1-1-2008

Writing representations over proper division subrings

Stephen P. Glasby

Writing representations over proper division subrings

Dedicated to Prof. Cheryl Praeger on the occasion of her 60th birthday

S. P. GLASBY

Abstract. Let $\mathbb{E}$ be a division ring, and G a finite group of automorphisms of $\mathbb{E}$ whose elements are distinct modulo inner automorphisms of $\mathbb{E}$. Let $\mathbb{F} = \mathbb{E}^G$ be the division subring of elements of $\mathbb{E}$ fixed by G. Given a representation $\rho\colon \mathfrak{A} \to \mathbb{E}^{d\times d}$ of an $\mathbb{F}$-algebra $\mathfrak{A}$, we give necessary and sufficient conditions for ρ to be *writable* over $\mathbb{F}$. (Here $\mathbb{E}^{d\times d}$ denotes the algebra of $d\times d$ matrices over $\mathbb{E}$, and a matrix A writes ρ over $\mathbb{F}$ if $A^{-1}\rho(\mathfrak{A})A \subseteq \mathbb{F}^{d\times d}$.) We give an algorithm for constructing an A, or proving that no A exists. The case of particular interest to us is when $\mathbb{E}$ is a field, and ρ is absolutely irreducible. The algorithm relies on an explicit formula for A, and a generalization of Hilbert's Theorem 90 that arises in galois cohomology. The algorithm has applications to the construction of absolutely irreducible group representations (especially for solvable groups), and to the recognition of class $\mathcal{C}_5$ in Aschbacher's matrix group classification scheme [1, 13].

Keywords: Hilbert's Theorem 90, division subrings

2000 Mathematics subject classification: 20C40, 20C10

Part I: The general case

1. Introduction

Throughout this paper $\mathbb{E}$ denotes a division ring, G a finite group of automorphisms of $\mathbb{E}$ whose elements are distinct modulo inner automorphisms of $\mathbb{E}$, and $\mathbb{F} = \mathbb{E}^G$ is the division subring fixed elementwise by G. It follows from [21, §2] that $\mathbb{E} : \mathbb{F}$ is a galois extension with group G. In Part II of this paper, we shall specialize to the case when $\mathbb{E} : \mathbb{F}$ is a finite galois extension of *fields*. Denote by $\mathbb{E}^{d\times d}$ the algebra of $d \times d$ matrices over $\mathbb{E}$, and by $\mathrm{GL}_d(\mathbb{E})$ its group of units. We say that a representation $\rho\colon \mathfrak{A} \to \mathbb{E}^{d\times d}$ of an $\mathbb{F}$-algebra $\mathfrak{A}$ *can be written over* $\mathbb{F}$ if there exists an $A \in \mathrm{GL}_d(\mathbb{E})$ such that

$$A^{-1}\rho(x)A \in \mathbb{F}^{d\times d} \qquad \text{for all } x \in \mathfrak{A}.$$

Date: Submitted: 20 November 2003;Resubmitted: 17 May, 2007.

The purpose of this paper is threefold: (1) to describe the connection between galois cohomology and the problem of writing ρ over $\mathbb{F}$, (2) to describe properties of a map Π_C used to construct A, and (3) to give an algorithm that takes as input an absolutely irreducible ρ and either constructs an A, or proves that no such A exists.

Section 2 describes briefly how A gives rise to a certain function $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ called a 1-cocycle. The more interesting problem of how C gives rise to A is discussed in Section 3. The heart of this problem involves a generalization of Hilbert's Theorem 90: namely, there exists a matrix $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C(\alpha) = A\alpha(A)^{-1}$ for $\alpha \in G$, where $\alpha(A)$ denotes the $d \times d$ matrix obtained by applying α to the entries of A. Equivalently, using the language of galois cohomology, it says that $H^1(G, \mathrm{GL}_d(\mathbb{E})) = \{I\}$. This result was proved by Serre [19] when $\mathbb{E}$ is a field, and by Nuss [14] when $\mathbb{E}$ is a division ring. Neither the proof by Serre nor Nuss is constructive: both proofs require modification in order to suggest an algorithm. We shall give a completely elementary proof in Theorem 3 of these results which suggests both a deterministic and a probabilistic algorithm for constructing A. Although some of our results can be rephrased in terms of galois cohomology [19], and descent theory for noncommutative rings [14], we prefer to state our results with minimal background in terms of matrices over $\mathbb{E}$ and automorphisms.

In Sections 3 and 4 we study properties of a certain endomorphism $\Pi_C\colon \mathbb{E}^{d\times d} \to \mathbb{E}^{d\times d}$ that depends on a given 1-cocycle $C\colon G \to \mathrm{GL}_d(\mathbb{E})$. We see that $A \in \mathrm{im}(\Pi_C)$ writes ρ over $\mathbb{F}$ if and only if A is invertible. If X is a random element of $\mathbb{E}^{d\times d}$, then the probability that $A = \Pi_C(X)$ is invertible is at least $\prod_{i=1}^{\infty}(1 - 2^{-i}) > 2/7$. In Part II, we shall assume that $\mathbb{E}$ is a (commutative) field. Different choices for X can give different choices for A, and a random X can be a poor choice e.g. the entries of A may be 100 digit integers. We show in Theorem 10 that if $\mathbb{E}$ is a field and $|\mathbb{F}| \geqslant d$, then we may take X to be a scalar matrix. This result, which is best possible, appears to be helpful in producing "nice" conjugating matrices A. Furthermore, whether $\lambda \in \mathbb{E}^{\times}$ or $X \in \mathbb{E}^{d\times d}$, it appears that the probabilities $\mathrm{Prob}(\Pi_C(\lambda I)$ invertible) and $\mathrm{Prob}(\Pi_C(X)$ invertible) are very close.

Section 5 focuses on the case when ρ is an absolutely irreducible representation. In this case we construct a map $D\colon G \to \mathrm{GL}_d(\mathbb{E})$ and seek a function $\mu\colon G \to \mathbb{E}^{\times}$ such that μD is a 1-cocycle. The existence of D and μ determines whether or not ρ can be written over $\mathbb{F}$. In the cases of interest to us, namely when G is solvable, it suffices to solve, if possible, certain norm equations. (For example, if $\mathbb{E}$ is a cyclotomic number field or a finite field, then G is abelian and hence solvable.)

When G is not solvable, more general equations in the group of units of the ring of algebraic integers of $\mathbb{E}$ need to be solved.

In Section 6 we investigate the probability that $\Pi_C(X)$ is invertible where $X \in \mathbb{E}^{d\times d}$, and the probability that $\Pi_C(\lambda I)$ is invertible where $\lambda \in \mathbb{E}^\times$. We show that the first probability is always high, and we give heuristic arguments that the second probability should be close to the first. Section 6 also gives examples arising from the representation theory of groups. Although our results apply to arbitrary $\mathbb{F}$-algebras $\mathfrak{A}$, the examples presented have $\mathfrak{A} = \mathbb{F}H$ where $\mathbb{F}H$ is a group algebra of a not necessarily finite group H. If $\sigma\colon H \to \mathrm{GL}_d(\mathbb{E})$ is a group representation, then σ may be extended, via a familiar argument, to a representation $\rho\colon \mathfrak{A} \to \mathbb{E}^{d\times d}$ of the group algebra $\mathfrak{A} = \mathbb{F}H$. Of course, ρ can be written over $\mathbb{F}$ precisely when σ can.

Our work has been influenced by [6], which considers the case when G is cyclic, and by Brückner's PhD thesis [2]. In [2] Brückner independently discovers some results in [6], and describes an unpublished result due to Plesken [2, Satz 3] which gives a necessary and sufficient condition for an absolutely irreducible group representation over a field $\mathbb{E}$ to be writable over $\mathbb{F}$ where $\mathbb{E} : \mathbb{F}$ is a finite galois extension of fields. An algorithm is given in [2, Lemma 7] for writing ρ over $\mathbb{F}$ when G is cyclic. (The proof of Lemma 7 contains errors that are easily corrected.) It involves choosing a random column vector $x \in \mathbb{E}^{d\times 1}$ rather than choosing a random matrix $X \in \mathbb{E}^{d\times d}$. This viewpoint motivated our Proposition 5. The research for this paper has different emphases to the work in [7, 4].

In the sequel we will denote $\mathbb{F}$-automorphisms of $\mathbb{E}$ by α, β, γ, elements of $\mathbb{E}$ by λ, μ, ν, and representations of $\mathfrak{A}$ by ρ, ρ', σ.

2. From A to C_α

Let $\rho\colon \mathfrak{A} \to \mathbb{E}^{d\times d}$ be a representation of an $\mathbb{F}$-algebra $\mathfrak{A}$. We shall say that ρ *can be written over* $\mathbb{F}$ if there exists an $A \in \mathrm{GL}_d(\mathbb{E})$ such that

$$A^{-1}\rho(x)A \in \mathbb{F}^{d\times d} \qquad \text{for all } x \in \mathfrak{A}.$$

Our goal is to construct a conjugating matrix A, or prove that one does not exist.

