# CONJUGATE REDUCIBILITY OF FAMILIES OF BLOCK-DIAGONAL MATRICES OVER AN EXTENSION FIELD OF A PERFECT FIELD, AND APPLICATIONS TO MATRIX SUBALGEBRAS AND SUBGROUPS

by

MARTIN L. BROCK

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2004

UMI Number: 3115232

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

12-17-03
Date

Chair of Examining Committee

12-18-03
Date

Alvany Rocha
Executive Officer

Professor Carlos Moreno, The Graduate Center

Professor Alphonse Vasquez, The Graduate Center

Professor William Singer, Fordham University

Professor Martin Moskowitz, The Graduate Center
Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

# Abstract

Conjugate Reducibility of Families of Block-Diagonal Matrices,
Over an Extension Field of a Perfect Field;
and Applications to Matrix Subalgebras and Subgroups

by

Martin L. Brock

Advisor: Professor Martin Moskowitz

For $L/k$ a field extension, $k$ perfect, and $M(n, F)$ the $n \times n$ matrices over field $F$, the main question is when can certain families of $M(n, L)$ be conjugated into $M(n, k)$, by an operator from $G\ell(n, L)$. We say such a family is $k$–rationalizable over $L$. Henceforth, let $L$ be any extension of $\overline{k}$. We also determine the maximal subsets of $M(n, L)$ that can normalize a diagonal family of $M(n, L)$ and be $k$–rationalized over $L$ together with it. The primary methods are Galois Theory and the imbeddings of a field extension into the algebraic closure of its ground field.

Chapter 1 introduces a set of matrices viewable as block-diagonal "discriminant" matrices, and another viewable as block-horizontal "discriminant" matrices.

Chapter 2 exhibits all invertible matrices, that $k$–rationalize over $\overline{k}$, certain block-

diagonal "discriminant" subsets. Those emerge, basically, as the block-horizontal "discriminant" matrices. Results over $\overline{k}$ are then extended to *any* extension of $\overline{k}$.

Chapter 3 exhibits general block-diagonal subsets, with suitably restricted centralizers, which are $k$–rationalized over $L$ by some block-horizontal "discriminant" matrix. Those emerge as the block-diagonal "discriminant" matrices; thus a reverse form of the previous.

Chapter 4 exhibits all diagonal families of $M(n, L)$ which are $k$–rationalizable over $L$, and an important tight property of this exhibition. Chapter 5 gives an alternative, aesthetic, and quick way to "see" them.

Chapter 6 exhibits, for any $k$–rationalizable over $L$ diagonal family of $M(n, L)$, a superset for its normalizing elements in $G\ell(n, L)$ which can be $k$–rationalized over $L$ together with the family. This superset is achieved with certain "maximal" diagonal families. Exhibition results are given for certain non-"maximal" diagonal families, and even block-diagonal families.

Chapter 7 gives applications to the diagonalizable subsets of $M(n, k)$, $k$ a perfect field. These include exhibitions and classifications of the subsets of $M(n, k)$ that are: diagonalizable, second centralizers of some diagonalizable subset, and maximal diagonalizable; with their centralizers, second centralizers, and normalizers (or strong inclusions/imbeddings thereof) in $M(n, k)$ and $M(n, L)$.

Applications to $M(n, k)$ can easily be a research subject: finite solvable or torsional abelian subgroups; $k = \mathbb{Q}$ or $GF(p^n)$; small $n$; the solvable subgroups of $M(n, \mathbb{Z}_2)$.

# Acknowledgements

First and foremost, I would like to thank Professors Martin Moskowitz, Alphonse Vasquez, and Carlos Moreno, for their very many growth-producing and enjoyable mathematical conversations over the years. I would also like to thank them for their very generous and constant personal support and help over these same years, and, most graciously, for their very generous patience throughout my graduate-studentship, and the writing of this dissertation.

These remarks also apply to Professor William Singer of Fordham University, over the past recent years, and our shared love of careful detail. I also want to thank him for his very generous and full personal support, constantly applied, for which I am most deeply indebted.

I would like to express my deepest thanks for the great privilege of knowing and working with Professor Martin Moskowitz, my advisor. He has helped me not only with the most generous personal support and advice, but with every possible aspect of one's graduate student process — from the specific and perfect language to use in cover letters and communications, to solving problems of multiple varieties, to details of proof technique and to insights on results. I am most very deeply indebted to him, and with great personal, and very heartfelt, gratitude.

I would also like to thank the late Professor Louis Auslander, and Professors Gerard Bricogne, and Ravi Kulkarni, for their helpful conversations on this dissertation, including information and insights.

I owe very much to Professors Michael Artin, Richard Shafer, Georg Lustig, and Nesmith Ankeny, from MIT, where I was an undergraduate and graduate (Master's), for richly and insightfully providing me with fundamentals of Algebra and Number Theory, and from which some ideas have been used in this dissertation.

Lastly, I would like to express my most deepest and fundamental indebtedness, and greatly heartfelt gratitude, well beyond words, to the late Professor Arnold E. Ross — who truly made me a mathematician. I had the very great privilege and pleasure of attending, three times, the NSF summer programs he founded, ran, and personally taught, for high-school and early college students specially interested in mathematics, at the Ohio State University. He taught me the fundamental and true intent of Number Theory, Algebra, and Mathematics.

And finally, I would like to thank my late grandfather, Arthur Rose, my parents, Carol and Arthur, my sister, Alice, my brother, James, and my warm, furry friends, Miles, Tabú, Ginger, and Xena, for their constant, consistent, and ever-present support and encouragement, and without whom this, and many things, would not have even begun to be possible.

# Contents

# Chapter 1

# Introduction and Basic Notation

## 1.1 Introduction

Let $k$ be a perfect field and $L$ an extension field of $k$. Let $M(n, L)$ be the set of $n \times n$ matrices with coefficients from $L$. The main question to be considered here, is when certain families $\mathcal{M} \subseteq M(n, L)$, can be conjugated into $M(n, k)$, by an operator $P \in G\ell(n, L)$. When there is such a $P$, we shall call this a $k$–rationalization over $L$, of $\mathcal{M}$, and say that $\mathcal{M}$ is $k$–rationalizable over $L$. We let $\mathcal{N}_L(\mathcal{M})$ be the elements of $G\ell(n, L)$ that normalize $\mathcal{M}$, and $\mathcal{C}_L(\mathcal{M})$ be those in $M(n, L)$ that centralize $\mathcal{M}$. Henceforth, suppose $L$ is any extension field of $\overline{k}$. We shall also determine, for a $k$–rationalizable diagonal family $\mathcal{Z} \subseteq M(n, L)$, the maximal subsets of $\mathcal{N}_L(\mathcal{Z})$, which, when joined together with $\mathcal{Z}$, can still be $k$–rationalized. The methods used are primarily Galois Theory and the set of imbeddings of a field extension into the algebraic closure of its ground field. The only restriction on the ground field is that it be perfect. (This is a "weak" restriction; it includes all fields of characteristic 0, all finite fields, as well as certain infinite fields of characteristic $p$.)

Among a number of objects defined and discussed in Chapter 1, are the map $\Delta_\Phi$, the block-diagonal matrices which form its image, and the set of matrices $V_\Phi^\times$. In the former, the block-diagonal matrices are each formed first, by a single matrix over an intermediate field of $\overline{k}/k$, block-diagonalized together with all its images under the imbeddings of that intermediate field in $\overline{k}$; and then, blocked-diagonalized together, similarly, with other matrices (of arbitrary dimension) over other such intermediate fields, together with all their similar such imbedding images; all together in one matrix. Each such resulting matrix might be thought of as a block-diagonal "discriminant" matrix of matrices, using submatrices of arbitrary dimension. In the latter, the matrices of $V_\Phi^\times$ are also formed, first, by a single matrix over an intermediate field of $\overline{k}/k$, but joined together horizontally with all its images under the imbeddings of that intermediate field in $\overline{k}$; and then further joined together horizontally, similarly, with other matrices (of arbitrary column, but constant row, dimension) over other such intermediate fields, together with all their similar such imbedding images; all together in one matrix. Each such resulting matrix might be thought of as a block-horizontal "discriminant" matrix of matrices, using submatrices of arbitrary column, and constant row, dimension.

In Chapter 2, all invertible matrices are exhibited, that $k$–rationalize over $\overline{k}$, subsets of the image of the map $\Delta_\Phi$ [necessarily block-diagonal], with suitable restrictions on their centralizers. These invertible matrices are found to be, basically, the set of matrices $V_\Phi^\times$ itself; i.e., a certain set of block-horizontal "discriminant" matrices. The complete result is stated in Corollary 2.C.6. This result relies, among other things, on Lemmas 2.C.1, and 2.C.3; and these are where the key underlying arguments are contained. The argument in the latter lemma is deeper, and involves the "untwisting" of an implicit condition, found in the first line of Step 2 of its proof. Possible further exploration of the last condition stated, in the above-mentioned Corollary 2.C.6, could be a subject for further research. The previous results of Chapter 2 were all established over $\overline{k}$. These results are extended to *any* extension of $\overline{k}$, in Section 2.5.

In Chapter 3, all subsets of block-diagonal matrices, with suitable restrictions on their centralizers, are exhibited, which are $k$–rationalized over $L$, by a given element of $V_\Phi^\times$. These subsets are found to be precisely the subsets of the image of $\Delta_\Phi$ itself; i.e., a certain set of block-diagonal "discriminant" matrices. The result is stated in Theorem 3.B.1; and is a reverse form of the above Corollary 2.C.6. The key, and deeper part of the argument is in the reverse direction of its proof, and involves the "untwisting" of an implicit condition, found in the last line of Step 4 of the proof. This result allows an important extension, that exhibits all "sufficiently large" families of block-diagonal matrices, with suitable restrictions on their centralizers, which are $k$–rationalizable over $L$ – *at all*. The result is given in Theorem 3.B.2.

Now let $D(n, L)$ stand for the diagonal matrices in $M(n, L)$. In Chapter 4, the families of $D(n, L)$ are exhibited which are $k$–rationalizable over $L$, together with an important tight property as part of this exhibition. This result is to be found in Theorem 4.B.4; with that important property the last item in its statement. An alternative way, simple and succinct, to view the previous result – the families of $D(n, L)$ that are $k$–rationalizable over $L$, is given in Theorem 5.C.1. This is an aesthetically important result, which, among other things, allows one a quick way to "see" these families.

Referring back to Chapter 1 for a moment, a simple construct called a field setting, and usually denoted by $\Phi$, is defined. It is an $r$-tuple of 3-tuples, where each 3-tuple is (essentially) an intermediate field of $\bar{k}/k$ and its imbeddings into $\bar{k}$. A reduced field setting, which is defined in Chapter 6, is a simpler and more natural type of field setting, and which also turns out (easily) to be "equivalent" to any field setting. Most results are stated using one of these constructs, including the next result.

If $\mathcal{Z}$ is a family of $D(n, L)$, which is $k$–rationalizable over $L$, we determine the maximal subset of $\mathcal{N}_L(\mathcal{Z})$ that can be $k$–rationalized over $L$, together with $\mathcal{Z}$. The result, organized slightly differently, is essentially contained in Theorem 6.F.1, Part (1) [Theorem 2.D.2 and Theorem 6.C.2 make the result complete, virtually at once]. This maximal subset is actually achieved in certain "maximal" cases of $\mathcal{Z}$; and this result is similarly given in Theorem 6.F.2. This maximal subset is:

**the product of** $\big\{$the image of the map $\Delta_\Phi\big\}$ **and**

$\big\{\{$certain powers of permutationally-represented Galois groups (over $k$) of the intermediate fields of $\Phi$ $\}$ **times**

$\{$a set of larger-dimensioned permutation matrices, simply derived from $\Phi\}\big\}$.

Structurally (and this result is also given in Theorem 6.F.1), this maximal subset is a group isomorphic to:

$$\left[\prod_{i=1}^{r} G\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u} [Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]\right];$$

where $K_1, \ldots, K_r$ are intermediate fields of $\overline{k}/k$ (and also the intermediate fields of $\Phi$); $K_{i_1}, \ldots, K_{i_u}$ are a subsequence of these intermediate fields; $S_{m_h}$ is the symmetric group on $m_h$ letters; and several constraints exist among these and the other quantities above, including: $\sum_{i=1}^{r} a_i[K_i : k] = \sum_{h=1}^{u} a_{i_h}[K_{i_h} : k]m_h = n$; $\sum_{h=1}^{u} m_h = r$. In the previous, for families $\mathcal{Z}$ which may not be "maximal", the above maximal subset may give more than the desired elements of $\mathcal{N}_L(\mathcal{M})$ which are $k$–rationalizable over $L$, together with $\mathcal{Z}$. Finer work on an exhibition for these "in-between" cases can be a subject for further research. Some significant results of this type are to be found (though not stated in this full format) in Lemma 6.E.2, Part (1) and Lemma 6.E.5. We note that Lemma 6.E.2, Part (1) actually goes a little further than the present context, which applies to diagonal matrices, in that this Lemma applies, at the start, to certain families of block-diagonal matrices.

Chapter 7 applies the results of the previous chapters to the diagonalizable subsets of $M(n,k)$, $k$ any perfect field. Let $L$ be any extension field of $\overline{k}$. The main results are in Section 7.3, and include exhibitions and classifications of:

i) all the diagonalizable subsets of $M(n,k)$; their centralizers in $M(n,k)$ and $M(n,L)$, their second centralizers in $M(n,k)$ and $M(n,L)$, and strong inclusions (or imbeddings) for their normalizers in $M(n,k)$ and $M(n,L)$;

ii) all the subsets of $M(n,k)$ which are second centralizers of some diagonalizable subset of $M(n,k)$ [i.e, $C_k^2(\cdots)$ ]; their centralizers, their second centralizers, and their normalizers in $M(n,k)$ and $M(n,L)$;

iii) all the *maximal* diagonalizable subsets of $M(n,k)$; their centralizers, their second centralizers, and their normalizers in $M(n,k)$ and $M(n,L)$.

Specific results regarding the latter — the maximal diagonalizable subsets of $M(n,k)$, include: these subsets are isomorphic to $\prod_{i=1}^{r} K_i$, for some intermediate fields $K_1,\ldots,K_r$ of $\overline{k}/k$; their first and second centralizers are both isomorphic to the same product of intermediate fields; their normalizers are isomorphic to: $\left[\prod_{i=1}^{r} K_i^{\times}\right] \rtimes \left[\prod_{h=1}^{u} \left[\mathcal{Gal}\left(K_{i_h}/k\right)^{m_h} \rtimes S_{m_h}\right]\right]$, where $K_{i_1},\ldots,K_{i_u}$ are a subsequence of the previous intermediate fields, $S_{m_h}$ is the symmetric group on $m_h$ letters, and several constraints exist among these and the other quantities above, including: $\sum_{i=1}^{r}[K_i : k] = \sum_{h=1}^{u}[K_{i_h} : k]m_h = n$; $\sum_{h=1}^{u} m_h = r$; and, lastly, the quotient of their normalizers by their invertible centralizing elements is isomorphic to: $\prod_{h=1}^{u} \left[\mathcal{Gal}\left(K_{i_h}/k\right)^{m_h} \rtimes S_{m_h}\right]$.

Using the results, particularly of Chapter 7, applications to $M(n, k)$ can well be a subject for further research (and sometimes obtained or explored rapidly). For example: applications to those subgroups which are finite solvable [because they normalize a non-trivial diagonalizable subgroup], or are torsional abelian [the results imbed these in direct products of the multiplicative groups of cyclotomic extensions of $k$]; when the field $k$ is $\mathbb{Q}$ or $GF(p^n)$; when the dimension $n$ is low, e.g., $n = 2, 3$ [much drops out of many constraints given in those results, such as the summation contraints mentioned above]. A particular application to the solvable subgroups of $M(n, \mathbb{Z}_2)$ can well be a subject for further research; particularly given that there, the set of scalar matrices (the center) is trivial.

Some results of the Appendix may be interesting in their own right; e.g., Proposition App. 16, and Corollary App. 17.

## 1.2 Basic Notation–General

The main objects we will be using are: fields, imbeddings of fields, matrices over fields, permutations and permutation matrices. In this section, we make definitions of, give notations for, and list properties of various constructs that will be used in connection with the above (and other) objects.

