, p. 13], the extended algebra A_S is faithful, finitely generated and projective as an S-module. Thus by [DI, Hom-Tensor Relation 2.4, p. 14], the natural homomorphism $\mathrm{End}_R(A)_S \to \mathrm{End}_S(A_S)$ is an isomorphism of S-algebras. Identifying A°_S with $(A^\circ)_S$, we obtain a sequence of isomorphisms

$$A_S \otimes_S A^\circ_S \cong (A \otimes_R A^\circ)_S \cong \mathrm{End}_R(A)_S \cong \mathrm{End}_S(A_S)$$

the composition of which is the required isomorphism. □

Part (a) of Theorem 4.3 is usually called the Double Centralizer Theorem as it implies that the subalgebra A of B is equal to the double centralizer $\mathbf{C}_B(\mathbf{C}_B(A))$.

Theorem 4.3. *Let R be a commutative ring.*

(a) *If A is an Azumaya R-subalgebra of the Azumaya R-algebra B then the centralizer $\mathbf{C}_B(A)$ of A in B is also an Azumaya R-algebra, and the natural homomorphism $A \otimes_R \mathbf{C}_B(A) \to B$ is an isomorphism of R-algebras.*

(b) *Every homomorphism of Azumaya R-algebras $\varphi\colon A \to B$ is monic. If the ranks of A and B are equal then φ is an isomorphism.*

Proof. Part (a) is [DI, Theorem 4.3, p. 57]. For part (b), since the kernel of φ is a two-sided ideal of A, by [DI, Corollary 3.7, p. 54] it must be of the form $I \cdot A$ for some ideal I of R. As φ is R-linear, this implies that $I \cdot \varphi(A) = 0$. Since the image of φ contains the isomorphic copy of R in B, we see that $I \cdot R = 0$. Since I is an ideal of R, this implies that $I = 0$ as desired. For the second half of (b), we may as well assume that A is an R-subalgebra of B. Applying part (a) the natural map $A \otimes_R \mathbf{C}_B(A) \to B$ is an isomorphism. By comparing ranks, we see that the centralizer of A in B must be an Azumaya R-algebra of rank one. But by [DI, Lemma 3.1, p. 51], the only rank one Azumaya R-algebra is R itself. It follows that A equals B. □

Two Azumaya algebras R-algebras, A and B are said to be *Brauer equivalent* if there exist two faithful, finitely generated, projective R-modules P and Q, and an isomorphism of R-algebras

$$A \otimes_R \mathrm{End}_R(P) \cong B \otimes_R \mathrm{End}_R(Q)$$

By [DI, Proposition 2.3 (d), p. 13] the tensor product $P \otimes_R Q$ is also faithful, finitely generated and projective and by [DI, Hom-Tensor Relation 2.4, p. 14] the natural homomorphism $\mathrm{End}_R(P) \to \mathrm{End}_R(Q) \to \mathrm{End}_R(P \otimes_R R)$ is an isomorphism of R-modules. Thus for each pair of Azumaya R-algebras A and B and each pair of faithful, finitely generated, projective R-modules P and Q there exists an isomorphism

$$(A \otimes_R \mathrm{End}_R(P)) \otimes_R (B \otimes_R \mathrm{End}_R(Q)) \cong (A \otimes_R B) \otimes_R \mathrm{End}_R(P \otimes_R Q).$$

For each Azumaya R-algebra A, we denote the Brauer equivalence class of A by $[A]$ and we let $\mathbf{Br}(R)$ denote the set of equivalence classes of Azumaya R-algebras. From the isomorphism above, it follows that the rule $[A] + [B] = [A \otimes_R B]$ gives a well-defined operation on $\mathbf{Br}(R)$.

Theorem 4.4. *Let R be a commutative ring.*

(a) *The pair $(\mathbf{Br}(R), +)$ is an abelian group.*

(b) *For each homomorphism of commutative rings $\varphi\colon R \to S$, there exists a unique homomorphism of groups $\varphi_*\colon \mathbf{Br}(R) \to \mathbf{Br}(S)$ such that $\varphi_*[A] = [A_S]$ for each Azumaya R-algebra A.*

(c) *The rules $R \mapsto (\mathbf{Br}(R), +)$ and $\varphi \mapsto \varphi_*$ comprise a covariant functor from the category of commutative rings to the category of abelian groups.*

Proof. The associativity and commutativity of the tensor product $\otimes_R$ imply the same properties for $+$. Hence it is enough to exhibit an identity element and to show that every class has an inverse. For each R-algebra A, the algebras $A \otimes_R R$ and $R \otimes_R A$ are both isomorphic to A and hence the class $[R]$ is a two sided identity for $+$. And by definition, if A is an Azumaya R-algebra, then $A \otimes_R A^\circ \cong \mathrm{End}_R(A)$. Since $[\mathrm{End}_R(A)]$ is the identity with respect to $+$, it follows that $[A]$ and $[A^\circ]$ are inverses. This proves (a).

For part (b), if such a homomorphism exists then it is certainly unique. By [DI, Hom-Tensor Relation 2.4, p. 14], if P is a faithful, finitely generated, projective R-module then $P \otimes_R S$ is a faithful, finitely generated, projective S-module and we have an isomorphism of S-algebras $\mathrm{End}_R(P)_S \cong \mathrm{End}_S(P \otimes_R S)$. Therefore $[A] = [B]$ implies $[A_S] = [B_S]$ and thus there exists a function $\varphi_*\colon \mathbf{Br}(R) \to \mathbf{Br}(S)$ such that $\varphi_*[A] = [A_S]$. Since $(A \otimes_R B)_S$ and $A_S \otimes_S B_S$ are isomorphic as S-algebras, it follows that φ_* is a homomorphism.

Since A and $A \otimes_R R$ are naturally isomorphic, it follows that the identity $\mathbf{1}_R \colon R \to R$ induces the identity homomorphism on $\mathbf{Br}(R)$. Let φ be as in part (b) and above let $\psi \colon S \to T$ be a homomorphism from S to the commutative ring T. We need to show that the induced homomorphisms $\psi_* \circ \varphi_*$ and $(\psi \circ \varphi)_*$ are equal. This follows from transitivity of base extension, namely the composition

$$(A \otimes_R S) \otimes_S T \to A \otimes_R (S \otimes_S T) \to A \otimes_R T$$

is an isomorphism of T-algebras. This proves (c). □

We call $\mathbf{Br}(R)$ the *Brauer group of* R. If S/R is an extension of commutative rings then we will write $\mathbf{\Psi}_R^S$ for the induced homomorphism $\mathbf{Br}(R) \to \mathbf{Br}(S)$ and we let $\mathbf{Br}(S/R)$ denote the kernel of $\mathbf{\Psi}_R^S$. We call $\mathbf{Br}(S/R)$ the *relative Brauer group of* S/R. If A is an Azumaya R-algebra such that $[A]$ belongs to $\mathbf{Br}(S/R)$ then we say that A *is split by* S.

4.2 Crossed Product Algebras

For each finite Galois extension of fields L/K, the Crossed Product Theorem [Dr, p. 96] gives an isomorphism between the second cohomology group $\mathbf{H}^2(L/K, L^\times)$ and the relative Brauer group $\mathbf{Br}(L/K)$. In this section we will state a generalization of that theorem to the case of a Galois extension of commutative rings, a notion which we define below. The passage from Galois extensions of fields to Galois extensions of commutative rings naturally parallels the generalization from central simple algebras to Azumaya algebras in the last section. Let S and T be commutative rings, and G a group that acts by automorphisms of S. For each homomorphism $\varphi \colon S \to T$ and each $\sigma \in G$ the composition $\varphi \circ \sigma$ is again a homomorphism of commutative rings, and thus there is a naturally defined right action of G on the set of homomorphisms from S to T.

Definition. Let S/R be an extension of commutative rings and G a finite group that acts by automorphisms of S. We call S/R a *G-Galois extension of commutative rings* if R is the fixed ring of G in S, and for each commutative ring T, the group G acts freely on the set of homomorphisms from S to T.

A few comments about this definition are in order. First when we say that G acts freely on a set X we mean that each $x \in X$ has trivial stabilizer in G. Thus if X is nonempty and G acts freely on X then G acts faithfully on X. Since the set of ring homomorphisms

from S to itself is nonempty, it follows that for S/R to be G-Galois, the group G must act faithfully on S. Also we assume that every commutative ring has a nonzero identity element and that each homomorphism of commutative rings $\varphi\colon S \to T$ sends the identity of S to that of T. In particular, the map from S to T that sends every element of S to zero is not a homomorphism of commutative rings. By Zorn's Lemma, our convention also implies that S has at least one maximal ideal. It follows that the second condition above is equivalent to each of the following.

(a) For each proper ideal I of S and each nontrivial $\sigma \in G$, there exists $x \in S$ such that $\sigma(x) \not\equiv x \mod I$.

(b) For each maximal ideal Q of S and each nontrivial $\sigma \in G$, there exists $x \in S$ such that $\sigma(x) \not\equiv x \mod Q$.

(c) For each field F, the group G acts freely on the set of homomorphisms from S to F.

Hence our definition of a Galois extension of commutative rings is equivalent to that of DeMeyer & Ingraham [DI, p. 84]. That our definition is equivalent to the definition given by Saltman [Sa2, p. 37] is Theorem 4.7 below. We should also note that, in contrast to the classical case, the extension S/R does not determine the group G. The first theorem of this section is just the observation that we have correctly generalized the usual definition of Galois.

Theorem 4.5. *Let L/K be an extension of fields and G finite group that acts by automorphisms of L. Then L/K is a G-Galois extension of commutative rings if and only if K is the fixed field of G in L, and G acts faithfully.*

Proof. The proof is immediate. □

Theorem 4.6 is approximately half of the Fundamental Theorem of Galois Theorem for commutative rings as formulated by DeMeyer & Ingraham [DI, p. 80]. Part (a) of the theorem has the important consequence that, if S/R is a G-Galois extension of commutative rings then S is a projective R-module of rank equal to the order of G. In particular, if S/R is G-Galois for some finite group G, then S/R is necessarily an integral extension.

Theorem 4.6. *Let G be a finite group and S/R a G-Galois extension of commutative rings.*

(a) *For each subgroup $H \leq G$, the extension S/S^H is H-Galois and the fixed ring S^H is projective as an R-module of rank equal to $[G : H]$.*

(b) *For each normal subgroup $N \trianglelefteq G$, the extension S^N/R is G/N-Galois.*

(c) *Let $\varphi\colon R \to U$ be a homomorphism of commutative rings and $V = S \otimes_R U$. Define an action of G on V by setting $\sigma(s \otimes u) = \sigma(s) \otimes u$. Then V/U is a G-Galois extension of commutative rings.*

Proof. Parts (a) and (b) are contained in [DI, Theorem 1.1, p. 80]. For part (c), see [DI, Corollary 1.3, p. 85]. □

We turn now to the promised application of Galois extensions of commutative rings, the notion of an Azumaya crossed product. Let S/R be an extension of commutative rings, G a finite group that acts by automorphisms of S/R, and f a normalized 2-cocycle of G in $S^\times$. We define the *crossed product algebra associated to S/R, G and f*, denoted $(S/R, G, f)$, to be the R-algebra $(A, +, *)$ constructed below. Let $(A, +, *)$ denote the free left S-module on the symbols $\{e(\sigma)\}_{\sigma \in G}$

$$(A, +) = \bigoplus_{\sigma \in G} S \cdot e(\sigma)$$

endowed with multiplication defined by setting

$$(x \cdot e(\sigma)) * (y \cdot e(\tau)) = x\sigma(y) f(\sigma, \tau) \cdot e(\sigma\tau) \qquad \text{for all } x, y \in S,\ \sigma, \tau \in G.$$

and then extending by linearity. The 2-cocycle condition

$$f(\rho, \sigma) \cdot f(\rho\sigma, \tau) = \rho(f(\sigma, \tau)) \cdot f(\rho, \sigma\tau)$$

ensures that the resulting operation is associative. Because we are assuming that f is normalized, the element $e(1)$ acts as a two-sided identity with respect to $*$. Accordingly, we identify S with the R-subalgebra $S \cdot e(1)$ of $(A, +, *)$.

The crossed product construction offer an alternative definition for Galois extensions of commutative rings. Let S/R be an extension of commutative rings and G a finite group that acts by automorphisms of S/R. There is an R-linear action of the crossed product $(S/R, G, 1)$ on S defined by setting

$$(x \cdot e(\sigma))(y) = x\sigma(y) \qquad \text{for all } x, y \in S,\ \sigma \in G.$$

Let $\varphi\colon (S/R, G, 1) \to \mathrm{End}_R(S)$ be the homomorphism of R-algebras defined thereby.

Theorem 4.7. *Let S/R be an extension of commutative rings and G a finite group that acts by automorphisms of S/R. Assume that S is finitely generated and projective as an R-module. Then the following conditions are equivalent.*

(a) *The extension S/R is a G-Galois extension of commutative rings.*

(b) *The homomorphism $\varphi\colon (S/R, G, 1) \to \mathrm{End}_R(S)$ is an isomorphism of R-algebras.*

(c) *The crossed product $(S/R, G, 1)$ is an Azumaya R-algebra.*

Proof. For the equivalence of conditions (a) and (b), see [DI, Proposition 1.2, p. 80]. Since we are assuming that S contains R, it is automatically faithful as an R-module and therefore the endomorphism ring $\mathrm{End}_R(S)$ is an Azumaya R-algebra by Theorem 4.2 part (a). This shows that (b) implies (c). The converse follows by counting ranks and applying the Double Centralizer Theorem 4.3. □

For our purposes, the point of considering Galois extensions of commutative rings, is their connection to the Brauer group. We begin by noting that crossed products over Galois extensions of commutative rings are Azumaya.

Theorem 4.8. *Let G be a finite group, and S/R a G-Galois extension of commutative rings.*

(a) *For each normalized 2-cocycle f of G in $S^\times$, the crossed product $(S/R, G, f)$ is an Azumaya R-algebra split by S.*

(b) *For each pair of normalized 2-cocycles f_1, f_2 of G in $S^\times$, the crossed product algebra $(S/R, G, f_1 \cdot f_2)$ is Brauer equivalent to the tensor product $(S/R, G, f_1) \otimes_R (S/R, G, f_2)$. If $f_1 \cdot f_2^{-1}$ is a 2-coboundary then $(S/R, G, f_1)$ and $(S/R, G, f_2)$ are isomorphic R-algebras.*

Proof. See [Sa2, Theorem 7.1, p. 44]. □

We call an Azumaya R-algebra of the form $(S/R, G, f)$ an *Azumaya crossed product*, and we denote by $[S/R, G, f]$ the Brauer equivalence class of $(S/R, G, f)$.

Theorem 4.9. *Let G be a finite group and S/R a G-Galois extension of commutative rings.*

(a) *There is a unique homomorphism* $\mathbf{H}^2(G, S^\times) \to \mathbf{Br}(S/R)$ *that maps the cohomology class of each normalized 2-cocycle* f *to the equivalence class of the Azumaya crossed product* $(S/R, G, f)$.

(b) *Let* $\varphi\colon R \to U$ *a homomorphism of commutative rings and* V/U *the induced* G*-Galois extension. Then the homomorphisms* $[f] \mapsto [S/R, G, f]$ *and* $[f] \mapsto [V/U, G, f]$ *give a commutative diagram*

$$\begin{array}{ccc} \mathbf{H}^2(G, S^\times) & \xrightarrow{\varphi_*} & \mathbf{H}^2(G, V^\times) \\ \downarrow & & \downarrow \\ \mathbf{Br}(S/R) & \xrightarrow{\mathbf{\Psi}_R^U} & \mathbf{Br}(V/U) \end{array}$$

Proof. By part (a) of Theorem 4.8, for each normalized 2-cocycle f the class $[S/R, G, f]$ belongs to $\mathbf{Br}(S/R)$. And part (b) of the same theorem implies that the rule $[f] \mapsto [S/R, G, f]$ is well-defined and that it gives a homomorphism from $\mathbf{H}^2(G, S^\times)$ to $\mathbf{Br}(R)$. Uniqueness is clear. This proves (a).

For part (b), it is enough to show that for each normalized 2-cocycle f of G in $S^\times$, the U-algebras $(S/R, G, f) \otimes_R U$ and $(S \otimes_R U, G, f \otimes 1)$ are equivalent. As an R-module $(S/R, G, f)$ is just a direct sum of $|G|$ copies of S. Hence there is a natural isomorphism of U-modules

$$(S/R, G, f) \otimes_R U \to (S \otimes_R U, G, f \otimes 1)$$

given by

$$\left(\sum_i s_i \cdot e(\sigma_i)\right) \otimes u \mapsto \sum_i (s_i \otimes u) \cdot e(\sigma_i)$$

But since $\sigma(1 \otimes u) = (1 \otimes u)$ for all $\sigma \in G$ and $u \in U$ it is easy to see that the isomorphism above is also an isomorphism of U-algebras. □

If S/R is a G-Galois extension of commutative rings, we will write $\mathbf{\Phi}_R^S$ for the homomorphism given by part (a) of Theorem 4.9. This is a mild abuse of notation, as the extension S/R does not determine the group G, but the homomorphism $\mathbf{\Phi}_R^S$ certainly depends on G. In our applications of Theorem 4.9, this will never be an issue as the extensions we consider will always determine their group. In these cases, we will write $(S/R, f)$ and $[S/R, f]$ instead of $(S/R, G, f)$ and $[S/R, G, f]$. We call $\mathbf{\Phi}_R^S$ the *crossed product homomorphism associated to* S/R *and* G.