An $\mathbb{F}$-automorphism $\alpha \in \mathrm{Aut}_{\mathbb{F}}(\mathbb{E})$ induces an automorphism, also denoted α, of the algebra $\mathbb{E}^{d\times d}$ of $d\times d$ matrices over $\mathbb{E}$: $(\mu_{i,j}) \mapsto (\alpha(\mu_{i,j}))$. Since $\mathbb{E}^G = \mathbb{F}$, it follows that $(\mathbb{E}^{d\times d})^G = \mathbb{F}^{d\times d}$ and hence A writes ρ over $\mathbb{F}$ if and only if

$$\alpha(A^{-1}\rho(x)A) = A^{-1}\rho(x)A \qquad \text{for all } x \in \mathfrak{A}, \alpha \in G.$$

In subsequent equations, which hold for all $x \in \mathfrak{A}$, we shall omit the x's and simply write

$$\alpha(A^{-1}\rho A) = A^{-1}\rho A \qquad \text{for all } \alpha \in G. \tag{1}$$

Let $\alpha \circ \rho$ denote the composite of ρ and the automorphism α of $\mathbb{E}^{d\times d}$, and let C_α denote $A\alpha(A)^{-1}$. It follows from (1) that

$$C_\alpha^{-1}\rho\, C_\alpha = \alpha \circ \rho \qquad \text{for all } \alpha \in G. \tag{2}$$

Furthermore, $A\alpha\beta(A)^{-1} = A\alpha(A)^{-1}\alpha(A\beta(A)^{-1})$ clearly holds, and so

$$C_{\alpha\beta} = C_\alpha \alpha(C_\beta) \qquad \text{for all } \alpha, \beta \in G. \tag{3}$$

We chose our automorphisms to act on the left, to avoid the "twisted" equation $C_{\alpha\beta} = C_\beta(C_\alpha)^\beta$, which follows from $C_\alpha = A(A^\alpha)^{-1}$.

A map $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ defined by $\alpha \mapsto C_\alpha$ satisfying Eq. (3) is called a *1-cocycle*, and if there exists an $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$, then C is called a 1-*coboundary*. In summary, a necessary condition for ρ to be writable over $\mathbb{F}$ is that there exist a 1-cocycle C satisfying Eq. (2). More significantly, a 1-cocycle C is a 1-coboundary, by a generalization of Hilbert's Theorem 90 (see Theorem 3 below), and there exist constructive methods for finding A from C, and hence for writing ρ over $\mathbb{F}$.

3. From C_α to A

The following result generalizes a well-known result of Artin [12, VIII §4, Theorem 7] which says that distinct characters $H \to \mathbb{E}^\times$ of a group H with values in a field $\mathbb{E}$, are linearly independent over $\mathbb{E}$.

Lemma 1. *Let $\mathbb{E}$ be a division ring.*

(a) *Let $\chi_1, \ldots, \chi_n$ be group homomorphisms $H \to \mathbb{E}^\times$ which are distinct modulo inner automorphisms of $\mathbb{E}$. Then $\chi_1, \ldots, \chi_n$ are linearly independent over $\mathbb{E}$.*

(b) *Let G be a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ whose elements are distinct modulo $\mathrm{Inn}(\mathbb{E})$, and set $\mathbb{F} = \mathbb{E}^G$. Then the trace map $\mathrm{Tr}\colon \mathbb{E} \to \mathbb{F}\colon \lambda \mapsto \sum_{\alpha\in G} \alpha(\lambda)$ is surjective.*

Proof. (a) We shall consider left linear combinations of $\chi_1, \ldots, \chi_n$. The proof for right linear combinations is the same *mutatis mutandis*. Suppose that $\lambda_1, \ldots, \lambda_n \in \mathbb{E}$ satisfy $\lambda_1\chi_1 + \cdots + \lambda_n\chi_n = 0$ where not all λ_i are zero, and n is positive and minimal. Then $n \geqslant 2$ and each λ_i is nonzero. Fix $h, k \in H$. Then

$$\lambda_1\chi_1(k) + \cdots + \lambda_n\chi_n(k) = 0,$$
$$\lambda_1\chi_1(hk) + \cdots + \lambda_n\chi_n(hk) = 0.$$

Premultiplying the first equation by $\lambda_1\chi_1(h)\lambda_1^{-1}$ and subtracting the second equation gives $\sum_{i=2}^{n}\left(\lambda_1\chi_1(h)\lambda_1^{-1}\lambda_i - \lambda_i\chi_i(h)\right)\chi_i(k) = 0$ for all $h, k \in H$. The minimality of n implies that each coefficient is zero. Therefore $\chi_i(h) = \lambda_i^{-1}\lambda_1\chi_1(h)\lambda_1^{-1}\lambda_i$ for all $h \in H$, and χ_i is equivalent modulo $\mathrm{Inn}(\mathbb{E})$ to χ_1 for $i \geqslant 2$, a contradiction.

(b) Let $\chi_1, \ldots, \chi_n$ denote the elements of G and let $H = \mathbb{E}^\times$. By part (a), $\chi_1, \ldots, \chi_n$ are $\mathbb{E}$-linearly independent and hence $\sum_{\alpha\in G}\alpha \neq 0$. As $\mathbb{E}^G = \mathbb{F}$, it follows that $\mathrm{Tr}(\mathbb{E}) \subseteq \mathbb{F}$, and hence the $\mathbb{F}$-linear map $\mathrm{Tr}\colon \mathbb{E} \to \mathbb{F}$ is surjective. □

Assume we know matrices $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$ satisfying Eq. (3). In Theorem 3 we show how to construct $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C_\alpha = A\alpha(A)^{-1}$ for $\alpha \in G$. It relies on the following simple lemma.

Lemma 2. *Let $G \leqslant \mathrm{Aut}(\mathbb{E})$ be finite, where $\mathbb{E}$ is a division ring.*

(a) *If $C_\alpha \in \mathbb{E}^{d\times d}$ satisfies $C_{\alpha\beta} = C_\alpha + \alpha(C_\beta)$ for all $\alpha, \beta \in G$, then $\Pi_C(X) = \sum_{\beta\in G} C_\beta + \beta(X)$ satisfies $C_\alpha + \alpha(\Pi_C(X)) = \Pi_C(X)$ for all $X \in \mathbb{E}^{d\times d}$ and $\alpha \in G$.*

(b) *If $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$ satisfies* Eq. (3)*, then $\Pi_C(X) = \sum_{\beta\in G} C_\beta\beta(X)$ satisfies $C_\alpha\alpha(\Pi_C(X)) = \Pi_C(X)$ for all $X \in \mathbb{E}^{d\times d}$ and $\alpha \in G$.*

(c) *If $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$ satisfies* Eq. (3) *and the elements of G are distinct modulo $\mathrm{Inn}(\mathbb{E})$, then there exists a $\lambda \in \mathbb{E}$ such that the first column, x, of $\Pi_C(I\lambda)$ is nonzero, and x satisfies $C_\alpha\alpha(x) = x$ for all $\alpha \in G$.*

Proof. We omit the proof of part (a) as it follows from the proof of part (b) with products replaced by sums. It follows from Eq. (3) that

$$C_\alpha\alpha(\Pi_C(X)) = C_\alpha\alpha\left(\sum_{\beta\in G} C_\beta\beta(X)\right) = \sum_{\alpha\in G} C_{\alpha\beta}\alpha\beta(X) = \Pi_C(X).$$

Consider part (c). Let e be the column vector with 1 in the first row, and zeroes elsewhere. Set $x = \Pi_C(I\lambda)e$, where $\lambda \neq 0$ is chosen later. By part (b)

$$C_\alpha\alpha(x) = C_\alpha\alpha(\Pi_C(I\lambda)e) = C_\alpha\alpha(\Pi_C(I\lambda))e = \Pi_C(I\lambda)e = x.$$

As $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$, the first column vector of $C_\alpha\alpha(\lambda)$ is nonzero for each $\alpha \in G$. By Lemma 1(a), the elements of G are $\mathbb{E}$-linearly independent. Hence there exists a $\lambda \in \mathbb{E}$ such that $x = \sum_{\alpha\in G} C_\alpha\alpha(\lambda)e \neq 0$. □

The sum $\sum C_\alpha\alpha(X)$ was considered in [6]. I have learned recently that this sum dates back to Poincaré [19, p. 159]. I attribute the following theorem to Serre [19, Prop. 3] when $\mathbb{E}$ is a field, and to Nuss [14, Theorem B] when $\mathbb{E}$ is a division ring. We offer an elementary proof

conducive to practical implementation. A discussion of non-matrix versions of Hilbert's Theorem 90 over division rings can be found in [11].

Theorem 3. *Let* $\mathbb{E}$ *be a division ring, and* G *a finite subgroup of* $\mathrm{Aut}(\mathbb{E})$ *whose elements are distinct modulo* $\mathrm{Inn}(\mathbb{E})$.

(a) *Let* $C_\alpha \in \mathbb{E}^{d\times d}$, $\alpha \in G$. *There exists an* $A \in \mathbb{E}^{d\times d}$ *satisfying* $C_\alpha = A - \alpha(A)$, $\alpha \in G$, *if and only if* $C_{\alpha\beta} = C_\alpha + \alpha(C_\beta)$ *for all* $\alpha, \beta \in G$.

(b) *Let* $C_\alpha \in \mathrm{GL}_d(\mathbb{E})$, $\alpha \in G$. *There exists an* $A \in \mathrm{GL}_d(\mathbb{E})$ *satisfying* $C_\alpha = A\alpha(A)^{-1}$, $\alpha \in G$, *if and only if* $C_{\alpha\beta} = C_\alpha\alpha(C_\beta)$ *for all* $\alpha, \beta \in G$.