### 1.2.1 Functions

a) Let $S$ and $T$ be sets, and let $f: S \to T$. We let:

$$\text{the image of } f \equiv Im(f) \equiv \{t \in T | \exists s \in S: f(s) = t\}.$$

b) Let $S$ be a set. We let:

$$\text{the identity function on } S \equiv id_S \equiv (id_S: S \to S, id_S: s \mapsto s).$$

c) Let $S$ be a finite set.

  i) We let:

$$\text{the cardinality of } S \equiv |S|; \text{ so that } |S| \in \mathbb{N}$$

  ii) We say that a function $f$ is *an enumerator of* $S$, when $f$ is *a bijection from* $\{1, \ldots, |S|\}$ *to* $S$. I.e.:

$$\text{the set of enumerators of } S \equiv \text{ the set of bijective elements of } S^{\{1,\ldots,|S|\}}.$$

### 1.2.2 Fields

a) Let $k$ be a field. We let:

$$\text{algebraic closure of } k \equiv \overline{k}.$$

b) Let $K/F$ be an extension of fields. We let:

$$\begin{aligned} \text{the set of } F\text{-imbeddings of } K/F \text{ into } \overline{K} &\equiv Iso(K/F) \\ &\equiv \left\{\tau: K \hookrightarrow \overline{K} \,\middle|\, \tau|F = id_F\right\}. \end{aligned}$$

We note that if $K/F$ is a finite extension, then $Iso(K/F)$ is finite, and $|Iso(K/F)| \leq [K : F]$. Moreover, if $K/F$ is a finite, separable extension, then $|Iso(K/F)| = [K : F]$. In our applications, $F$ will always be perfect, making all finite extensions of $F$ separable.

c) Let $K/F$ be an extension of fields. We let:

$$\text{the Galois Group of } K/F \equiv Gal(K/F) \equiv \left\{\sigma : K \overset{\text{iso}}{\rightarrow} K \middle| \sigma|F = id_F\right\}.$$

Clearly, $Gal(K/F) \subseteq Iso(K/F)$.

d) Let $K/F$ be an extension of fields. We let:

$$\text{the set of intermediate fields of } K/F \text{ which are finite extensions of } F \equiv$$

$$Int'(K/F) \equiv \{L \text{ an intermediate field of } K/F | \, L \text{ is a finite extension of } F\}.$$

e) **Field-theoretic Conjugacy**

Let $k$ be any field.

i) **Conjugacy of Elements of Fields**

Let $\alpha, \beta \in \overline{k}$. We let:

$$\alpha \text{ is } k\text{-conjugate to } \beta \equiv \alpha \sim_k \beta \overset{\text{def}}{\Longleftrightarrow} \exists \sigma \in Iso\,(k(\alpha)/k) : \ \sigma(\alpha) = \beta.$$

So, clearly, we note that $\sim_k$ is an equivalence relation on $\overline{k}$. Moreover, the $\sim_k$-equivalence class of $\alpha$ is finite, and is, in fact, the set of roots of the minimal polynomial of $\alpha$ over $k$.

ii) **Conjugacy of Fields**

Let $K, L$ be intermediate fields of $\overline{k}/k$. We let:

$$K \text{ is } k\text{-conjugate to } L \equiv K \sim_k L \overset{\text{def}}{\Longleftrightarrow} \exists \sigma \in Iso(K/k)\colon\ \sigma(K) = L.$$

Again, clearly, we note that $\sim_k$ is an equivalence relation on the set of intermediate fields of $\overline{k}/k$ (and where all $\sim_k$–equivalence classes of finite extensions of $k$ in $\overline{k}$ are finite).

### 1.2.3 Rings

Let $R$ be a ring with identity, the latter denoted by $1_R$. We let:

$$\text{the group of units of } R \ \equiv R^\times \equiv \{u \in R \mid \exists v \in R\colon\ uv = vu = 1_R\}.$$

### 1.2.4 Matrices

Matrices are main objects of concern here, and will be used often. In particular, there will be notation for several ways of joining matrices together to construct larger (or, technically, no smaller) matrices. The notation for the block-diagonal way of joining matrices together, described below, will be used frequently throughout this paper.

**Part A: Basic Sets of Matrices**

Let $R$ be any commutative ring with identity, and let its additive identity element be $0_R$, and let its multiplicative identity element be $1_R$.

Let $n, m, a \in \mathbb{Z}^+$.

We define the following sets of matrices:

i) $M(n \times m, R) \equiv$ the $R$-module of $n \times m$ matrices over $R$;

ii) $M(n, R) \equiv M(n \times n, R) =$ the $R$-algebra of $n \times n$ matrices over $R$;

iii) $Gl(n, R) \equiv (M(n, R))^{\times} =$ the group of invertible $n \times n$ matrices over $R$;

thus we have also: $Gl(n, R) = \{P \in M(n, R) | det(P) \in R^{\times}\}$;

iv) $D(n, R) \equiv$ the $R$-algebra of diagonal $n \times n$ matrices over $R$;

v) Scalar$(n, R) \equiv$ the $R$-algebra of scalar $n \times n$ matrices over $R$;

i.e., Scalar$(n, R) \equiv \{rI_n \in M(n, R) | r \in R\}$ (here, $I_n$ is the $n \times n$ identity matrix over $R$, defined next).

We define the following particular matrices:

vi) the zero matrix:

$$\text{the } a \times a \text{ zero-matrix over } R \equiv O_a(R) \equiv \begin{bmatrix} 0_R & \cdots & 0_R \\ \vdots & \cdots & \vdots \\ 0_R & \cdots & 0_R \end{bmatrix} \in M(a, R).$$

vii) the identity matrix:

$$\text{the } a \times a \text{ identity matrix over } R \equiv I_a(R) \equiv \begin{bmatrix} 1_R & & \\ & \ddots & \\ & & 1_R \end{bmatrix} \in M(a, R).$$

viii) the canonical nilpotent matrix:

the canonical $a \times a$ nilpotent matrix over $R$

$$\equiv N_a(R) \equiv \begin{bmatrix} 0_R & 1_R & & \\ & \ddots & \ddots & \\ & & \ddots & 1_R \\ & & & 0_R \end{bmatrix} \in M(a, R)$$

$$(N_1(R) \equiv [0_R]).$$

When clear, we abbreviate $(M(n, R))^{\times}$ by $M^{\times}(n, R)$, and $O_a(R), I_a(R), N_a(R)$ by, respectively, $O_a, I_a, N_a$.

## Part B: Concatenation of Matrices

This is one of the constructions for joining matrices together to form a larger (technically, no smaller) matrix. Here, $R$ is any commutative ring with identity.

1) Let $A \in M(n \times p, R)$ and $B \in M(n \times q, R)$; $n, p, q \in \mathbb{Z}^{+}$. We let:

   the concatenation of $A$ and $B \equiv A \circledparallel B \equiv \begin{bmatrix} A & \vdots & B \end{bmatrix} \in M(n \times (p+q), R)$.

   We note that the only constraints on the matrix arguments of " $\circledparallel$ " is that these arguments have *the same number of rows.*

2) As " $\circledparallel$ " is clearly associative, we may define its iterates in the following obvious and recursive way:

$$\mathop{\circledparallel}\limits_{i=1}^{r} A_i \equiv \left(\mathop{\circledparallel}\limits_{i=1}^{r-1} A_i\right) \circledparallel A_r \in M\left(n \times \left(\sum_{i=1}^{r} p_i\right), R\right);$$

$$\overset{r}{\underset{i=1}{\circledparallel}}\ \overset{s}{\underset{j=1}{\circledparallel}} A_{ij} \equiv \overset{r}{\underset{i=1}{\circledparallel}} \left( \overset{s}{\underset{j=1}{\circledparallel}} A_{ij} \right) \in M\left( n \times \left( \sum_{i=1}^{r} \sum_{j=1}^{s} p_{ij} \right), R \right);\ \text{etc.}$$

In this paper, with few exceptions, we will have no need to extend the iterations of " $\circledparallel$ " beyond the double level indicated above.

3) The definition in item (1) above may be extended naturally from individual matrices to subsets of matrices, as follows.

Let $\mathcal{A} \subseteq M(n \times p, R)$ and $\mathcal{B} \subseteq M(n \times q, R)$. We let:

$$\mathcal{A} \circledparallel \mathcal{B} \equiv \{ A \circledparallel B \mid A \in \mathcal{A}, B \in \mathcal{B} \} \subseteq M\left(n \times (p+q), R\right).$$

Similar to item (2) above, we define the iterates: $\overset{r}{\underset{i=1}{\circledparallel}} \mathcal{A}_i,\ \overset{r}{\underset{i=1}{\circledparallel}} \overset{s}{\underset{j=1}{\circledparallel}} \mathcal{A}_{ij}$.

## Part C: Block-diagonal Join of Matrices

This will be, by far, the most important, and frequently used, construction for joining matrices together. Here, $R$ is any commutative ring with identity.

1) Let $A \in M(n \times m, R)$ and $B \in M(p \times q, R)$; $n, m, p, q \in \mathbb{Z}^{+}$. We let:

the block-diagonal join of $A$ and $B$

$$\equiv A \obslash B \equiv \begin{bmatrix} A & \bigcirc \\ \bigcirc & B \end{bmatrix} \in M\left((n+p) \times (m+q), R\right).$$

We note that $\obslash$ applies to *any* two matrices; there are no constraints on the arguments of " $\obslash$ ".

2) As “$\mathop{\bigcirc\kern-0.78em\triangle}$ ” is clearly associative, we may define its iterates in the following obvious and recursive way:

$$\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} A_i \equiv \left(\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r-1} A_i\right) \mathop{\bigcirc\kern-0.78em\triangle} A_r \in M\left(\left(\sum_{i=1}^{r} n_i\right) \times \left(\sum_{i=1}^{r} m_i\right), R\right);$$

$$\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{s} A_{ij} \equiv \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \left(\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{s} A_{ij}\right) \in M\left(\left(\sum_{i=1}^{r}\sum_{j=1}^{s} n_{ij}\right) \times \left(\sum_{i=1}^{r}\sum_{j=1}^{s} m_{ij}\right), R\right); \text{ etc.}$$

In this paper, with few exceptions, we will have no need to extend the iterations of “ $\mathop{\bigcirc\kern-0.78em\triangle}$ ” beyond the double level indicated above.

3) The definition in item (1) above may be extended naturally from individual matrices to subsets of matrices, as follows.

Let $\mathcal{A} \subseteq M(n \times m, R)$ and $\mathcal{B} \subseteq M(p \times q, R)$. We let:

$$\mathcal{A} \mathop{\bigcirc\kern-0.78em\triangle} \mathcal{B} \equiv \{A \mathop{\bigcirc\kern-0.78em\triangle} B \mid A \in \mathcal{A}, B \in \mathcal{B}\} \subseteq M((n+p) \times (m+q), R).$$

Similar to item (2) above, we define the iterates: $\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathcal{A}_i$, $\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{s} \mathcal{A}_{ij}$.

4) Frequently, we will be iterating “ $\mathop{\bigcirc\kern-0.78em\triangle}$ ” over identical matrices, or over identical subsets of matrices. In order to emphasize this, and as an important convenience, we introduce the following notation.

Let $A \in M(n \times m, R)$ and $r \in \mathbb{Z}^+$. We let:

$$A^{(r)} \equiv \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} A \in M(rn \times rm, R).$$

So, $A^{(r)}$ is the “$r$-fold” block-diagonal join of $A$ with itself.

This definition may be naturally extended to subsets of matrices, as follows.

Let $\mathcal{A} \subseteq M(n \times m, R)$ and $r \in \mathbb{Z}^{+}$. We let:

$$\mathcal{A}^{(r)} \equiv \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \mathcal{A} \subseteq M(rn \times rm, R).$$

**N.B.:** By definition: $\mathcal{A}^{(r)} \equiv \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \mathcal{A} = \left\{ \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} A_i \middle| A_i \in \mathcal{A} \right\}$. Take care to note, thus: $\mathcal{A}^{(r)} \neq \left\{ A^{(r)} \middle| A \in \mathcal{A} \right\}$ (unless, of course, $|\mathcal{A}| \leq 1$).

## Part D: Permutation Matrices

These matrices will be used liberally throughout this paper. In particular, the *block permutation matrices*, described below, will be used especially.

Let $R$ be any commutative ring with identity, and let its additive identity element be $0_R$, and let its multiplicative identity element be $1_R$.

1) Let $n \in \mathbb{Z}^{+}$. We let:

the group of permutations on $n$ letters $\equiv S_n$

$\equiv$ the set of bijective elements of $\{1, \ldots, n\}^{\{1,\ldots,n\}}$.

### 2) Basic Permutation Matrices

Let $n \in \mathbb{Z}^{+}$. We let the map $\Pi_n$, a standard map, be defined as follows.

$$\Pi_n \colon S_n \longrightarrow M(n, R) \quad \Pi_n \colon p \longmapsto (a_{ij}), \text{ where } a_{ij} \equiv \begin{cases} 1_R, & i = p(j) \\ 0_R, & \text{else.} \end{cases}$$

So, we note the following.

i) For $A \in M(n, R)$:

$$A\Pi_n(p) = \text{“}A\text{, where column}(i)\ \textit{has become}\ \text{column}(p(i))\text{”}.$$

ii) For $A \in M(n, R)$:

$$\Pi_n(p)A = \text{“}A\text{, where row}(i)\ \textit{has been moved to}\ \text{row}(p(i))\text{”}.$$

iii) $\Pi_n$ is a group imbedding of $S_n$ into $Gl(n, R)$.

iv) For $D \in D(n, R)$:

$$\Pi_n(p)^{-1}\, D\, \Pi_n(p) = \text{“}D\text{, where the } i^{th} \text{ diagonal entry } \textit{has become} \text{ the } p(i)^{th} \text{ diagonal entry”}.$$

v) For $D \in D(n, R)$:

$$\Pi_n(p)\, D\, \Pi_n(p)^{-1} = \text{“}D\text{, where the } i^{th} \text{ diagonal entry } \textit{has been moved to} \text{ the } p(i)^{th} \text{ diagonal entry”}.$$

3) **Block Permutation Matrices**

Let $n \in \mathbb{Z}^+$. We define the map $\widehat{\Pi}_n$, as below. This map generalizes the previous map, $\Pi_n$, to “block” permutation matrices.

$$\widehat{\Pi}_n \colon S_n \times \mathbb{Z}^+ \longrightarrow \bigcup_{i=1}^{\infty} M(in, R)$$

$$\widehat{\Pi}_n \colon (p, a) \longmapsto \text{“ } \Pi_n(p), \text{ with each } \begin{cases} 1_R \text{ ‘replaced by’ } I_a \\ 0_R \text{ ‘replaced by’ } O_a \end{cases} \text{”}.$$

So, for $a \in \mathbb{Z}^+$, we note the following.

i) For $B \in M(an, R)$: $B\widehat{\Pi}_n(p, a)$ = “$B$, where the $i^{th}$ block of ‘$a$’ columns *has become* the $p(i)^{th}$ block of ‘$a$’ columns”.

ii) For $B \in M(an, R)$: $\widehat{\Pi}_n(p, a)B =$ "$B$, where the $i^{th}$ block of '$a$' rows *has been moved to* the $p(i)^{th}$ block of '$a$' rows".

iii) $\widehat{\Pi}_n\Big|(S_n \times \{a\})$ is a group imbedding of $S_n$ into $Gl(an, R)$.

iv) For $E \in M(a, R)^{(n)}$: $\widehat{\Pi}_n(p, a)^{-1}E\widehat{\Pi}_n(p, a) =$ "$E$, where the $i^{th}$ $(a \times a)$–diagonal subblock *has become* the $p(i)^{th}$ $(a \times a)$–diagonal subblock".

v) For $E \in M(a, R)^{(n)}$: $\widehat{\Pi}_n(p, a)E\widehat{\Pi}_n(p, a)^{-1} =$ "$E$, where the $i^{th}$ $(a \times a)$–diagonal subblock *has been moved to* the $p(i)^{th}$ $(a \times a)$–diagonal subblock".

vi) $\Pi_n(p) = \widehat{\Pi}_n(p, 1)$.

4) **Sets of Permutation Matrices**

Let $n, a \in \mathbb{Z}^+$. We define the following sets of permutation matrices.

a) $\text{Perm}(n, R) \equiv Im(\Pi_n) \subseteq Gl(n, R)$. The elements of $\text{Perm}(n, R)$ will be called *basic permutation matrices* on $n$ letters. When clear, they will simply be called permutation matrices.

b) $\text{Perm}(an, I_a, R) \equiv \widehat{\Pi}_n(S_n \times \{a\}) \subseteq Gl(an, R)$. The elements of $\text{Perm}(an, I_a, R)$ will be called $(a \times a)$*–block permutation matrices* on $n$ letters.

So, we note the following.

i) $\text{Perm}(n, R) \approx S_n$.

ii) $\text{Perm}(an, I_a, R) \approx S_n$.