Theorem 4.10. *Let G be a finite group and S/R a G-Galois extension of commutative rings. For each subgroup $H \leq G$, the crossed product homomorphisms give a commutative diagram*

$$\begin{array}{ccc} \mathbf{H}^2(G, S^\times) & \xrightarrow{\mathbf{Res}^G_H} & \mathbf{H}^2(H, S^\times) \\ \downarrow{\scriptstyle \mathbf{\Phi}^S_R} & & \downarrow{\scriptstyle \mathbf{\Phi}^S_{S^H}} \\ \mathbf{Br}(S/R) & \xrightarrow{\mathbf{\Psi}^{S^H}_R} & \mathbf{Br}(S/S^H) \end{array}$$

Proof. Let f be a normalized 2-cocycle of G in $S^\times$, $A = (S/R, G, f)$ the corresponding Azumaya crossed product algebra, and $T = S^H$ the fixed ring of H in S. We need to show that the extended algebra $A_T = A \otimes_R T$ is Brauer equivalent to the crossed product $(S/T, H, f)$. Let B denote the subring of A generated by S and the elements $e(\eta)$ for all $\eta \in H$. There is an obvious isomorphism of T-algebras between B and $(S/T, H, f)$. Since S/T is Galois, Theorem 4.6 implies that S is finitely generated and projective as an T-module. Since A is isomorphic to a direct sum of $|G|$ copies of S it must also be finitely generated and projective as an T-module. And by Theorem 4.6, the fixed ring T is projective as an R-module of rank equal to $[G : H]$.

Let C denote the centralizer of T in A. Then T is an R-subalgebra of C and [Sa2, Theorem 3.10, p. 24] implies that C is an Azumaya T-algebra equivalent to A_T and that

$$[A : R] = [C : T] \cdot [T : R]^2.$$

We have shown that $[A : R] = |G|^2$ and $[T : R] = [G : H]$, and therefore we must have $[C : S^H] = |H|^2$. Since $B \subseteq C$ and $[B : T]$ also equals $|H|^2$, part (b) of Theorem 4.3 implies that $B = C$. Hence $(S/T, H, f)$ is isomorphic to B, which equals C, which is equivalent to A_T, which proves the theorem. □

The next theorem gives the analogous diagram for the inflation, which corresponds under the crossed product homomorphisms to an inclusion of relative Brauer groups.

Theorem 4.11. *Let G be a finite group and S/R a G-Galois extension of commutative rings. Let $N \trianglelefteq G$ be a normal subgroup and $T = S^N$ the fixed ring of N in S. Then the*

crossed product homomorphisms give a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(G/N, T^\times) & \xrightarrow{\mathbf{Inf}_G^{G/N}} & \mathbf{H}^2(G, S^\times) \\ \Big\downarrow{\scriptstyle \mathbf{\Phi}_R^T} & & \Big\downarrow{\scriptstyle \mathbf{\Phi}_R^S} \\ \mathbf{Br}(T/R) & \longrightarrow & \mathbf{Br}(S/R) \end{array}$$

Proof. See [Sa2, Proposition 7.7, p. 47]. □

Let G be a finite group and S/R a G-Galois extension of commutative rings. Let $H \leq G$ be a subgroup and $T = S^H$ the fixed field of H in S. Fix $\sigma \in G$ and let $T^\sigma = \sigma^{-1}(T)$. Then T^σ is the fixed field of H^σ in S, and σ restricts to an isomorphism from T^σ to T. Therefore σ induces an isomorphism

$$\sigma_* \colon \mathbf{Br}(S/T^\sigma) \to \mathbf{Br}(S/T) \qquad \sigma_*[A] = [A \otimes_{T^\sigma} T].$$

In the tensor product $A \otimes_{T^\sigma} T$ we have $\sigma^{-1}(x) \otimes 1 = 1 \otimes x$ for all $x \in T$. It follows that the extended algebra $A \otimes_{T^\sigma} T$ is isomorphic to the T-algebra, denoted ${}^\sigma A$, which is obtained by composing the isomorphism $\sigma^{-1} \colon T \to T^\sigma$ with the inclusion of T^σ in A.

Theorem 4.12. *With assumptions as above, the crossed product homomorphisms give a commutative diagram*

$$\begin{array}{ccccc} \mathbf{H}^2(H^\sigma, S^\times) & \xrightarrow{\sigma_*} & \mathbf{H}^2(H, S^\times) & \qquad [f] \xmapsto{\sigma_*} & [{}^\sigma f] \\ \Big\downarrow{\scriptstyle \mathbf{\Phi}_{T^\sigma}^S} & & \Big\downarrow{\scriptstyle \mathbf{\Phi}_T^S} & & \\ \mathbf{Br}(S/T^\sigma) & \xrightarrow{\sigma_*} & \mathbf{Br}(S/T) & \qquad [A] \xmapsto{\sigma_*} & [{}^\sigma A] \end{array}$$

Proof. Let $A = (S/T^\sigma, H^\sigma, f)$ and $B = (S/T, H, {}^\sigma f)$. There is a unique isomorphism of R-modules $\varphi \colon A \to B$ such that $\varphi(x \cdot e(\eta^\sigma)) = \sigma(x) \cdot e(\eta)$ for all $x \in S$ and $\eta \in H$. It is easy to check that φ is an isomorphism of R-algebras which gives a commutative diagram of R-algebras

$$\begin{array}{ccc} T^\sigma & \xrightarrow{\sigma} & T \\ \Big\downarrow & & \Big\downarrow \\ A & \xrightarrow{\varphi} & B \end{array}$$

Thus φ and the inclusion $T \to B$ extend uniquely to a homomorphism of R-algebras

$$\varphi \otimes 1 \colon A \otimes_{T^\sigma} T \to B$$

which is automatically a homomorphism of T-algebras. Since $\sigma \colon T^\sigma \to T$ is an isomorphism, we see that the natural map $A \to A \otimes_{T^\sigma} T$ is also an isomorphism and thus so is $\varphi \otimes 1$. Thus the T-algebras ${}^\sigma A$ and B are isomorphic, which proves the theorem. □

If L/K is a finite Galois extension of fields then the crossed product homomorphism is known to be an isomorphism between $\mathbf{H}^2(L/K, L^\times)$ and $\mathbf{Br}(L/K)$. The so-called Generalized Crossed Product Theorem has this classical result as a special case.

Theorem 4.13. *Let G be a finite group, and S/R a G-Galois extension of commutative rings. If every projective S-module of rank one is free then the crossed product homomorphism $\mathbf{\Phi}_R^S \colon \mathbf{H}^2(G, S^\times) \to \mathbf{Br}(S/R)$ is an isomorphism.*

Proof. See [DI, Theorem 1.1, p. 116] or [Sa2, Theorem 7.2, p. 45]. □

Theorem 4.14. *Let K be a field and K_s a separable closure of K. As L ranges over the over the finite Galois extensions of K contained in K_s, the crossed product isomorphisms $\mathbf{\Phi}_K^L \colon \mathbf{H}^2(L/K, L^\times) \to \mathbf{Br}(L/K)$ induce an isomorphism*

$$\mathbf{\Phi}_K \colon \mathbf{H}^2(\mathrm{G}_K, K_s^\times) \to \mathbf{Br}(K)$$

Proof. By Köthe's Theorem [Dr, Corollary 6, p. 65], for each central simple K-algebra $\mathfrak{A}$, there exists finite separable extension L of K in K_s that splits $\mathfrak{A}$. This shows that $\mathbf{Br}(K)$ is the union, and hence the direct limit, of the subgroups $\mathbf{Br}(L/K)$ as L ranges over the finite Galois extensions of K contained in K_s. With Theorem 3.10, we see that by passage to the limit, the crossed product isomorphisms define the desired isomorphism $\mathbf{\Phi}_K \colon \mathbf{H}^2(\mathrm{G}_K, K_s^\times) \to \mathbf{Br}(K)$. □

4.3 Norm Residue Symbols

This section offers a treatment of the theory of m-th power norm residue symbols over a commutative ring. Classically, they are defined, for each field K that contains primitive m-th root of unity, as the Brauer equivalence classes of certain central simple K-algebras, the

so-called m-th power norm residue algebras. In this way, the norm residue symbol gives, for each pair of units $a, b \in K^\times$, a certain Brauer equivalence class $[a, b]$ which belongs to the m-torsion part of $\mathbf{Br}(K)$. The attractiveness of this construction is twofold. First, every class in $\mathbf{Br}(K)$ split by an extension of the form $K(a^{1/m})$ is equal to a symbol of the form $[a, b]$ for some $b \in K^\times$. And second, the symbol $[a, b]$ is multiplicative and alternating in a and b, and satisfies certain easily expressed relations which facilitate computations.

Norm residue symbols over an arbitrary commutative ring R will not possess all of these properties, but they will have enough of them to constitute a worthwhile generalization. In passing from fields to rings, the construction all is fairly automatic, the only obstacle being that the notion of a primitive m-th root of unity is not well behaved in the context of commutative rings. To address this problem, we propose the following, we call an element $\zeta \in R$ a *generalized primitive m-th root of unity* if $\Phi_m(\zeta) = 0$ where $\Phi_m(x) \in \mathbb{Z}[x]$ is the m-th cyclotomic polynomial. If R is a field of characteristic prime to m we recover the usual notion of a primitive m-th root of unity. Moreover, since $\Phi_m(x)$ divides $x^m - 1$, we see that every generalized primitive m-th root of unity is a unit of R, and is of m-torsion as an element of $R^\times$. Also, because the definition is stated as a vanishing condition, the property of begin a generalized primitive m-th root of unity is preserved under homomorphisms of commutative rings.

For the rest of the section, we fix a commutative ring R, which we assume to contain a generalized primitive m-th root of unity ζ. We will define norm reside algebras over R directly, but to establish some of their properties it will be convenient to show that they are isomorphic to certain Azumaya crossed products defined with respect to cyclic Kummer extensions of R. To describe these we fix a unit $a \in R^\times$, and set $S = R[\alpha]$ the extension of obtained by adjoining to R a formal m-th root α of a. To make this precise, we put $S = R[x]/(x^m - a)$, and write α for the image of x under the canonical epimorphism. We should remark that we do not assume a to be such that the polynomial $x^m - a$ is irreducible in $R[x]$. Let $G = \langle \sigma : \sigma^m \rangle$ be the cyclic group of order m, generated by σ. Then setting $\sigma(\alpha) = \zeta \cdot \alpha$ defines an action of G by automorphisms of S/R. It is reasonable to suspect that S/R might be G-Galois, but in fact this depends on R. One problem is that ζ might not even be of order m. But simply requiring ζ to have the right order is insufficient for S/R to be G-Galois. For a necessary and sufficient condition, we present the first lemma.

Lemma 4.15. *In the situation above, S/R is a G-Galois extension of commutative rings if and only if m is invertible in R.*

Proof. The essential point is that

$$m = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{m-1})$$

To see this, assume temporarily that R is the integral domain $\mathbb{Z}[z]/(\Phi_m(z))$, and ζ is the image of z. Then in the polynomial ring $R[x]$, we have $x^m - 1 = \prod_{i=0}^{m-1}(x-\zeta^i)$, and on dividing both polynomials by $x-1$, we see that

$$x^{m-1} + \cdots + x + 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{m-1})$$

By evaluating both sides at $x = 1$, we obtain the desired relation. In the general case, it is enough to observe that mapping $z \mapsto \zeta$ defines a homomorphism $\mathbb{Z}[z]/(f_m(z)) \to R$. Therefore if m is invertible in R, then so are $1-\zeta^i$ $(i = 1, 2, \ldots, m-1)$, and conversely.

Now assume m is invertible in R. Since the action of G preserves the decomposition of S in to a direct sum of R-modules $S = \oplus_{i=0}^{m-1} R\cdot\alpha^i$, to show that R is the fixed ring of G in S, it is enough to show that $(R\cdot\alpha^i)^G = 0$ unless $m \mid i$. For $r \in R$, the product $r\cdot\alpha^i$ is fixed by σ if and only if $r(\zeta^i - 1)\alpha^i = 0$. If $m \nmid i$, then $(\zeta^i - 1)\alpha^i$ is a unit in S, and therefore $r = 0$. Thus to show that S/R is G-Galois, it remains only to show G acts freely on the set of homomorphisms $\varphi\colon S \to L$ from S to a field L. For this, it suffices to check that the elements $\varphi(\sigma^i(\alpha)) = \varphi(\zeta)^i\cdot\varphi(\alpha)$, $i = 0, 1, 2, \ldots, m$ are pairwise distinct, or equivalently that $\varphi(\zeta)$ is a primitive m-th root of unity in L. But the differences $1-\zeta^i$, $i = 1, 2, \ldots, m-1$ are units of S, and hence their images under φ are all nonzero in L. For the converse, if m is not a unit of R, then there is a maximal ideal P of R, that contains $1-\zeta^i$ for some $i = 1, 2, \ldots, m-1$. We leave it to the reader to check that σ^i induces the identity automorphism on $S\otimes_R R/P$, which implies that S/R cannot be a G-Galois extension of commutative rings. □

In addition to our assumption that R contains the generalized primitive m-th root of unity ζ, for the rest of the section, we will assume that m is invertible in R. For each pair of units $a, b \in R^\times$, we denote by $(a, b; R, \zeta)$ the R-algebra generated by the noncommuting symbols x and y, subject to the relations

$$x^m = a \qquad y^m = b \qquad y\cdot x = \zeta\cdot x\cdot y$$

Since a and b are units of R, it follows that x and y are units of $(a, b; K, \zeta)$, and because

they both commute with every element of R, the last relation implies that

$$y^j \cdot x^i = \zeta^{ij} \cdot x^i \cdot y^j \qquad \text{for all } i, j \in \mathbb{Z}.$$

It follows that $(a, b; R, \zeta)$ is a free R-module of rank m^2, with basis $\{x^i \cdot y^j : i, j = 0, 1, 2, \ldots, m-1\}$. We call a R-algebra of the form $(a, b; K, \zeta)$ an *m-th power norm residue algebra*, for reasons which are explained by Theorem 4.16 below. Our first goal is to show that $(a, b; R, \zeta)$ is an Azumaya R-algebra.

This is accomplished by showing that $(a, b; R, \zeta)$ is isomorphic to a certain Azumaya crossed product. We retain the notation introduced above, so that $S = R[\alpha]$ where α is a formal m-th root of the element $a \in R^\times$, and $G = \langle \sigma \rangle$. Since G is cyclic, Theorem 3.8 provides an isomorphism

$$\mathbf{H}^2(G, S^\times) \to R^\times / \mathbf{Nm}_G(S^\times) \qquad [f] \mapsto f(\sigma, \sigma^{m-1})$$

where $\mathbf{Nm}_G \colon S \to R$ is G-norm $\mathbf{Nm}_G(\beta) = \prod_{i=0}^{m-1} \sigma^i(\beta)$. Under this isomorphism a second cohomology class that maps to $b \in R^\times$ is represented by a 2-cocycle f that satisfies

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < m \\ b & \text{if } i + j \geq m \end{cases} \qquad \text{for all } i, j = 0, 1, 2, \ldots, m-1.$$

The corresponding crossed product $(S/R, G, f)$ is generated as an R-algebra by elements α and $e(\sigma)$, which satisfy the relations

$$\alpha^m = a \qquad e(\sigma)^m = b \qquad e(\sigma) \cdot \alpha = \zeta \alpha \cdot e(\sigma)$$

Thus after fixing a generator for G, the crossed product algebra is completely determined by the choice of b. For this reason, the algebra $(S/R, G, f)$ is customarily denoted by $(S/R, \sigma, b)$ and called a *cyclic algebra*. The relations displayed above show that there is an isomorphism of R-algebras $(a, b; R, \zeta) \to (S/R, \sigma, b)$ under which $x \mapsto \alpha$ and $y \mapsto e(\sigma)$. This proves most of Theorem 4.16 below. In the the statement of the theorem, and more generally when no confusion can occur, we abbreviate $(a, b; R, \zeta)$ by (a, b).

Theorem 4.16. *Assume as above that the commutative ring R contains a generalized primitive m-th root of unity ζ, and that m is invertible in R. Then for each pair of units $a, b \in R^\times$, the m-th power norm residue algebra (a, b) is an Azumaya R-algebra split by*

every homomorphism of R that sends a to an m-th power. The norm residue algebra (a, b) is split over R if b is of the form $\mathbf{Nm}_G(\beta)$ for some $\beta \in S$.

Proof. As the norm residue algebra (a, b) is isomorphic to the cyclic algebra $(S/R, \sigma, b)$, it follows by Theorem 4.9 that S splits (a, b). More generally if $\varphi\colon R \to T$ is a homomorphism of commutative rings, such that $\varphi(a)$ is an m-th power in T, then φ extends to a homomorphism $\tilde{\varphi}\colon S \to T$. Therefore since φ factors through S, we see that T also splits (a, b). For the last part, if $b = \mathbf{Nm}_G(\beta)$ then the 2-cocycle f defined above is a 2-coboundary by Theorem 3.8, and therefore (a, b) is isomorphic to the trivial crossed product $(S/R, G, 1)$. □

We note that by Theorem 4.13, if every rank one projective S-module is free, notably if R and S are both fields, then the condition that (a, b) be split over R is sufficient to imply that b is a norm from S to R. For each pair of units $a, b \in R^\times$, we denote by $[a, b]$ of $[a, b; R, \zeta]$ the equivalence class of $(a, b; K, \zeta)$ in $\mathbf{Br}(R)$. We call $[a, b]$ an *m-th power norm residue symbol*. The utility of norm residue symbols is due in large part to the next theorem.