Proof. The forward implication is straightforward for parts (a) and (b). The reverse implication follows from Lemma 2 for part (a), and for part (b) *provided* there exists and $X \in \mathbb{E}^{d\times d}$ such that $A = \Pi_C(X)$ is invertible. While it is clear that the image of Π_C contains *nonzero* matrices, it is more subtle that $\mathrm{im}(\Pi_C)$ contains *invertible* matrices. We prove this second fact via induction on d. It is noteworthy that our proof of part (b) uses part (a).

The result is true when $d = 1$ by Lemma 2(c) since if $x \neq 0$, then the 1×1 matrix $[x]$ is invertible. Suppose that $d > 1$ and that the result is true for dimension $d - 1$. By Lemma 2(c) there exists an invertible matrix Y with first column x, satisfying $C_\alpha\alpha(x) = x$ for all $\alpha \in G$. Therefore,

$$Y^{-1}C_\alpha\alpha(Y) = \begin{pmatrix} 1 & y_\alpha \\ 0 & C'_\alpha \end{pmatrix} \qquad \text{for all } \alpha \in G$$

where $C'_\alpha \in \mathrm{GL}_{d-1}(\mathbb{E})$. Since $Y^{-1}C_\alpha\alpha(Y)$ satisfies Eq. (3), so too does C'_α. By induction, there exists an $A' \in \mathrm{GL}_{d-1}(\mathbb{E})$ satisfying $C'_\alpha\alpha(A') = A'$ for all $\alpha \in G$. Thus

$$\begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}^{-1} Y^{-1}C_\alpha\alpha(Y)\alpha \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix} = \begin{pmatrix} 1 & z_\alpha \\ 0 & I \end{pmatrix} =: C''_\alpha \text{ for all } \alpha \in G.$$

Since C''_α satisfies Eq. (3), the z_α satisfy $z_{\alpha\beta} = z_\alpha + \alpha(z_\beta)$ for all $\alpha, \beta \in G$. By part (a) there exists a $1 \times (d-1)$ vector w such that $z_\alpha = w - \alpha(w)$ for all $\alpha \in G$. Therefore, $A = Y \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix} \begin{pmatrix} 1 & w \\ 0 & I \end{pmatrix}$ is invertible, and satisfies $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$. □

Lemma 2(b) entreats us to study the maps $\Pi_C, \Gamma_\alpha \colon \mathbb{E}^{d\times d} \to \mathbb{E}^{d\times d}$ defined by

$$\Pi_C(X) = \sum_{\alpha\in G} C_\alpha\alpha(X) \quad \text{and} \quad \Gamma_\alpha(X) = C_\alpha\alpha(X) - X.$$

When $\mathrm{char}(\mathbb{E}) \nmid |G|$, it is convenient to also define π_C by $\pi_C = |G|^{-1}\Pi_C$. The matrix A in Theorem 3 satisfying $C_\alpha = A\alpha(A)^{-1}$ is far from unique. Indeed the matrix AY, where $Y \in \mathrm{GL}_d(\mathbb{F})$, has the same property. It is useful to regard $\mathbb{E}^{d\times d}$ as a right $\mathbb{F}^{d\times d}$-module, where the scalar action is right matrix multiplication.

Proposition 4. *Let $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ be a 1-cocycle where $\mathbb{E}$ is a division ring, and G is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$. Set $\mathbb{F} = \mathbb{E}^G$.*

(a) *The maps Π_C and Γ_α are right $\mathbb{F}^{d\times d}$-module homomorphisms satisfying $\Pi_C \circ \Gamma_\alpha = \Gamma_\alpha \circ \Pi_C = 0$ and $\Pi_C^2 = |G|\Pi_C$.*

(b) *If $\mathrm{char}(\mathbb{E}) \nmid |G|$, then $\pi_C^2 = \pi_C$ and so $\mathbb{E}^{d\times d} = \mathrm{im}(\pi_C) \oplus \ker(\pi_C)$ where $\ker(\pi_C) = \mathrm{im}(1 - \pi_C)$. Moreover, if $\pi_C(X) = XY$ where $Y \in \mathrm{GL}_d(\mathbb{F})$, then $\pi_C(X) = X$.*

(c) *If $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$, then $\Pi_C(X) = A\mathrm{Tr}(A^{-1}X)$ where $\mathrm{Tr}\colon \mathbb{E}^{d\times d} \to \mathbb{F}^{d\times d}$ is the trace function: $X \mapsto \sum_{\alpha\in G} \alpha(X)$. Moreover, $\Pi_C(A\lambda) = A\mathrm{Tr}(\lambda)$, $\Pi_C(A) = |G|A$ and $\pi_C(A) = A$.*

(d) *Let $Y \in \mathrm{GL}_d(\mathbb{E})$ be fixed, and let $D\colon G \to \mathrm{GL}_d(\mathbb{E})$ be defined by $D_\alpha = Y^{-1}C_\alpha\alpha(Y)$. Then D_α satisfies* Eq. (3), *and*

$$\Pi_D(X) = Y^{-1}\Pi_C(YX).$$

Proof. (a) It is clear that $\Pi_C(X_1 + X_2) = \Pi_C(X_1) + \Pi_C(X_2)$ and $\Pi_C(XY) = \Pi_C(X)Y$ for all $Y \in \mathbb{F}^{d\times d}$. Thus Π_C, and similarly Γ_α, are right $\mathbb{F}^{d\times d}$-module homomorphisms. Lemma 2(b) shows that $\Gamma_\alpha \circ \Pi_C = 0$, and the following argument shows that $\Pi_C \circ \Gamma_\beta = 0$:

$$\Pi_C(C_\beta\beta(X)) = \sum_{\alpha\in G} C_\alpha\alpha(C_\beta\beta(X)) = \sum_{\alpha\in G} C_{\alpha\beta}\alpha\beta(X) = \Pi_C(X).$$

In addition, by the above equation:

$$\Pi_C^2(X) = \sum_{\beta\in G} \Pi_C(C_\beta\beta(X)) = \sum_{\beta\in G} \Pi_C(X) = |G|\Pi_C(X).$$

(b) Multiplying the equation $\Pi_C^2 = |G|\Pi_C$ by $|G|^{-2}$ gives $\pi_C^2 = \pi_C$. Standard arguments show that $\mathbb{E}^{d\times d} = \mathrm{im}(\pi_C)\oplus\ker(\pi_C)$ where $\ker(\pi_C)$ equals $\mathrm{im}(1-\pi_C)$. If $\pi_C(X) = XY$ where $Y \in \mathrm{GL}_d(\mathbb{F})$, then by part (a)

$$XY = \pi_C(X) = \pi_C^2(X) = \pi_C(XY) = \pi_C(X)Y = XY^2.$$

Postmultiplying by Y^{-1} gives $X = XY$. Thus $\pi_C(X) = X$.

Consider part (c):

$$\Pi_C(X) = \sum_{\alpha\in G} A\alpha(A)^{-1}\alpha(X) = A\sum_{\alpha\in G} \alpha(A^{-1}X) = A\mathrm{Tr}(A^{-1}X).$$

Setting $X = A\lambda$ shows $\Pi_C(A\lambda) = A\mathrm{Tr}(I\lambda) = A\mathrm{Tr}(\lambda)$, and setting $\lambda = 1$ shows $\Pi_C(A) = |G|A$ and $\pi_C(A) = A$. Part (d) is straightforward. (The 1-cocycles C and D are called *cohomologous*.) □

The endomorphisms Π_C, Γ_α of $\mathbb{E}^{d\times d}$ give rise to endomorphisms $\widehat{\Pi}_C$, $\widehat{\Gamma}_\alpha$ of the space $\mathbb{E}^{d\times 1}$ of $d \times 1$ column vectors:

$$\widehat{\Pi}_C(x) = \sum_{\alpha\in G} C_\alpha\alpha(x), \quad \widehat{\Gamma}_\alpha(x) = C_\alpha\alpha(x) - x \qquad \text{for } \alpha \in G.$$

When $\mathrm{char}(\mathbb{E}) \nmid |G|$, it is convenient to also define $\widehat{\pi}_C$ by $\widehat{\pi}_C = |G|^{-1}\widehat{\Pi}_C$. If $x \in \mathbb{E}^{d\times 1}$ is the first column of $X \in \mathbb{E}^{d\times d}$, and $Y = \mathrm{diag}(1, 0, \ldots, 0)$, then the first columns of $\Pi_C(XY) = \Pi_C(X)Y$ and $\Gamma_\alpha(XY) = \Gamma_\alpha(X)Y$ are $\widehat{\Pi}_C(x)$ and $\widehat{\Gamma}_\alpha(x)$ respectively.

It is worth recording some simple generalizations of Prop. 4(a,b,c) such as: $\widehat{\Gamma}_\alpha \circ \widehat{\Pi}_C = \widehat{\Pi}_C \circ \widehat{\Gamma}_\alpha = 0$, $\widehat{\Pi}_C^2 = |G|\widehat{\Pi}_C$, $\mathbb{E}^{d\times 1} = \mathrm{im}(\widehat{\pi}_C) \oplus \ker(\widehat{\pi}_C)$ and $\widehat{\Pi}_C(x) = A\mathrm{Tr}(A^{-1}x)$ where Tr denotes the trace map $\mathbb{E}^{d\times 1} \to \mathbb{F}^{d\times 1}$.