## Part E: Block-diagonal Join of Matrix Maps

In a natural way, we extend the block-diagonal join operator, " $\textcircled{\scriptsize$\triangle$}$ ", from matrices to matrix maps, as follows.

Let $R$ be any commutative ring with identity.

1) Let $X, Y$ be any sets; and let $n, m, p, q \in \mathbb{Z}^+$. Let $f\colon X \to M(n \times m, R)$, $g\colon Y \to M(p \times q, R)$. We let:

   the block-diagonal join of $f$ and $g \equiv f \textcircled{\scriptsize$\triangle$} g$

$$\equiv \left( \begin{array}{c} f \textcircled{\scriptsize$\triangle$} g\colon X \times Y \to M(n \times m, R) \textcircled{\scriptsize$\triangle$} M(p \times q, R) \\ f \textcircled{\scriptsize$\triangle$} g\colon (x, y) \mapsto f(x) \textcircled{\scriptsize$\triangle$} g(y) \end{array} \right).$$

   We note that " $\textcircled{\scriptsize$\triangle$}$ " applies to any two matrix functions; there are no other constraints on the arguments of " $\textcircled{\scriptsize$\triangle$}$ ".

2) As " $\textcircled{\scriptsize$\triangle$}$ " is virtually, but not actually, associative on matrix maps, we define its iterates in the following obvious and explicit way:

$$\mathop{\textcircled{\scriptsize$\triangle$}}_{i=1}^{r} f_i \equiv \left( \begin{array}{c} \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} f_i\colon \prod\limits_{i=1}^{r} X_i \to \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} M(n_i \times m_i, R) \\ \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} f_i\colon (M_1, \ldots, M_r) \mapsto \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} f_i(M_i) \end{array} \right);$$

$$\mathop{\textcircled{\scriptsize$\triangle$}}_{i=1}^{r} \mathop{\textcircled{\scriptsize$\triangle$}}_{j=1}^{s} f_{ij} \equiv \left( \begin{array}{c} \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{j=1}^{s} f_{ij}\colon \prod\limits_{i=1}^{r} \prod\limits_{j=1}^{s} X_{ij} \to \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{j=1}^{s} M(n_{ij} \times m_{ij}, R) \\ \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{j=1}^{s} f_{ij}\colon (M_{1,1}, \ldots, \ldots, M_{r,s}) \mapsto \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{\scriptsize$\triangle$}}\limits_{j=1}^{s} f_{ij}(M_{i,j}) \end{array} \right); \text{ etc.}$$

3) Additionally, as an important convenience when iterating " $\textcircled{\scriptsize$\triangle$}$ " over identical functions, we introduce the following notation.

Let $f\colon X \to M(n \times m, R)$, and let $r \in \mathbb{Z}^{+}$. We let:

$$f^{(r)} \equiv \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{r} f;\ \text{so that } f^{(r)}\colon X^{r} \to M(n \times m, R)^{(r)}.$$

## Part F: Definitions Referring To "Rationalizing"

We make the following definitions, which refer to the notion of "rationalizing", and which will be used liberally throughout the paper.

Let $R$ be a commutative ring with identity. Let $A \subseteq R$ be a subring. Let $n \in \mathbb{Z}^{+}$, $\mathcal{Y} \subseteq M(n, R)$, $P \in G\ell(n, R)$. We let:

1) $P$ $A$–rationalizes $\mathcal{Y} \overset{def}{\iff} P\mathcal{Y}P^{-1} \subseteq M(n, A)$.

2) $\mathcal{Y}$ is $A$–rationalizable over $R \overset{def}{\iff} \exists P \in G\ell(n, R)\colon$ $P$ $A$–rationalizes $\mathcal{Y}$.

In most of our applications, we will have a field extension, $L/k$, and, in the above definitions, we will be taking $R \equiv L$, $A \equiv k$.

## Part G: Matrix Centralizers and Normalizers

We make the following definitions for the centralizer and normalizer of subsets of matrices. The former will be used liberally throughout the paper, and the latter will be used liberally throughout the latter part of the paper.

Let $R$ be a commutative ring with identity. Let $n \in \mathbb{Z}^{+}$, $\mathcal{A} \subseteq M(n, R)$. We let:

1) the centralizer of $\mathcal{A}$ in $M(n, R)$ $\equiv C_R(\mathcal{A})$

$$\equiv \{M \in M(n, R) \mid \forall A \in \mathcal{A}\colon\ MA = AM\} \subseteq M(n, R).$$

2) the normalizer of $\mathcal{A}$ in $G\ell(n,R) \equiv N_R(\mathcal{A})$

$$\equiv \{P \in G\ell(n,R) | P^{-1}\mathcal{A}P = \mathcal{A}\} \subseteq G\ell(n,R).$$

## 1.3 Basic Notation–Specific

The notation defined here refers to constructs that are probably very specific to this paper. The constructs, 'field element' and 'field setting', defined below, are both simple and fundamental to this paper. Their definitions were motivated out of what (for the most part) seemed to be the objects frequently recurring in at least both the main arguments and conclusions of this paper. They also seem to be (for the most part) perhaps the fundamental objects upon which at least the main the arguments and results of this paper refer.

Please note that these constructs are not intended to represent anything rich or deep, and are mainly intended as what seems a natural convenience.

These constructs, together with the several functions defined on them below, are the constructs with which most definitions are made, with which most results are stated, and are used throughout this paper. Note that the functions defined below on these constructs would seem to have, at times, a richer and deeper structure.

Here, as virtually throughout this paper, *we take $k$ to be a perfect field.* (So, in particular, $k$ can be any field of characteristic 0, or any finite field.)

### 1.3.1 Field Elements

*A field element over* $k$, say $\phi$, is a triple: $\phi = (K, \sigma, a)$, where:

i) $k \subseteq K \subseteq \overline{k}$, and $K/k$ is a finite extension of fields;

ii) $\sigma$ is an enumerator for $Iso(K/k)$;

iii) $a \in \mathbb{Z}^+$.

We immediately note the following: $\sigma\colon \{1, \ldots, n\} \xrightarrow{bij} Iso(K/k)$, where $n \equiv |Iso(K/k)| = [K : k]$. (The final equality being true as $k$ is perfect.)

*When clear, we will denote* $\sigma(i)$ *by* $\sigma_i$.

### 1.3.2 Basic Functions on Field Elements

Let $\phi = (K, \sigma, a)$ be a field element over $k$.

We make the following definitions.

i) $K_\phi \equiv K$; $\sigma^{(\phi)} \equiv \sigma$; $a_\phi \equiv a$.

ii) $n_\phi \equiv [K\colon k] = |Iso(K/k)| \in \mathbb{Z}^+$.

iii) $\dim \phi \equiv a n_\phi \in \mathbb{Z}^+$.

iv) The map $\Delta_\phi$ is defined as follows:

$$\Delta_\phi\colon M(a, K) \to \mathop{\bigcirc\kern-0.95em\triangle}\limits_{i=1}^{n_\phi} M\left(a, \sigma_i(K)\right)$$

$$\Delta_\phi\colon M \mapsto \mathop{\bigcirc\kern-0.95em\triangle}\limits_{i=1}^{n_\phi} \sigma_i(M).$$

Clearly, $\Delta_\phi$ is a $k$-algebra imbedding.

**Remarks**

a) Clearly, we have the following.

   i) $Im(\Delta_\phi) \subseteq M(a, \overline{k})^{(n_\phi)}$.

   In particular, $Im(\Delta_\phi) \subseteq M(\dim \phi, \overline{k})$.

   ii) In fact, $Im(\Delta_\phi) \subseteq M(a, E)^{(n_\phi)}$ and $Im(\Delta_\phi) \subseteq M(\dim \phi, E)$, where $E$ is any intermediate field of $\overline{k}/k$ containing $\bigcup\{\sigma(K) | \sigma \in Iso(K/k)\}$.

These observations will be used throughout the paper.

b) Clearly we have:

$$\sigma \colon \{1, \dots, n_\phi\} \xrightarrow{bij} Iso(K/k).$$

This observation will also be used throughout the paper.

### 1.3.3 Parameterized Functions on Field Elements

Let $\phi = (K, \sigma, a)$ be a field element over $k$.

We make the following definitions.

#### a) Matrices of a Field Element

Let $N \in \mathbb{Z}^+$. We let:

$$V_{N,\phi} \equiv \left\{ \bigoplus_{j=1}^{n_\phi} \sigma_j(Q) \middle| Q \in M(N \times a, K) \right\} \subseteq M(N \times an_\phi, \overline{k}).$$

Then we may say that $V_{N,\phi}$ is the set of matrices (necessarily $N \times an_\phi$) consisting of the $K/k$–conjugates of the matrices of $M(N \times a, K)$, laid out, horizontally, in " $\sigma$ " order.

## b) Permutation Matrices of a Field Element

Let $E$ be any intermediate field of $\overline{k}/k$ containing $\bigcup\{\sigma(K) | \sigma \in Iso(K/k)\}$.

Let $\tau \in Iso(E/k)$ and $\gamma \in Gal(K/k)$.

We let the following be defined.

1) i) $\mu_{\tau,\phi}: Iso(K/k) \to Iso(K/k)$, $\mu_{\tau,\phi}: \theta \mapsto \tau \circ \theta$.

Clearly, $\mu_{\tau,\phi}$ is bijective.

Clearly, also, we may say that $\mu_{\tau,\phi}$ is " left-multiplication by $\tau$ ".

ii) $p_{\tau,\phi} \equiv \sigma^{-1} \circ \mu_{\tau,\phi} \circ \sigma: \{1, \ldots, n_\phi\} \to \{1, \ldots, n_\phi\}$.

Clearly, $p_{\tau,\phi} \in S_{n_\phi}$, as both $\sigma$ and $\mu_{\tau,\phi}$ are bijections.

Clearly, also, we may say that $p_{\tau,\phi}$ is " the index–representation of left-multiplication by $\tau$, according to $\sigma$ ".

iii) $\Pi_{\tau,\phi} \equiv \widehat{\Pi}_{n_\phi}(p_{\tau,\phi}, a) \in \mathrm{Perm}(an_\phi, I_a, k)$.

Clearly, we may say that $\Pi_{\tau,\phi}$ is the (canonical) representation of $p_{\tau,\phi}$ as an $(a \times a)$–block permutation matrix.

2) i) $\nu_{\gamma,\phi}: Iso(K/k) \to Iso(K/k)$, $\nu_{\gamma,\phi}: \delta \mapsto \delta \circ \gamma^{-1}$.

Clearly, $\nu_{\gamma,\phi}$ is bijective.

Clearly, also, we may say that $\nu_{\gamma,\phi}$ is " right-multiplication by $\gamma^{-1}$ ".

ii) $r_{\gamma,\phi} \equiv \sigma^{-1} \circ \nu_{\gamma,\phi} \circ \sigma \colon \{1,\ldots,n_\phi\} \to \{1,\ldots,n_\phi\}$.

Clearly, $r_{\gamma,\phi} \in S_{n_\phi}$, as both $\sigma$ and $\nu_{\gamma,\phi}$ are bijections.

Clearly, also, we may say that $r_{\gamma,\phi}$ is " the index-representation of right-multiplication by $\gamma^{-1}$, according to $\sigma$ ".

iii) $\Gamma_{\gamma,\phi} \equiv \widehat{\Pi}_{n_\phi}(r_{\gamma,\phi}, a) \in \mathrm{Perm}(an_\phi, I_a, k)$.

Clearly, we may say that $\Gamma_{\gamma,\phi}$ is the (canonical) representation of $r_{\gamma,\phi}$ as an $(a \times a)$–block permutation matrix.

### 1.3.4 Field Settings

*A field setting over* $k$, say $\Phi$, is a finite sequence of field elements over $k$: $\Phi = (\phi_1, \ldots, \phi_r)$, where:

i) $r \in \mathbb{Z}^+$;

ii) $\forall i \in \{1,\ldots,r\}$: $\phi_i = (K_i, \sigma^{(i)}, a_i)$ is a field element over $k$.

*When clear, we will denote* $\sigma^{(i)}(j)$ *by* $\sigma_j^{(i)}$.

### 1.3.5 Basic Functions on Field Settings

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

We make the following definitions.

i) $n_\Phi \equiv \sum_{i=1}^{r} n_{\phi_i} = \sum_{i=1}^{r} [K_i : k]$.

ii) $\dim \Phi \equiv \sum_{i=1}^{r} \dim \phi_i = \sum_{i=1}^{r} a_i [K_i : k]$.

iii) The map $\Delta_\Phi$ is defined as follows:

$$\Delta_\Phi \equiv \bigoplus_{i=1}^{r} \Delta_{\phi_i} \colon \prod_{i=1}^{r} M(a_i, K_i) \to \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_{\phi_i}} M\left(a_i, \sigma_j^{(i)}(K_i)\right)$$

$$\Delta_\Phi \colon (M_1, \ldots, M_r) \mapsto \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(M_i).$$

Clearly, $\Delta_\Phi$ is a $k$-algebra imbedding.

## Remarks

a) Clearly, we have the following.

i) $Im(\Delta_\Phi) \subseteq \bigoplus_{i=1}^{r} M(a_i, \overline{k})^{(n_{\phi_i})}$.

In particular, $Im(\Delta_\Phi) \subseteq M(\dim \Phi, \overline{k})$.

ii) In fact, $Im(\Delta_\Phi) \subseteq \bigoplus_{i=1}^{r} M(a_i, E)^{(n_{\phi_i})}$ and $Im(\Delta_\Phi) \subseteq M(\dim \Phi, E)$, where $E$ is any intermediate field of $\overline{k}/k$ containing $\bigcup_{i=1}^{r} \bigcup \{\sigma(K_i) | \sigma \in Iso(K_i/k)\}$.

These observations will be used throughout the paper.

b) Clearly, we have:

$$\sigma^{(i)} \colon \{1, \ldots, n_{\phi_i}\} \overset{bij}{\to} Iso(K_i/k).$$

This observation will also be used throughout the paper.

### 1.3.6 Parameterized Functions on Field Settings

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

We make the following definitions.

**a) Matrices of a Field Setting**

We let:

$$V_\Phi \equiv \mathop{\textcircled{$\|$}}\limits_{i=1}^{r} V_{\dim \Phi, \phi_i} \subseteq M(\dim \Phi, \overline{k}).$$

**b) Permutation Matrices of a Field Setting**

Let $E$ be any intermediate field of $\overline{k}/k$ containing $\bigcup_{i=1}^{r} \bigcup \{\sigma(K_i) | \sigma \in Iso(K_i/k)\}$.

Let $\tau \in Iso(E/k)$ and $\vec{\gamma} = (\gamma_1, \ldots, \gamma_r) \in \prod_{i=1}^{r} Gal(K_i/k)$.

We let the following be defined.

1) $\Pi_{\tau,\Phi} \equiv \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \Pi_{\tau,\phi_i} \in \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k).$

2) $\Gamma_{\vec{\gamma},\Phi} \equiv \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \Gamma_{\gamma_i,\phi_i} \in \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k).$

### 1.3.7 Indexing Scheme Induced by a Field Setting for Diagonal Matrices

Frequently in this paper, we will be working with diagonal matrices. A field setting naturally induces a useful, but non-standard, way of indexing the diagonal entries of a diagonal matrix. We define this below.

## a) Standard Indexing Scheme for Diagonal Matrices

Let $n \in \mathbb{Z}^+$, $R$ be a ring.

Let $Y \in D(n, R)$.

We make the following standard definition.

For $i \in \{1, \ldots, r\}$, we let:

$$Y_i \equiv \text{the } i^{\underline{th}} \text{ diagonal entry of } Y; \text{ so that } Y_i \in R.$$

## b) Indexing Scheme Induced by a Field Setting for Diagonal Matrices

Let $k$ be a perfect field.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

We make the following definitions.

1) $\mathcal{I}_\Phi \equiv \bigcup_{i=1}^{r} (\{i\} \times \{1, \ldots, n_{\phi_i}\} \times \{1, \ldots, a_i\}) \subseteq (\mathbb{Z}^+)^3$.

We observe easily:

$$|\mathcal{I}_\Phi| = \sum_{i=1}^{r} a_i n_{\phi_i} = \dim \Phi.$$

2) The map $h_\Phi$ is defined as follows:

$$h_\Phi \colon \mathcal{I}_\Phi \longrightarrow \{1, \ldots, \dim \Phi\}$$

$$h_\Phi \colon (i, j, t) \longmapsto \left( \sum_{g=1}^{i-1} a_g n_{\phi_g} \right) + (j - 1) a_i + t.$$

It is easy to check that $h_\Phi$ is bijective.