Theorem 4.17. *Let R be a commutative ring that contains a generalized primitive m-th root of unity ζ, and assume that m is invertible in R. The map $R^\times \times R^\times \to \mathbf{Br}(R)$ that sends each pair of units $a, b \in R^\times$ to the norm residue symbol $[a, b]$ is bimultiplicative and alternating; we have*

$$[a, b \cdot c] = [a, b] + [a, c] \qquad [a \cdot b, c] = [a, c] + [b, c] \qquad [b, a] = -[a, b]$$

for all $a, b, c, \in R^\times$. Let $\varphi\colon R \to T$ be a homomorphism of commutative rings, and $\varphi_*\colon \mathbf{Br}(R) \to \mathbf{Br}(T)$ the induced homomorphism. Then

$$\varphi_*[a, b; R, \zeta] = [\varphi(a), \varphi(b); T, \varphi(\zeta)] \qquad \text{for all } a, b \in R^\times.$$

Proof. We already know that the rule $b \mapsto (S/R, \sigma, b)$ defines a homomorphism $R^\times \to \mathbf{Br}(R)$. This shows that the symbol $[*, *]$ is multiplicative in the second position. After we prove that $[*, *]$ is alternating, this will entail multiplicativity in the first position as well. The opposite algebra $(a, b)^\circ$ is generated as an R-algebra by elements x and y which satisfy the relations $x^m = a$, $y^m = b$ and $x \cdot y = \zeta \cdot y \cdot x$. Interchanging x and y gives a presentation for (b, a), showing that $(a, b)^\circ$ and (b, a) are isomorphic as R-algebras.

For the second half of the theorem, the obvious homomorphism of R-algebras $(a, b; R, \zeta) \to (\varphi(a), \varphi(b); T, \varphi(\zeta))$, and the inclusion T in $(\varphi(a), \varphi(b); T, \varphi(\zeta))$, define a homomorphism of Azumaya T-algebras

$$(a, b; R, \zeta) \otimes_R T \to (\varphi(a), \varphi(b); T, \varphi(\zeta))$$

Which is seen to be an isomorphism by Theorem 4.3. □

Lemma 4.18. *With assumptions on R, ζ, and m as above, let $a, b \in R^\times$.*

(a) *We have $m \cdot [a, b] = [a^m, b] = [a, b^m] = 0$. If $a + b$ is an m-th power in R then $[a, b]$ is also trivial.*

(b) *The symbols $[a, -a]$ and $[b, 1 - b]$, ($b \neq 1$) are both trivial.*

(c) *If $a - b \in R^\times$ then $[a, b] + [a, -1] = [a/b, a - b]$.*

Proof. We have $[a, b^m] = 0$ because, with $S = R[\alpha]$ as above, we see that $\mathbf{Nm}_G(b) = b^m$ for all $b \in R^\times$, and therefore $(R^\times)^m \leq \mathbf{Nm}_G(S^\times)$. Since $[*, *]$ is bimultiplicative and alternating, this implies that $m \cdot [a, b] = [a^m, b] = 0$ as well. The second half of part (a) follows from the claim that $\mathbf{Nm}_G(c - \alpha) = c^m - a$ for all $c \in R$. To see this, we note that the relation

$$x^m - 1 = \prod_{i=0}^{m-1} (x - \zeta^i)$$

holds in $R[x]$, since it can be checked over $\mathbb{Z}[z]/(\Phi_m(z))$. Replacing x with x/α, and multiplying both sides by $a = \alpha^m$, we obtain the expected factorization of $x^m - a$ in $S[x]$, namely

$$x^m - a = \prod_{i=0}^{m-1} (x - \alpha\zeta^i)$$

Evaluating both sides at $x = c$, and recognizing that product becomes the norm $\mathbf{Nm}_G(c - \alpha)$, gives the desired relation. Now if $a + b = c^m$ then $b = \mathbf{Nm}_G(c - \alpha)$ and $[a, b]$ is trivial by Theorem 4.16. Part (b) follows immediately, as $a + (-a) = 0$ and $b + (1 - b) = 1$ are both m-th powers.

For the last part, let $c = a/b$. By part (b) of the lemma, the symbols $[b, -b]$ and

$[c, 1-c]$ are both trivial, and therefore

$$\begin{aligned}[a,b]+[a,-1] &= [a,b]+[a,-1]-[b,-b]+[c,1-c] \\ &= [a,-b]-[b,-b]+[c,1-c] \\ &= [c,-b]+[c,1-c] \\ &= [c,bc-b]\end{aligned}$$

Since $bc - b = a - b$, this proves (c). □

We close the section with a theorem that gives a second expression for the norm residue symbol as the class of a Azumaya crossed product. We will do so only in the case that m is odd.

Fix units $a, b \in R^\times$, and let $T = R[\alpha, \beta]$ be the extension obtained by adjoining formal m-th roots α and β of a and b. Thus we define T as a quotient of the polynomial ring $T = R[x, y]/(x^m - a, y^m - b)$.

Let $H = \langle \sigma, \tau \rangle$ be the abelian group of exponent m and order m^2, generated by σ and τ. There is a unique action of H by automorphisms of T/R defined by setting

$$\sigma(\alpha) = \alpha\zeta \qquad \sigma(\beta) = \beta \qquad \tau(\alpha) = \alpha \qquad \tau(\beta) = \beta\zeta.$$

Since m is odd and $\zeta^m = 1$, the expression

$$f(\sigma^{i_1}\tau^{j_i}, \sigma^{i_2}\tau^{j_2}) = \zeta^{\frac{1}{2}(i_1 \cdot j_2 - i_2 \cdot j_1)}$$

is well defined for all $i_1, i_2, j_1, j_2 \in \mathbb{Z}$. Now that all of this is in place we can state the advertised theorem.

Theorem 4.19. *Assume as above that ζ is a generalized primitive m-th root of unity, and m is odd and invertible in R. Then T/R is an H-Galois extension of commutative rings, f is a normalized 2-cocycle of H in $T^\times$, and the class of the Azumaya crossed product $[T/R, H, f]$ is equal to the norm residue symbol $[a, b]$.*

Proof. That the extension T/R is H-Galois can be checked directly as in the proof of Lemma 4.15. It is an immediate consequence of bimultiplicativity, that f satisfies the 2-cocycle condition and is normalized. Therefore the crossed product $(T/R, H, f)$ is an Azumaya R-algebra by Theorem 4.8. As in the last section, we represent the crossed

product algebra as the direct sum

$$(T/R, H, f) = \oplus_{\eta \in H} T \cdot e(\eta)$$

with multiplication defined by $(s \cdot e(\gamma)) * (t \cdot e(\eta)) = s\gamma(t) f(\gamma, \eta) \cdot e(\gamma\eta)$, and we identify T with the subring $T \cdot e(1)$. Thus $(T/R, H, f)$ is generated as an R-algebra by the elements α, β, $e(\sigma)$ and $e(\tau)$.

Let A denote the R-subalgebra of $(T/R, H, f)$ generated by the units α and $\beta \cdot e(\sigma)$. Then $\alpha^m = a$ and $(\beta \cdot e(\sigma)) * \alpha = \zeta \cdot \alpha * (\beta \cdot e(\sigma))$. Since σ fixes β, and $f(\sigma^i, \sigma^j) = 1$ for all i, j, we have $(\beta \cdot e(\sigma))^m = b$. By comparing this presentation for A with the definition of the norm residue algebra (a, b), we see that the two are isomorphic as R-algebras. In particular, A is an Azumaya R-algebra and $[A] = [a, b]$. Let C denote the centralizer of A in the crossed product $(T/R, H, f)$. Then Theorem 4.3 implies that C is also an Azumaya R-algebra, and that $(T/R, H, f)$ is isomorphic to the tensor product $A \otimes_R C$. Therefore we have $[T/R, H, f] = [a, b] + [C]$, and to prove the theorem, it is enough to show that $[C] = 0$. Since the isomorphism $A \otimes_R C \cong (T/R, H, f)$ implies that $[C : R] = m^2$, we see that C is the R-subalgebra of $(T/R, H, f)$ generated by β and $e(\tau)$. But then C is isomorphic to the norm residue algebra $(b, 1)$. Since $[b, 1] = 0$, this proves the theorem. □

4.4 The Brauer Group of a Dedekind Domain

In this section we specialize the theory of Azumaya algebras and the Brauer group to the case in which the base ring R is Dedekind domain. We will see that the theory obtained is tightly connected to that of the field of fractions K of R, and of the discrete valuation rings that lie between R and K. We show that the natural map between the Brauer groups of R and K is monic, and that the Brauer group of R is the intersection of the Brauer groups of its localizations. We close the section with two applications. The first is to compute the Brauer group of a polynomial ring over a perfect field, and the second is to relate the Brauer groups of a discrete valuation ring and its field of fractions to those of their completions. We begin by recalling the basic notions.

A *Dedekind domain* is an integrally closed Noetherian domain in which every nonzero prime ideal is maximal. A *discrete valuation ring* is a principal ideal domain with exactly one nonzero prime ideal. In particular, every discrete valuation ring is a Dedekind domain. By [Se1, Proposition 4, p. 10], if R is Dedekind domain then for each

nonzero prime ideal P of R, the local ring R_P is a discrete valuation ring. In what follows, by a *prime of* R we will always mean a nonzero prime ideal of R. Let R be a Dedekind domain, K its field of fractions, and V a finite dimensional K-vector space. An *R-lattice in V* is a finitely generated R-submodule M of V, such that $V = K \cdot M$. By [Bo3, Proposition 22, p. 543], every R-lattice is projective as an R-module. If $\mathfrak{A}$ is a central simple K-algebra then and *R-order in $\mathfrak{A}$* is an R-subalgebra of $\mathfrak{A}$ that is also an R-lattice in $\mathfrak{A}$. A *maximal R-order* in $\mathfrak{A}$ is an R-order that is maximal with respect to inclusion.

The results of the first half of this section will be built on our understanding of the relationship between Azumaya R-algebras and maximal R-orders. We begin with the observation that every Azumaya R-algebra arises as a maximal R-order.

Lemma 4.20. *Let R be a Dedekind domain and K its field of fractions.*

(a) *If A is an Azumaya R-algebra then A is a maximal R-order in the central simple K-algebra A_K.*

(b) *If A is an Azumaya R-subalgebra of the Azumaya R-algebra B then the centralizer $\mathbf{C}_B(A)$ of A in B is a maximal R-order in $\mathbf{C}_{B_K}(A_K)$.*

Proof. For part (a), we refer the reader to [Sa2, Theorem 9.4, p. 63]. For part (b), let C denote the centralizer $\mathbf{C}_B(A)$. By the Double Centralizer Theorem (4.3), C is an Azumaya R-algebra, and B is isomorphic to $A \otimes_R C$. Thus we may identify B_K with $A_K \otimes_K C_K$. Under this identification, we have $C_K = \mathbf{C}_{B_K}(A_K)$. As part (a) implies that C is a maximal R-order in C_K, this proves (b). □

Theorem 4.21. *Let R be a Dedekind domain and K its field of fractions.*

(a) *Let A be an Azumaya R-algebra and $\mathfrak{B}$ a central simple K-algebra. If A_K and $\mathfrak{B}$ are Brauer equivalent then every maximal R-order B in $\mathfrak{B}$ is an Azumaya R-algebra equivalent to A.*

(b) *The natural homomorphism $\mathbf{\Psi}_R \colon \mathbf{Br}(R) \to \mathbf{Br}(K)$ is monic.*

Proof. We divide the proof of (a) in to two cases. First assume that A_K and $\mathfrak{B}$ are isomorphic as K-algebras and identify A with the corresponding Azumaya R-order in $\mathfrak{B}$. Let P denote the R-submodule of $\mathfrak{B}$ generated by all products of the form $a \cdot b$ with $a \in A$ and $b \in B$. Then P is a left A-module, a right B-module, and an R-lattice in $\mathfrak{B}$. Since R is a Dedekind domain, P is projective as an R-module and hence $\mathrm{End}_R(P)$ is an Azumaya

R-algebra by Theorem 4.2 part (a). As P is an (A, B)-bimodule that contains both A and B, there are natural embeddings of A and B as commuting R-subalgebras of $\mathrm{End}_R(P)$.

Since the ranks of A, B and P are all equal, $\mathrm{End}_R(P)$ may be identified with an Azumaya R-order in $\mathfrak{B} \otimes_K \mathfrak{B}^\circ$ that contains $A = A \otimes 1$ and $B^\circ = 1 \otimes B^\circ$. Let C denote the centralizer of A in $\mathrm{End}_R(P)$. By applying the Double Centralizer Theorem, we see that C is an Azumaya R-subalgebra of $\mathrm{End}_R(P)$ equivalent to A°. And Lemma 4.20 implies that C is an R-order in $\mathfrak{B}^\circ = 1 \otimes \mathfrak{B}^\circ$. Since B° centralizes A, it follows that C contains B°. As we are assuming that B is maximal, this implies that $B^\circ = C$. Hence B is an Azumaya R-algebra equivalent to A.

Now assume that A_K and $\mathfrak{B}$ are merely equivalent. Hence there exists an isomorphism of K-algebras

$$A_K \otimes_K \mathrm{End}_K(V) \cong \mathfrak{B} \otimes_K \mathrm{End}_K(W).$$

for two finite dimensional K-vector spaces V and W. Let P and Q be R-lattices in V and W. Since R is a Dedekind domain, P and Q are projective as R-modules and therefore the endomorphism rings $\mathrm{End}_R(P)$ and $\mathrm{End}_R(Q)$ are Azumaya R-algebras. Let M be a maximal R-order in $\mathfrak{B} \otimes_K \mathrm{End}_K(W)$ that contains $B \otimes_R \mathrm{End}_R(Q)$. Then we have isomorphisms of K-algebras

$$(A \otimes_R \mathrm{End}_R(P))_K \cong (B \otimes_R \mathrm{End}_R(Q))_K \cong M_K$$

From the previous paragraph, we see that M is an Azumaya R-algebra which is Brauer equivalent to $A \otimes_R \mathrm{End}_R(P)$ and thus to A. Let C denote the centralizer of $\mathrm{End}_R(Q)$ in M. Then C is an Azumaya R-algebra equivalent to M, and an R-order in $\mathfrak{B}$ that contains B. Since B is maximal, we must have $B = C$. Therefore B is an Azumaya R-algebra equivalent to M. Since M is equivalent to A, this completes the proof of part (a). For part (b), let A and B be two Azumaya R-algebras. By Lemma 4.20, A is a maximal R-order in A_K. Hence if A_K and B_K are equivalent then so are A and B by part (a) of the theorem. This shows that $\mathbf{\Psi}_R$ is monic. □

Theorem 4.21 also implies that the natural homomorphism $\mathbf{Br}(R) \to \mathbf{Br}(R_P)$ is monic for each prime P of R. The relationship between the Brauer groups of R, the local rings R_P and the field of fractions K will be a central theme in the proof of the first main theorem. Since each element of K belongs to the local ring R_P for all but finitely many primes P of R, and being Azumaya is defined by finitely many elements, is not hard to see that each class in $\mathbf{Br}(K)$ belongs to the image of $\mathbf{\Psi}_P \colon \mathbf{Br}(R_P) \to \mathbf{Br}(K)$ for all but

finitely many primes P of R. By [Se1, Proposition 4, p. 10], every Dedekind domain R is the intersection of the local rings R_P as P ranges over the primes of R. In Theorem 4.22, we have a sort of Brauer group-ification of this well-known fact. The proof we give is loosely based on the proofs of [Sa2, Lemma 9.3 & Theorem 9.7, pp. 62,64].

Theorem 4.22. *Let R be a Dedekind domain, K its field of fractions, and $\xi \in \mathbf{Br}(K)$. Then ξ belongs to the image of $\mathbf{\Psi}_R\colon \mathbf{Br}(R) \to \mathbf{Br}(K)$ if and only if ξ belongs to the image of $\mathbf{\Psi}_P\colon \mathbf{Br}(R_P) \to \mathbf{Br}(K)$ for each prime P of R.*

Proof. If ξ belongs to the image of $\mathbf{\Psi}_R$ then functoriality requires that is belong to the image of $\mathbf{\Psi}_P$ for each P. Conversely, assume that ξ belongs to the image of $\mathbf{\Psi}_P$ for all P. Let $\mathfrak{A}$ be a central simple K-algebra that represents ξ, and A a maximal R-order in $\mathfrak{A}$. Since $\mathfrak{A} = A_K$, the theorem will follow if we can show that A is an Azumaya R-algebra. By [Sa2, Theorem 2.2, p. 12], it is enough to show that A_P is an Azumaya R_P-algebra for each prime P. Since ξ belongs to the image of $\mathbf{\Psi}_P$ for every P, by Theorem 4.21, we need only prove that A_P is a maximal R_P-order for each P. In order to do so, we need to prove a claim about lattices.

Let L be an R-lattice in $\mathfrak{A}$ and let $\mathcal{O}(L)$ denote the set of all $x \in \mathfrak{A}$ such that $xL \leq L$. Then it is easy to see that $\mathcal{O}(L)$ is an R-order in $\mathfrak{A}$. Moreover, if A is an R-order in $\mathfrak{A}$ then $\mathcal{O}(A)$ equals A. Our claim is that the map $L \mapsto \mathcal{O}(L)$ commutes with localization at the primes of R. More precisely, for each prime P of R, we claim that the R_P-orders $\mathcal{O}(L)_P$ and $\mathcal{O}(L_P)$ are equal. That $\mathcal{O}(L)_P$ is contained in $\mathcal{O}(L_P)$ is elementary. For the reverse inclusion, fix $x \in \mathcal{O}(L_P)$ and assume that the elements $\ell_1, \ldots, \ell_d$ generate L as an R-module. It follows that $\ell_1, \ldots, \ell_d$ also generate L_P as an R_P-module. Thus by writing $x\ell_i$ as an R_P-linear combination of the generators and taking a common denominator, we can find $u \in R \setminus P$ such that $x\ell_i$ belongs to $u^{-1}L$ for all $i = 1, \ldots, d$. Hence, we have $xL \leq u^{-1}L$ and therefore ux belongs to $\mathcal{O}(L)$. Since u is a unit of R_P, this implies that x belongs to $\mathcal{O}(L)_P$. Thus $\mathcal{O}(L_P) \subseteq \mathcal{O}(L)_P$ and therefore the two orders are equal.