Proposition 5. *Let $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ be a 1-cocycle where $\mathbb{E}$ is a division ring, and G is a finite subgroup of $\mathrm{Aut}(\mathbb{E})$ whose elements are distinct modulo $\mathrm{Inn}(\mathbb{E})$. Let S be a generating set for G, and set $\mathbb{F} = \mathbb{E}^G$. Then*

(a) $\mathrm{im}(\widehat{\Pi}_C) = \bigcap_{\alpha\in S} \ker(\widehat{\Gamma}_C)$ *is the $\mathbb{F}$-linear span of the columns of any matrix A satisfying $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$.*
(b) *If $\mathrm{char}(\mathbb{E}) \nmid |G|$, then $\ker(\widehat{\Pi}_C) = \sum_{\alpha\in S} \mathrm{im}(\widehat{\Gamma}_\alpha)$.*
(c) *If $\alpha \neq 1$, then $\mathrm{im}(\widehat{\Gamma}_\alpha)$ spans $\mathbb{E}^{d\times 1}$ as an $\mathbb{E}$-space.*
(d) *If $0 \neq x \in \ker(\widehat{\Pi}_C)$, then $x\mathbb{E} \not\subseteq \ker(\widehat{\Pi}_C)$.*

Proof. (a) $\widehat{\Gamma}_\alpha \circ \widehat{\Pi}_C = 0$, implies $\mathrm{im}(\widehat{\Pi}_C) \subseteq \bigcap_{\alpha\in S} \ker(\widehat{\Gamma}_\alpha)$. Conversely, if $x \in \bigcap_{\alpha\in S} \ker(\widehat{\Gamma}_\alpha)$, then $C_\alpha\alpha(x) = x$ for $\alpha \in S$. It follows from Eq. (3) that $C_\alpha\alpha(x) = x$ for all $\alpha \in G$. Thus

$$\widehat{\Pi}_C(x\lambda) = \sum_{\alpha\in G} C_\alpha\alpha(x)\alpha(\lambda) = \sum_{\alpha\in G} x\alpha(\lambda) = x\mathrm{Tr}(\lambda).$$

By Lemma 1(b), there exists a $\lambda \in \mathbb{E}$ such that $\mathrm{Tr}(\lambda) = 1$. Thus $x \in \mathrm{im}(\widehat{\Pi}_C)$ and so $\mathrm{im}(\widehat{\Pi}_C) = \bigcap_{\alpha\in S} \ker(\widehat{\Gamma}_\alpha)$. It follows from Prop. 4(c) that $\mathrm{im}(\widehat{\Pi}_C) = A\mathbb{F}^{d\times 1}$, and so $\mathrm{im}(\widehat{\Pi}_C)$ is the $\mathbb{F}$-linear span of columns of A.

(b) $\widehat{\Pi}_C \circ \widehat{\Gamma}_\alpha = 0$, implies $\ker(\widehat{\Pi}_C) \supseteq \sum_{\alpha\in S} \mathrm{im}(\widehat{\Gamma}_\alpha)$. It follows from Eq. (3) that

$$C_{\alpha\beta}\alpha\beta(x) - x = [C_\alpha\alpha(C_\beta\beta(x)) - C_\beta\beta(x)] + [C_\beta\beta(x) - x].$$

Hence $\operatorname{im}(\widehat{\Gamma}_{\alpha\beta}) \subseteq \operatorname{im}(\widehat{\Gamma}_\alpha) + \operatorname{im}(\widehat{\Gamma}_\beta)$ and $\sum_{\alpha\in G} \operatorname{im}(\widehat{\Gamma}_\alpha) = \sum_{\alpha\in S} \operatorname{im}(\widehat{\Gamma}_\alpha)$. Conversely, if $x \in \ker(\widehat{\Pi}_C)$, then $\sum_{\alpha\in G} C_\alpha\alpha(x) = 0$ and hence

$$x = \sum_{\alpha\in G} |G|^{-1}x = \sum_{\alpha\in G} \widehat{\Gamma}_\alpha(-|G|^{-1}x) \in \sum_{\alpha\in G} \operatorname{im}(\widehat{\Gamma}_\alpha) = \sum_{\alpha\in S} \operatorname{im}(\widehat{\Gamma}_\alpha).$$

Thus $\ker(\widehat{\Pi}_C) = \sum_{\alpha\in S} \operatorname{im}(\widehat{\Gamma}_\alpha)$ as desired.

(c) Let $\phi\colon \mathbb{E}^{d\times 1} \to \mathbb{E}$ be an $\mathbb{E}$-linear map containing $\operatorname{im}(\widehat{\Gamma}_\alpha)$ in its kernel. Then for all $x \in \mathbb{E}^{d\times 1}$ and $\lambda \in \mathbb{E}$:

$$0 = \phi(\widehat{\Gamma}_\alpha(x\lambda)) = \phi(C_\alpha\alpha(x))\alpha(\lambda) - \phi(x)\lambda.$$

Since $\alpha \neq 1$ it follows from Lemma 1(a) that $\phi(x) = 0$ for all x and hence $\phi = 0$. This proves that the $\mathbb{E}$-linear span of $\operatorname{im}(\widehat{\Gamma}_\alpha)$ equals $\mathbb{E}^{d\times 1}$, and hence $\dim_{\mathbb{F}}(\operatorname{im}(\widehat{\Gamma}_\alpha)) \geqslant d$.

(d) Suppose that $0 \neq x \in \ker(\widehat{\Pi}_C)$. If $\widehat{\Pi}_C(x\lambda) = 0$ for all $\lambda \in \mathbb{E}$, then $\sum_{\alpha\in G} C_\alpha\alpha(x)\alpha(\lambda) = 0$. Since $C_\alpha\alpha(x) \neq 0$, this contradicts Lemma 1(a). Thus $x\mathbb{E} \not\subseteq \ker(\widehat{\Pi}_C)$ as claimed. □

Proposition 6. *Let $(\lambda_\alpha)_{\alpha\in G}$ be a basis for $\mathbb{E}$ as a right $\mathbb{F}$-space, and let $E_{i,j} \in \mathbb{E}^{d\times d}$ be the matrix with 1 in the (i,j)th entry and zeroes elsewhere. Then $\mathbb{E}^{d\times d}$ is freely generated as a right $\mathbb{F}^{d\times d}$-module by $E_{i,1}\lambda_\alpha$, $\alpha \in G$, $i = 1, \ldots, d$.*

Proof. Taking right $\mathbb{F}$-linear combinations of $E_{i,1}\lambda_\alpha$ gives a matrix with arbitrary first column. Taking right $\mathbb{F}^{d\times d}$-multiples gives every element of $\mathbb{E}^{d\times d}$. The fact that the $E_{i,1}\lambda_\alpha$ freely generate $\mathbb{E}^{d\times d}$ follows from the observation that $E_{i,1}\mathbb{F}^{d\times d}$ comprises matrices with all rows zero except the ith, and the ith row can be an arbitrary vector in $\mathbb{F}^{1\times d}$. □

It follows from Theorem 3 and Prop. 4 and 6 that an invertible matrix can be found by taking $\mathbb{F}^{d\times d}$-linear combinations of the matrices $\Pi_C(\lambda_\alpha E_{i,1})$. Since each $\Pi_C(\lambda_\alpha E_{i,1})$ is singular (unless $d = 1$), it is better to consider $\mathbb{F}^{d\times d}$-linear combinations of $\Pi_C(\lambda_\alpha D^i)$ where D is the permutation matrix corresponding to the d-cycle $(1, 2, \ldots, d)$. A simple argument shows that the $\lambda_\alpha D^i$ generate $\mathbb{E}^{d\times d}$ as a $\mathbb{F}^{d\times d}$-module, although not freely. In practice $\mathbb{F}^{d\times d}$-linear combinations are not necessary as $\Pi_C(\lambda_\alpha D^i)$ is commonly invertible. Thus we typically do not evaluate $\Pi_C(X)$ at a random matrix X. Doing so can result in "bad" matrices $A = \Pi_C(X)$, e.g. with 100 digit integer entries. More significantly, the matrices $A^{-1}\rho(x)A$ can be "bad". Choosing X to be a scalar matrix seems to result in "good" matrices $\Pi_C(X)$. This imprecise statement has some theoretical underpinning in Theorem 10.

4. Invertible elements in $\mathrm{im}(\Pi_c)$

The primary aim of this section is to prove in Theorem 10 that if $|\mathbb{F}| \geqslant d$ there exists a $\lambda \in \mathbb{E}$ such that $\Pi_C(I\lambda)$ is invertible. We show in Theorem 8 that the assumption $|\mathbb{F}| \geqslant d$ is best possible by considering a special case when A, and hence each C_α, is upper-triangular.

We need a preliminary lemma.