3) For $Y \in D(\dim\Phi, R)$, and $(i,j,t) \in \mathcal{I}_\Phi$, we let:

$$Y_{(i,j,t)} \equiv Y_{h_\Phi(i,j,t)} = \text{the } h_\Phi(i,j,t)^{\underline{th}} \text{ diagonal entry of } Y;$$

$$\text{so that} \quad Y_{(i,j,t)} \in R.$$

The above indexing scheme, " $Y_{(i,j,t)}$ ", will be called *the 3-tuple indexing scheme of* $\Phi$. Its principal use and convenience derives from the following observation, which follows at once from the constructions of the maps $h_\Phi$ and $\Delta_\Phi$.

**Observation**

For $i \in \{1,\ldots,r\}$, let $D^{(i)} \in D(a_i, K_i)$.

Let $Y \equiv \Delta_\Phi(D^{(1)},\ldots,D^{(r)}) \in D(\dim\Phi, \overline{k})$.

Then, clearly, by construction of the maps $h_\Phi$ and $\Delta_\Phi$, we have:

$$Y_{(i,j,t)} = \sigma_j^{(i)}(D_t^{(i)}).$$

(Here, of course, $D_t^{(i)}$ = the $t^{\underline{th}}$ diagonal entry of the diagonal matrix $D^{(i)}$; so that $D_t^{(i)} \in K_i$; the notation in the quantity, " $D_t^{(i)}$ ", being a use of the standard indexing scheme for diagonal matrices, as described in part (a) above.)

## 1.4 Basic Lemmas

Throughout this section, $k$ *is a perfect field.*

Additionally, for $A$ any invertible matrix, we let $conj_A(M) \equiv AMA^{-1}$. (Notice that $conj_{A^{-1}}(M) = A^{-1}MA$.)

### 1.4.1 On Block-Diagonal Joins of Square Matrices

The following fundamental and simple lemma, concerning block-diagonal joins of square matrices, will be used many times.

**Lemma 1.D.1**

Let $R$ be a ring.

Let $n \in \mathbb{Z}^+$; $a_1, \ldots, a_n \in \mathbb{Z}^+$.

Let $\sigma \in S_n$.

Let $P_\sigma$ be the map defined by:

$$P_\sigma \colon \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n} M(a_i, R) \longrightarrow \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n} M(a_{\sigma(i)}, R)$$

$$P_\sigma \colon \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n} A_i \longmapsto \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n} A_{\sigma(i)}.$$

**Then:** $\exists \Pi \in \mathrm{Perm}(a_1 + \cdots + a_n, R)$: $P_\sigma = conj_\Pi$.

**Proof.**

Clearly, it suffices to prove the result for $n = 2$.

Let $a, b \in \mathbb{Z}^+$. We will show that, for some $\Pi \in \mathrm{Perm}(a+b, R)$, we have $\Pi(A \mathbin{\triangle\!\!\!\!\!\bigcirc} B)\Pi^{-1} = B \mathbin{\triangle\!\!\!\!\!\bigcirc} A$, for all $A \in M(a, R)$, $B \in M(b, R)$. WLOG, we may assume $a \le b$, for then the other case follows by using $\Pi^{-1}$.

Define the following permutation matrices (recall that here $b - a \ge 0$):

$$\xi \equiv \begin{bmatrix} O & O & I_a \\ O & I_{b-a} & O \\ I_a & O & O \end{bmatrix}, \quad \Psi \equiv \begin{bmatrix} O & I_{b-a} & O \\ I_a & O & O \\ O & O & I_a \end{bmatrix};$$

and let $\Pi \equiv \Psi\xi$. Clearly, we have $\xi^{-1} = \xi$, $\Psi^{-1} = \Psi$, and $\xi, \Psi, \Pi \in \mathrm{Perm}(a+b, R)$. For $A \in M(a, R)$ and $B \in M(b, R)$, we calculate and follow the matrix multiplications as below, where the matrices $B^{(1)}, B^{(2)}, B^{(3)}, B^{(4)}$ have, respectively, the dimensions $(b-a) \times b$, $a \times b$, $b \times (b-a)$, $b \times a$.

$$\begin{aligned}
\Pi(A \mathbin{\triangle\!\!\!\!\!\bigcirc} B)\Pi^{-1} &= (\Psi\xi)(A \mathbin{\triangle\!\!\!\!\!\bigcirc} B)(\xi^{-1}\Psi^{-1}) \\
&= (\Psi\xi) \begin{bmatrix} A & O \\ O & B \end{bmatrix} (\xi^{-1}\Psi^{-1}) \\
&= \Psi \begin{bmatrix} O & O & I_a \\ O & I_{b-a} & O \\ I_a & O & O \end{bmatrix} \begin{bmatrix} A & O \\ O & B^{(1)} \\ O & B^{(2)} \end{bmatrix} (\xi^{-1}\Psi^{-1})
\end{aligned}$$

$$= \Psi \begin{bmatrix} \bigcirc & B^{(2)} \\ \bigcirc & B^{(1)} \\ A & \bigcirc \end{bmatrix} (\xi^{-1}\Psi^{-1})$$

$$= \begin{bmatrix} \bigcirc & I_{b-a} & \bigcirc \\ I_a & \bigcirc & \bigcirc \\ \bigcirc & \bigcirc & I_a \end{bmatrix} \begin{bmatrix} \bigcirc & B^{(2)} \\ \bigcirc & B^{(1)} \\ A & \bigcirc \end{bmatrix} (\xi^{-1}\Psi^{-1})$$

$$= \begin{bmatrix} \bigcirc & B \\ A & \bigcirc \end{bmatrix} (\xi^{-1}\Psi^{-1})$$

$$= \begin{bmatrix} \bigcirc & B^{(3)} & B^{(4)} \\ A & \bigcirc & \bigcirc \end{bmatrix} \begin{bmatrix} \bigcirc & \bigcirc & I_a \\ \bigcirc & I_{b-a} & \bigcirc \\ I_a & \bigcirc & \bigcirc \end{bmatrix} \Psi^{-1} \qquad [\text{as } \ \xi^{-1} = \xi]$$

$$= \begin{bmatrix} B^{(4)} & B^{(3)} & \bigcirc \\ \bigcirc & \bigcirc & A \end{bmatrix} \Psi^{-1}$$

$$= \begin{bmatrix} B^{(4)} & B^{(3)} & \bigcirc \\ \bigcirc & \bigcirc & A \end{bmatrix} \begin{bmatrix} \bigcirc & I_{b-a} & \bigcirc \\ I_a\bigcirc & \bigcirc & \\ \bigcirc & \bigcirc & I_a \end{bmatrix} \qquad [\text{as } \ \Psi^{-1} = \Psi]$$

$$= \begin{bmatrix} B & \bigcirc \\ \bigcirc & A \end{bmatrix}$$

$$= B \mathbin{\bigcirc\!\!\!\!\!\triangle} A.$$

Thus, we have: $\Pi \in \mathrm{Perm}(a+b, R)$; and, for all $A \in M(a,R)$ and $B \in M(b,R)$, we have $\Pi(A \mathbin{\bigcirc\!\!\!\!\!\triangle} B)\Pi^{-1} = B \mathbin{\bigcirc\!\!\!\!\!\triangle} A$. □

### 1.4.2 On the Permutation Matrices of Field Elements and Field Settings

The following lemmas concern some fundamental properties of the permutation matrices defined in Sections 1.3.3 and 1.3.6. Some of these lemmas will be used often.

**Lemma 1.D.2**

Let $\phi = (K, \sigma, a)$ be a field element over $k$.

Let $E$ be any intermediate field of $\overline{k}/k$ which contains $\bigcup \{\sigma(K) | \sigma \in Iso(K/k)\}$.

Let $\tau \in Iso(E/k)$ and $\gamma \in Gal(K/k)$.

**Then:**

a) $Im(\Delta_\phi) \subseteq M(\dim \phi, E)$.

b) $\forall M \in M(a, K)$: $\tau(\Delta_\phi(M)) = \Pi_{\tau,\phi}^{-1} \Delta_\phi(M) \Pi_{\tau,\phi}$.

c) $\forall M \in M(a, K)$: $\Delta_\phi(\gamma(M)) = \Gamma_{\gamma^{-1},\phi}^{-1} \Delta_\phi(M) \Gamma_{\gamma^{-1},\phi}$.

d) $\Pi_{\tau,\phi}$ and $\Gamma_{\gamma,\phi}$ commute.

e) i) The map, $(f : Gal(K/k) \to \mathrm{Perm}(an_\phi, I_a, k), f : \gamma \mapsto \Gamma_{\gamma,\phi})$, is a group imbedding.

  ii) $Gal(K/k) \approx \{\Gamma_{\gamma,\phi} | \gamma \in Gal(K/k)\} \subseteq \mathrm{Perm}(an_\phi, I_a, k)$.

f) $\forall N \in \mathbb{Z}^+ : \forall V \in V_{N,\phi}$: $\tau(V) = V \Pi_{\tau,\phi}$.

**Proof.**

a) This is immediate by construction of the map $\Delta_\phi$.

b) Let $M \in M(a, K)$. We calculate as below, using Sections 1.3.2 and 1.3.3.

$$\begin{aligned}
\tau\left(\Delta_\phi(M)\right) &= \tau\left(\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \sigma_j(M)\right) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} (\tau \circ \sigma_j)(M) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left(\mu_{\tau,\phi}(\sigma_j)\right)(M) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left((\mu_{\tau,\phi} \circ \sigma)(j)\right)(M) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \Big((\sigma \circ \sigma^{-1} \circ \mu_{\tau,\phi} \circ \sigma)(j)\Big)(M) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left((\sigma \circ p_{\tau,\phi})(j)\right)(M) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left(\sigma\left(p_{\tau,\phi}(j)\right)\right)(M) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \sigma_{p_{\tau,\phi}(j)}(M) \\
&= \left(\widehat{\Pi}_{n_\phi}(p_{\tau,\phi}, a)\right)^{-1} \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \sigma_j(M)\right] \widehat{\Pi}_{n_\phi}(p_{\tau,\phi}, a) \\
&= {\Pi_{\tau,\phi}}^{-1} \left[\Delta_\phi(M)\right] \Pi_{\tau,\phi}.
\end{aligned}$$

(The second-to-last equality above is provided by Section 1.2.4, Part D, subpart (3), item (iv). The last equality above follows by definition of $\Pi_{\tau,\phi}$.)

c) Let $M \in M(a, K)$. Then we calculate as below, similar to the previous.

$$\begin{aligned}
\Delta_\phi\left(\gamma(M)\right) &= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \sigma_j\left(\gamma(M)\right) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left(\nu_{\gamma^{-1},\phi}(\sigma_j)\right)(M) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left((\nu_{\gamma^{-1},\phi} \circ \sigma)(j)\right)(M) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \Big((\sigma \circ \sigma^{-1} \circ \nu_{\gamma^{-1},\phi} \circ \sigma)(j)\Big)(M) \\
&= \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \left((\sigma \circ r_{\gamma^{-1},\phi})(j)\right)(M) \\
&= \left(\widehat{\Pi}_{n_\phi}(r_{\gamma^{-1},\phi}, a)\right)^{-1} \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n_\phi} \sigma_j(M)\right] \widehat{\Pi}_{n_\phi}(r_{\gamma^{-1},\phi}, a) \\
&= \Gamma_{\gamma^{-1},\phi}^{-1} \left[\Delta_\phi(M)\right] \Gamma_{\gamma^{-1},\phi}.
\end{aligned}$$

d) We prove the desired result (d) in three simple steps, as below.

i) Let $\omega \in Iso(K/k)$. We observe the following.

$$\begin{aligned}(\nu_{\gamma,\phi} \circ \mu_{\tau,\phi})(\omega) &= \nu_{\gamma,\phi}(\mu_{\tau,\phi}(\omega)) &&= (\mu_{\tau,\phi}(\omega)) \circ \gamma^{-1} &&= (\tau \circ \omega) \circ \gamma^{-1} \\ &= \tau \circ (\omega \circ \gamma^{-1}) &&= \tau \circ (\nu_{\gamma,\phi}(\omega)) &&= \mu_{\tau,\phi}(\nu_{\gamma,\phi}(\omega)) \\ &= (\mu_{\tau,\phi} \circ \nu_{\gamma,\phi})(\omega).\end{aligned}$$

As $\omega$ is arbitrary in the above, we conclude:

$$\nu_{\gamma,\phi} \circ \mu_{\tau,\phi} = \mu_{\tau,\phi} \circ \nu_{\gamma,\phi}.$$

ii) As $p_{\tau,\phi} = \sigma^{-1} \circ \mu_{\tau,\phi} \circ \sigma$ and $r_{\gamma,\phi} = \sigma^{-1} \circ \nu_{\gamma,\phi} \circ \sigma$, the previous conclusion shows at once that $p_{\tau,\phi}$ and $r_{\gamma,\phi}$ commute.

iii) As $\Pi_{\tau,\phi} = \widehat{\Pi}_{n_\phi}(p_{\tau,\phi}, a)$ and $\Gamma_{\gamma,\phi} = \widehat{\Pi}_{n_\phi}(r_{\gamma,\phi}, a)$, and as $\widehat{\Pi}_{n_\phi}\big| (S_{n_\phi} \times \{a\})$ is a group homomorphism [as it is a group imbedding] of $S_{n_\phi}$, clearly the result of step (ii) above shows at once that $\Pi_{\tau,\phi}$ and $\Gamma_{\gamma,\phi}$ commute.

e) i) Let the map $f$ be defined as:

$$f: Gal(K/k) \to \mathrm{Perm}(an_\phi, I_a, k) \ , \ f: \gamma \mapsto \Gamma_{\gamma,\phi}.$$

That $f$ is a group imbedding follows at once, since, clearly, $f(\gamma) = \Gamma_{\gamma,\phi} = \widehat{\Pi}_{n_\phi}(r_{\gamma,\phi}, a) = \widehat{\Pi}_{n_\phi}(\sigma^{-1} \circ \nu_{\gamma,\phi} \circ \sigma, a)$ and all of the following three maps are group imbeddings: $\widehat{\Pi}_{n_\phi}\big| (S_{n_\phi} \times \{a\})$, "$\sigma^{-1} \circ (\cdot) \circ \sigma$", "$\nu_{(\cdot),\phi}$."

(The last fact follows as, clearly:

$$\begin{aligned}\nu_{\gamma\gamma',\phi}(\omega) &= \omega\circ(\gamma\gamma')^{-1}\\ &= \omega\circ\gamma'^{-1}\circ\gamma^{-1}\\ &= (\nu_{\gamma',\phi}(\omega))\circ\gamma^{-1}\\ &= \nu_{\gamma,\phi}\left(\nu_{\gamma',\phi}(\omega)\right)\\ &= (\nu_{\gamma,\phi}\circ\nu_{\gamma',\phi})(\omega),\end{aligned}$$

for all $\omega\in Iso(K/k)$;

and

$$\begin{aligned}&\nu_{\gamma,\phi}=\nu_{\gamma',\phi}\\ &\Rightarrow \nu_{\gamma,\phi}(id_K)=\nu_{\gamma',\phi}(id_K)\\ &\Rightarrow id_K\circ\gamma^{-1}=id_K\circ\gamma'^{-1}\\ &\Rightarrow \gamma^{-1}=\gamma'^{-1}\\ &\Rightarrow \gamma=\gamma'.\end{aligned}$$

)

ii) As the map $f$ defined above is a group imbedding, we have at once that:

$$Gal(K/k)\approx Im(f)\subseteq \mathrm{Perm}(an_\phi, I_a, k);$$

and here,

$$Im(f)=\{\Gamma_{\gamma,\phi}|\gamma\in Gal(K/k)\}.$$

f) Let $N\in\mathbb{Z}^+$, and $V\in V_{N,\phi}$. So, by definition of $V_{N,\phi}$, we have:

$$(1)\qquad V=\mathop{\bigcirc\mkern-15mu\Vert}\limits_{j=1}^{n_\phi}\sigma_j(Q),\ \text{ for some } Q\in M(N\times a,K).$$

We calculate as below, following the same steps as in part (b) above:

$$\begin{aligned}
\tau(V) &= \tau\left(\mathop{⦷}_{j=1}^{n_\phi} \sigma_j(Q)\right)\\
&= \mathop{⦷}_{j=1}^{n_\phi} (\tau \circ \sigma_j)(Q) = \mathop{⦷}_{j=1}^{n_\phi} \left(\mu_{\tau,\phi}(\sigma_j)\right)(Q)\\
&= (\dots \text{ exactly as in part (b) above } \dots)\\
&= \mathop{⦷}_{j=1}^{n_\phi} \sigma_{p_{\tau,\phi}(j)}(Q)\\
&= \left[\mathop{⦷}_{j=1}^{n_\phi} \sigma_j(Q)\right] \widehat{\Pi}_{n_\phi}(p_{\tau,\phi}, a)\\
&= V\Pi_{\tau,\phi}.
\end{aligned}$$

(The second-to-last equality above is provided by Section 1.2.4, Part D, subpart (3), item (i). The last equality above follows by (1) above and the definition of $\Pi_{\tau,\phi}$.)