Now assume that B is an R_P-order in $\mathfrak{A}$ that contains A_P. Since A_P and B are both R_P-lattices, there exists an $y \in R_P$ such that $By \leq A_P$. Let $L = A \cap By$. Then L is an R-lattice in $\mathfrak{A}$ and $AL \leq L$. Thus $A \leq \mathcal{O}(L)$ and by the maximality of A, the two orders are equal. Localizing at P, it is easy to see that $(A \cap By)_P = A_P \cap By$ and therefore $L_P = By$. It follows that $B \leq \mathcal{O}(L_P)$. Since $A = \mathcal{O}(L)$ and we have $\mathcal{O}(L_P) = \mathcal{O}(L)_P$ by the previous paragraph, this implies that $B \leq A_P$. Therefore A_P is a maximal order. $\square$

In certain cases Theorem 4.21 allows us to the describe the Brauer group of a

polynomial ring.

Theorem 4.23. *Let k be a field and x an indeterminate. If k is perfect then natural homomorphism $\mathbf{Br}(k) \to \mathbf{Br}(k[x])$ is an isomorphism.*

Proof. Let $R = k[x]$ and $K = k(x)$. Even if k is not perfect, the natural homomorphism $\mathbf{Br}(k) \to \mathbf{Br}(R)$ must be monic, as the inclusion $k \to R$ is split by the obvious projection of R onto k. Now assume that k is perfect and fix $\xi \in \mathbf{Br}(R)$. Let k_a denote an algebraic closure of k. Tsen's Theorem [Sh, p. 109] asserts that the Brauer group of the rational function field $k_a(x)$ is trivial. It follows that there is a finite extension F of K contained in $k_a(x)$ such that F splits ξ. It is easy to see that we have $F \subseteq \ell(x)$ for some finite extension ℓ of k contained in k_a. As we are assuming that k is perfect we may assume that ℓ/k is Galois.

Let $S = \ell[x]$. By the previous paragraph ξ vanishes in the composition

$$\mathbf{Br}(R) \to \mathbf{Br}(S) \to \mathbf{Br}(\ell(x)).$$

Since S is a Dedekind domain, Theorem 4.21 implies that the second arrow is monic. Therefore ξ belongs to the relative Brauer group $\mathbf{Br}(S/R)$. Since S/R is a Galois extension of commutative rings induced by the extension ℓ/k, Theorem 4.9 implies that we have a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(\ell/k, \ell^\times) & \longrightarrow & \mathbf{H}^2(S/R, S^\times) \\ \downarrow{\scriptstyle \mathbf{\Phi}_k^\ell} & & \downarrow{\scriptstyle \mathbf{\Phi}_R^S} \\ \mathbf{Br}(\ell/k) & \longrightarrow & \mathbf{Br}(S/R) \end{array}$$

As ℓ is a field and S is a principal ideal domain, the vertical arrows are isomorphisms by the Crossed Product Theorem. Since the units of S are just the units of ℓ, the upper horizontal arrow is also an isomorphism. Therefore the lower horizontal arrow must be an isomorphism as well. Hence ξ belongs to the image of $\mathbf{Br}(\ell/k) \to \mathbf{Br}(R/S)$. □

In general, the extension of a Dedekind domain associated to some finite Galois extension of its field of fractions will not be a Galois extension of commutative rings. The only obstruction however, is the ramification of primes. In the local case we will demonstrate this in Theorem 4.25. Before we get to that theorem, we need a few definitions and a theorem that collects a few basic facts about ramification which will also be useful in the next chapter. To fix ideas, let R be a Dedekind domain, K its field of fractions, L

a finite separable extension of K, and S the integral closure of R in L. It is well-known [Se1, Propositions 8 & 9, p. 13] that S is a Dedekind domain and an R-lattice in L. Thus S is a finitely generated projective R-submodule of L. Also $L = K \cdot S$, which implies that L is the field of fractions of S. Let P be a prime of R, and Q a prime of S. Recall that Q is said to *lie over* P if $Q \cap R = P$. By [Se1, Proposition 10, p. 14], there are only finitely many primes of Q that lie over a given prime of R. Moreover, if $Q_1, \ldots, Q_n$ are the primes of S that lie over P, then by [Se1, Proposition 7, p. 12], the extended ideal $P \cdot S$ has a unique factorization into a product of powers of the primes Q_i, $i = 1, \ldots, n$. That is, there are uniquely determined positive integers $e_1, \ldots, e_n$ such that

$$P \cdot S = Q_1^{e_1} \cdots Q_n^{e_n}.$$

The integer e_i is called the *ramification index of Q_i in L/K*. We say that Q_i is *unramified in L/K* if $e_i = 1$ and the associated extension of residue fields $(S/Q_i)/(R/P)$ is separable. Otherwise we say that Q_i *ramifies in L/K*. We say that P is unramified in S/R if each every prime of S that lies over P is unramified in S/R.

The ramification of primes in S/R is governed by the a certain ideal of S, called the *different of S/R*, and denoted $\mathfrak{D}(S/R)$. The different of S/R is defined to be the inverse of the codifferent of S/R, a fractional ideal of S, which we define below. Recall that a fractional ideal of S is by definition just an S-lattice in L. If I is a fractional ideal of S then the inverse of I, denoted I^{-1} is by definition the set of all $x \in L$ such that $x \cdot I \leq S$. To define the codifferent, let $S^* = \mathrm{Hom}_R(S, R)$ denote the R-module of all R-linear mappings from S to R. Then S^* is naturally identified with the analogously formed K-vector space $L^* = \mathrm{Hom}_K(L, K)$. For each $x \in L$, define

$$T_x \colon L \to K \qquad T_x(y) = \mathbf{Tr}_K^L(xy)$$

The K-linearity of the trace implies that T_x belongs to L^* for each $x \in L$. Let $\mathfrak{C}$ denote the set of all $x \in L$ such that $T_x \in S^*$. Then $\mathfrak{C}$ is a fractional ideal of S, and $S \leq \mathfrak{C}$. It follows that the inverse $\mathfrak{C}^{-1}$ is an ideal of S, and we define this ideal to be the different of S/R. For justifications of the claims in this paragraph, see [Se1, pp. 2–15, 50,51].

Theorem 4.24. *Let R be a Dedekind domain, K its field of fractions, L a finite separable extension of K, and S the integral closure of R in L.*

(a) *The only primes of S that ramify in L/K are the divisors of the different $\mathfrak{D}(S/R)$.*

(b) *If F is an extension of K contained in L, and T is the integral closure of R in F, then $\mathfrak{D}(S/R) = \mathfrak{D}(S/T) \cdot \mathfrak{D}(T/R)$.*

(c) *Assume $L = K(\alpha)$ where α is a root of a monic irreducible polynomial $f(x) \in R[x]$. Then $\mathfrak{D}(S/R)$ divides the principal ideal generated by $f'(\alpha)$, with equality if and only if $S = R[\alpha]$.*

Proof. See [Se1, Proposition 8, Theorem 1 & Corollary 2, pp. 51,53,56]. □

Now assume that the extension L/K is Galois. If $x \in L$ is integral over R then so is $\sigma(x)$ for each $\sigma \in \mathrm{Gal}(L/K)$. Hence the action of $\mathrm{Gal}(L/K)$ preserves S. Since $L = K \cdot S$ and $R = K \cap S$ we see moreover that $\mathrm{Gal}(L/K)$ acts faithfully on S and that R is the fixed ring of $\mathrm{Gal}(L/K)$ in S. For each prime P of R, the action of $\mathrm{Gal}(L/K)$ permutes the primes of S that lie over P among themselves. Although we do not use it here, it is interesting to note that this action is transitive [Se1, Proposition 19, p. 21]. If Q is a prime of S then the *decomposition subgroup of Q in L/K*, denoted $\mathbf{D}_Q(L/K)$, is by definition the stabilizer of Q in $\mathrm{Gal}(L/K)$.

Theorem 4.25. *Let R be a discrete valuation ring, K its field of fractions, L is a finite Galois extension of K, and S the integral closure of R in L. If S/R is unramified then it is a Galois extension of commutative rings and the crossed product homomorphism $\mathbf{\Phi}_R^S \colon \mathbf{H}^2(S/R, S^\times) \to \mathbf{Br}(S/R)$ is an isomorphism.*

Proof. We have already observed that $\mathrm{Gal}(L/K)$ acts faithfully on S and that R is the fixed ring of $\mathrm{Gal}(L/K)$ in S. Let F be a field and assume that there exists a homomorphism $\varphi \colon S \to F$. Let $\sigma \in \mathrm{Gal}(L/K)$ be such that $\varphi \circ \sigma = \varphi$. If φ is monic, then σ must be the identity since $\mathrm{Gal}(L/K)$ acts faithfully on S. Otherwise since S is a Dedekind domain, the kernel of φ is a prime Q of S, and we may assume that F is the residue field S/Q. Let P denote the unique prime of R. Since $\varphi \circ \sigma = \varphi$, we see that σ belongs to $\mathbf{D}_Q(L/K)$ the decomposition subgroup of Q in L/K. However as S/R is unramified, it is well-known [Se1, Proposition 20, p. 21] that the induced action of $\mathbf{D}_Q(L/K)$ on S/Q defines an isomorphism $\mathbf{D}_Q(L/K) \to \mathrm{Gal}((S/Q)/(R/P))$. Therefore as σ acts as the identity on the quotient S/Q, it must act as the identity on S as well. This shows that S/R is Galois.

Since each prime of S lies over P, and $\mathrm{Gal}(L/K)$ acts transitively on the primes of S that lie over P, it follows that S has at most $[L : K]$ primes. An application of the Weak Approximation Theorem [Se1, pp. 12–13] shows that a Dedekind domain with only

finitely many primes is a principal ideal domain. Thus every finitely generated projective S-module is free and therefore the crossed product homomorphism $\mathbf{\Phi}_R^S$ is an isomorphism by Theorem 4.13. □

We close this section with two theorems relating the Brauer group of a field to that of its completion with respect to a discrete valuation. Assume as above that L/K is a finite Galois extension. Let v be a discrete valuation of K, and w an extension of v to a discrete valuation of L. Let K_v and L_w denote the respective completions. There is a unique embedding of K_v in to L_w that is compatible with the respective inclusion of K in L, and the canonical embeddings $K \to K_v$ and $L \to L_w$. We will regard K_v as a subfield of L_w by means of that embedding. Then L_w is the compositum of L and K_v taken inside of L_w. It follows that the natural homomorphism $\mathbf{Br}(K) \to \mathbf{Br}(K_v)$ maps the relative Brauer group $\mathbf{Br}(L/K)$ to $\mathbf{Br}(L_w/K_v)$. Let R denote the valuation ring of v in K, and S the integral closure of R in L. The set Q_w consisting of all $s \in S$ such that $w(s) > 0$ is a maximal ideal of S, called the *ideal of w in S*. We define the decomposition group of w in L/K, denoted $\mathbf{D}_w(L/K)$, to be the decomposition subgroup Q_w of $\mathrm{Gal}(L/K)$.

Theorem 4.26. *Let L/K be a finite Galois extension of fields, v a discrete valuation of K, w an extension of v to a discrete valuation of L, and $\xi \in \mathbf{H}^2(L/K, L^\times)$. If ξ has trivial restriction to $\mathbf{D}_w(L/K)$ then the class $\mathbf{\Phi}_K^L(\xi) \in \mathbf{Br}(L/K)$ is split by K_v.*

Proof. By [Se1, Corollary 4, p. 31], restriction of automorphisms from L_w to L defines an isomorphism from the relative Galois group of the completions $\mathrm{Gal}(L_w/K_v)$ to the decomposition group $\mathbf{D}_w(L/K)$. Since L_w is the compositum of L and K_v, this implies by elementary Galois theory [La1, Theorem 1.12, p. 266] that the intersection of L and K_v is equal to the fixed field of $\mathbf{D}_w(L/K)$ in L. Thus by applying Theorems 4.8 and 4.10, we obtain a commutative diagram

$$\begin{array}{ccccc}
\mathbf{H}^2(L/K, L^\times) & \longrightarrow & \mathbf{H}^2(\mathbf{D}_w(L/K), L^\times) & \longrightarrow & \mathbf{H}^2(L_w/K_v, L_w^\times) \\
\downarrow{\scriptstyle \mathbf{\Phi}_K^L} & & \downarrow{\scriptstyle \mathbf{\Phi}_{K_v\cap L}^L} & & \downarrow{\scriptstyle \mathbf{\Phi}_{K_v}^{L_w}} \\
\mathbf{Br}(L/K) & \longrightarrow & \mathbf{Br}(L/(K_v \cap L)) & \longrightarrow & \mathbf{Br}(L_w/K_v)
\end{array}$$

Assuming that ξ has trivial restriction to $\mathbf{D}_w(L/K)$, commutativity of the diagram requires that $\mathbf{\Phi}_K^L(\xi)$ must belong to the kernel of $\mathbf{Br}(L/K) \to \mathbf{Br}(L_w/K_v)$. Thus K_v splits ξ which proves the theorem. □

The last theorem of the section allows us to determine if a class in $\mathbf{Br}(K)$ comes from $\mathbf{Br}(R)$ by passing to the completion. Although never explicitly formulated as below, Theorem 4.27 can be found within the proof of [Sa2, Theorem 10.3, pp. 68–69]. For the convenience of the reader we give a proof below.

Theorem 4.27. *Let K be a field, v a discrete valuation of K, and R the ring of v. Let K_v and R_v denote the completions of K and R with respect to v. Fix $\xi \in \mathbf{Br}(K)$ and let ξ_v denote the image of ξ in $\mathbf{Br}(K_v)$. Then ξ belongs to the image of $\mathbf{Br}(R) \to \mathbf{Br}(K)$ if and only if ξ_v belongs to the image of $\mathbf{Br}(R_v) \to \mathbf{Br}(K_v)$.*

Proof. If ξ belongs to the image of $\mathbf{Br}(R)$ then ξ_v must belong to the image of $\mathbf{Br}(R_v)$ by functoriality. For the converse, suppose that ξ is the class of the central simple K-algebra $\mathfrak{A}$, and let A be a maximal R-order in $\mathfrak{A}$. Let $A_v = A \otimes_R R_v$, and $\mathfrak{A}_v = \mathfrak{A} \otimes_K K_v$. Then ξ_v is the class of $\mathfrak{A}_v$ and [Sa2, Lemma 9.3, p. 62] implies that A_v is a maximal R_v-order in $\mathfrak{A}_v$. Now assume that $\xi_v \in \mathbf{Br}(R_v)$. Then A_v is an Azumaya R_v-algebra by part (a) of Theorem 4.21. As the completion R_v is a faithfully flat extension of R, see [Bo3, Proposition 9, p. 206], the fact that A_v is an Azumaya R_v-algebra implies that A is an Azumaya R-algebra by [Sa2, Theorem 2.2, p. 12]. Since $\mathfrak{A} = A \otimes_R K$, it follows that ξ coincides with the image of $[A]$. □

Chapter 5

The Main Chapter

5.1 Statement of the Main Theorems

Main Theorem 1. *Let p be an odd prime, n a natural number, and k a field that contains a primitive p^{n+1}-th root of unity. Then every extension of $\mathcal{C}_{p^n} \wr \mathcal{C}_{p^n}$ by $\mathcal{C}_p$ is regular over k.*

Main Theorem 2. *Let p be an odd prime and k a field that contains a primitive p^3-th root of unity. Then every group of order p^5 is regular over k.*

The next section contains the necessary cohomological preparations for the proof of the first main theorem, and Section 5.3 contains the proof itself. In Section 5.4 we prove the second main theorem by showing that every irreducible group of order p^5 is isomorphic to a quotient of some group known to be realized over k by the first main theorem. This makes one interested in knowing if irreducible groups of order p^5 actually exist, and we close Section 5.4 with an example to show that they do.

5.2 Cohomology of the Wreath Product

Let p be an odd prime, n a positive integer, and $q = p^n$. In this section we compute $\mathbf{H}^2(\Gamma, U)$ where Γ is the wreath product $\mathcal{C}_q \wr \mathcal{C}_q$ of two copies of the cyclic group of order q, and U is the cyclic group of order p with necessarily trivial Γ-module structure. To facilitate this computation, we will use the factorization of Γ in to the semidirect product $\Sigma \ltimes T$ defined below. It will be convenient to have J denote the set of congruence classes modulo q. Let $\Sigma = \langle \sigma \rangle$ be a cyclic group of order q. For each $j \in J$, let $T_j = \langle \tau_j \rangle$ be cyclic

of order q. Let $T = \prod_{j\in J} T_J$ be the direct product. We give T the structure of a right Σ-module by setting

$$\tau_j^\sigma = \tau_{j-1} \qquad \text{for all } j \in J$$

where subscripts are interpreted modulo q. Then Γ is isomorphic to the semidirect product $\Sigma \ltimes T$, and henceforth we will regard the two groups as being equal.