Lemma 7. *Let V be a vector space over a division ring $\mathbb{F}$. If V is a union of m proper subspaces, then $\dim_{\mathbb{F}}(V) \geqslant 2$ and $|\mathbb{F}| < m$. Conversely, if $\dim_{\mathbb{F}}(V) \geqslant 2$ and $\mathbb{F}$ is finite, then V is a union of $|\mathbb{F}|+1$ hyperplanes.*

Proof. The proof in [8, Problem 24] generalizes to division rings, so the first claim is true. Conversely, suppose $\dim_{\mathbb{F}}(V) \geqslant 2$ and $|\mathbb{F}| < \infty$. Then $V = H_\infty \cup \bigcup_{\lambda\in\mathbb{F}} H_\lambda$ where H_∞ and H_λ are the hyperplanes $x_1 = 0$, and $x_1\lambda + x_2 = 0$. Thus V is a union of $|\mathbb{F}| + 1$ hyperplanes. □

Theorem 8. *Let $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ be a 1-cocycle where G and $\mathbb{E}$ are as in* Theorem 3. *Set $\mathbb{F} = \mathbb{E}^G$. Suppose that there exist an upper-triangular matrix $A \in \mathrm{GL}_d(\mathbb{E})$ such that $C_\alpha = A\alpha(A)^{-1}$, for all $\alpha \in G$.*

(a) *If $|\mathbb{F}| \geqslant d$, then there exists a $\lambda \in \mathbb{E}^\times$ such that $\det(\Pi_C(I\lambda)) \neq 0$.*
(b) *If $|\mathbb{F}| < d$, then an upper-triangular matrix $A \in \mathrm{GL}_d(\mathbb{E})$ can be chosen so that $\det(\Pi_C(I\lambda)) = 0$ for all $\lambda \in \mathbb{E}$.*

Proof. (a) It follows from Prop. 4(c) that $\Pi_C(I\lambda)$ is invertible if and only if $\mathrm{Tr}(A^{-1}\lambda)$ is invertible. If a_{ii} denotes the (i,i)th entry of A, then $\mathrm{Tr}(A^{-1}\lambda)$ is upper-triangular with (i,i)th entry $\mathrm{Tr}(a_{ii}^{-1}\lambda)$. Let $K(a_{ii}^{-1})$ denote the kernel of the map $\lambda \mapsto \mathrm{Tr}(a_{ii}^{-1}\lambda)$. By Lemma 1(b), the $\mathbb{F}$-subspace $K(a_{ii}^{-1})$ of $\mathbb{E}$ has codimension 1. If $|\mathbb{F}| \geqslant d$, then $\mathbb{E}$ is not a union of d proper subspaces by Lemma 7. Thus there exists a $\lambda \in \mathbb{E}$ not in $\bigcup_{i=1}^d K(a_{ii}^{-1})$. Since $\mathrm{Tr}(a_{ii}^{-1}\lambda) \neq 0$ for each i, it follows that $\Pi_C(I\lambda)$ is invertible.

(b) Suppose that $|\mathbb{F}| < d$. By Lemma 7, $\mathbb{E}$ is a union of $|\mathbb{F}| + 1$ hyperplanes, say $\mathbb{E} = \bigcup_{i=1}^d K(a_{ii}^{-1})$ for some $a_{11}^{-1}, \ldots, a_{dd}^{-1} \in \mathbb{E}^\times$. Choose A so that its (i,i)th entry is a_{ii}. Then for each $\lambda \in \mathbb{E}$, at least one diagonal entry of the upper-triangular matrix $\mathrm{Tr}(A^{-1}\lambda)$ is zero. Put differently, $\Pi_C(I\lambda)$ is singular for all $\lambda \in \mathbb{E}$. □

Part II: The commutative case

In this part, $\mathbb{E}$ always denotes a (commutative) *field*. In Theorem 10 below, we shall generalize Theorem 8 to deal with arbitrary $d \times d$ matrices A. Its proof depends on the following well-known result.

Lemma 9. *Let f be an element of the polynomial ring $\mathbb{F}[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in \mathbb{F}^n$.*

(a) *If the degree of f in each variable is less than $|\mathbb{F}|$, then $f = 0$.*
(b) *If the degree of f is at most q where $|\mathbb{F}| = q$, then there exists $\nu_1, \ldots, \nu_n \in \mathbb{F}$ such that $f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \nu_i(x_i^q - x_i)$.*

Proof. (a) See [12, Chapter V, Theorem 5] for the case when $\mathbb{F}$ is finite, and [12, Corollary 3] for the case when $\mathbb{F}$ is infinite. Consider part (b). Recall that the degree of a nonzero polynomial is the maximum degree of a monomial summand, and $\deg(x_1^{k_1} \cdots x_n^{k_n}) = k_1 + \cdots + k_n$. The result is true when $n = 1$. Suppose that $n > 1$ and $f = \sum_{i=0}^{q} f_i x_n^{q-i}$ where f_i is a polynomial in $x_1, \ldots, x_{n-1}$ of degree at most i. Fix $(a_1, \ldots, a_{n-1}) \in \mathbb{F}^{n-1}$ and consider $f(a_1, \ldots, a_{n-1}, x_n)$. By the $n = 1$ case, $f_i(a_1, \ldots, a_{n-1}) = 0$ for $i = 1, \ldots, q-2$ and $f_0 = -f_{q-1} = \nu_n$ is a constant polynomial. By part (a), $f_i = 0$ for $i = 1, \ldots, q-2$ and by induction there exist $\nu_1, \ldots, \nu_{n-1} \in \mathbb{F}$ such that $f_q = \sum_{i=1}^{n-1} \nu_i(x_i^q - x_i)$. In summary, $f = \sum_{i=1}^{n} \nu_i(x_i^q - x_i)$. □

The reader may like to compare Lemma 9(b) with a theorem due to Chevalley [18, §1.7, Theorem 2] on roots of homogeneous polynomials.

Theorem 10. *Let $\mathbb{E}$ be a field, and $\mathbb{E} : \mathbb{F}$ a finite galois extension with group G. Suppose that $C\colon G \to \mathrm{GL}_d(\mathbb{E})$ is a 1-cocycle and $|\mathbb{F}| \geqslant d$. Then there exists a $\lambda \in \mathbb{E}^\times$ such that $\Pi_C(I\lambda) = \sum_{\alpha \in G} C_\alpha \alpha(\lambda)$ is invertible.*

Proof. By Theorem 3 there exists an invertible matrix A satisfying $C_\alpha = A\alpha(A)^{-1}$, $\alpha \in G$. By Prop. 4(c), $\Pi_C(\lambda I) = A\mathrm{Tr}(\lambda A^{-1})$. Thus $\Pi_C(\lambda I)$ is invertible precisely when $\mathrm{Tr}(\lambda A^{-1})$ is invertible. Our problem can be rephrased: Given $X \in \mathrm{GL}_d(\mathbb{E})$, find $\lambda \in \mathbb{E}$ such that $\mathrm{Tr}(\lambda X)$ is invertible.

By [17, Theorems 7.4.2, 8.7.2] there exists $\zeta \in \mathbb{E}$ such that $(\alpha(\zeta))_{\alpha \in G}$ is a basis for $\mathbb{E}$ over $\mathbb{F}$ (such a basis is called a *normal basis*). Now $\mathrm{Tr}(\zeta) \in \mathbb{F}^\times$ by Lemma 1(b). By replacing ζ by $\mathrm{Tr}(\zeta)^{-1}\zeta$ we may additionally assume that $\mathrm{Tr}(\zeta) = 1$. A typical element of $\mathbb{E}$ has the form $\sum_{\alpha \in G} x_\alpha \alpha(\zeta)$ where $x_\alpha \in \mathbb{F}$. Write

$$x_{i,j} = \sum_{\alpha \in G} x_\alpha^{i,j} \alpha(\zeta) \quad \text{and} \quad \lambda = \sum_{\beta \in G} \lambda_\beta \beta(\zeta)$$

where $x_{i,j}$ denotes the (i,j)th entry of X. We shall view the $x_\alpha^{i,j}$ as *elements* of $\mathbb{F}$, and the λ_β as algebraically independent commuting *variables* that are fixed by G.

Let $(\mu_{\alpha,\beta})$ be the matrix of the $\mathbb{F}$-linear transformation $\mathbb{E} \to \mathbb{E}$ defined by $\lambda \mapsto \zeta\lambda$. That is,

$$\zeta\alpha(\zeta) = \sum_{\beta \in G} \mu_{\alpha,\beta}\beta(\zeta) \quad \text{where } \mu_{\alpha,\beta} \in \mathbb{F}. \tag{4}$$

Set $x = \sum_\alpha x_\alpha \alpha(\zeta)$. Then by Eq. (4)

$$\begin{aligned} x\lambda &= \left(\sum_\alpha x_\alpha \alpha(\zeta)\right)\left(\sum_\beta \lambda_\beta \beta(\zeta)\right) = \sum_{\alpha,\beta} x_\alpha \lambda_\beta \alpha(\zeta\alpha^{-1}\beta(\zeta)) \\ &= \sum_{\alpha,\beta,\gamma} x_\alpha \lambda_\beta \mu_{\alpha^{-1}\beta,\gamma}\ \alpha\gamma(\zeta). \end{aligned}$$