□

**Lemma 1.D.3**

Let $\Phi = (\phi_1, \dots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

Let $E$ be any intermediate field of $\bar{k}/k$ containing $\bigcup_{i=1}^{r} \bigcup\{\sigma(K_i) | \sigma \in Iso(K_i/k)\}$.

Let $\tau \in Iso(E/k)$ and $\vec{\gamma} = (\gamma_1, \dots, \gamma_r) \in \Pi_{i=1}^{r} Gal(K_i/k)$,

and let $\overrightarrow{\gamma^{-1}} \equiv (\gamma_1^{-1}, \dots, \gamma_r^{-1}) \in \Pi_{i=1}^{r} Gal(K_i/k)$.

**Then:**

a) $Im(\Delta_\Phi) \subseteq M(\dim \Phi, E)$.

b) $\forall M = (M_1, \ldots, M_r) \in \prod_{i=1}^{r} M(a_i, K_i)$:

$$\tau\left(\Delta_\Phi(M)\right) = \Pi_{\tau,\Phi}^{-1} \Delta_\Phi(M) \Pi_{\tau,\Phi}.$$

c) $\forall M = (M_1, \ldots, M_r) \in \prod_{i=1}^{r} M(a_i, K_i)$:

$$\Delta_\Phi\left((\gamma_1(M_1), \ldots, \gamma_r(M_r))\right) = \Gamma^{-1}_{\overrightarrow{\gamma^{-1}},\Phi} \Delta_\Phi(M) \Gamma_{\overrightarrow{\gamma^{-1}},\Phi}.$$

d) $\Pi_{\tau,\Phi}$ and $\Gamma_{\vec{\gamma},\Phi}$ commute.

e) $\forall V \in V_\Phi$: $\tau(V) = V\Pi_{\tau,\Phi}$.

**Proof.**

a) This follows immediately by construction of the map $\Delta_\Phi$.

b,c,d,e) These results follow at once from the definitions of $\Pi_{\tau,\Phi} = \mathop{\textcircled{$\vartriangle$}}_{i=1}^{r} \Pi_{\tau,\phi_i}$ and $\Gamma_{\vec{\gamma},\Phi} = \mathop{\textcircled{$\vartriangle$}}_{i=1}^{r} \Gamma_{\gamma_i,\phi_i}$, and the results of the previous Lemma 1.D.2.

□

### 1.4.3 The Galois Group of a Field Element

This is a fairly simple and natural definition, made largely for later convenience.

Let $\phi$ be a field element over $k$. We let:

$$\begin{aligned}\text{the Galois Group of } \phi \text{ over } k \ &\equiv Gal(\phi/k) \\ &\equiv \left\{\Gamma_{\gamma,\phi} \middle| \gamma \in Gal(K_\phi/k)\right\} \subseteq \text{Perm}\left(a_\phi n_\phi, I_{a_\phi}, k\right).\end{aligned}$$

Thus, by Lemma 1.D.2, part (e), we have at once:

$Gal(\phi/k)$ is, indeed, a group, and is a group of permutation matrices,

and

$$Gal(\phi/k) \approx Gal(K_\phi/k).$$

### 1.4.4 A Fundamental Equivalence Relation on Field Elements, and on Field Settings

Here, we introduce a fundamental equivalence relation on field elements, and a related one on field settings. Both are fairly simple, and will be of main importance, later, in the work on normalizers.

**a) On Field Elements**

Let $\phi = (K, \sigma, a)$ and $\theta = (L, \tau, b)$ be two field elements over $k$. We let:

$\phi$ is $k$–equivalent to $\theta \equiv \phi \sim_k \theta \overset{\text{def}}{\Longleftrightarrow} K \sim_k L$ and $a = b$.

Clearly, $\sim_k$ is an equivalence relation on the set of field elements over $k$.

## b) On Field Settings

Let $\Phi = (\phi_1, \ldots, \phi_r)$ and $\Omega = (\omega_1, \ldots, \omega_s)$ be two field settings over $k$. We let:

$\Phi$ is $k$–equivalent to $\Omega \equiv \Phi \sim_k \Omega \overset{\text{def}}{\Longleftrightarrow}$

$$r = s \text{ and } \exists p \in S_r : \forall i \in \{1, \ldots, r\}: \ \phi_{p(i)} \sim_k \omega_i.$$

By part (a) above, clearly $\sim_k$ is an equivalence relation on the set of field settings over $k$.

## c) Lemmas

In addition to a few preliminary items, the following two lemmas describe, respectively, the connection between the "$\Delta$"–maps of $k$–equivalent field elements, and of $k$–equivalent field settings.

For the purposes of these two lemmas, we make the following specific definition. Suppose $f$ is a function of two arguments: a positive integer, $a$, and an intermediate field of $\overline{k}/k$, $K$, and such that $f(a, K) \subseteq M(a, K)$. We will call such a function *k-morphic* if, whenever $\sigma \in Iso(K/k)$, we have $\sigma\left(f(a, K)\right) = f\left(a, \sigma(K)\right)$. (Note that $f\left(a, \sigma(K)\right) \subseteq M\left(a, \sigma(K)\right)$, by supposition on $f$ here.) Examples of such $k$–morphic functions include: $f(a, K) = M(a, K)$, $f(a, K) = \text{Scalar}(a, K)$, $f(a, K) = \text{Perm}(a, K)$, etc.

**Lemma 1.D.4**

Let $\phi = (K, \sigma, a)$, $\theta = (L, \tau, b)$ be two $k$–equivalent field elements over $k$.

**Then:**

1) $a = b$, $n_\phi = n_\theta$, $\dim \phi = \dim \theta$.

2) $\exists \eta \in Iso(K/k)\colon \exists \Pi \in \mathrm{Perm}(an_\phi, I_a, k)$:

   a) $\eta(K) = L$;

   b) $M \in M(a, K) \Rightarrow \Delta_\phi(M) = \Pi \Delta_\theta(\eta(M))\,\Pi^{-1}$;

   c) i) $f$ a $k$–morphic function $\Rightarrow \Delta_\phi(f(a, K)) = \Pi \Delta_\theta(f(b, L))\,\Pi^{-1}$,

      ii) $\Delta_\phi(M(a, K)) = \Pi \Delta_\theta(M(b, L))\,\Pi^{-1}$,

      iii) $\Delta_\phi(\mathrm{Scalar}(a, K)) = \Pi \Delta_\theta(\mathrm{Scalar}(b, L))\,\Pi^{-1}$.

**Proof.**

1) As given $\phi \sim_k \theta$, we have, by definition, that $a = b$ and $K \sim_k L$. The latter gives, in particular, that $[K : k] = [L : k]$; i.e., $n_\phi = n_\theta$. Finally, as now $a = b$ and $n_\phi = n_\theta$, we have at once that $\dim \phi = \dim \theta$.

2) As mentioned in step (1) above, we have that $K \sim_k L$. Thus, by definition, we have:

$$\eta(K) = L, \text{ for some } \eta \in Iso(K/k).$$

Also, by step (1), we may let $n \equiv n_\phi = n_\theta$. So, we may write $\sigma\colon \{1,\ldots,n\} \overset{bij}{\to} Iso(K/k)$ and $\tau\colon \{1,\ldots,n\} \overset{bij}{\to} Iso(L/k)$. Moreover, we may let $\mu'_\eta$ be the map defined as:

$$\mu'_\eta : Iso(L/k) \to Iso(K/k)$$

$$\mu'_\eta : \zeta \mapsto \zeta \circ \eta.$$

So, clearly, $\mu'_\eta$ is bijective. Thus, using the three bijections, $\sigma, \mu'_\eta, \tau$, we have:

$$p \equiv \sigma^{-1} \circ \mu'_\eta \circ \tau \in S_n.$$

Furthermore, clearly, $j \in \{1,\ldots,n\} \Rightarrow \tau_j \circ \eta = \mu'_\eta(\tau_j) \in Iso(K/k)$, and so we calculate:

$$\begin{aligned} \tau_j \circ \eta &= (\sigma \circ \sigma^{-1})\,(\tau_j \circ \eta) \\ &= (\sigma \circ \sigma^{-1})\left(\mu'_\eta\,(\tau(j))\right) \\ &= (\sigma \circ \sigma^{-1})\left(\left(\mu'_\eta \circ \tau\right)(j)\right) \\ &= \sigma\left(\left(\sigma^{-1} \circ \mu'_\eta \circ \tau\right)(j)\right) \\ &= \sigma\,(p(j)) = \sigma_{p(j)}. \end{aligned}$$

Therefore:

$$(1) \qquad j \in \{1,\ldots,n\} \;\Rightarrow\; \tau_j \circ \eta = \sigma_{p(j)}.$$

3) Let $\Pi$ be the following block permutation matrix:

$$\Pi \equiv \widehat{\Pi}_n(p,a) \in \mathrm{Perm}(an, I_a, k).$$

Thus, using Section 1.2.4, Part D, subpart (3), item (iv), we have at once:

$$(2) \qquad A_1,\ldots,A_n \in M(a,\overline{k}) \;\Rightarrow\; \Pi^{-1}\left[\bigoplus_{i=1}^{n} A_i\right]\Pi = \bigoplus_{i=1}^{n} A_{p(i)}.$$

4) For $M \in M(a,K)$, and with the above, we calculate:

$$\begin{aligned}
\Pi^{-1}\left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n}\sigma_j(M)\right]\Pi = {} & \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n}\sigma_{p(j)}(M) && \text{[by (2)]}\\
= {} & \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n}\left(\tau_j \circ \eta\right)(M) && \text{[by (1)]}\\
= {} & \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{n}\tau_j\left(\eta(M)\right).
\end{aligned}$$

I.e., therefore:

$$\Pi^{-1}\Delta_\phi(M)\Pi = \Delta_\theta\left(\eta(M)\right).$$

Thus:

$$\text{(3)} \qquad M \in M(a,K) \;\Rightarrow\; \Delta_\phi(M) = \Pi\Delta_\theta\left(\eta(M)\right)\Pi^{-1}.$$

5) Now let $f$ be a $k$–morphic function. Then, at once, by (3), and by the definition of $k$–morphic, we have:

$$\begin{aligned}
\Delta_\phi\left(f(a,K)\right) = {} & \Pi\Delta_\theta\left(\eta\left(f(a,K)\right)\right)\Pi^{-1}\\
= {} & \Pi\Delta_\theta\left(f\left(a,\eta(K)\right)\right)\Pi^{-1}\\
= {} & \Pi\Delta_\theta\left(f(b,L)\right)\Pi^{-1}.
\end{aligned}$$

(The last equality follows from the above-established conclusions that $a = b$ and that $\eta(K) = L$.)

This proves the desired result (2,c,i). The desired results in (2,c,ii), (2,c,iii) follow at once from this, by letting $f(a,K) \equiv M(a,K)$, $f(a,K) \equiv \mathrm{Scalar}(a,K)$, respectively.

□

**Lemma 1.D.5**

Let $\Phi = (\phi_1, \ldots, \phi_r)$, $\Omega = (\omega_1, \ldots, \omega_s)$ be two $k$-equivalent field settings over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$, $\omega_i = (L_i, \tau^{(i)}, b_i)$ all field elements over $k$.

**Then:**

1) $r = s$, $n_\Phi = n_\Omega$, $\dim \Phi = \dim \Omega$.

2) $\exists p \in S_r\colon \exists \eta_i \in Iso(K_i/k)\colon \exists \Pi \in \mathrm{Perm}(\dim \Phi, k)$:

a) $a_{p(i)} = b_i$, $\eta_{p(i)}\left(K_{p(i)}\right) = L_i$;

b) $(M_1, \ldots, M_r) \in \prod_{i=1}^{r} M(a_i, K_i) \;\Rightarrow$

$$\Delta_\Phi(M_1, \ldots, M_r) = \Pi \Delta_\Omega\left(\eta_{p(1)}\left(M_{p(1)}\right), \ldots, \eta_{p(r)}\left(M_{p(r)}\right)\right)\Pi^{-1};$$

c) i) $f$ a $k$–morphic function $\Rightarrow$

$$\Delta_\Phi\left(\prod_{i=1}^{r} f(a_i, K_i)\right) = \Pi \Delta_\Omega\left(\prod_{i=1}^{r} f(b_i, L_i)\right)\Pi^{-1},$$

ii) $\Delta_\Phi\left(\prod_{i=1}^{r} M(a_i, K_i)\right) = \Pi \Delta_\Omega\left(\prod_{i=1}^{r} M(b_i, L_i)\right)\Pi^{-1}$,

iii) $\Delta_\Phi\left(\prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i)\right) = \Pi \Delta_\Omega\left(\prod_{i=1}^{r} \mathrm{Scalar}(b_i, L_i)\right)\Pi^{-1}$.

**Proof.**

1) As given $\Phi \sim_k \Omega$, we have, by definition, that $r = s$ and $\exists p \in S_r\colon \forall i \in \{1, \ldots, r\}\colon$ $\phi_{p(i)} \sim_k \omega_i$. Furthermore, using that $p \in S_r$, using the previous Lemma 1.D.4, part (1) [with "$\phi$" $\equiv \phi_{p(i)}$ and "$\theta$" $\equiv \omega_i$], and using that $r = s$,

we find $n_\Phi \equiv \sum_{i=1}^{r} n_{\phi_i} = \sum_{i=1}^{r} n_{\phi_{p(i)}} = \sum_{i=1}^{r} n_{\omega_i} = \sum_{i=1}^{s} n_{\omega_i} \equiv n_\Omega$. Similarly, we find $\dim\Phi = \dim\Omega$.

2) As mentioned in step (1) above, we have that $\phi_{p(i)} \sim_k \omega_i$. In particular, this gives, by definition, that $a_{p(i)} = b_i$. Now as $\phi_{p(i)} \sim_k \omega_i$, and as $p$ is certainly injective, by using Lemma 1.D.4, part (2) [with "$\phi$" $\equiv \phi_{p(i)}$ and "$\theta$" $\equiv \omega_i$], we may let $\eta_{p(i)} \in Iso\left(K_{p(i)}\big/ k\right)$ and $\Pi_{p(i)} \in \operatorname{Perm}\left(a_{p(i)}n_{\phi_{p(i)}}, I_{a_{p(i)}}, k\right)$ be as in part (2) of the conclusion of that Lemma. In particular then, we have $\eta_{p(i)}\left(K_{p(i)}\right) = L_i$, and we note that certainly $\eta_i = \eta_{p(p^{-1}(i))} \in Iso\left(K_{p(p^{-1}(i))}\big/ k\right) = Iso\left(K_i/k\right)$.

3) By Lemma 1.D.1:

(1) $\exists\psi \in \operatorname{Perm}(\dim\Phi, k)$: $\quad A_i \in M(\dim\phi_i, \overline{k}) \;\Rightarrow\; \psi^{-1}\left[\mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r} A_i\right]\psi = \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r} A_{p(i)}$.