We begin with the first in a series of theorems giving a direct sum decomposition for the second cohomology group $\mathbf{H}^2(\Gamma, U)$. We note that Theorem 5.1 can be derived from the Hochschild-Serre spectral sequence, but we choose to offer a direct proof.

Theorem 5.1. *The homomorphism defined by the restrictions*

$$\mathbf{H}^2(\Gamma, U) \to \mathbf{H}^2(\Sigma, U) \oplus \mathbf{H}^2(T, U)^\Sigma \qquad \xi \mapsto (\mathbf{Res}^\Gamma_\Sigma(\xi), \mathbf{Res}^\Gamma_T(\xi))$$

is an isomorphism.

Proof. Because Γ is a split extension of Σ by T, and Γ acts trivially on U, it follows that the composition $\mathbf{Res}^\Gamma_\Sigma \circ \mathbf{Inf}^\Sigma_\Gamma$ is the identity on $\mathbf{H}^2(\Sigma, U)$. In Section 3.1, we showed that the composition $\mathbf{Res}^\Gamma_T \circ \mathbf{Inf}^\Sigma_\Gamma$ is zero. Hence, we have a complex

$$0 \to \mathbf{H}^2(\Sigma, U) \xrightarrow{\mathbf{Inf}} \mathbf{H}^2(\Gamma, U) \xrightarrow{\mathbf{Res}} \mathbf{H}^2(T, U)^\Sigma \to 0$$

which is exact at $\mathbf{H}^2(\Sigma, U)$. Therefore to prove the theorem, it is enough to show exactness at $\mathbf{H}^2(\Gamma, U)$ and $\mathbf{H}^2(T, U)^\Sigma$. For exactness at $\mathbf{H}^2(\Gamma, U)$ it is enough to prove that the kernels of $\mathbf{Res}^\Gamma_\Sigma$ and $\mathbf{Res}^\Gamma_T$ intersect trivially. Indeed, assume $\mathbf{Res}^\Gamma_T(\xi) = 0$ and let $\xi_\Sigma = \mathbf{Inf}^\Sigma_\Gamma(\mathbf{Res}^\Gamma_\Sigma(\xi))$. Then $\xi - \xi_\Sigma$ belongs to the kernels of $\mathbf{Res}^\Gamma_T$ and $\mathbf{Res}^\Gamma_\Sigma$. If they intersect trivially then $\xi = \xi_\Sigma$ and hence ξ belongs to the image of $\mathbf{Inf}^\Sigma_\Gamma$. Thus the theorem follows from 5.2 and 5.3 below. □

Before we get to Theorems 5.2 and 5.3, it will be convenient to fix some notation. Let G be a group, A a G-module, and (E, π) an extension of G by A. For each subgroup $H \leq G$, we let $E_H = \pi^{-1}(H)$ the preimage of H under π. We define the *restriction of* (E, π) *to* H, denoted $(E, \pi)_H$, to be the pair $(E_H, \pi|_{E_H})$. By construction, the restriction $(E, \pi)_H$ is an extension of H by A. Theorem 3.17 implies that, if $\xi \in \mathbf{H}^2(G, A)$ is the class determined by (E, π) then $\mathbf{Res}^G_H(\xi) \in \mathbf{H}^2(H, A)$ is the class determined by the restriction $(E, \pi)_H$.

Theorem 5.2. *Let (E,π) be a central extension of Γ by U. If $(E,\pi)_\Sigma$ and $(E,\pi)_T$ are both trivial then so is (E,π)*

Proof. Assume the restrictions $(E,\pi)_\Sigma$ and $(E,\pi)_T$ are both trivial. Theorem 3.16 implies that there are homomorphisms $\alpha\colon \Sigma \to E$ and $\beta\colon T \to E$ such that $\pi\circ\alpha = \mathbf{1}_\Sigma$ and $\pi\circ\beta = \mathbf{1}_T$. It follows that E_T is an abelian normal subgroup of E, and that E is a split extension of Σ by E_T. Let $\beta_1\colon T_1 \to E_T$ be the restriction of β. Since T is induced by T_1, it follows by Lemma 2.2 that there exists a homomorphism $\gamma\colon \Gamma \to E$ that extends α and β_1, and is such that the restriction $\gamma|_T\colon T \to E_T$ is a homomorphism of Σ-modules. Because γ extends α and β_1, we see that

$$\pi(\gamma(\sigma)) = \pi(\alpha(\sigma)) = \sigma \qquad \pi(\gamma(\tau_1)) = \pi(\beta_1(\tau_1)) = \tau_1$$

And since $\Gamma = \langle\sigma,\tau_1\rangle$, this implies that $\pi\circ\gamma = \mathbf{1}_\Gamma$. Hence (E,π) is trivial by Theorem 3.16. □

In order to prove exactness at $\mathbf{H}^2(T,U)^\Sigma$, we need to describe the action of Σ on $\mathbf{H}^2(T,U)$ in terms of extensions. Let (F,ρ) be an extension of T by U, and define ${}^\sigma\rho\colon F \to T$ by $({}^\sigma\rho)(x) = \sigma\rho(x)\sigma^{-1}$. The pair $(F,{}^\sigma\rho)$ is again an extension of T by U. Our claim is that, if $\xi \in \mathbf{H}^2(T,U)$ is the class determined by (F,ρ) then $\sigma_*(\xi)$ is the class determined by $(F,{}^\sigma\rho)$. To see this, define $\theta\colon T \to T$ by $\theta(t) = t^\sigma$. Since Σ acts trivially on U, we see that

$$\sigma_*(\xi) = \theta^*(\xi) \qquad \text{for all } \xi \in \mathbf{H}^2(T,U).$$

Let (G,ρ_*,θ_*) be the pullback of ρ and θ. By Theorem 3.17, the class $\sigma_*(\xi)$ corresponds to the equivalence class the extension (G,ρ_*) of T by U. In this situation we have a commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U & \longrightarrow & G & \xrightarrow{\rho_*} & T & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle\theta_*} & & \| & & \\
1 & \longrightarrow & U & \longrightarrow & F & \xrightarrow{{}^\sigma\rho} & T & \longrightarrow & 1
\end{array}$$

Therefore θ_* is an equivalence from (F,ρ_*) to $(F,{}^\sigma\rho)$. This proves the claim.

Theorem 5.3. *The following conditions on an extension (F,ρ) of T by U are equivalent.*

(a) *The action of Σ on T lifts to an action of Σ by automorphisms of F.*

(b) *The extension (F,ρ) is of the form $(E,\pi)_T$ for some extension (E,π) of Γ by U.*

(c) *The extensions* (F, ρ) *and* $(F, {}^{\sigma}\rho)$ *are equivalent extensions of* T *by* U*.*

We will have several occasions to use the next lemma.

Lemma 5.4. *If* G *is a finite cyclic group and* A *is an induced* Σ*-module then* $A^G = \mathbf{Nm}_G(A)$*.*

Proof. Assume that A is induced. Then Shapiro's Lemma implies that the second cohomology group $\mathbf{H}^2(G, A)$ is trivial. With the description of the cohomology of a cyclic group given in Theorem 3.8, this implies that $A^G = \mathbf{Nm}_G(A)$. □

Proof of Theorem 5.3. Assume that the action of Σ on T lifts to F. Let $E = \Sigma \ltimes F$ the semidirect product of Σ and F with respect to the lifted action. By Lemma 2.2, there exists a homomorphism $\pi\colon E \to \Gamma$ that extends the identity on Σ and ρ on F. It is easy to check that (F, ρ) is the restriction of (E, π) to T. Therefore (a) implies (b). Since Σ acts trivially on $\mathbf{H}^2(\Gamma, U)$ and Theorem 3.6 implies that conjugation commutes with restriction, we see also that (b) implies (c). Hence it is enough to show that (c) implies (a).

Let $\varphi\colon F \to F$ be an equivalence from (F, ρ) to $(F, {}^{\sigma}\rho)$. Then φ is an automorphism of F that restricts to the identity on U and $\rho(x) = ({}^{\sigma}\rho)(\varphi(x))$ for all $x \in F$. It follows that

$$\rho(x)^{\sigma^i} = \rho(\varphi^i(x)) \qquad \text{for all } x \in F,\ i \in \mathbb{Z}.$$

In particular φ^q induces the identity on T. If φ^q is the trivial automorphism of F then setting $x^{\sigma^i} = \varphi^i(x)$ gives a suitable lift of the action of Σ to F. Otherwise, the idea is to modify φ so that it remains an equivalence from (F, ρ) to $(F, {}^{\sigma}\rho)$, but has order q as an automorphism of F.

Define $f\colon F \to F$ by $f(x) = \varphi^q(x) \cdot x^{-1}$. Then it is easy to see that f is a homomorphism and that $\mathbf{img}(f) \leq U \leq \mathbf{ker}(f)$. Thus by passage to the quotient f defines a homomorphism $\tilde{f}\colon T \to U$. We claim that $\tilde{f}$ is fixed by the action of Σ on $\mathrm{Hom}(T, U)$. This is equivalent to showing that $f(x) = f(\varphi(x))$ for all $x \in E$. Since φ is the identity on the image of f, it is enough to show that φ and f are commuting endomorphisms of F.

But this follows easily from the definition of f. Namely for each $x \in F$, we have

$$\begin{aligned}\varphi(f(x)) &= \varphi(\varphi^q(x) \cdot x^{-1}) \\ &= \varphi^{q+1}(x) \cdot \varphi(x^{-1}) \\ &= \varphi^q(\varphi(x)) \cdot \varphi(x)^{-1} \\ &= f(\varphi(x))\end{aligned}$$

which proves the claim.

Now we apply Lemma 5.4 to the induced Σ-module $\mathrm{Hom}(T, U)$ and the Σ-fixed element $\tilde{f}$. The lemma implies that there exists a homomorphism $b\colon E \to U$ such that $\mathbf{ker}(b) \leq U$ and $\mathbf{Nm}_\Sigma(\tilde{b}) = \tilde{f}$. Define $\lambda\colon F \to F$ by $\lambda(x) = \varphi(x) \cdot b(x)^{-1}$. Then it is easy to check that λ is also an automorphism of F and since $\mathbf{img}(b) \leq \mathbf{ker}(\rho)$, we even have

$$\rho(x)^{\sigma^i} = \rho(\lambda^i(x)) \qquad \text{for all } x \in F,\ i \in \mathbb{Z}.$$

Moreover since $\mathbf{img}(b) \leq U \leq \mathbf{ker}(b)$ and φ is the identity on U, it follows that

$$\lambda^i(x) = \varphi^i(x) \cdot b(x \cdot \varphi(x) \cdots \varphi^{i-1}(x))^{-1} \qquad \text{for all } x \in F,\ i \in \mathbb{Z}.$$

As $\tilde{f} = \mathbf{Nm}_\Sigma(\tilde{b})$, we have

$$f(x) = b(x \cdot \varphi(x) \cdots \varphi^{q-1}(x)) \qquad \text{for all } x \in F.$$

Consequently λ^q is the identity on F. Thus setting $x^{\sigma^i} = \lambda^i(x)$ provides the required action of Σ on F. Therefore (c) implies (a). □

Since Σ is cyclic, we have a complete description of $\mathbf{H}^2(\Sigma, U)$ given by Theorem 3.8. So we turn our attention to the other summand $\mathbf{H}^2(T, U)^\Sigma$. In computing in $\mathbf{H}^2(T, U)$ it will often be convenient to regard U as an additive module. We note that, because U is cyclic of odd order, the rule $u \mapsto 2u$ is an automorphism of U. Hence for each $u \in U$, the expression $u/2$ is well-defined and the rule $u \mapsto u/2$ is again an automorphism of U.

In terms of 2-cocycles the action of Σ on $\mathbf{H}^2(T, U)$ is defined by the rule $\sigma[f] = [{}^\sigma f]$ where

$$({}^\sigma f)(t_1, t_2) = f(t_1^\sigma, t_2^\sigma) \qquad \text{for all } f \in \mathrm{Z}^2(T, U),\ t_1, t_2 \in T.$$

Let $\mathrm{Bil}(T, U)$ denote the space of bilinear forms of T with values in U. Then $\mathrm{Bil}(T, U)$ is

a Σ-module in the same way as $\mathrm{Z}^2(T,U)$ above. Let $\mathrm{Sym}(T,U)$ and $\mathrm{Alt}(T,U)$ denote the subspaces of $\mathrm{Bil}(T,U)$ consisting of all symmetric and alternating forms. Then $\mathrm{Sym}(T,U)$ and $\mathrm{Alt}(T,U)$ are both Σ-submodules of $\mathrm{Bil}(T,U)$ which is their direct sum.

A trivial computation shows that every $f \in \mathrm{Bil}(T,U)$ is a normalized 2-cocycle of T in U. It follows that $\mathrm{Bil}(T,U)$ is a Σ-submodule of $\mathrm{Z}^2(T,U)$. We claim that $\mathrm{B}^2(T,U) \cap \mathrm{Bil}(T,U) \leq \mathrm{Sym}(T,U)$. We will prove the stronger statement that every $f \in \mathrm{B}^2(T,U)$ is symmetric. Assume f is a 2-coboundary. By definition this means that there exists $b\colon T \to U$ such that $f(t_1,t_2) = b(t_1) + t_1 \cdot b(t_2) - b(t_1t_2)$ for all $t_1, t_2 \in T$. Since T is abelian, and U has trivial T-action, we see that

$$f(t_1,t_2) = b(t_1) + b(t_2) - b(t_1t_2) = b(t_2) + b(t_1) - b(t_2t_1) = f(t_2,t_1) \qquad \text{for all } t_1, t_2 \in T$$

which proves the claim.

The claim implies that $\mathrm{B}^2(T,U) \cap \mathrm{Alt}(T,U) = 0$. Thus the epimorphism $\mathrm{Z}^2(T,U) \to \mathbf{H}^2(T,U)$ defines by restriction a monomorphism of Σ-modules $\mathrm{Alt}(T,U) \to \mathbf{H}^2(T,U)$. We will identify $\mathrm{Alt}(T,U)$ with its image in $\mathbf{H}^2(T,U)$ thereby. The canonical projection

$$\mathrm{alt}\colon \mathrm{Bil}(T,U) \to \mathrm{Alt}(T,U) \qquad (\mathrm{alt}\, f)(t_1,t_2) = \tfrac{1}{2}(f(t_1,t_2) - f(t_2,t_1))$$

extends by the same rule to a Σ-linear endomorphism of $\mathrm{Z}^2(T,U)$ which is seen to vanish on 2-coboundaries. Hence the formula $\mathrm{alt}[f] = [\mathrm{alt}(f)]$ is well-defined and gives a Σ-linear operator on $\mathbf{H}^2(T,U)$. Let $\mathrm{Ext}(T,U)$ denote its kernel. We will show that $\mathbf{H}^2(T,U)$ is the direct sum of $\mathrm{Alt}(T,U)$ and $\mathrm{Ext}(T,U)$ and that $\mathrm{Ext}(T,U)$ represents the classes abelian extensions of T by U.

Theorem 5.5. *The operator* alt *defines a Σ-linear projection of $\mathbf{H}^2(T,U)$ onto* $\mathrm{Alt}(T,U)$*; we have*

$$\mathbf{H}^2(T,U) = \mathrm{Alt}(T,U) \oplus \mathrm{Ext}(T,U)$$

Let (F,ρ) be a central extension of T by U, and $\xi \in \mathbf{H}^2(T,U)$ the class it determines. Then ξ belongs to $\mathrm{Ext}(T,U)$ *if and only if F is abelian.*

Proof. Let f be a normalized 2-cocycle of T in U. That $\mathrm{alt}(f)$ is bilinear can be established by a direct computation or by connecting alt with the so called *commutator pairing* [Br, Exercise 8, p. 97]. Since $\mathrm{alt}(f)$ is bilinear and $(\mathrm{alt}(f))(t,t) = 0$ for all $t \in T$ it is easy to see that $\mathrm{alt}(f)$ is alternating. On $\mathrm{Alt}(T,U)$ the newly defined alt equals the usual alt and

thus we have $\mathrm{alt}[f] = [f]$ for each $[f] \in \mathrm{Alt}(T, U)$. Therefore alt is a projection of $\mathbf{H}^2(T, U)$ onto $\mathrm{Alt}(T, U)$. This proves the first half of the theorem.

Let $e\colon T \to F$ be a normalized section of ρ and f the associated factor set. Thus if ξ belongs to $\mathrm{Ext}(T, U)$ then $\mathrm{alt}(f)$ is a 2-coboundary. Since $\mathrm{B}^2(T, U) \cap \mathrm{Alt}(T, U) = 0$, we must have $\mathrm{alt}(f) = 0$. Therefore f belongs to $\mathrm{Sym}(T, U)$, and this implies that $e(t_1) \cdot e(t_2) = e(t_2) \cdot e(t_1)$ for all $t_1, t_2 \in T$. Since E is generated by $e(T)$ and its central subgroup U, this implies that E is abelian. Conversely, assuming that E is abelian, a reversal of the argument just given shows that ξ belongs to $\mathrm{Ext}(T, U)$. □

By the previous theorem, in order to understand $\mathbf{H}^2(T, U)$, it is enough to understand $\mathrm{Alt}(T, U)$ and $\mathrm{Ext}(T, U)$ individually. We start with the $\mathrm{Ext}(T, U)$. For each $j \in J$, let $I_j\colon \mathbf{H}^2(T_j, U) \to \mathbf{H}^2(T, U)$ denote the inflation homomorphism corresponding to the projection $T \to T_j$. Also, let Δ be the smallest Σ-submodule of T such that Σ acts trivially on the quotient T/Δ. Then it is easy to see that Δ is normal in Γ and that T/Δ is cyclic of order q.