Replacing $\alpha\gamma$ by γ gives $x\lambda = \sum x_\alpha \lambda_\beta \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma}\ \gamma(\zeta)$. Our normalization implies that $\mathrm{Tr}(\gamma(\zeta)) = 1$, and hence

$$\begin{aligned} \mathrm{Tr}(x\lambda) &= \sum_{\alpha,\beta,\gamma} x_\alpha \lambda_\beta \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma}\ \mathrm{Tr}(\gamma(\zeta)) \\ &= \sum_\alpha \left(\sum_{\beta,\gamma} \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma}\lambda_\beta\right) x_\alpha = \sum_\alpha z_\alpha x_\alpha. \end{aligned} \tag{5}$$

where we abbreviate the above inner sum by z_α. Then by Eq. (4)

$$\begin{aligned} z_\alpha &= \sum_\beta \left(\sum_\gamma \mu_{\alpha^{-1}\beta,\alpha^{-1}\gamma}\right)\lambda_\beta = \sum_\beta \mathrm{Tr}(\zeta\alpha^{-1}\beta(\zeta))\lambda_\beta \\ &= \sum_\beta \mathrm{Tr}(\alpha(\zeta)\beta(\zeta))\lambda_\beta. \end{aligned} \tag{6}$$

Replacing x_α in Eq. (5) by $x_\alpha^{i,j}$ shows

$$\det \mathrm{Tr}(X\lambda) = \det(\mathrm{Tr}(x_{i,j}\lambda)) = \det\left(\sum_\alpha z_\alpha x_\alpha^{i,j}\right).$$

This determinant is a polynomial in the variables z_α which is either the zero polynomial, or is homogeneous of degree d in the z_α. Specifically,

$$\det\left(\sum_\alpha z_\alpha x_\alpha^{i,j}\right) = \sum p_{\{\alpha_1,\ldots,\alpha_d\}} z_{\alpha_1}\cdots z_{\alpha_d} \tag{7}$$

where the sum is taken over all orbits of the symmetric group S_d on the group G^d. Such orbits are in bijective correspondence with the multisets $\{\alpha_1,\ldots,\alpha_d\}$ of G having at least one, and at most d, distinct elements. We view the coefficient $p_{\{\alpha_1,\ldots,\alpha_d\}}$ of $z_{\alpha_1}\cdots z_{\alpha_d}$ as an element of $\mathbb{F}$, not a polynomial over $\mathbb{F}$ in the $x_\alpha^{i,j}$.

The matrix $(\mathrm{Tr}(\alpha(\zeta)\beta(\zeta)))_{\alpha,\beta\in G}$ is invertible (see [17, §7.2]), and its determinant equals the discriminant $\prod_{\alpha\neq\beta}(\alpha(\zeta)-\beta(\zeta))$ of the minimal polynomial $\prod_\alpha(t-\alpha(\zeta))$ of ζ over $\mathbb{F}$. By Eq. (6) as (λ_β) runs through the vectors in the vector space $\mathbb{F}^{|G|}$, (z_α) does the same.

The determinant $\det(X)=\det(\sum_\alpha x_\alpha^{i,j}\alpha(\zeta))$ can be evaluated using the same reasoning used for Eq. (7). Replacing z_α by $\alpha(\zeta)$ in Eq. (7) shows

$$\det(X)=\sum p_{\{\alpha_1,\dots,\alpha_d\}}\alpha_1(\zeta)\cdots\alpha_d(\zeta). \tag{8}$$

Let us assume that X is fixed and that $\det\mathrm{Tr}(X\lambda)=0$ for all $\lambda\in\mathbb{E}$ (or equivalently, all $(\lambda_\beta)\in\mathbb{F}^{|G|}$). By virtue of the previous paragraph, this says that the polynomial Eq. (7) is zero for all $(z_\alpha)\in\mathbb{F}^{|G|}$. If $|\mathbb{F}|>d$, then Lemma 9(a) implies that each $p_{\{\alpha_1,\dots,\alpha_d\}}$ equals zero. By Eq. (8), $\det(X)=0$. In summary, we have proved that if $|\mathbb{F}|>d$ and $\det(X)\neq 0$, then there exists a $\lambda\in\mathbb{E}$ such that $\det\mathrm{Tr}(\lambda X)\neq 0$.

Finally, suppose that $|\mathbb{F}|=d$ is finite, and $\det\mathrm{Tr}(X\lambda)=0$ for all $\lambda\in\mathbb{E}$. By Lemma 9(b), $\det\mathrm{Tr}(X\lambda)=\sum_{\alpha\in G}\nu_\alpha(z_\alpha^{|\mathbb{F}|}-z_\alpha)$. Since this polynomial is not homogeneous, each ν_α is zero. Thus each $p_{\{\alpha_1,\dots,\alpha_d\}}$ equals zero, and $\det(X)=0$ by Eq. (8). This completes the proof. □

In the light of Theorem 8, one may suspect that Theorem 10 holds more generally: namely when $\mathbb{E}$ is a division ring.

5. Algorithmic considerations

Suppose henceforth $G\leqslant\mathrm{Aut}(\mathbb{E})$, $\mathbb{F}=\mathbb{E}^G$ and $\rho\colon\mathfrak{A}\to\mathbb{E}^{d\times d}$ is an *absolutely irreducible* representation of an $\mathbb{F}$-algebra $\mathfrak{A}$. We wish to constructively answer the question: Can ρ be written over $\mathbb{F}$?

There are two fundamentally different approaches to solve this problem. The first finds, if possible, certain matrices $D_\alpha\in\mathrm{GL}_d(\mathbb{E})$, and then finds, if possible, certain scalars $\mu_\alpha\in\mathbb{E}$ such that $C_\alpha=\mu_\alpha D_\alpha$ defines a 1-cocycle. Then a conjugating matrix $A=\Pi_C(X)$ is constructed by choosing an appropriate $X\in\mathbb{E}^{d\times d}$. The second approach is based on a generalization of the MeatAxe and is described, when $\mathbb{E}$ is finite, in [7]. We shall comment here on the first approach.

Suppose that $G=\langle S\rangle$, and $\mathfrak{A}=\langle T\rangle$ where S and T are finite. If ρ can be written over $\mathbb{F}$, then there exist matrices $D_\alpha\in\mathrm{GL}_d(\mathbb{E})$ satisfying

$$D_\alpha^{-1}\rho D_\alpha=\alpha\circ\rho\qquad\text{for all }\alpha\in S \tag{9}$$

where $\alpha\circ\rho$ means ρ composed with α. There are a variety of methods for calculating all D_α, or proving that some do not exist. These include (a) using the MeatAxe algorithm [10, 16], (b) solving for each $\alpha\in S$ the $d^2|T|$ homogeneous linear equations $\rho(x)D_\alpha=D_\alpha(\alpha\circ\rho)(x)$, $x\in T$,

over $\mathbb{E}$ in d^2 unknowns, and (c) averaging over a chain of $\mathbb{F}$-algebras $\mathfrak{A} = \mathfrak{A}_1 \supset \cdots \supset \mathfrak{A}_{n+1} = \{0\}$ where the indices $|\mathfrak{A}_i : \mathfrak{A}_{i+1}|$ are "small".

In Section 2 we saw that if ρ can be written over $\mathbb{F}$, then there exist matrices D_α satisfying Eq (9). Assume that we have found D_α, for $\alpha \in S$, otherwise our question has a negative answer. As ρ is absolutely irreducible, each D_α is unique up to a scalar multiple, and we must find scalars $\mu_\alpha \in \mathbb{E}^\times$ for $\alpha \in S$ such that $C_\alpha = \mu_\alpha D_\alpha$ satisfies Eq. (3) for all $\alpha, \beta \in G$.

Assume henceforth that G is finite and solvable. (The fields $\mathbb{E}$ of most interest to us are subfields of cyclotomic fields, and finite fields. In both cases G is finite and abelian, and hence solvable.) By using induction on $|G|$, we can reduce to the case when G is cyclic: If H is a normal subgroup of G such that G/H is cyclic, then recursively write ρ over $\mathbb{E}^H$, and then write ρ over $\mathbb{F} = (\mathbb{E}^H)^G$.

Suppose now that $G = \langle \alpha \rangle$ is cyclic of finite order m. Then

$$D_\alpha \alpha(D_\alpha) \cdots \alpha^{m-1}(D_\alpha) = \lambda_\alpha I. \tag{10}$$

Since $\alpha^m = 1$, we see $D_\alpha^{-1}(\lambda_\alpha I) D_\alpha = \alpha(\lambda_\alpha) I$ and so $\lambda_\alpha \in \mathbb{F}$. Denote by N or N_G the norm map $\mathbb{E}^\times \to \mathbb{F}^\times \colon \mu \mapsto \prod_{\beta \in G} \beta(\mu)$. If $\lambda_\alpha \in \mathrm{im}(N)$, then there exists $\mu_\alpha \in \mathbb{E}^\times$ satisfying $N(\mu_\alpha) = \lambda_\alpha^{-1}$ and thus $C_\alpha = \mu_\alpha D_\alpha$ defines a 1-cocycle. For finite fields, N is surjective, however, for infinite fields this is need not be so. If $\lambda_\alpha \notin \mathrm{im}(N)$, then ρ can not be written over $\mathbb{F}$, see Example 2 below.