4) Finally, let $\Pi' \equiv \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r}\Pi_{p(i)} \in \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r}\operatorname{Perm}\left(a_{p(i)}n_{\phi_{p(i)}}, I_{a_{p(i)}}, k\right)$. Thus, using $p \in S_r$, we observe clearly, that:

$$\begin{aligned}
\Pi' \in & \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r}\operatorname{Perm}\left(a_{p(i)}n_{\phi_{p(i)}}, I_{a_{p(i)}}, k\right) = \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r}\operatorname{Perm}\left(\dim\phi_{p(i)}, I_{a_{p(i)}}, k\right) \\
& \subseteq \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r}\operatorname{Perm}\left(\dim\phi_{p(i)}, k\right) \subseteq \operatorname{Perm}\left(\sum_{i=1}^{r}\dim\phi_{p(i)}, k\right) \\
& = \operatorname{Perm}\left(\sum_{i=1}^{r}\dim\phi_i, k\right) = \operatorname{Perm}\left(\dim\Phi, k\right).
\end{aligned}$$

Thus, $\Pi' \in \operatorname{Perm}\left(\dim\Phi, k\right)$. Let $\Pi \equiv \psi\Pi' \in \operatorname{Perm}\left(\dim\Phi, k\right)$. With this and the above, for $M_i \in M(a_i, K_i)$, we calculate:

$$\begin{aligned}
\Pi^{-1}\Delta_{\Phi}(M_1,\ldots,M_r)\Pi &= \Pi'^{-1}\psi^{-1}\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r}\Delta_{\phi_i}(M_i)\right]\psi\Pi' && [\text{by def. } \Delta_{\Phi}] \\
&= \Pi'^{-1}\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r}\Delta_{\phi_{p(i)}}\left(M_{p(i)}\right)\right]\Pi' && [\text{by (1)}] \\
&= \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\left[\Pi_{p(i)}^{-1}\Delta_{\phi_{p(i)}}\left(M_{p(i)}\right)\Pi_{p(i)}\right] && [\text{by def. } \Pi'] \\
&= \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\Delta_{\omega_i}\left(\eta_{p(i)}\left(M_{p(i)}\right)\right) \\
&= \Delta_{\Omega}\left(\eta_{p(1)}\left(M_{p(1)}\right),\ldots,\eta_{p(r)}\left(M_{p(r)}\right)\right) && [\text{by def. } \Delta_{\Omega}].
\end{aligned}$$

(The second-to-last equality above follows from the properties of $\eta_{p(i)}$ and $\Pi_{p(i)}$, which were given by Lemma 1.D.4 and taken in step (2) above.) Thus, taking the above result, and moving the "$\Pi$" 's around, we have:

$$\Delta_{\Phi}(M_1,\ldots,M_r) = \Pi\Delta_{\Omega}\left(\eta_{p(1)}\left(M_{p(1)}\right),\ldots,\eta_{p(r)}\left(M_{p(r)}\right)\right)\Pi^{-1}.$$

This proves the desired result (2,b). All of the desired results in (2,c) follow at once from this, as in the proof of Lemma 1.D.4, and recalling from step (2) above that $a_{p(i)} = b_i$, and that $\eta_{p(i)}\left(K_{p(i)}\right) = L_i$. □

# Chapter 2

# Matrices that Rationalize Certain Subsets of Block-Diagonal Matrices

## 2.1 Introduction

In this chapter, we exhibit all matrices that $k$–rationalize certain general subsets of $Im(\Delta_\Phi)$, where $\Phi$ is a field setting over a perfect field $k$.

While some of the principal needs for these results would perhaps best be seen in the next, and succeeding chapters, the logical placement of these results is here.

Throughout this chapter, *$k$ is a perfect field.*

## 2.2 Initial Lemmas

These lemmas both start the process toward the main results of this chapter, as well as are later called upon. We will often be referring to matrix centralizers here (and throughout the paper). We recall, specifically, that, for $\mathcal{A} \subseteq M(n, \overline{k})$, the centralizer of $\mathcal{A}$ in $M(n, \overline{k})$ is denoted $C_{\overline{k}}(\mathcal{A})$ [see Section 1.2.4, Part G]. I.e., $C_{\overline{k}}(\mathcal{A}) \equiv \{M \in M(n, \overline{k}) | \forall A \in \mathcal{A}\colon\ MA = AM\} \subseteq M(n, \overline{k})$.

**Lemma 2.B.1**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

Let $E$ be any intermediate field of $\overline{k}/k$, which is a Galois extension of $k$, containing $K_1, \ldots, K_r$. (This is OK, thanks to the fact that $k$ is given perfect.)

Let $\mathcal{Y} \subseteq Im(\Delta_\Phi)$, let $\mathcal{C} \equiv C_{\overline{k}}(\mathcal{Y})$, and let $P \in G\ell(\dim \Phi, E)$.

(Recall the matrices, $\Pi_{\tau,\Phi}$, defined in Section 1.3.6, item (b).)

**Then:**

$$P\ k\text{-rationalizes } \mathcal{Y} \Longleftrightarrow \forall \tau \in Gal(E/k)\colon \exists C_\tau \in \mathcal{C}\colon\ \tau(P) = PC_\tau \Pi_{\tau,\Phi}.$$

**Proof.**

As $E/k$ is Galois, $P \in G\ell(\dim \Phi, E)$, $\mathcal{Y} \subseteq Im(\Delta_\Phi)$ and so then also $\mathcal{Y} \subseteq M(\dim \Phi, E)$ [by Lemma 1.D.3, part (a), and using $E/k$ is Galois], and using Lemma 1.D.3, part (b) in the fourth step below, we have the following.

$$\begin{aligned}
P\ k\text{–rationalizes } \mathcal{Y} &\iff \forall Y \in \mathcal{Y}: && PYP^{-1} \in M(n,k) \\
&\iff \forall Y \in \mathcal{Y}: \forall \tau \in Gal(E/k): && \tau(PYP^{-1}) = PYP^{-1} \\
&\iff \forall Y \in \mathcal{Y}: \forall \tau \in Gal(E/k): && \tau(P)\tau(Y)\tau(P)^{-1} = PYP^{-1} \\
&\iff \forall Y \in \mathcal{Y}: \forall \tau \in Gal(E/k): && \\
& && \tau(P)\Pi_{\tau,\Phi}^{-1} Y \Pi_{\tau,\Phi}\tau(P)^{-1} = PYP^{-1} \\
&\iff \forall Y \in \mathcal{Y}: \forall \tau \in Gal(E/k): && P^{-1}\tau(P)\Pi_{\tau,\Phi}^{-1} \in C_{\bar{k}}(Y) \\
&\iff \forall \tau \in Gal(E/k): \forall Y \in \mathcal{Y}: && P^{-1}\tau(P)\Pi_{\tau,\Phi}^{-1} \in C_{\bar{k}}(Y) \\
&\iff \forall \tau \in Gal(E/k): && \\
& && P^{-1}\tau(P)\Pi_{\tau,\Phi}^{-1} \in \textstyle\bigcap_{Y \in \mathcal{Y}} C_{\bar{k}}(Y) \\
& && \qquad\qquad = C_{\bar{k}}(\mathcal{Y}) = \mathcal{C} \\
&\iff \forall \tau \in Gal(E/k): \exists C_\tau \in \mathcal{C}: && P^{-1}\tau(P)\Pi_{\tau,\Phi}^{-1} = C_\tau.
\end{aligned}$$

□

**Corollary 2.B.2**

Let $\Phi$ be a field setting over $k$.

Let $\mathcal{Y}, \mathcal{Z} \subseteq Im(\Delta_\Phi)$.

Let $P \in G\ell(\dim \Phi, \bar{k})$.

**Then:**

a) Suppose $C_{\bar{k}}(\mathcal{Y}) \subseteq C_{\bar{k}}(\mathcal{Z})$. Then: $P$ $k$–rationalizes $\mathcal{Y} \Longrightarrow P$ $k$–rationalizes $\mathcal{Z}$.

b) Suppose $C_{\overline{k}}(\mathcal{Y}) = C_{\overline{k}}(\mathcal{Z})$. Then: $P$ $k$–rationalizes $\mathcal{Y} \Longleftrightarrow P$ $k$–rationalizes $\mathcal{Z}$.

**Proof.**

Let $\Phi = (\phi_1, \ldots, \phi_r)$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$. Then the results of this corollary follow at once from Lemma 2.B.1, by letting $E$ be any Galois extension of $k$ in $\overline{k}$, where $E$ contains both $K_1, \ldots, K_r$ and the $(\dim \Phi)^2$ entries of $P \in G\ell(\dim \Phi, \overline{k})$, the latter entries necessarily all in $\overline{k}$.

□

## 2.3 Main Technical Lemmas

This section contains a key, and perhaps difficult, argument which proves Lemma 2.C.3, ($\Longrightarrow$). This lemma gives a crucial result that is the principal basis for all the subsequent results of this chapter.

*Throughout this section, we let:* $\Phi = (\phi_1, \ldots, \phi_r)$ a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$; $E$ = any intermediate field of $\overline{k}/k$, which is a Galois extension of $k$ containing $K_1, \ldots, K_r$.

**Lemma 2.C.1**

Let $\mathcal{C} \subseteq \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} M(a_i n_{\phi_i}, \overline{k})$; and, for all $C \in \mathcal{C}$, express $C$ in the obvious (and unique) way as:

$$C = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} C^{(i)}, \text{ where } C^{(i)} \in M(a_i n_{\phi_i}, \overline{k}).$$

Let $P \in G\ell(\dim \Phi, E)$; and, express $P$ in the obvious (and unique) way as:

$$P = \mathop{\textcircled{$\|$}}\limits_{i=1}^{r} P^{(i)}, \text{ where } P^{(i)} \in M(\dim \Phi \times a_i n_{\phi_i}, \overline{k}).$$

(This is OK, as $\dim \Phi = \sum_{i=1}^{r} a_i n_{\phi_i}$.)

**Then:**

$$\forall \tau \in Gal(E/k) \colon \exists C_\tau \in \mathcal{C} \colon \ \tau(P) = P C_\tau \Pi_{\tau,\Phi} \quad \Longleftrightarrow$$

$$\forall \tau \in Gal(E/k) \colon \exists C_\tau \in \mathcal{C} \colon \forall i \in \{1, \ldots, r\} \colon \ \tau(P^{(i)}) = P^{(i)} C_\tau^{(i)} \Pi_{\tau,\phi_i}.$$

**Proof.**

We simply calculate, as below, and follow the matrix multiplications.

$$\begin{aligned}
\tau(P) &= P C_\tau \Pi_{\tau,\Phi} \\
&\Leftrightarrow \tau\left(\mathop{\textcircled{$\|$}}\limits_{i=1}^{r} P^{(i)}\right) = \left(\mathop{\textcircled{$\|$}}\limits_{i=1}^{r} P^{(i)}\right)\left(\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} C_\tau^{(i)}\right)\left(\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \Pi_{\tau,\phi_i}\right) \\
&\Leftrightarrow \mathop{\textcircled{$\|$}}\limits_{i=1}^{r} \tau(P^{(i)}) = \left(\mathop{\textcircled{$\|$}}\limits_{i=1}^{r} P^{(i)}\right)\left(\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} C_\tau^{(i)} \Pi_{\tau,\phi_i}\right) \\
&\Leftrightarrow \mathop{\textcircled{$\|$}}\limits_{i=1}^{r} \tau(P^{(i)}) = \mathop{\textcircled{$\|$}}\limits_{i=1}^{r} P^{(i)} C_\tau^{(i)} \Pi_{\tau,\phi_i} \\
&\Leftrightarrow \forall i \in \{1, \ldots, r\} \colon \ \tau(P^{(i)}) = P^{(i)} C_\tau^{(i)} \Pi_{\tau,\phi_i}.
\end{aligned}$$

□

**Lemma 2.C.2**

Let $\mathcal{C} \subseteq \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} M(a_i, \overline{k})$; and, for all $C \in \mathcal{C}$, express $C$ in the obvious (and unique) way as:

$$C = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} C^{(i)}\,, \ \text{where } C^{(i)} = \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)}\,, \ \text{where } C_j^{(i)} \in M(a_i, \overline{k}).$$

Let $P \in G\ell(dim\Phi, E)$; and, express $P$ in the obvious (and unique) way as:

$$P = \mathop{\textcircled{$\|$}}\limits_{i=1}^{r} P^{(i)}\,, \ \text{where } P^{(i)} = \mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} P_j^{(i)}\,, \ \text{where } P_j^{(i)} \in M(dim\Phi \times a_i, \overline{k}).$$

(This is OK, as $dim\Phi = \sum_{i=1}^{r} a_i n_{\phi_i}$.)

**Then:**

$$\forall \tau \in Gal(E/k) \colon \exists C_\tau \in \mathcal{C} \colon \forall i \in \{1, \ldots, r\} \colon \ \tau(P^{(i)}) = P^{(i)} C_\tau^{(i)} \Pi_{\tau,\phi_i} \quad \Longleftrightarrow$$

$$\forall \tau \in Gal(E/k) \colon \exists C_\tau \in \mathcal{C} \colon \forall i \in \{1, \ldots, r\} \colon \forall j \in \{1, \ldots, n_{\phi_i}\} \colon$$

$$\tau(P_j^{(i)}) = P^{(i)}_{p_{\tau,\phi_i}(j)} (C_\tau)^{(i)}_{p_{\tau,\phi_i}(j)}.$$

[Recall, the permutation, $p_{\tau,\phi_i} \in S_{n_{\phi_i}}$, as defined in Section 1.3.3:

$$p_{\tau,\phi_i} \equiv \sigma^{(i)^{-1}} \circ \mu_{\tau,\phi_i} \circ \sigma^{(i)} \in S_{n_{\phi_i}}] \,.$$

**Proof.**

Recall that $\Pi_{\tau,\phi_i} \equiv \widehat{\Pi}_{n_{\phi_i}}(p_{\tau,\phi_i}, a_i) \in Perm(a_i n_{\phi_i}, I_{a_i}, k)$. With this, we simply calculate, as below, follow the matrix multiplications, and use Section 1.2.4, Part (d), subpart (3), items (i) and (iv) in the third step below.

$$\begin{aligned}
\tau(P^{(i)}) &= P^{(i)}C_\tau^{(i)}\Pi_{\tau,\phi_i} \\
&\Leftrightarrow \tau\left(\mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right) = \left(\mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right)\left(\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} (C_\tau)_j^{(i)}\right)\Pi_{\tau,\phi_i} \\
&\Leftrightarrow \mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} \tau(P_j^{(i)}) = \left(\mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right)\Pi_{\tau,\phi_i}\left(\Pi_{\tau,\phi_i}^{-1}\left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} (C_\tau)_j^{(i)}\right]\Pi_{\tau,\phi_i}\right) \\
&\Leftrightarrow \mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} \tau(P_j^{(i)}) = \left(\mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} P_{p_{\tau,\phi_i}(j)}^{(i)}\right)\left(\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} (C_\tau)_{p_{\tau,\phi_i}(j)}^{(i)}\right) \\
&\Leftrightarrow \mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} \tau(P_j^{(i)}) = \mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} P_{p_{\tau,\phi_i}(j)}^{(i)}(C_\tau)_{p_{\tau,\phi_i}(j)}^{(i)} \\
&\Leftrightarrow \forall j \in \{1,\ldots,n_{\phi_i}\}\colon\ \tau(P_j^{(i)}) = P_{p_{\tau,\phi_i}(j)}^{(i)}(C_\tau)_{p_{\tau,\phi_i}(j)}^{(i)}.
\end{aligned}$$

□

**Lemma 2.C.3** (A Key Argument)

Let $\mathcal{C} \subseteq \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} M(a_i,\overline{k})$; and, as in Lemma 2.C.2, for all $C \in \mathcal{C}$, express $C$ in the obvious (and unique) way as:

$$C = \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} C_j^{(i)}, \text{ where } C_j^{(i)} \in M(a_i,\overline{k}).$$

Let $P \in G\ell(dim\Phi, E)$; and, as in Lemma 2.C.2, express $P$ in the obvious (and unique) way as:

$$P = \mathop{\textcircled{$\|$}}_{i=1}^{r}\mathop{\textcircled{$\|$}}_{j=1}^{n_{\phi_i}} P_j^{(i)}, \text{ where } P_j^{(i)} \in M(dim\Phi \times a_i,\overline{k}).$$

(This is OK, as $dim\Phi = \sum_{i=1}^{r} a_i n_{\phi_i}$.)

**Then:**

$$\forall \tau \in Gal(E/k) \colon \exists C_\tau \in \mathcal{C} \colon \forall i \in \{1, \ldots, r\} \colon \forall j \in \{1, \ldots, n_{\phi_i}\} \colon$$

$$\tau(P_j^{(i)}) = P^{(i)}_{p_{\tau,\phi_i}(j)} (C_\tau)^{(i)}_{p_{\tau,\phi_i}(j)}$$

$$\Longleftrightarrow$$

$$\exists V \in V_\Phi^\times \colon \exists C \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} G\ell(a_i, E) \colon \;\; P = VC$$

and

$$\left[\forall \tau \in Gal(E/k) \colon \;\; C^{-1} \Pi_{\tau,\Phi} \tau(C) \Pi_{\tau,\Phi}^{-1} \in \mathcal{C}\right].$$

[Recall the matrices, $V_\Phi$, as defined in Section 1.3.6.]

**Proof.**

($\Longrightarrow$)

1. We make the following preliminary observations and notations.

   (a) Applying Proposition App. 1, of the Appendix, to $P$, we have at once: $\forall i \in \{1, \ldots, r\} \colon \forall j \in \{1, \ldots, n_{\phi_i}\} \colon$ $\exists$ an $a_i \times a_i$ submatrix of rows (not necessarily consecutive rows) of $P_j^{(i)}$, *call it* $B_{i,j}$, which is invertible – $B_{i,j} \in G\ell(a_i, E)$.