Theorem 5.6. *The inflation homomorphisms define an isomorphism*

$$\oplus_J \mathbf{H}^2(T_j, U) \to \mathrm{Ext}(T, U) \qquad (\xi_j) \mapsto \sum_J I_j(\xi_j)$$

The inflation homomorphism

$$\mathbf{Inf}_T^{T/\Delta}\colon \mathbf{H}^2(T/\Delta, U) \to \mathbf{H}^2(T, U)$$

is monic and its image equals $\mathrm{Ext}(T, U)^{\Sigma}$.

Lemma 5.7. *Let (E, π) and (F, ρ) be central extensions of T by U. For each $j \in J$, assume there exists an equivalence φ_j from $(E, \pi)_{T_j}$ to $(F, \rho)_{T_j}$. If E and F are both abelian then there exists an equivalence φ from (E, π) to (F, ρ) that extends φ_j for each $j \in J$.*

Proof. Assume E and F are both abelian. Let $(E_j, \pi_j) = (E, \pi)_{T_j}$ and $(F_j, \rho_j) = (F, \rho)_{T_j}$. Then each $x \in E$ has a factorization into a product $\prod_J x_j$ with $x_j \in E_j$. By considering the the image of x under the compositions $E \to T \to T_j$, we see that any other factorization of x must be of the form $\prod_J x_j u_j$ for some $u_j \in U$. As E is abelian and $\prod_J x_j = \prod_J x_j u_j$, we must have $\prod_J u_j = 1$.

Then as we have $\varphi_j(u) = u$ for all $u \in U$ and $j \in J$, it follows that $\prod_J \varphi_j(x_j) = \prod_J \varphi_j(x_j u_j)$. Thus the product $\prod_J \varphi_j(x_j)$ does not depend on the factorization of x and

therefore the formula $\varphi(x) = \prod_J \varphi_j(x_j)$ is well-defined for each $x \in E$. Now it is easy to check that φ is an equivalence from (E, π) to (F, ρ) and that φ extends φ_j for all $j \in J$. $\square$

Proof of Theorem 5.6. Let I denote the sum of the inflations. Thus we have

$$I(\xi_j) = \sum_J I_j(\xi_j) \qquad \text{for all } (\xi_j) \in \oplus_J \mathbf{H}^2(T_j, U).$$

To show that the image of I is contained in $\mathrm{Ext}(T, U)$, it is enough to show the same of I_j for each $j \in J$. As we will see, this follows from the observation that, because T_j is cyclic, every central extension of T_j by U is abelian. Indeed, assume $\xi_j \in \mathbf{H}^2(T_j, U)$ is the class determined by the central extension (E_j, π_j) of T_j by U. By Theorem 3.17, the inflation $I_j(\xi_j)$ corresponds to the equivalence class of the extension (E, π) where E is the fiber product of $\pi_j \colon E_j \to T_j$ and the projection $T \to T_j$. Now, as E_j and T are both abelian, and E is a subgroup of their direct product, E is also abelian. Now Theorem 5.5 implies that $I_j(\xi_j)$ belongs to $\mathrm{Ext}(T, U)$.

For each $j \in j$, let $R_j \colon \mathbf{H}^2(T, U) \to \mathbf{H}^2(T_j, U)$ be the restriction from T to T_j and define

$$R \colon \mathrm{Ext}(T, U) \to \oplus_J \mathbf{H}^2(T_j, U) \qquad R(\xi) = (R_j(\xi))$$

Since I_j is defined by the projection $T \to T_j$, and R_j by the inclusion $T_j \leq T$, functoriality requires that the composition $R_j \circ I_j$ be the identity on $\mathbf{H}^2(T_j, U)$. Similarly if $i \neq j$ then $R_i \circ I_j$ is trivial. Now it is easy to see that the composition

$$R \circ I \colon \ \oplus_J \mathbf{H}^2(T_j, U) \to \oplus_J \mathbf{H}^2(T_j, U)$$

is the identity. This shows that I is monic and that R is epic. As the lemma implies that R is monic, it follows that I is an isomorphism.

By Theorem 3.8, for each $j \in J$, we have an isomorphism $\mathbf{H}^2(T_j, U) \to U$. Thus $\mathrm{Ext}(T, U)$ is an elementary abelian group of rank q. As the conjugation action of Σ freely permutes the factors T_j, $j \in J$ of T, it follows that $\mathrm{Ext}(T, U)$ is a free $\mathbb{F}_p[\Sigma]$-module of rank one. By Lemma 5.4, this implies that the subgroup of Σ-fixed elements $\mathrm{Ext}(T, U)$ is the image of the norm $\mathbf{Nm}_\Sigma$. As $\mathrm{Ext}(T, U)$ has rank one over Σ, we see that $\mathrm{Ext}(T, U)^\Sigma$ is cyclic of order p. For the second half of the theorem, as the canonical epimorphism $T \to T/\Delta$ is split, arguing as above shows that the inflation $\mathbf{Inf}_T^{T/\Delta}$ is monic. Moreover as Σ acts trivially on the quotient T/Δ, and conjugation commutes with inflation, it follows

that the image of $\mathbf{Inf}_T^{T/\Delta}$ is fixed by Σ. Thus by comparing orders, we see that the image of $\mathbf{Inf}_T^{T/\Delta}$ equals $\mathbf{H}^2(T,U)^\Sigma$. $\square$

It remains only to consider $\mathrm{Alt}(T,U)$. For this we need to fix some notation. For each right Σ-module A, let $\wedge^2 A$ denote the second exterior product of A given the structure of a right Σ-module by the action

$$(a_1 \wedge a_2)^\sigma = a_1^\sigma \wedge a_2^\sigma \qquad \text{for all } a_1, a_2 \in A$$

and let A^* denote $\mathrm{Hom}(A, \mathbb{F}_p)$ as a left Σ-module under the usual action

$$({}^\sigma f)(a) = f(a^\sigma) \qquad \text{for all } a \in A,\ f \in A^*.$$

And we define $\wedge^2 A$ and A^* similarly for left Σ-modules.

By the universality of the exterior product, an alternating form of T in $\mathbb{F}_p$ defines a unique homomorphism $\wedge^2 T \to \mathbb{F}_p$. And consequently, we obtain an isomorphism $\mathrm{Alt}(T, \mathbb{F}_p) \to (\wedge^2 T)^*$ which is even an isomorphism of left Σ-modules for the above defined action of Σ on $(\wedge^2 T)^*$. Furthermore, it is easy to see that the pairing

$$\wedge^2(T^*) \times \wedge^2 T \to \mathbb{F}_p \qquad \langle f_1 \wedge f_2, t_1 \wedge t_2 \rangle = \tfrac{1}{2}(f_1(t_1) \cdot f_2(t_2) - f_1(t_2) \cdot f_2(t_1))$$

is well-defined, nonsingular, and satisfies

$$\langle {}^\sigma f_1 \wedge {}^\sigma f_2, t_1 \wedge t_2 \rangle = \langle f_1 \wedge f_2, t_1^\sigma \wedge t_2^\sigma \rangle \qquad \text{for all } f_1, f_2 \in T^*,\ t_1, t_2 \in T.$$

Hence the pairing $\langle *, * \rangle$ defines an isomorphism of Σ-modules

$$\wedge^2(T^*) \to \mathrm{Alt}(T, \mathbb{F}_p) \qquad f_1 \wedge f_2 \mapsto \langle f_1 \wedge f_2, * \rangle$$

Let $\{b_j\}_{j \in J}$ be the basis for T^* which is dual to the basis $\{\tau_j\}_{j \in J}$ for T. For each pair $i, j \in J$, we identify $b_i \wedge b_j \in \wedge^2(T^*)$ with its image in $\mathrm{Alt}(T, \mathbb{F}_p)$.

Theorem 5.8. *As an abelian group,* $\mathrm{Alt}(T, \mathbb{F}_p)$ *is elementary abelian of rank* $q(q-1)/2$ *with basis* $\{b_i \wedge b_j : i, j \in J, i < j\}$. *As a* Σ*-module,* $\mathrm{Alt}(T, \mathbb{F}_p)$ *is induced.*

Proof. Let $m = (q-1)/2$ and for each $k = 1, 2, \ldots, m$, let

$$A_k = \langle b_i \wedge b_j : \text{for all } i, j \in J \text{ such that } q \mid i - j + k. \rangle$$

Then each A_k is elementary abelian of rank q and a Σ-submodule of $\mathrm{Alt}(T, \mathbb{F}_p)$. In fact for each fixed $i \in J$, the set $\{\sigma^j(b_i \wedge b_{i+k})\}_{j\in J}$ is a $\mathbb{F}_p$-basis for A_k. It follows that each A_k is a free $\mathbb{F}_p[\Sigma]$-module of rank 1. Moreover if $i \neq j$ then the product $b_i \wedge b_j$ is contained in exactly one of the A_k. By comparing ranks, we see that we must have a direct sum decomposition

$$\mathrm{Alt}(T, \mathbb{F}_p) = \oplus_{k=1}^{m} A_k.$$

For each $j = 2, \ldots, m+1$, the product $b_1 \wedge b_j$ belongs to exactly one of the subgroups $A_1, \ldots, A_m$ and it generates that subgroup as a Σ-module. Now it follows that the subgroup

$$\langle b_1 \wedge b_j : \ j = 2, \ldots, m+1 \rangle$$

induces $\mathrm{Alt}(T, \mathbb{F}_p)$. □

5.3 Proof of the First Main Theorem

We retain the notation of the previous section. Thus p is an odd prime, n is a natural number, $q = p^n$, and J is the set of residue classes modulo q. We represent the wreath product Γ of two copies of $\mathcal{C}_q$, as the semidirect product $\Sigma \ltimes T$, where $\Sigma = \langle \sigma \rangle$ is cyclic of order q, and $T = \prod_{j\in J} T_j$ is the direct product of the groups $T_j = \langle \tau \rangle$ each cyclic of order q. The action of Σ on T is given by

$$\tau_j^{\sigma^i} = \tau_{j-i} \qquad \text{for all } i, j \in J.$$

where subscripts are interpreted modulo q. We denote by U the cyclic group of order p, endowed with trivial Γ-module structure.

Proof of Main Theorem 1. Let (E, π) be an extension of Γ by U. Thus U is a normal subgroup of E and we have a short exact sequence

$$1 \to U \to E \xrightarrow{\pi} \Gamma \to 1.$$

Since E is a p-group and U is normal subgroup of order p, it follows that $U \leq \mathbf{Z}(E)$. From here, to show that E is regular over k there are two essentially different cases to consider. First assume that $U \not\leq \mathbf{\Phi}(E)$. Then by Theorem 2.3 there exists a proper subgroup $G < E$ such that $E = GU$. Since G is a proper subgroup of E, it follows that $U \not\leq G$ and hence

that G and U intersect trivially. Now as $GU = E$ and $G \cap U = 1$, the epimorphism π must restrict to an isomorphism from G to Γ. It follows that $[E : G] = p$, and thus by Theorem 2.6 part (b), that G is normal in E. Therefore E is isomorphic to the direct product of $\Gamma \times U$. But by Theorems 2.15 and 2.14, we already know that $\Gamma \times U$ is regular over k.

Henceforth we will assume that $U \leq \mathbf{\Phi}(E)$. We will also assume that k is perfect. If k is of characteristic zero then this is automatic. Otherwise there exists a finite subfield ℓ of k that also contains the p^{n+1}-th roots of unity. Being finite, the field ℓ is perfect and by Theorem 2.13, if E is regular over ℓ then E is regular over k as well. Therefore, after replacing k by ℓ if necessary, we may assume that k is a perfect field.

Let $\zeta \in k$ be a primitive q-th root of unity, and x an indeterminate. Let $K = k(x)$ and let K_s denote a separable closure of K. Let $\alpha \in K_s$ be a q-th root of x. Then the extension $K(\alpha)/K$ is Galois and $\mathrm{Gal}(K(\alpha)/K)$ is cyclic of order q. We will identify Σ with $\mathrm{Gal}(K(\alpha)/K)$ by setting

$$\sigma^i(\alpha) = \alpha \cdot \zeta^i \qquad \text{for all } i \in \mathbb{Z}.$$

For each $j \in J$, we set $b_j = 1 - \alpha \cdot \zeta^j$ and we let B denote the subgroup of $K(\alpha)^\times$ generated by $\{b_j\}_{j \in J}$. Interpreting subscripts modulo q, we have

$$\sigma^i(b_j) = b_{i+j} \qquad \text{for all } i, j \in J.$$

Thus the action of Σ on $K(\alpha)^\times$ preserves B. We claim that B is a free $\mathbb{Z}[\Sigma]$-module of rank one and a direct factor of $K(\alpha)^\times$. To see this we consider the subring $k[\alpha]$ of $K(\alpha)$. Since α is a q-th root of x and $K = k(x)$, we have $K(\alpha) = k(\alpha)$. Thus $k[\alpha]$ is a unique factorization domain which has $K(\alpha)$ as its field of fractions. Now it is immediate that the elements b_j for $j \in J$ are all irreducible in $k[\alpha]$ and pairwise coprime. It follows that the subgroup they generate is a direct factor of the multiplicative group of $K(\alpha)$.

Let $L = K(\alpha)_B$ the q-th power Kummer extension of $K(\alpha)$ associated to B. Thus L is the extension of $K(\alpha)$ formed by adjoining every $\beta \in K_s$ such that $\beta^q \in B$. The extension $L/K(\alpha)$ is Galois and since B is a direct factor of $K(\alpha)^\times$ it follows that the Kummer pairing defines an isomorphism

$$\mathrm{Gal}(L/K(\alpha)) \to \mathrm{Hom}(B, \boldsymbol{\mu}(q)).$$

In particular $\mathrm{Gal}(L/K(\alpha))$ is an abelian group of rank q and exponent q. Moreover because

the action of Σ preserves B, we see by the work of Section 3.2, that L/K is Galois and the isomorphism above is an isomorphism of Σ-modules for the action by right conjugation on $\mathrm{Gal}(L/K(\alpha))$, and the action on $\mathrm{Hom}(B, \boldsymbol{\mu}(q))$ under which

$$(\chi^\sigma)(b) = \chi(\sigma(b)) \qquad \text{for all } b \in B,\ \chi \in \mathrm{Hom}(B, \boldsymbol{\mu}(q)).$$

From all of this we conclude that there exists a isomorphism of Σ-modules from T to $\mathrm{Gal}(L/K(\alpha))$ with respect to which $\{\tau_j\}_{j\in J}$ and $\{b_j\}_{j\in J}$ are dual bases for the Kummer pairing. To make this explicit, for each $j \in J$, we let β_j denote a fixed q-th root of b_j in L. Then L is the extension of $K(\alpha)$ gotten by adjoining β_j for all $j \in J$. The action of T on L satisfies

$$\tau_i(\beta_j) = \beta_j \cdot \zeta^{\delta(i,j)} \qquad \text{for all } i, j \in J.$$

Since T is an induced Σ-module, Shapiro's Lemma implies that the second cohomology group $\mathbf{H}^2(\Sigma, T)$ is trivial. Thus by Schreier's Theorem every extension of Σ by T is equivalent to the split extension. Consequently, there exists an isomorphism from Γ to $\mathrm{Gal}(L/K)$ that extends the identifications $\Sigma \to \mathrm{Gal}(K(\alpha))$ and $T \to \mathrm{Gal}(L/K(\alpha))$ made above. By means of that isomorphism, we will henceforth identify Γ with $\mathrm{Gal}(L/K)$.

We will also identify U with $\boldsymbol{\mu}(p)$ and we let $\epsilon\colon \boldsymbol{\mu}(p) \to L^\times$ be the inclusion. Since U is central in E and $\boldsymbol{\mu}(p)$ is contained in K, the homomorphism ϵ is automatically compatible with the two actions by Γ. Thus the quadruple $(L/K, E, \pi, \epsilon)$ forms a central embedding problem. Let $\epsilon_*\colon \mathbf{H}^2(L/K, \boldsymbol{\mu}(p)) \to \mathbf{H}^2(L/K, L^\times)$ be the homomorphism induced by ϵ and $\xi \in \mathbf{H}^2(L/K, \boldsymbol{\mu}(p))$ the class determined by the central extension

$$1 \to \boldsymbol{\mu}(p) \to E \xrightarrow{\pi} \mathrm{Gal}(L/K) \to 1.$$

The obstruction to $(L/K, E, \pi, \epsilon)$ is the 2-nd cohomology class $\epsilon_*(\xi) \in \mathbf{H}^2(L/K, L^\times)$. In order to apply Theorem 3.18, we need to show that this class is trivial. In doing so it will be convenient to identify $\epsilon_*(\xi)$ with its image $\xi_K \in \mathbf{Br}(L/K)$ under the crossed product isomorphism $\boldsymbol{\Phi}_K\colon \mathbf{H}^2(\Gamma, L^\times) \to \mathbf{Br}(L/K)$.

Let $R = k[x]$. Then R is a Dedekind domain with K as its field of fractions and the integral closure S of R in L is also a Dedekind domain. For each prime P of R, the local ring R_P is a discrete valuation ring with K as its field of fractions and we denote by $\boldsymbol{\Psi}_P\colon \mathbf{Br}(R_P) \to \mathbf{Br}(K)$ the natural homomorphism. We will show that ξ_K belongs to the image of $\boldsymbol{\Psi}_P$ for each prime P. We start with the unramified primes.