Although evaluating $\Pi_C(X)$ is clearly useful, it is time-consuming when $|G|$ is large unless an averaging argument is used. We describe how to use a subgroup chain $G = G_0 > G_1 > \cdots > G_{t+1} = 1$ to reduce the cost of computing $\Pi_C(X)$ from $\mathrm{O}(|G|)$ to $\mathrm{O}(\sum_{i=1}^t |G_{i-1} : G_i|)$. If $G = \alpha_1 H \cup \cdots \cup \alpha_r H$ is a decomposition of G into left cosets of H, then

$$\Pi_C(X) = \sum_{i=1}^{r} \sum_{\beta \in H} C_{\alpha_i \beta} \alpha_i \beta(X) = \sum_{i=1}^{r} C_{\alpha_i} \alpha_i \left(\sum_{\beta \in H} C_\beta \beta(X) \right).$$

Put differently, $\Pi_{C|G} = \sum_{i=1}^r C_{\alpha_i} \alpha_i \Pi_{C|H}$. If G is finite and solvable, then we may choose G_i so that $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is cyclic. In this case, an idea in [6, p. 1705] further reduces the complexity of evaluating $\Pi_C(X)$ to $\mathrm{O}(\log |G|)$.

6. Probabilities and examples

Lemma 2(b) suggests a probabilistic algorithm for splitting a 1-cocycle $C \colon G \to \mathrm{GL}_d(\mathbb{E})$: repeatedly select random matrices $X \in \mathbb{E}^{d \times d}$ until $A = \Pi_C(X)$ is invertible. Then $C_\alpha = A\alpha(A)^{-1}$ for all $\alpha \in G$. (In

our context, A writes ρ over $\mathbb{F} = \mathbb{E}^G$.) It is natural to ask the expected number of matrices X chosen in order to find an invertible $A = \Pi_C(X)$. If $|\mathbb{F}| = q$ is finite, and a uniform distribution is used for $\mathbb{E}^{d\times d}$, then by Prop. 4(c), $A^{-1}\Pi_C(X) = \mathrm{Tr}(A^{-1}X)$ is a uniformly random element of $\mathbb{F}^{d\times d}$. Hence the probability that $\Pi_C(X)$ is invertible is

$$f(d,q) = \frac{|\mathrm{GL}_d(\mathbb{F})|}{|\mathbb{F}^{d\times d}|} = \prod_{i=1}^{d}(1-q^{-i}).$$

Remarkably, this probability is independent of C and $|\mathbb{E}:\mathbb{F}|$. Note that

$$\limsup_q f(d,q) = f(d,\infty) = 1 \quad \text{and} \quad \liminf_{d,q} f(d,q) = f(\infty,2).$$

The following bounds for $f(d,q)$ are useful:

$$1 - q^{-1} \geqslant f(d,q) > \prod_{i=1}^{\infty}(1-q^{-i}) > 1 - q^{-1} - q^{-2}.$$

Now $f(d,q) > f(\infty,2) = 0.288788\cdots > 2/7$, and hence one would expect to make on average at most 3.5 choices for X. The probability that our probabilistic algorithm fails to terminate after N selections is $(1-f(d,q))^N < (q^{-1}+q^{-2})^N$. If $\mathbb{E}$ is infinite, then it follows by localization, and a local-global argument, that the probability that $\Pi_C(X)$ is invertible is 1.

Theorem 10 entreats us to consider the probability, p_C, that a random $\lambda \in \mathbb{E}^\times$ has $\Pi_C(\lambda I)$ invertible. This probability depends on C, $|\mathbb{E}:\mathbb{F}|$ and the probability measure used on $\mathbb{E}^\times$. (It is most natural to use a Haar measure on $\mathbb{E}^\times$.) It is an open problem to find a positive lower bound for p_C when $|\mathbb{F}| \geqslant d$. When $|\mathbb{E}|$ and d are "small," empirical evidence suggests that the average value of p_C, averaged over all 1-cocycles C, is a number very close to $f(d,q)$ where $|\mathbb{F}| = q$. The following example shows that p_C can be 1.

Example 1. Let $G = \langle\alpha\rangle$ have order 2. Fix $\mu \in \mathbb{E}^\times$, and define a 1-cocycle $C\colon G \to \mathrm{GL}_2(\mathbb{E})$ by $C_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $C_\alpha = \begin{pmatrix} 0 & \alpha(\mu) \\ \mu^{-1} & 0 \end{pmatrix}$. Let $\lambda \in \mathbb{E}^\times$. Then

$$\det(\Pi_C(\lambda I)) = \begin{vmatrix} \lambda & \alpha(\mu)\alpha(\lambda) \\ \mu^{-1}\alpha(\lambda) & \lambda \end{vmatrix} = \lambda^2 - \alpha(\mu)\mu^{-1}\alpha(\lambda)^2 = 0$$

if and only if $(\lambda\alpha(\lambda)^{-1})^2 = \alpha(\mu)\mu^{-1}$. There are many choices for μ such that $\eta = \alpha(\mu)\mu^{-1}$ has no square root in the kernel of the norm map $N_{\langle\alpha\rangle}$. For example, if $\mathbb{E} = \mathbb{Q}(i)$ and $\mu = 2-i$, then $\eta = (3+4i)/5$ has no square root in $\mathbb{E}$ (as $\pm(2+i)/\sqrt{5} \notin \mathbb{E}$). For another example, suppose

that $|\mathbb{F}| = q$ is odd, and μ has order q^2-1. Then η has order $q+1$ and $(\lambda\alpha(\lambda)^{-1})^2$ has order at most $(q+1)/2$. Both of these examples have $p_C = 1$, as $\det(\Pi_C(\lambda I)) \neq 0$ for all $\lambda \in \mathbb{E}^\times$.

Our probabilistic algorithm for finding an invertible $\Pi_C(X)$ is not trivial even when $d = 1$. When $|\mathbb{F}| = q$ is finite, it gives rise to an a probabilistic algorithm for computing $(q-1)$th roots of elements of elements of $\mathbb{E}^\times$ of norm 1. It also gives rise to a novel divide-and-conquer algorithm for solving norm equations. A full discussion of these points would divert us from the focus of this paper.

If ρ is irreducible but not absolutely irreducible, then the MeatAxe [10, 16] may be used to find D. In this case, however, the arithmetic needed to solve for μ (and hence find C) takes place in the division algebra $\mathrm{End}(\rho)$ of matrices commuting with $\rho(\mathfrak{A})$. See [5] for a description of some of the relevant noncommutative theory. We shall assume henceforth that $\mathfrak{A} = \mathbb{F}H$ is a group algebra over $\mathbb{F}$.

The connection between $\mathbb{E}H$-modules and $\mathbb{F}H$-modules is clarified by considering normal bases. The following simple observation is not made explicitly in texts covering modular representation theory such as [9]. Let $(\alpha(\lambda))_{\alpha\in G}$ be a normal basis for $\mathbb{E}$ over $\mathbb{F}$. Let $V = \mathbb{E}^{d\times 1}$ and $U = \mathbb{F}^{d\times 1}$. Then V viewed as an $\mathbb{F}H$-module is a direct sum of $|G|$ galois conjugate $\mathbb{F}H$-submodules: $V = \oplus_{\alpha\in G}\alpha(\lambda)U$. Note that $A^{-1}\rho(h)A \in \mathrm{GL}_d(\mathbb{F})$ for $h \in H$ and so

$$\alpha(\lambda)UA^{-1}\rho(h)A = \alpha(\lambda)U.$$

Thus the $\alpha(\lambda)U = \alpha(\lambda U)$ are $A^{-1}\rho A$ invariant, and galois conjugate.

In the examples below $\mathbb{Q}$ denotes the rational field, and ζ_n denotes the complex number $e^{2\pi i/n}$. Recall that $\alpha \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is determined by a number k satisfying $\alpha(\zeta_n) = \zeta_n^k$, and $\gcd(k,n) = 1$.

Example 2. Let H be the dicyclic group of order $8n$

$$H = \langle a, b \mid a^2 = b^{2n}, b^{4n} = 1, a^{-1}ba = b^{-1}\rangle.$$

Let $\mathbb{E} = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_{4n}$. Define $\alpha \in \mathrm{Aut}(\mathbb{E})$ by $\alpha(\zeta) = \zeta^{-1}$. Then α has order 2, and $\mathbb{F} = \mathbb{E}^{\langle\alpha\rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$. Define $\rho\colon H \to \mathrm{GL}_2(\mathbb{E})$ by

$$\rho(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}.$$

Then $D_\alpha = \rho(a)$ and $D_1 = \rho(1)$ satisfies Eq. (9). Since $N_{\langle\alpha\rangle}(D_\alpha)$ equals $D_\alpha\alpha(D_\alpha) = D_\alpha^2 = -I$, it follows that $\lambda_\alpha = -1$. Since α is complex conjugation, $N_{\langle\alpha\rangle}(\mu_\alpha) = \mu_\alpha\overline{\mu_\alpha} = ||\mu_\alpha||^2 \geqslant 0$, so $N_{\langle\alpha\rangle}(\mu_\alpha) = -1$ has no solution. Consequently, ρ can not be written over $\mathbb{F}$.