   (b) As $\sigma^{(i)}$ enumerates $Iso(K_i/k)$, we may let:

   $$b_i \in \{1, \ldots, n_{\phi_i}\}, \text{ where } \sigma_{b_i}^{(i)} = id_{K_i}.$$

   (c) For $i \in \{1, \ldots, r\}$, we let:

   $$B_i \equiv B_{i,b_i} \in G\ell(a_i, E).$$

So, in particular, $B_i$ is an invertible $a_i \times a_i$ submatrix of $P_{b_i}^{(i)}$.

(d) For $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, n_{\phi_i}\}$, we let: $A_{i,j} \equiv$ the $a_i \times a_i$ submatrix (again, not necessarily of consecutive rows) of $P_j^{(i)}$ which occupies the same position in $P_j^{(i)}$, as does $B_i$ in $P_{b_i}^{(i)}$; so, in particular, $A_{i,j} \in M(a_i, E)$. (We are not asserting that $A_{i,j}$ is also invertible, as is $B_i$. However, as we show shortly, the former is, in fact, true.)

(e) We note that, by construction, we have immediately:

$$\forall i \in \{1, \ldots, r\}\colon\ A_{i,b_i} = B_i.$$

2. Now, to prove ($\Longrightarrow$), we suppose the hypothesis of ($\Longrightarrow$); i.e., with $\tau, C_\tau, i, j$ as in that hypothesis, we suppose:

$$\tau(P_j^{(i)}) = P_{p_{\tau,\phi_i}(j)}^{(i)} (C_\tau)_{p_{\tau,\phi_i}(j)}^{(i)}.$$

So, in particular, with $j = b_i$, we have:

(1)
$$\tau(P_{b_i}^{(i)}) = P_{p_{\tau,\phi_i}(b_i)}^{(i)} (C_\tau)_{p_{\tau,\phi_i}(b_i)}^{(i)}.$$

*Temporarily, we will abbreviate $\sigma^{(i)}$ by $\sigma$*; this will cause no confusion. From the definition of $p_{\tau,\phi_i}$, we see:

$$\begin{aligned} p_{\tau,\phi_i}(b_i) &= (\sigma^{-1} \circ \mu_{\tau,\phi_i} \circ \sigma)(b_i) \\ &= \sigma^{-1}(\mu_{\tau,\phi_i}(\sigma(b_i))) \\ &= \sigma^{-1}(\mu_{\tau,\phi_i}(id_{K_i})) && \text{[by step 1, part (b) above]} \\ &= \sigma^{-1}(\tau \circ id_{K_i}) \\ &= \sigma^{-1}(\tau | K_i). \end{aligned}$$

Substituting the previous in (1), we now have:

$$\tau(P_{b_i}^{(i)}) = P_{\sigma^{-1}(\tau|K_i)}^{(i)}(C_\tau)_{\sigma^{-1}(\tau|K_i)}^{(i)}. \tag{2}$$

In particular, then, from the constructed locations of $B_i$ within $P_{b_i}^{(i)}$, and $A_{i,j}$ within $P_j^{(i)}$, the above result shows:

$$\tau(B_i) = A_{i,\sigma^{-1}(\tau|K_i)}(C_\tau)_{\sigma^{-1}(\tau|K_i)}^{(i)}.$$

As $B_i$ is invertible (by step 1, part (c) above), and recalling that $\tau$ is an imbedding of fields, the previous shows that so then $A_{i,\sigma^{-1}(\tau|K_i)}$ and $(C_\tau)_{\sigma^{-1}(\tau|K_i)}^{(i)}$ are invertible. Hence:

$$(C_\tau)_{\sigma^{-1}(\tau|K_i)}^{(i)} = A_{i,\sigma^{-1}(\tau|K_i)}^{-1}\tau(B_i).$$

Substituting this in (2), and multiplying both sides of the resulting equation, on the right, by $\tau(B_i^{-1})$, we get (recalling that $\tau$ is an imbedding of fields):

$$\tau(P_{b_i}^{(i)}B_i^{-1}) = P_{\sigma^{-1}(\tau|K_i)}^{(i)}A_{i,\sigma^{-1}(\tau|K_i)}^{-1}.$$

Thus, summarizing, we have now:

$$\forall\tau \in Gal(E/k) : \forall i \in \{1,\ldots,r\} : \ \tau(P_{b_i}^{(i)}B_i^{-1}) = P_{\sigma^{-1}(\tau|K_i)}^{(i)}A_{i,\sigma^{-1}(\tau|K_i)}^{-1}. \tag{3}$$

Note that (3) is a statement concerning the matrix $P$ alone; the matrix $C_\tau$ is no longer present.

3. Now let $i_0 \in \{1,\ldots,r\}$, and let $\psi \in Gal(E/K_{i_0})$. So, in particular, $\psi \in Gal(E/k)$. Moreover, $\psi|K_{i_0} = id_{K_{i_0}}$, and so $\sigma^{-1}(\psi|K_{i_0}) = b_{i_0}$. Using this, and

thus, by (3), with $\tau = \psi$ and $i = i_0$, we have:

$$(4) \qquad \psi(P^{(i_0)}_{b_{i_0}} B^{-1}_{i_0}) = P^{(i_0)}_{\sigma^{-1}(\psi|K_{i_0})} A^{-1}_{i_0,\sigma^{-1}(\psi|K_{i_0})} = P^{(i_0)}_{b_{i_0}} A^{-1}_{i_0,b_{i_0}}.$$

As noted in step 1, part (e), we have $A_{i_0,b_{i_0}} = B_{i_0}$. Substituting this in (4) gives:

$$\psi(P^{(i_0)}_{b_{i_0}} B^{-1}_{i_0}) = P^{(i_0)}_{b_{i_0}} B^{-1}_{i_0}.$$

Summarizing, we have now:

$$\forall \psi \in Gal(E/K_{i_0}): \quad \psi(P^{(i_0)}_{b_{i_0}} B^{-1}_{i_0}) = P^{(i_0)}_{b_{i_0}} B^{-1}_{i_0}.$$

Recall that $E/k$ is a Galois extension and that $E \supseteq K_{i_0} \supseteq k$; thus $E/K_{i_0}$ is Galois. This, with the previous result above, gives at once: the matrix $P^{(i_0)}_{b_{i_0}} B^{-1}_{i_0}$ is, actually, over the field $K_{i_0}$. As $i_0$ was taken arbitrarily in $\{1, \ldots, r\}$, we conclude:

$$(5) \qquad \forall i \in \{1, \ldots, r\}: \; Q_i \equiv P^{(i)}_{b_i} B^{-1}_i \in M(dim\Phi \times a_i, K_i).$$

4. Finally, for $j \in \{1, \ldots, n_{\phi_i}\}$, let $\tau^{(i)}_j$ be a $k$–imbedding which extends $\sigma^{(i)}_j$ from $K_i$ to E. So $\tau^{(i)}_j \in Gal(E/k)$ [as $E/k$ is taken Galois]; and $\tau^{(i)}_j | K_i = \sigma^{(i)}_j$, and so $\sigma^{-1}(\tau^{(i)}_j | K_i) = j$. Using this, and with (5) and (3), we now calculate as below.

$$\begin{aligned} \sigma^{(i)}_j(Q_i) &= \tau^{(i)}_j(Q_i) = \tau^{(i)}_j(P^{(i)}_{b_i} B^{-1}_i) \\ &= P^{(i)}_{\sigma^{-1}(\tau^{(i)}_j|K_i)} A^{-1}_{i,\sigma^{-1}(\tau^{(i)}_j|K_i)} \\ &= P^{(i)}_j A^{-1}_{i,j}. \end{aligned}$$

Therefore:

$$P^{(i)}_j = \sigma^{(i)}_j(Q_i) A_{i,j}.$$

Thus:

$$(6)\qquad \forall i \in \{1,\dots,r\}\colon \forall j \in \{1,\dots,n_{\phi_i}\}\colon\quad P_j^{(i)} = \sigma_j^{(i)}(Q_i)A_{i,j}.$$

5. Thus, with the expression for $P$ in the given, and with (6) and (5), we calculate as below, recalling the dimensions of $Q_i$ and $A_{i,j}$, and following the matrix factorizations:

$$\begin{aligned} P &= \mathop{\bigcirc\kern-0.72em\|}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.72em\|}\limits_{j=1}^{n_{\phi_i}} P_j^{(i)} = \mathop{\bigcirc\kern-0.72em\|}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.72em\|}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i)A_{i,j} \\ &= \left(\mathop{\bigcirc\kern-0.72em\|}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.72em\|}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i)\right)\left(\mathop{\bigcirc\kern-0.8em\vartriangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.8em\vartriangle}\limits_{j=1}^{n_{\phi_i}} A_{i,j}\right). \end{aligned}$$

Thus:

$$(7)\qquad P = VC;\quad V \equiv \mathop{\bigcirc\kern-0.72em\|}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.72em\|}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i),\quad C \equiv \mathop{\bigcirc\kern-0.8em\vartriangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.8em\vartriangle}\limits_{j=1}^{n_{\phi_i}} A_{i,j}.$$

In particular, as $P$ is invertible, so then are $V$ and $C$. Moreover, by (5) and the definition of $V_\Phi$, we have $V \in V_\Phi$. These two remarks show $V \in V_\Phi^\times$. Finally, as $A_{i,j} \in M(a_i, E)$ [by step 1, part (d) above], the first remark here shows

$$C \in \mathop{\bigcirc\kern-0.8em\vartriangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.8em\vartriangle}\limits_{j=1}^{n_{\phi_i}} G\ell(a_i, E).$$

6. To complete the proof of ($\Longrightarrow$), it remains to show:

$$\forall \tau \in Gal(E/k)\colon\quad C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} \in \mathcal{C}.$$

By (7), we have $P = VC$, and so

$$(8)\qquad \tau(P) = \tau(V)\tau(C) = V\Pi_{\tau,\Phi}\tau(C);$$

where the last equality follows by Lemma 1.D.3, part (e). Now, by the supposition at the start of step (2) above, we have:

$$\tau(P_j^{(i)}) = P^{(i)}_{p_{\tau,\phi_i}(j)}(C_\tau)^{(i)}_{p_{\tau,\phi_i}(j)}.$$

This allows, recalling the matrix dimensions and following the matrix factorizations, the following:

$$\begin{aligned}
\mathop{⦷}_{j=1}^{n_{\phi_i}} \tau(P_j^{(i)}) &= \mathop{⦷}_{j=1}^{n_{\phi_i}} P^{(i)}_{p_{\tau,\phi_i}(j)}(C_\tau)^{(i)}_{p_{\tau,\phi_i}(j)} \\
&= \left[\mathop{⦷}_{j=1}^{n_{\phi_i}} P^{(i)}_{p_{\tau,\phi_i}(j)}\right] \cdot \left[\mathop{◬}_{j=1}^{n_{\phi_i}} (C_\tau)^{(i)}_{p_{\tau,\phi_i}(j)}\right] \\
&= \left(\left[\mathop{⦷}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right]\Pi_{\tau,\phi_i}\right) \cdot \left(\Pi^{-1}_{\tau,\phi_i}\left[\mathop{◬}_{j=1}^{n_{\phi_i}} (C_\tau)_j^{(i)}\right]\Pi_{\tau,\phi_i}\right) \\
&= \left[\mathop{⦷}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right] \cdot \left[\mathop{◬}_{j=1}^{n_{\phi_i}} (C_\tau)_j^{(i)}\right]\Pi_{\tau,\phi_i}.
\end{aligned}$$

(The second-to-last equality follows from the basic properties of block permutation matrices and the definition of $\Pi_{\tau,\phi_i}$, discussed in Chapter 1.) Using this in the third equality below, following the matrix factorizations in the fourth equality below, and by the first part of (7), thus, at once:

$$\begin{aligned}
\tau(P) &= \tau\left(\mathop{⦷}_{i=1}^{r}\mathop{⦷}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right) = \mathop{⦷}_{i=1}^{r}\mathop{⦷}_{j=1}^{n_{\phi_i}} \tau(P_j^{(i)}) \\
&= \mathop{⦷}_{i=1}^{r}\left(\left[\mathop{⦷}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right] \cdot \left[\mathop{◬}_{j=1}^{n_{\phi_i}} (C_\tau)_j^{(i)}\right]\Pi_{\tau,\phi_i}\right) \\
&= \left[\mathop{⦷}_{i=1}^{r}\mathop{⦷}_{j=1}^{n_{\phi_i}} P_j^{(i)}\right] \cdot \left[\mathop{◬}_{i=1}^{r}\mathop{◬}_{j=1}^{n_{\phi_i}} (C_\tau)_j^{(i)}\right] \cdot \left[\mathop{◬}_{i=1}^{r}\Pi_{\tau,\phi_i}\right] \\
&= PC_\tau\Pi_{\tau,\Phi} \\
&= VCC_\tau\Pi_{\tau,\Phi}.
\end{aligned}$$

Thus:

$$\tau(P) = VCC_\tau\Pi_{\tau,\Phi}. \tag{9}$$

So, equating (8) and (9):

$$V\Pi_{\tau,\Phi}\tau(C) = VCC_\tau\Pi_{\tau,\Phi}.$$

As $V$ is invertible:

$$\Pi_{\tau,\Phi}\tau(C) = CC_\tau\Pi_{\tau,\Phi}.$$

As $C$ is invertible, and as $C_\tau \in \mathcal{C}$ by supposition in step (2) above, the previous allows:

$$C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} = C_\tau \in \mathcal{C}.$$

This completes the proof of ($\Longrightarrow$).

($\Longleftarrow$)

7. We now suppose the hypothesis of ($\Longleftarrow$); i.e., with $V$ and $C$ as in that hypothesis, we suppose:

$$P = VC; \qquad \text{with } V \in V_\Phi^\times,\ C \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} G\ell(a_i, E)$$

and

(10) $$\forall\tau \in Gal(E/k)\colon\ C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} \in \mathcal{C}.$$

Now, $V \in V_\Phi^\times \subseteq V_\Phi$ gives, by construction of $V_\Phi$:

$$V = \mathop{\bigcirc\mkern-15mu\Vert}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-15mu\Vert}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i), \quad \text{for some } Q_i \in M(dim\Phi \times a_i, K_i).$$

And $C \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} G\ell(a_i, E)$, gives: $C = \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)}$, for some $C_j^{(i)} \in G\ell(a_i, E)$. As $P = VC$ by supposition; the previous for $V$ and $C$, and the Lemma's hypothesis for $P$, show:

$$\begin{aligned}\mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} P_j^{(i)} &= P = \left(\mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i)\right)\left(\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)}\right) \\ &= \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i)C_j^{(i)}.\end{aligned}$$

Therefore:

$$P_j^{(i)} = \sigma_j^{(i)}(Q_i)C_j^{(i)}.$$

For $\tau \in Gal(E/k)$, we see by definition(s):

$$\begin{aligned}\tau \circ \sigma_j^{(i)} &= \mu_{\tau,\phi_i}\left(\sigma_j^{(i)}\right) \\ &= \left(\mu_{\tau,\phi_i} \circ \sigma^{(i)}\right)(j) \\ &= \left(\sigma^{(i)} \circ \sigma^{(i)^{-1}} \circ \mu_{\tau,\phi_i} \circ \sigma^{(i)}\right)(j) \\ &= \left(\sigma^{(i)} \circ p_{\tau,\phi_i}\right)(j) \\ &= \sigma^{(i)}\left(p_{\tau,\phi_i}(j)\right) = \sigma^{(i)}_{p_{\tau,\phi_i}(j)}.\end{aligned}$$

Combining these last two results, and using the first result again in the last step, we have:

$$\begin{aligned}\tau(P_j^{(i)}) &= \tau\left(\sigma_j^{(i)}(Q_i)\right)\tau(C_j^{(i)}) \\ &= \sigma^{(i)}_{p_{\tau,\phi_i}(j)}(Q_i)\tau(C_j^{(i)}) \\ &= \sigma^{(i)}_{p_{\tau,\phi_i}(j)}(Q_i)C^{(i)}_{p_{\tau,\phi_i}(j)}C^{(i)^{-1}}_{p_{\tau,\phi_i}(j)}\tau(C_j^{(i)}) \\ &= P^{(i)}_{p_{\tau,\phi_i}(j)}\left(C^{(i)^{-1}}_{p_{\tau,\phi_i}(j)}\tau(C_j^{(i)})\right).\end{aligned}$$

Therefore:

$$\tau(P_j^{(i)}) = P^{(i)}_{p_{\tau,\phi_i}(j)}\left(C^{(i)^{-1}}_{p_{\tau,\phi_i}(j)}\tau(C_j^{(i)})\right). \tag{11}$$

Finally, we let:

$$C_\tau \equiv \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} \left(C_j^{(i)^{-1}}\right)\tau\left(C^{(i)}_{p^{-1}_{\tau,\phi_i}(j)}\right) \in \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} G\ell(a_i, E).$$

From (11), and this definition of $C_\tau$, we clearly see:

$$\tau(P_j^{(i)}) = P^{(i)}_{p_{\tau,\phi_i}(j)}(C_\tau)^{(i)}_{p_{\tau,\phi_i}(j)}.$$

Thus, it remains only to show that $C_\tau \in \mathcal{C}$. This is easy, using (10) in the last step:

$$\begin{aligned}
C_\tau &\equiv \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} \left(C_j^{(i)^{-1}}\right)\tau\left(C^{(i)}_{p^{-1}_{\tau,\phi_i}(j)}\right)\\
&= \left(\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} C_j^{(i)^{-1}}\right)\left(\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} \tau\left(C^{(i)}_{p^{-1}_{\tau,\phi_i}(j)}\right)\right)\\
&= \left(\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} C_j^{(i)}\right)^{-1}\left(\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} [\tau(C)]^{(i)}_{p^{-1}_{\tau,\phi_i}(j)}\right)\\
&= (C)^{-1}\left(\Pi_{\tau,\Phi}\left[\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{r}\mathop{\text{\textcircled{$\triangle$}}}_{j=1}^{n_{\phi_i}} [\tau(C)]_j^{(i)}\right]\Pi^{-1}_{\tau,\Phi}\right)\\
&= C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi^{-1}_{\tau,\Phi} \in \mathcal{C}.
\end{aligned}$$

(The second-to-last equality follows from the basic properties of block permutation matrices [re-expressed in a "backward" statement], and the definition of $\Pi_{\tau,\Phi}$, discussed in Chapter 1.)