Claim 1. *If P is unramified in L/K then ξ_K belongs to the image of $\mathbf{\Psi}_P$.*

Proof. Assume P is unramified in L/K and let S_P denote the localization of S at the complement of P in R. Thus S_P is the subring of L consisting of all elements of the form s/r for some $s \in S$ and $r \in R \setminus P$. By the remark following [Se1, Proposition 4, p. 10], the localization S_P is the integral closure of R_P in L. Since P is unramified, Theorem 4.25 implies that S_P/R_P is a Γ-Galois extension of commutative rings and that the associated crossed product homomorphism

$$\mathbf{\Phi}_P \colon \mathbf{H}^2(\Gamma, S_P^\times) \to \mathbf{Br}(S_P/R_P).$$

is an isomorphism. From Theorem 4.9 and the inclusions $\boldsymbol{\mu}(p) \leq S_P^\times \leq L^\times$ we obtain a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(\Gamma, S_P^\times) & \xrightarrow{\mathbf{\Phi}_P} & \mathbf{Br}(S_P/R_P) \\ \downarrow & \nwarrow \quad \swarrow & \downarrow \mathbf{\Psi}_P \\ \mathbf{H}^2(\Gamma, L^\times) & \xrightarrow{\mathbf{\Phi}_K} & \mathbf{Br}(L/K) \end{array} \qquad \mathbf{H}^2(\Gamma, \boldsymbol{\mu}(p))$$

Let ξ_P denote the image of ξ in $\mathbf{H}^2(\Gamma, S_P^\times)$. By commutativity of the diagram above, we have $\mathbf{\Psi}_P(\mathbf{\Phi}_P(\xi_P)) = \mathbf{\Phi}_K(\xi_K)$. Since we are identifying ξ_K with its image under $\mathbf{\Phi}_K$, we see that that ξ_K belongs to the image of $\mathbf{\Psi}_P$. □

Claim 2. *The only primes of R that ramify in L/K are (x) and $(x-1)$.*

Proof. By part (a) of Theorem 4.24, it is enough to show that the only primes of S that divide the different $\mathfrak{D}(S/R)$ are those that lie over (x) or $(x-1)$. To see this, put $L_0 = K(\alpha)$, and for each $j = 1, 2, 3, \ldots, q$, let $L_j = L_{j-1}(\beta_j)$, and S_j the integral closure of R in L_j. Since we have $L = L_q$ and hence $S = S_q$, part (b) of the same theorem implies that the different of S/R is the product of the differents corresponding to each layer

$$\mathfrak{D}(S/R) = \mathfrak{D}(S_0/R) \cdot \mathfrak{D}(S_1/S_0) \cdot \mathfrak{D}(S_2/S_1) \cdots \mathfrak{D}(S_q/S_{q-1})$$

For each $j = 1, 2, 3, \ldots, q$, the minimal polynomial for β_j over L_{j-1} is $g_j(x) = x^q - b_j$. Hence

by part (c) of Theorem 4.24, for each $j = 1, 2, 3, \ldots, q$, the different $\mathfrak{D}(S_j/S_{j-1})$ divides $q \cdot \beta_j^{q-1}$. As $S_0 = R[\alpha]$, we see similarly that $\mathfrak{D}(S_0/R) = q \cdot \alpha^{q-1}$. Since q is invertible in R, it follows that the different of S/R divides the principal ideal of S generated by

$$(\alpha \cdot \beta_1 \cdot \beta_2 \cdot \beta_3 \cdots \beta_q)^{q-1}$$

Since $\mathbf{Nm}_K^L(\alpha)$ is a power of x, and $\mathbf{Nm}_K^L(\beta_j)$ a power of $1 - x$, this proves the claim. $\square$

Claim 3. *If $H \leq \Gamma$ is cyclic of order q then ξ_K has trivial restriction to H.*

Proof. Assume $H \leq \Gamma$ is cyclic of order q and let F denote the fixed field of H in L. Since restriction is a morphism of functors, we have a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(\Gamma, \boldsymbol{\mu}(p)) & \xrightarrow{\mathbf{Res}} & \mathbf{H}^2(H, \boldsymbol{\mu}(p)) \\ \downarrow{\scriptstyle \epsilon_*} & & \downarrow{\scriptstyle \epsilon_*} \\ \mathbf{H}^2(\Gamma, L^\times) & \xrightarrow{\mathbf{Res}} & \mathbf{H}^2(H, L^\times) \end{array}$$

Therefore to prove the claim, it is enough to show that the induced homomorphism $\epsilon_* \colon \mathbf{H}^2(H, \boldsymbol{\mu}(p)) \to \mathbf{H}^2(H, L^\times)$ is trivial. By fixing a generator for H, and applying Theorem 3.8, we obtain a representation of the induced homomorphism. Namely, we have a commutative diagram, in which the horizontal arrows are isomorphisms

$$\begin{array}{ccc} \mathbf{H}^2(H, \boldsymbol{\mu}(p)) & \xrightarrow{\varphi^2} & \boldsymbol{\mu}(p) \\ \downarrow{\scriptstyle \epsilon_*} & & \downarrow{\scriptstyle \epsilon} \\ \mathbf{H}^2(H, L^\times) & \xrightarrow{\varphi^2} & F^\times/\mathbf{Nm}_F^L(L^\times) \end{array}$$

Hence it is enough to show that $\boldsymbol{\mu}(p) \leq \mathbf{Nm}_F^L(L^\times)$. But when restricted to $F^\times$ the norm is just the q-th power map. As K is a subfield of F, and we are assuming that K contains the p^{n+1}-th roots of unity, it follows that each p-th root of unity is a norm from L to F. $\square$

Claim 4. *The Laurent series field $k(\!(x)\!)$ splits ξ_K.*

Proof. We identify the Laurent series field $k(\!(x)\!)$ with the completion K_v of K at v the normalized discrete valuation of K that has x as a uniformizing parameter. Since α is a q-th root of a uniformizer for v, the extension $K(\alpha)/K$ is totally ramified at v. Hence there

is a unique extension of v to a discrete valuation of $K(\alpha)$ and that extension has α as a uniformizing parameter. By abuse of notation, we will also denote this valuation by v. We will identify the Laurent series field $k(\!(\alpha)\!)$ with the extension $K_v(\alpha)$ and the completion $K(\alpha)_v$.

Let w be an extension of v to L, and L_w the corresponding completion. There is a unique continuous embedding $K_v \to L_w$, compatible with the inclusion of K in L and the canonical embeddings $K \to K_v$ and $L \to L_w$. Accordingly, we will regard K_v as a subfield of L_w. We claim that $K_v(\alpha) = L_w$. Since $L_w = LK_v$, it is enough to show that $\beta_j \in K_v(\alpha)$ for each $j \in J$. But by definition, the element β_j is a q-th root of $1 - \alpha \cdot \zeta^j$, and Hensel's Lemma shows that $1 - \alpha \cdot \zeta^j$ is a q-th power in the power series ring $k[\![\alpha]\!]$. Hence $K_v(\alpha) = L_w$ as claimed.

By [Se1, Proposition 22, p. 22] the canonical sequence restricts to a short exact sequence of decomposition subgroups

$$1 \to \mathbf{D}_w(L/K(\alpha)) \to \mathbf{D}_w(L/K) \to \mathbf{D}_v(K(\alpha)/K) \to 1.$$

Hence from the last two paragraphs, we see that the decomposition group of v in $K(\alpha)/K$ is equal to Σ and that the decomposition subgroup of w in $L/K(\alpha)$ is trivial. Since $\mathbf{D}_w(L/K(\alpha))$ is trivial, the canonical epimorphism $\Gamma \to \Sigma$ must restrict to an isomorphism from $\mathbf{D}_w(L/K)$ to Σ. In particular the decomposition group of w in L is cyclic of order q. Now Claim 3 implies that ξ_K has trivial restriction to $\mathbf{D}_w(L/K)$ and it follows by Theorem 4.26 that K_v splits ξ_K. □

Claim 5. *The obstruction ξ_K has trivial restriction to T.*

Proof. From the commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(\Gamma, \boldsymbol{\mu}(p)) & \xrightarrow{\mathbf{Res}} & \mathbf{H}^2(T, \boldsymbol{\mu}(p))^{\Sigma} \\ \downarrow{\scriptstyle \epsilon_*} & & \downarrow{\scriptstyle \epsilon_*} \\ \mathbf{H}^2(\Gamma, L^{\times}) & \xrightarrow{\mathbf{Res}} & \mathbf{H}^2(T, L^{\times})^{\Sigma} \end{array}$$

we see that the restriction of ξ_K to T belongs to the image of $\mathbf{H}^2(T, \boldsymbol{\mu}(p))^{\Sigma} \to \mathbf{H}^2(T, L^{\times})^{\Sigma}$ and so it is enough to show that this is the trivial homomorphism. By Theorem 5.5 the second cohomology group $\mathbf{H}^2(T, \boldsymbol{\mu}(p))$ is the direct sum of its Σ-submodules $\mathrm{Alt}(T, \boldsymbol{\mu}(p))$ and $\mathrm{Ext}(T, \boldsymbol{\mu}(p))$. Hence the subgroup of Σ-fixed elements in $\mathbf{H}^2(T, \boldsymbol{\mu}(p))$ also decomposes

into a direct sum

$$\mathbf{H}^2(T, \boldsymbol{\mu}(p))^{\Sigma} = \mathrm{Alt}(T, \boldsymbol{\mu}(p))^{\Sigma} \oplus \mathrm{Ext}(T, \boldsymbol{\mu}(p))^{\Sigma}$$

We will consider $\mathrm{Ext}(T, \boldsymbol{\mu}(p))^{\Sigma}$ first.

Let $\Delta \leq T$ be the subgroup defined in the last section. That is, Δ is the smallest normal subgroup of Γ contained in T, such that Σ acts trivially on the quotient T/Δ. By Theorem 5.6, the subgroup of Σ-fixed elements in $\mathrm{Ext}(T, \boldsymbol{\mu}(p))$ equals the image of the inflation homomorphism $\mathbf{Inf}\colon \mathbf{H}^2(T/\Delta, \boldsymbol{\mu}(p)) \to \mathbf{H}^2(T, \boldsymbol{\mu}(p))$. Let F denote the fixed field of Δ in L. As T/Δ is cyclic of order q, an argument almost identical to that given in the proof of Claim 3 shows that the homomorphism

$$\epsilon_*\colon \mathbf{H}^2(T/\Delta, \boldsymbol{\mu}(p)) \to \mathbf{H}^2(T/\Delta, F^{\times})$$

is trivial. Since we have a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(T/\Delta, \boldsymbol{\mu}(p)) & \xrightarrow{\mathbf{Inf}} & \mathbf{H}^2(T, \boldsymbol{\mu}(p)) \\ \big\downarrow{\scriptstyle \epsilon_*} & & \big\downarrow{\scriptstyle \epsilon_*} \\ \mathbf{H}^2(T/\Delta, F^{\times}) & \xrightarrow{\mathbf{Inf}} & \mathbf{H}^2(T, L^{\times}) \end{array}$$

this implies that the image of $\mathrm{Ext}(T, \boldsymbol{\mu}(p))^{\Sigma} \to \mathbf{H}^2(T, L^{\times})$ is also trivial.

Now we turn our attention to the image of $\mathrm{Alt}(T, \boldsymbol{\mu}(p))^{\Sigma}$. Define

$$\Omega\colon \mathrm{Alt}(T, \boldsymbol{\mu}(p)) \to \mathbf{Br}(L/K(\alpha)) \qquad \Omega(f) = [L/K(\alpha), f]$$

Note that $\Omega = \boldsymbol{\Psi}_{K(\alpha)} \circ \epsilon_*$ and thus that Ω is a homomorphism of Σ-modules. In order to understand the image of Ω, we will apply the description of $\mathrm{Alt}(T, \boldsymbol{\mu}(p))$ implied by Theorem 5.8. But before we can do so we need to fix an identification between $\mathbb{F}_p$ and $\boldsymbol{\mu}(p)$. We equate the generator $1 \in \mathbb{F}_p$ with the primitive p-th root of unity $\zeta^{p^{n-1}}$. Under the p-th power Kummer pairing, the set $\{b_j\}_{j \in J}$ is a basis for $\mathrm{Hom}(T, \mathbb{F}_p)$ which is dual to the basis $\{\tau_j\}_{j \in J}$ for T. That is, we have $b_j(\tau_i) = \delta(i, j)$ for all $i, j \in J$. Thus the 2-cocycle of T in $\mathbb{F}_p$ determined by the product $b_i \wedge b_j$ satisfies

$$(b_i \wedge b_j)(t_1, t_2) = \frac{b_i(t_1) \cdot b_j(t_2) - b_i(t_2) \cdot b_j(t_1)}{2} \qquad \text{for all } t_1, t_2 \in T.$$

Theorem 5.8 implies that the corresponding 2-cocycles of T in $\boldsymbol{\mu}(p)$ generate $\mathrm{Alt}(T, \boldsymbol{\mu}(p))$. Let $T_{ij} = T_i T_j$ and $L_{ij} = K(\alpha, \beta_i, \beta_j)$. As a 2-cocycle, $b_i \wedge b_j$ depends only on the i-th and j-th components of its arguments, and so we see that $b_i \wedge b_j$ belongs to the image of the inflation homomorphism

$$\mathbf{Inf}_T^{T_{ij}} : \mathbf{H}^2(T_{ij}, \boldsymbol{\mu}(p)) \to \mathbf{H}^2(T, \boldsymbol{\mu}(p))$$

The projection of T onto T_{ij} coincides with the canonical epimorphism from $\mathrm{Gal}(L/K(\alpha))$ to $\mathrm{Gal}(L_{ij}/K(\alpha))$, thus it follows by Theorem 4.11 that

$$\Omega(b_i \wedge b_j) = [L_{ij}/K(\alpha), b_i \wedge b_j] \qquad \text{for all } i, j \in J$$

For each pair of units $c_1, c_2 \in K(\alpha)$, let $[c_1, c_2]$ denote the Brauer equivalence class of the norm residue algebra $(c_1, c_2; K(\alpha), \zeta^{p^{n-1}})$. Then by comparing the 2-cocycle determined by $b_i \wedge b_j$ with the construction given in Theorem 4.19, we conclude that

$$\Omega(b_i \wedge b_j) = [b_i, b_j] \qquad \text{for all } i, j \in J.$$

To proceed, we combine Lemma 5.4 with Theorem 5.8. Since Σ is cyclic, and $\mathrm{Alt}(T, \boldsymbol{\mu}(p))$ is an induced Σ-module, the image of Ω on $\mathrm{Alt}(T, \boldsymbol{\mu}(p))^{\Sigma}$ is the subgroup generated by the image of $\mathbf{Nm}_{\Sigma}$ acting on the symbols $[b_i, b_j]$ for all $i, j \in J$, $i < j$. Thus to finish the proof of the claim, it is enough to show that $\mathbf{Nm}_{\Sigma}[b_i, b_j]$ is trivial for each pair $i, j \in J$, $i < j$. Recall that we defined $b_j = 1 - \alpha \cdot \zeta^j$ for each $j \in J$ and consequently that $\sigma^i(b_j) = b_{i+j}$ for all $i, j \in J$. Applying Lemma 4.18 we have

$$\begin{aligned}
[b_i, b_j] &= [b_i/b_j, b_i - b_j] \\
&= [b_i/b_j, \alpha(\zeta^j - \zeta^i)] \\
&= [b_i, \alpha] - [b_j, \alpha] + [b_i/b_j, \zeta^j - \zeta^i]
\end{aligned}$$

Since ζ is a p-th power in $K(\alpha)$, we have $[b_j, \zeta^j] = 0$ for all $j \in J$. With Lemma 4.18, this

implies that

$$\begin{aligned}[b_j, \alpha] &= [b_j, \alpha] + [b_j, \zeta^j] \\ &= [b_j, \alpha \cdot \zeta^j] \\ &= [1 - \alpha \cdot \zeta^j, \alpha \cdot \zeta^j] \\ &= 0\end{aligned}$$

By combining the last two equations, we have

$$[b_i, b_j] = \left[b_i/b_j, \zeta^j - \zeta^i\right] \qquad \text{for all } i, j \in J,\ i < j.$$

By Theorem 4.17, the action of Σ on norm residue symbols in $\mathbf{Br}(K(\alpha))$ is given by the formula

$$\sigma_*[c_1, c_2] = [\sigma(c_1), \sigma(c_2)] \qquad \text{for all } c_1, c_2 \in L^\times.$$

Therefore since the second argument of $[b_i/b_j, \zeta^j - \zeta^i]$ is fixed by Σ, it follows that

$$\mathbf{Nm}_\Sigma[b_i, b_j] = [\mathbf{Nm}_\Sigma(b_i/b_j), \zeta^j - \zeta^i] \qquad \text{for all } i, j \in J,\ i < j.$$

As the norm $\mathbf{Nm}_\Sigma(b_i/b_j)$ is equal to 1, this completes the proof of the claim. □

Claim 6. *The Laurent series field $k(\!(x-1)\!)$ splits ξ_K.*

Proof. An easy application of Hensel's Lemma shows that x is a q-th power in the power series ring $k[\![x-1]\!]$. Hence there exists an embedding of $K(\alpha)$ into the Laurent series field $k(\!(x-1)\!)$ that extends the canonical embedding $K \to k(\!(x-1)\!)$. Thus to prove the claim, it is enough to show that $K(\alpha)$ splits ξ_K. Since $K(\alpha)$ is the fixed field of T in L, by Theorem 4.10, we have a commutative diagram

$$\begin{array}{ccc} \mathbf{H}^2(\Gamma, L^\times) & \xrightarrow{\mathbf{Res}} & \mathbf{H}^2(T, L^\times) \\ \Big\downarrow{\scriptstyle \mathbf{\Phi}_K^L} & & \Big\downarrow{\scriptstyle \mathbf{\Phi}_{K(\alpha)}^L} \\ \mathbf{Br}(L/K) & \longrightarrow & \mathbf{Br}(L/K(\alpha)) \end{array}$$

As we have already shown that ξ_K has trivial restriction to T, this proves the claim. □

We are finally ready to show that the obstruction ξ_K is trivial. Taken together

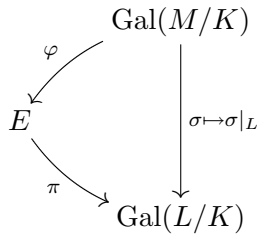
Claims 1 and 2 imply that the ξ_K belongs to the image of $\mathbf{\Psi}_P$ for every prime P of R with the possible exceptions of (x) and $(x-1)$. However by Claim 4, the obstruction is split by the Laurent series field $k(\!(x)\!)$. In particular, the image of ξ_K in the Brauer group of $k(\!(x)\!)$ belongs to the image of the natural homomorphism $\mathbf{Br}(k[\![x]\!]) \to \mathbf{Br}(k(\!(x)\!))$. By Theorem 4.27 this implies that ξ_K belongs to the image of $\mathbf{\Psi}_{(x)}$. Similarly from Claim 6 we see that the obstruction belongs to the image of $\mathbf{\Psi}_{(x-1)}$.