Example 3. Let $H = \langle a, b \mid a^2 = b^{4n}, b^{8n} = 1, a^{-1}ba = b^{1+4n}\rangle$ and let $\mathbb{E} = \mathbb{Q}(\zeta)$ where $\zeta = \zeta_{8n}$. Define $\alpha \in \mathrm{Aut}(\mathbb{E})$ by $\alpha(\zeta) = \zeta^{1+4n} = -\zeta$. Then α has order 2, and $\mathbb{F} = \mathbb{E}^{\langle\alpha\rangle} = \mathbb{Q}(\zeta^2)$. Define $\rho\colon H \to \mathrm{GL}_2(\mathbb{E})$ by

$$\rho(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{1+4n} \end{pmatrix}.$$

Set $D_1 = \rho(1)$ and $D_\alpha = \rho(a)$. Then $N_{\langle\alpha\rangle}(D_\alpha) = -I$, so $\lambda_\alpha = -1$. Now $\mu_\alpha = \zeta^{2n}$ satisfies $N_{\langle\alpha\rangle}(\mu_\alpha) = \mu_\alpha^2 = -1 = \lambda_\alpha^{-1}$. Thus $C_1 = \rho(1)$ and $C_\alpha = \zeta^{2n}\rho(a)$. The matrix

$$A := \Pi_C\left(\frac{1+\zeta}{2}\, I\right) = \frac{1}{2}\begin{pmatrix} 1+\zeta & \zeta^{2n}(1-\zeta) \\ -\zeta^{2n}(1-\zeta) & 1+\zeta \end{pmatrix}$$

has $\det(A) = \zeta \neq 0$, and hence writes ρ over $\mathbb{F}$. If $\rho' = A^{-1}\rho A$, then

$$\rho'(a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho'(b) = \frac{1}{2}\begin{pmatrix} 1+\zeta^2 & \zeta^{2n}(1-\zeta^2) \\ \zeta^{2n}(1-\zeta^2) & -1-\zeta^2 \end{pmatrix}.$$

The similarity between A and $\rho'(b)$ is interesting. For each n there are many choices for μ_α, and then many choices for ν such that $\Pi_C(\nu I)$ is invertible. Our choices $\mu_\alpha = \zeta^{2n}$, $\nu = (1+\zeta)/2$ give a simple expression for $\rho'(b)$. Another choice when n is odd is $\mu_\alpha = 1+\zeta^n-\zeta^{3n}$ and $\nu = 1$.

Example 4. Let $H = \langle a, b \mid a^m = b^n = 1, a^{-1}ba = b^r\rangle$ where $\gcd(m, n) = 1$ and r has order m modulo n. Let $\zeta = \zeta_n$, $\mathbb{E} = \mathbb{Q}(\zeta)$, and let $\mathbb{F} = \mathbb{E}^{\langle\alpha\rangle}$ where $\alpha \in \mathrm{Aut}(\mathbb{E})$ is defined by $\alpha(\zeta) = \zeta^r$. Define $\rho\colon H \to \mathrm{GL}_m(\mathbb{E})$ by

$$\rho(a) = \begin{pmatrix} 0 & 1 & 0 & \\ & & \ddots & \\ 0 & 0 & & 1 \\ 1 & 0 & & 0 \end{pmatrix} \quad \text{and} \quad \rho(b) = \begin{pmatrix} \zeta & & & \\ & \zeta^r & & \\ & & \ddots & \\ & & & \zeta^{r^{m-1}} \end{pmatrix}.$$

Then $C_\alpha = \rho(a)$ and $C_{\alpha^i} = C_\alpha\alpha(C_\alpha)\cdots\alpha^{i-1}(C_\alpha) = \rho(a)^i$ and

$$A = \Pi_C(\lambda I) = \sum_{i=0}^{m-1} C_\alpha^i \alpha^i(\lambda) = (\alpha^{i-j}(\lambda))$$

is invertible if and only if λ defines a normal basis for $\mathbb{E}$ over $\mathbb{F}$. If $\rho' = A^{-1}\rho A$, then $\rho'(a) = \rho(a)$ and the expression for $\rho'(b)$ is rather complicated, and depends on r.

Example 5. Let $\mathbb{E} : \mathbb{F}$ be a finite galois extension with group G. Let σ be the left regular representation $G \to \mathrm{Sym}(G)$ satisfying $\sigma_\alpha(\gamma) = \alpha\gamma$ and $\sigma_{\alpha\beta} = \sigma_\alpha \circ \sigma_\beta$. Let H be the split extension of $\mathbb{E}^\times$ by G. Specifically, let H be the set $G \times \mathbb{E}^\times$ endowed with the binary operation

$$(\alpha, \lambda)(\beta, \mu) = (\alpha\beta, \beta(\lambda)\mu) \qquad \text{for all } \alpha, \beta \in G, \lambda, \mu \in \mathbb{E}^\times.$$

Define $\rho\colon H \to \mathrm{GL}_{|G|}(\mathbb{E})$ by $\rho(\alpha, \lambda) = (\eta(\lambda)\delta_{\sigma_\alpha(\eta),\eta})$ where $(\delta_{\xi,\eta})$ is the identity matrix. The (ξ, η) entry of $\rho(\alpha, \lambda)$ is zero unless $\xi = \sigma_\alpha(\eta)$ in which case it equals $\eta(\lambda)$. The (ξ, η) entry of $\rho(\alpha, \lambda)\rho(\beta, \mu)$ is zero unless $\xi = \sigma_{\alpha\beta}(\eta)$ in which case it equals $\sigma_\beta(\eta)(\lambda)\eta(\mu) = \eta(\beta(\lambda)\mu)$. This proves that ρ is a homomorphism. Since ρ is induced from a 1-dimensional representation $\mathbb{E}^\times \to \mathrm{GL}_1(\mathbb{E})$ which is fixed only by the identity automorphism, it follows from Clifford's theorem that ρ is absolutely irreducible. We may take C_α to be the permutation matrix $\rho(\alpha, 1)$ corresponding to σ_α. Then $A = \Pi_C(\lambda I)$ is invertible if and only if λ defines a normal basis for $\mathbb{E}$ over $\mathbb{F}$. If $|\mathbb{F}| = q$ and $|\mathbb{E}| = q^n$, then the probability, p_C, that $\Pi_C(\lambda I)$ is invertible is $q^{-n} \sum_{d|n} \mu(n/d) q^d$, where μ denotes the Möbius function. A small calculation shows that that $p_C \geqslant \frac{1}{2}$ for all q and n.

Acknowledgment

I am indebted to both the referee, and Prof. Cheryl Praeger, for suggesting a number of improvements to an earlier draft of this paper.

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514. MR0746539

[2] H. Brückner, Algorithmen für endliche auflösbare Gruppen und Anwendungen. PhD thesis, Aachner Beiträge zur Mathematik **22**, RWTH Aachen, 1998.

[3] C. Fieker, Über relative Normgleichungen in algebraichen Zahlkörper. PhD thesis, Technische Univ. Berlin, 1997.

[4] C. Fieker, Minimizing representations over number fields, *J. Symbolic Comput.* **38** (2004), 833–842. MR2094558

[5] S.P. Glasby, Modules induced from a normal subgroup of prime index, in: *Rings, Modules, and Abelian Groups*, Eds. A. Facchini, E. Houston and L. Salce, Lecture Notes in Pure and Applied Mathematics **236** (2004), 257–270. MR2050716

[6] S.P. Glasby and R.B. Howlett, Writing representations over minimal fields, *Comm. Algebra* **25** (1997), 1703–1711. MR1446124

[7] S.P. Glasby, C.R. Leedham-Green and E.A. O'Brien, Writing projective representations over proper subfields, *J. Algebra* **295** (2006), 51–61. MR2188850

[8] P.R. Halmos, *Linear Algebra Problem Book* (Dolciani Mathematical Expositions **16**, Mathematical Association of America, 1995). MR1310775

[9] B. Huppert and N. Blackburn, *Finite Groups II* (Springer, Berlin, 1982). MR0650245
[10] D.F. Holt and S. Rees, Testing modules for irreducibility, *J. Austral. Math. Soc. Ser. A* **57** (1994), 1–16. MR1279282
[11] T.Y. Lam and A. Leroy, Hilbert 90 theorems over division rings, *Trans. Amer. Math. Soc.* **345** (1994), 595–622. MR1181184
[12] S. Lang, *Algebra*, Addison Wesley, 1965. MR0197234
[13] Shangzhi Li, On the subgroup structure of classical groups. Group theory in China, 70–90, Math. Appl. (China Ser.), 365, Kluwer Acad. Publ., Dordrecht, 1996. MR1447199
[14] P. Nuss, Noncommutative descent and nonabelian cohomology, *K-theory* **12** (1997), 23-74. MR1466623
[15] R.A. Parker, The computer calculation of modular characters (the meat-axe), in: *Computational Group Theory, Durham, 1982* (Academic Press, London, 1984), pp. 267–274. MR0760660
[16] R.A. Parker, An integral meataxe, in: *The Atlas of Finite Groups Ten Years On*, London Math. Soc. Lect. Notes **249** (1998), pp. 215–228. MR1647424
[17] S. Roman, *Field Theory* (Graduate Texts in Mathematics, **158**, Springer-Verlag, 1995). MR1329733
[18] P. Samuel, *Algebraic Theory of Numbers* (Hermann, Paris, 1971). Translated from the French by A.J. Silberger. MR0265266
[19] J.-P. Serre, *Corps Locaux* (Hermann, Paris, 1968). MR0354618
[20] D. Simon, Solving norm equations in relative number fields using S-units, *Math. Comp.* **71** (2002), 1287–1305. MR1898758
[21] J.H. Walter, On the Galois theory of division rings, *Proc. Amer. Math. Soc.* **10** (1959), 898–907. MR0113919

Department of Mathematics
Central Washington University
WA 98926-7424, USA
GlasbyS@cwu.edu
http://www.cwu.edu/∼glasbys/