Thus the obstruction belongs to the image of $\mathbf{\Psi}_P$ for every prime P of R. By Theorem 4.22 it must also belong to the image of $\mathbf{\Psi}_R \colon \mathbf{Br}(R) \to \mathbf{Br}(K)$. Since $R = k[x]$ and because we are assuming that k is perfect, Theorem 4.23 implies that the image of $\mathbf{\Psi}_R$ is precisely image of $\mathbf{\Psi}_k \colon \mathbf{Br}(k) \to \mathbf{Br}(K)$. Since we have shown that the Laurent series field $k(\!(x)\!)$ splits ξ_K, we see that ξ_K is the image of some class in $\mathbf{Br}(k)$ that vanishes in the composition

$$\mathbf{Br}(k) \to \mathbf{Br}(k[\![x]\!]) \to \mathbf{Br}(k(\!(x)\!)).$$

But the inclusion $k \to k[\![x]\!]$ is split by the projection $k[\![x]\!] \to k$ and therefore the first arrow is monic. As the power series ring $k[\![x]\!]$ is a discrete valuation ring that has $k(\!(x)\!)$ as its field of fractions, the second arrow is monic by Theorem 4.21. Therefore ξ_K is trivial.

By Theorem 3.18, the vanishing of ξ_K implies the existence of a solution to the central embedding problem $(L/K, E, \pi, \epsilon)$. Thus there exists a Galois extension M/K that has L/K as a subextension, and an isomorphism $\varphi \colon \mathrm{Gal}(M/K) \to E$ that makes the following diagram commute



It remains only to show that M is a regular extension of k.

Let $F = K(x^{1/p}, (1-x)^{1/p})$ the extension of K in K_s gotten by adjoining p-th roots of x and $1-x$. Since β_1 is a q-th root of $1 - \alpha \cdot \zeta$, it is easy to see that $\mathbf{Nm}_\Sigma(\beta_1)$ is a q-th root of $1-x$ in L. Therefore as L contains q-th roots of x and $1-x$, it must also contain the field F. Since F/K is Galois and $\mathrm{Gal}(F/K)$ is elementary abelian, we see by Theorem 2.6, that F is contained in the fixed field of $\mathbf{\Phi}(\Gamma)$ in L. In fact, since $\mathrm{Gal}(F/K)$ and Γ are both of rank two, F is the fixed field of $\mathbf{\Phi}(\Gamma)$ in L. Because we are assuming that

$U \leq \mathbf{\Phi}(E)$, Theorem 2.4 implies that the $\pi\colon E \to \Gamma$ maps $\mathbf{\Phi}(E)$ onto $\mathbf{\Phi}(\Gamma)$. Thus after identifying E with $\mathrm{Gal}(M/K)$ by means of φ, we see that F is also the fixed field of $\mathbf{\Phi}(E)$ in M. Since x and $1-x$ remain irreducible in the polynomial ring $k_a[x]$, we see that the translated extension $Fk_a/k_a(x)$ is also elementary abelian of rank two. By Theorem 2.12 this implies that F/k is regular. Since the fixed field of $\mathbf{\Phi}(E)$ in M is a regular extension of k, so is M by Theorem 3.19. □

5.4 Proof of the Second Main Theorem

We retain the notation of Section 5.2, but we specialize to the case of $n = 2$. Thus Γ denotes the wreath product of two copies of the cyclic group of order p^2.

Proof of Main Theorem 2. Let G be a group of order p^5. First assume that G is reducible to a group of smaller order. Then by Lemma 2.20, there exists a group H of order dividing p^4 such that G reduces to H. By Theorem 2.10, unless H is trivial, it has an abelian normal subgroup of index p. In either case H reduces to the trivial group. But then by transitivity, G also reduces to the trivial group. Therefore Theorem 2.18 implies that G is regular over k.

Now assume that G is irreducible. By Theorem 2.10 G possesses an abelian normal subgroup of order p^3. By Theorem 2.19, since G is irreducible, every such subgroup must be contained in $\mathbf{\Phi}(G)$. Hence the order of $\mathbf{\Phi}(G)$ is at least p^3. If the order of $\mathbf{\Phi}(G)$ is any greater then the Burnside Basis Theorem would imply that G is cyclic, which is impossible. Thus $\mathbf{\Phi}(G)$ has order p^3 and therefore G has rank two. Incidentally, we have shown that $\mathbf{\Phi}(G)$ is the unique maximal abelian normal subgroup of G.

We claim that the nilpotence class of G is at least three. Equivalently, we claim that third commutator subgroup $\mathbf{K}_3(G)$ is nontrivial. Assume for a contradiction that the nilpotence class of G is less that three. Then the second commutator subgroup $\mathbf{K}_2(G)$ is contained in the center of G. To derive a contradiction, fix $\gamma \in G$ such that $\gamma \notin \mathbf{\Phi}(G)$ and let $A = \langle \gamma, \mathbf{K}_2(G) \rangle$. As A contains $\mathbf{K}_2(G)$ and the quotient $G/\mathbf{K}_2(G)$ is abelian, it follows that A is normal in G. As $\mathbf{K}_2(G)$ is central in A and $A/\mathbf{K}_2(G)$ is cyclic, it follows also that A is abelian. Therefore A is an abelian normal subgroup of G that is not contained in $\mathbf{\Phi}(G)$. But we have already shown that $\mathbf{\Phi}(G)$ contains every abelian normal subgroup of G.

Since $\mathbf{K}_3(G)$ is a nontrivial normal subgroup of G, there exists a subgroup $U \leq$

$\mathbf{K}_3(G)$ such that U is cyclic of order p and normal in G. Let $H = G/U$. We claim that H also has rank two and that its exponent divides p^2. Since $U \leq \mathbf{K}_3(G)$ we have $U \leq \mathbf{\Phi}(G)$ and therefore $\mathbf{\Phi}(H) = \mathbf{\Phi}(G)/U$. Thus the quotients $G/\mathbf{\Phi}(G)$ and $H/\mathbf{\Phi}(H)$ are isomorphic. This shows that H has rank two. If the exponent of H is greater that p^2 then there exists $\eta \in H$ of order p^3. Then $\langle \eta \rangle$ is a cyclic subgroup of index p in H. Hence $\langle \eta \rangle$ is normal in H and the quotient $H/\langle \eta \rangle$ is also cyclic. Therefore H is metacyclic. From $U \leq \mathbf{K}_3(G)$ we have $\mathbf{K}_3(H) = \mathbf{K}_3(G)/U$ and so the quotients $G/\mathbf{K}_3(G)$ and $H/\mathbf{K}_3(H)$ are isomorphic. Thus Theorem 2.8 implies that G is also metacyclic. But this is impossible as we are assuming that G is irreducible.

We claim that there exists an epimorphism $\rho\colon \Gamma \to H$. To see this, let N be maximal among the abelian normal subgroups of H. Since H is a nonabelian group of order p^4 Theorem 2.10 implies that N has order p^3. Thus the quotient H/N is cyclic of order p and therefore $\mathbf{\Phi}(H) \leq N$ by part (d) of Theorem 2.6. It follows immediately that $N/\mathbf{\Phi}(H)$ is also cyclic of order p. Hence there exist elements $s \in H$ and $t \in N$ whose images generate the quotients H/N and $N/\mathbf{\Phi}(H)$. From Theorem 2.3, we see that $H = \langle s, t \rangle$.

Since the exponent of H divides p^2, there exist homomorphisms

$$\alpha\colon \Sigma \to H \qquad\qquad \alpha(\sigma) = s$$
$$\beta_1\colon T_1 \to N \qquad\qquad \beta_1(\tau_1) = t$$

Being an abelian normal subgroup, N is a right H-module under the conjugation action, and thus a right Σ-module through α. Now as T is induced by T_1, the homomorphism $\beta_1\colon T_1 \to N$, has a unique extension to a homomorphism of Σ-modules $\beta\colon T \to N$. And by Lemma 2.2 there is a homomorphism $\rho\colon \Gamma \to H$ that extends α and β. Since $s, t \in \mathbf{img}(\rho)$ and $H = \langle s, t \rangle$, we see that ρ is epic.

Let $\pi\colon G \to H$ be the canonical epimorphism and let (E, π_*, ρ_*) be the pullback of π and ρ. Since π and ρ are both epic, so are π_* and ρ_* by Lemma 2.1, and we have a commutative diagram with short exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U & \longrightarrow & E & \xrightarrow{\pi_*} & \Gamma & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle \rho_*} & & \downarrow{\scriptstyle \rho} & & \\
1 & \longrightarrow & U & \longrightarrow & G & \xrightarrow{\pi} & H & \longrightarrow & 1
\end{array}$$

Therefore E is an extension of Γ by U. Since we are assuming that k contains the p^3-th

roots of unity, the first main theorem implies that E is regular over k. As G is isomorphic to a quotient of E, Theorem 2.14 implies that G is also regular over k. $\square$

In the proof of the theorem it was shown that for every $n < 5$, there are no irreducible groups of order p^n. In fact, Dentzer has observed [De] that the are no irreducible groups of order 32. We close this section with an example to show that there exist irreducible groups of order p^5 for all $p > 3$. That this holds for $p = 3$ as well, can be verified with GAP [1].

Example. *Let p a prime number and E the group generated by two elements subject to the relations imposed by the conditions that E have exponent p and nilpotence class 3. If $p > 3$ then E is an irreducible group of order p^5.*

In proving that E has the properties claimed, we will use the following. Assume $E = \langle x, y\rangle$ is nilpotent of class 3. Then

$$\mathbf{K}_2(E) = \langle [y, x], \mathbf{K}_3(E)\rangle \qquad \mathbf{K}_3(E) = \langle [y, x, x], [y, x, y]\rangle$$

This follows from various well-known commutator identities. See [Hu, III, §1, pp. 252–259] for details.

Proof. Write $E = \langle s, t\rangle$. Then we have

$$\mathbf{K}_2(E) = \langle [t, s]\mathbf{K}_3(E)\rangle \qquad \mathbf{K}_3(E) = \langle [t, s, s], [t, s, t]\rangle$$

Let

$$t_1 = t \qquad t_2 = [t, s] \qquad t_3 = [t, s, s] \qquad u = [t, s, t]$$

As $E/\mathbf{K}_2(E)$ is elementary abelian of rank 2, it follows that every element of E has an expression of the form

$$s^i \cdot t_1^{j_1} \cdot t_2^{j_2} \cdot t_3^{j_3} \cdot u^k \qquad \text{for some } i, j_1, j_2, j_3, k = 0, 1, 2, \ldots, p-1.$$

In particular, the order of E is at most p^5. To prove that the order is no less, we need to show that there are no nonobvious relations among s, t_1, t_2, t_3, u. We take it for granted that $E/\mathbf{K}_3(E)$ is of order p^3, and that the elements $t_3, u \in \mathbf{K}_3(E)$ are both nontrivial. We are thus reduced to showing that $\mathbf{K}_3(E)$ is of rank 2. To see this, let G denote the

semidirect product $S \ltimes T$ of the cyclic group $S = \langle \sigma \rangle$ of order p, and the elementary abelian p-group $T = \langle \tau_1, \tau_2, \tau_3 \rangle$ with the right S-action defined by setting

$$\tau_1^\sigma = \tau_1\tau_2 \qquad \tau_2^\sigma = \tau_2\tau_3 \qquad \tau_3^\sigma = \tau_3$$

We leave it for the reader to check that the action specified is well-defined. We note that G has order p^4 and class 3. Direct computation shows that, because $p > 3$, the group G has exponent p. The rules $s \mapsto \sigma$ and $t_1 \mapsto \tau_1$ define an epimorphism $\pi\colon E \to G$. The fact that $\pi(u) = 1$ implies that t_3 and u are independent generators for $\mathbf{K}_3(E)$. Hence E has order p^5 as claimed.

We will show that E is irreducible by applying the criterion of Theorem 2.19. Thus if $A \trianglelefteq E$ is maximal among the abelian normal subgroups of E then we must show that $A \leq \mathbf{\Phi}(E)$. The maximality of A requires that $\mathbf{Z}(E) \leq A$. And because E has class 3, this implies that A contains $\mathbf{K}_3(E)$. Now assume for a contradiction that $A \not\leq \mathbf{\Phi}(E)$, and fix an element $x \in A$ that does not belong to $\mathbf{\Phi}(E)$. Since E has rank 2, there exists $y \in E$ such that $E = \langle x, y \rangle$ and hence

$$\mathbf{K}_2(E) = \langle [x, y], \mathbf{K}_3(E) \rangle \qquad \mathbf{K}_3(E) = \langle [x, y, x], [x, y, y] \rangle$$

As we are assuming that A is normal, the first equation implies that $\mathbf{K}_2(E) \leq A$. And since $\mathbf{K}_3(E)$ is elementary abelian of rank 2, the second implies that $[x, y, x] \neq 1$. Since x and $[x, y]$ both belong to A, this contradicts the assumption that A is abelian. □

Bibliography

[Bo1] N. Bourbaki. *Algebra I*. Springer-Verlag, Berlin, 1990.

[Bo2] N. Bourbaki. *Algebra II*. Springer-Verlag, Berlin, 1990.

[Bo3] N. Bourbaki. *Commutative Algebra*. Hermann, Paris, 1972.

[Br] K. S. Brown. *Cohomology of Groups*. Graduate Texts in Mathematics 87. Springer-Verlag, New York, 1982.

[DI] F. DeMeyer & E. Ingraham. *Separable Algebras Over Commutative Rings*. Lecture Notes in Mathematics 181. Springer-Verlag, Berlin, 1971.

[De] R. Dentzer. On Geometric Embedding Problems and Semiabelian Groups. *Manuscripta Mathematica* **86** (1995) 199–216.

[Dr] P. K. Draxl. *Skew Fields*. London Mathematical Society Lecture Note Series 81. Cambridge University Press, 1983.

[1] The GAP Group. *GAP–Groups, Algorithms, and Programming, Version 4.4.10*. `http://www.gap-system.org/` (2007).

[Hu] B. Huppert. *Endliche Gruppen I*. Die Grundlehren der Mathematischen Wissenschaften Band 134, Springer-Verlag, Berlin, 1967.

[JLY] C. U. Jensen, A. Ledet & N. Yui. *Generic Polynomials*. Cambridge (2002).

[KO] M.-A. Knus & M. Ojanguren. *Théorie de la descente et algèbres d'Azumaya*. Lecture Notes in Mathematics 389. Springer-Verlag, Berlin, 1974.

[La1] S. Lang. *Algebra*. Graduate Texts in Mathematics 211. Springer-Verlag, New York, 2002.

[La2] S. Lang. *Topics in Cohomology of Groups*. Lecture Notes in Mathematics 1625. Springer-Verlag, Berlin, 1996.

[Sa1] D. J. Saltman. Generic Galois Extensions and Problems in Field Theory. Advances in Mathematics **43(3)** (1982) 250–283.

[Sa2] D. J. Saltman. *Lectures on Division Algebras*. CBMS Regional Conference Series in Mathematics 94. American Mathematical Society, Providence, 1999.

[Sc] L. Schneps. On Reduction of p-Groups. *Communications in Algebra* **21(5)** (1993) 1603–1609.

[Se1] J.-P. Serre. *Local Fields*. Graduate Texts in Mathematics 67. Springer-Verlag, New York, 1995.

[Se2] J.-P. Serre. *Topics in Galois Theory*. Jones and Bartlett, Boston, 1992.

[Sh] S. Shatz. *Profinite Groups, Arithmetic, and Geometry*. Annals of Mathematics Studies 67. Princeton University Press, Princeton, 1972.

Vita

John Hammond was born in Dallas, Texas on August 15, 1977, the son of William and Deborah Hammond. After completing his work at Woodrow Wilson High School in Dallas, Texas, in 1996, he entered the University of Texas at Austin. He received the degree of Bachelors of Science from the University of Texas in August of 2001. Later that month, he entered the Graduate School at the same university to pursue a Ph.D. in Mathematics.

Permanent Address: 109 S Cuernavaca Dr
Austin TX 78733

This dissertation was typeset with LaTeX 2_ε[1] by the author.

[1] LaTeX 2_ε is an extension of LaTeX. LaTeX is a collection of macros for TeX. TeX is a trademark of the American Mathematical Society. The macros used in formatting this dissertation were written by Dinesh Das, Department of Computer Sciences, The University of Texas at Austin, and extended by Bert Kay, James A. Bednar, and Ayman El-Khashab.