This completes the proof of ($\Longleftarrow$), and so of the lemma as a whole.

$\square$

**Lemma 2.C.4**

Let $\mathcal{C} \subseteq \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{n_{\phi_i}} M(a_i, \overline{k})$; and, for all $C \in \mathcal{C}$, express $C$ in the obvious (and unique) way as:

$$C = \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)}, \quad \text{where } C_j^{(i)} \in M(a_i, \overline{k}).$$

Let $P \in G\ell(dim\Phi, E)$.

**Then:**

$$\forall \tau \in Gal(E/k)\colon \exists C_\tau \in \mathcal{C}\colon \; \tau(P) = PC_\tau \Pi_{\tau,\Phi}$$

$$\Leftrightarrow$$

$$\exists V \in V_\Phi^\times\colon \exists C \in \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{n_{\phi_i}} G\ell(a_i, E)\colon$$

1) $P = VC$

2) $\forall \tau \in Gal(E/k)$: $C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} = \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)^{-1}}\tau\left(C^{(i)}_{p^{-1}_{\tau,\phi_i}(j)}\right) \in \mathcal{C}$.

**Proof.**

This follows immediately by consecutive use of Lemmas 2.C.1, 2.C.2, and 2.C.3. The equality, $C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} = \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)^{-1}}\tau\left(C^{(i)}_{p^{-1}_{\tau,\phi_i}(j)}\right)$, follows purely by the basic properties of block permutation matrices and the definition of $\Pi_{\tau,\Phi}$ – the steps in this derivation being the verbatim equalities, in reverse, given in the demonstration at the very end of the proof of Lemma 2.C.3.

$\square$

**Corollary 2.C.5**

Let $P \in G\ell(dim\Phi, E)$.

**Then:**

$$\forall \tau \in Gal(E/k)\colon \exists C_\tau \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} M(a_i, \overline{k})\colon \quad \tau(P) = PC_\tau \Pi_{\tau,\Phi}$$

$$\Leftrightarrow$$

$$\exists V \in V_\Phi^\times \colon \exists C \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} G\ell(a_i, E)\colon \quad P = VC.$$

**Proof.**

This follows immediately from Lemma 2.C.4, by letting:

$$\mathcal{C} \equiv \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} M(a_i, \overline{k}).$$

$\square$

**Corollary 2.C.6**

Let $\mathcal{Y} \subseteq Im(\Delta_\Phi)$, where $\quad C_{\overline{k}}(\mathcal{Y}) \subseteq \mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, \overline{k})^{(n_{\phi_i})}$.

Let $P \in G\ell(dim\Phi, E)$.

**Then:**

$$P \ k\text{–rationalizes } \mathcal{Y}$$

$$\Leftrightarrow$$

$$\exists V \in V_\Phi^\times \colon \exists C \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} G\ell(a_i, E)^{(n_{\phi_i})}\colon$$

1) $P = VC$

2) $\forall \tau \in Gal(E/k)\colon \ C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} \in C_{\overline{k}}(\mathcal{Y})$.

**Proof.**

This follows at once from Lemma 2.B.1 and Lemma 2.C.4; where, in the latter, (by the given here) we may let:

$$\mathcal{C} \equiv C_{\overline{k}}(\mathcal{Y}) \subseteq \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M(a_i,\overline{k})^{(n_{\phi_i})} = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} M(a_i,\overline{k}).$$

$\square$

## 2.4 Main Results

Here we give the main results, some of which are exhibitions, on matrices that $k$–rationalize certain general subsets of $Im(\Delta_\Phi)$, where $\Phi$ is a field setting over $k$.

*Throughout this section, we let* $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

The following lemma contains basic facts about centralizers of certain subsets of matrices, which will be used frequently throughout this paper.

**Lemma 2.D.1**

Let $L$ be any extension field of $k$ which contains $\cup_{i=1}^{r} \cup_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(K_i)$.

Let $\prod_{i=1}^{r} Scalar(a_i, K_i) \subseteq \mathcal{U} \subseteq \prod_{i=1}^{r} M(a_i, K_i)$.

Let $\mathcal{U}^{(i)} \equiv$ the set of the $i^{th}$ components of the elements of $\mathcal{U}$, so that, in particular, $Scalar(a_i, K_i) \subseteq \mathcal{U}^{(i)} \subseteq M(a_i, K_i)$.

**Then:**

a) $C_L\left(\Delta_\Phi(\mathcal{U})\right) = C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r}\mathcal{U}^{(i)}\right)\right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.75em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right)\right).$

b) In particular:

i) $C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r} Scalar(a_i, K_i)\right)\right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})};$

ii) $C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r} K_i[N_{a_i}]\right)\right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} L[N_{a_i}]^{(n_{\phi_i})};$

iii) $C_L\left(Im(\Delta_\Phi)\right) = C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r} M(a_i, K_i)\right)\right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} Scalar(a_i, L)^{(n_{\phi_i})}.$

[Recall, $C_L(\mathcal{A})$ is the centralizer of $\mathcal{A}$ over $L$. Also, note that $K_i[N_{a_i}]$ is the $K_i$–algebra generated by $N_{a_i}$ – the canonical $a_i \times a_i$ nilpotent matrix.]

**Proof.**

1. For $(M_1, \ldots, M_r) \in \Pi_{i=1}^{r} M(a_i, K_i)$, we have, by construction of the maps $\Delta_\Phi$ and $\Delta_{\phi_i}$:

$$(1)\qquad \Delta_\Phi(M_1, \ldots, M_r) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\Delta_{\phi_i}(M_i) \quad\text{and}\quad \Delta_{\phi_i}(M_i) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{j=1}^{n_{\phi_i}}\sigma_j^{(i)}(M_i).$$

2. In particular, for $\mathcal{X}_i \subseteq M(a_i, K_i)$, we see, by definition(s), at once:

$$(2)\qquad \begin{aligned} \Delta_\Phi(\Pi_{i=1}^{r}\mathcal{X}_i) &= \{\Delta_\Phi(X_1, \ldots, X_r) | X_i \in \mathcal{X}_i\} \\ &= \left\{\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\Delta_{\phi_i}(X_i)\middle| X_i \in \mathcal{X}_i\right\} \\ &= \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\Delta_{\phi_i}(\mathcal{X}_i). \end{aligned}$$

So, in particular:

$$(3)\qquad C_L\left(\Delta_\Phi(\Pi_{i=1}^{r}\mathcal{X}_i)\right) = C_L\left(\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\Delta_{\phi_i}(\mathcal{X}_i)\right).$$

3. We prove desired conclusion (b, i) first. In any field we have $0 \neq 1$, so certainly $O_{a_i} \neq I_{a_i} \in Scalar(a_i, K_i)$. In particular, we have: $I_{a_1} \in Scalar(a_1, K_1)$, $O_{a_2} \in Scalar(a_2, K_2)$, ..., $O_{a_r} \in Scalar(a_r, K_r)$. With this observation, and Proposition App. 8 [ with $n \equiv 2$ ], part (a), of the Appendix, we have at once:

$$C_L\left(\mathop{\bigcirc\kern-0.85em\triangle}_{i=1}^{r} \Delta_{\phi_i}\left(Scalar(a_i, K_i)\right)\right) =$$

$$C_L\left(\Delta_{\phi_1}\left(Scalar(a_1, K_1)\right)\right) \mathbin{\bigcirc\kern-0.85em\triangle} C_L\left(\mathop{\bigcirc\kern-0.85em\triangle}_{i=2}^{r} \Delta_{\phi_i}\left(Scalar(a_i, K_i)\right)\right).$$

Iterating the previous, and using (3) [ with $\mathcal{X}_i \equiv Scalar(a_i, K_i)$ ], we have at once:

$$(4) \qquad C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r} Scalar(a_i, K_i)\right)\right) = \mathop{\bigcirc\kern-0.85em\triangle}_{i=1}^{r} C_L\left(\Delta_{\phi_i}\left(Scalar(a_i, K_i)\right)\right).$$

4. Now let $\lambda \in K_i$, and so $\lambda I_{a_i} \in Scalar(a_i, K_i)$. So, by the second half of (1):

$$(5) \qquad \Delta_{\phi_i}\left(\lambda I_{a_i}\right) = \mathop{\bigcirc\kern-0.85em\triangle}_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(\lambda) I_{a_i};$$

in particular,

$$\Delta_{\phi_i}\left(Scalar(a_i, K_i)\right) \subseteq \mathop{\bigcirc\kern-0.85em\triangle}_{j=1}^{n_{\phi_i}} Scalar(a_i, \overline{k}) \subseteq D(a_i n_{\phi_i}, \overline{k}).$$

Now let $j_1, j_2 \in \{1, \ldots, n_{\phi_i}\}$, and suppose that: $\left[\forall \lambda \in K_i\colon \quad \sigma_{j_1}^{(i)}(\lambda) = \sigma_{j_2}^{(i)}(\lambda)\right]$. Thus, immediately: $\sigma_{j_1}^{(i)} = \sigma_{j_2}^{(i)}$. So, as $\sigma^{(i)}$ is an enumerator, $\sigma^{(i)}$ is, in particular, injective, and so the previous equality gives: $j_1 = j_2$. Thus:

$$(6) \qquad \forall j_1 \neq j_2 \in \{1, \ldots, n_{\phi_i}\}\colon \exists \lambda \in K_i\colon \quad \sigma_{j_1}^{(i)}(\lambda) \neq \sigma_{j_2}^{(i)}(\lambda).$$

Thus, the observations in (5) and (6), together with Proposition App. 10, of the Appendix, show at once:

$$C_L\left(\Delta_{\phi_i}\left(\mathit{Scalar}(a_i, K_i)\right)\right) = M(a_i, L)^{(n_{\phi_i})}.$$

Substituting this in (4), we have:

$$C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r}\mathit{Scalar}(a_i, K_i)\right)\right) = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}. \tag{7}$$

5. Now, by the given on $\mathcal{U}$, and using (2), (1), we clearly have:

$$\begin{aligned}\Delta_\Phi\left(\prod_{i=1}^{r}\mathit{Scalar}(a_i, K_i)\right) \subseteq \Delta_\Phi(\mathcal{U}) \subseteq \Delta_\Phi\left(\prod_{i=1}^{r}\mathcal{U}^{(i)}\right) &= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\Delta_{\phi_i}\left(\mathcal{U}^{(i)}\right)\\ &\subseteq \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}}\sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right) \subseteq \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M(a_i, \overline{k})^{(n_{\phi_i})}.\end{aligned}$$

Using (7) (in reverse), with the above, we now clearly have, in particular:

$$\begin{aligned}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})} &\supseteq C_L\left(\Delta_\Phi(\mathcal{U})\right) \supseteq C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r}\mathcal{U}^{(i)}\right)\right)\\ &\supseteq C_L\left(\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}}\sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right)\right) \supseteq \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right)\right).\end{aligned} \tag{8}$$

Thus, at once by Proposition App. 6, of the Appendix [ with "$\mathcal{Y}$" $\equiv \Delta_\Phi(\mathcal{U})$, and so $\mathcal{Y} \subseteq \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} M(a_i, \overline{k})$; and, for $Y \in \mathcal{Y}$, writing $Y = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} Y_j^{(i)}$ in the obvious (and unique) way, where $Y_j^{(i)} \in M(a_i, \overline{k})$, and so clearly $\mathcal{Y}_j^{(i)} \equiv \left\{Y_j^{(i)} \middle| Y \in \mathcal{Y}\right\} = \left\{\sigma_j^{(i)}(U) \middle| U \in \mathcal{U}^{(i)}\right\} = \sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right)$ ], we have:

$$C_L\left(\Delta_\Phi(\mathcal{U})\right) = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right)\right).$$

This, together with (8), gives at once:

$$C_L\left(\Delta_\Phi(\mathcal{U})\right) = C_L\left(\Delta_\Phi\left(\prod_{i=1}^{r}\mathcal{U}^{(i)}\right)\right) = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\sigma_j^{(i)}\left(\mathcal{U}^{(i)}\right)\right). \tag{9}$$

This is desired conclusion (a).

6. The desired conclusion (b,i) has already been proved and is seen in (7) above.

   The desired conclusions (b, ii), (b,iii) follow at once from (9), letting, resp., $\mathcal{U} \equiv \prod_{i=1}^{r} K_i[N_{a_i}]$, $\mathcal{U} \equiv \prod_{i=1}^{r} M(a_i, K_i)$, and then immediately by Proposition App. 9, of the Appendix.

□

**Theorem 2.D.2**

$$V \in V_\Phi^\times \quad \Longrightarrow \quad V \quad k\text{-rationalizes} \quad Im(\Delta_\Phi).$$

**Proof.**

This follows at once from Corollary 2.C.6, ($\Longleftarrow$), with "$\mathcal{Y}$" $\equiv Im(\Delta_\Phi)$ [and using Lemma 2.D.1, part (b,iii)], and with "$P$" $\equiv V$ [and then observing "$P$" $= V = V \cdot I$].

□

**Remark**

The above result can also be obtained from "elementary" considerations, as follows. Let $E$ be an intermediate field of $\overline{k}/k$ which is a Galois extension of $k$ containing $K_1, \ldots, K_r$. Then, using Lemma 1.D.3, parts (b) and (e) for the second equality below, we calculate:

$$M \in \prod_{i=1}^{r} M(a_i, K_i) \quad \Longrightarrow$$

$$\begin{aligned}\forall \tau \in Gal(E/k)\colon \quad \tau\left(V\Delta_{\Phi}(M)V^{-1}\right) &= \tau(V)\tau\left(\Delta_{\Phi}(M)\right)\tau(V)^{-1} \\ &= V\Pi_{\tau,\Phi}\left(\Pi_{\tau,\Phi}^{-1}\Delta_{\Phi}(M)\Pi_{\tau,\Phi}\right)\Pi_{\tau,\Phi}^{-1}V^{-1} \\ &= V\Delta_{\Phi}(M)V^{-1}.\end{aligned}$$

Thus, as $E/k$ is Galois, we have at once: $V\Delta_{\Phi}(M)V^{-1} \in M(dim\Phi, k)$. Thus, $V$ $k$–rationalizes $Im(\Delta_{\Phi})$.

**Theorem 2.D.3**

Let $\mathcal{Y} \subseteq Im(\Delta_{\Phi})$, where $C_{\overline{k}}(\mathcal{Y}) \subseteq \mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} M\left(a_i, \overline{k}\right)^{(n_{\phi_i})}$.

Let $P \in G\ell\left(dim\Phi, \overline{k}\right)$.

**Then:**

a) $P$ $k$–rationalizes $\mathcal{Y}$ $\Longrightarrow$ $P \in V_{\Phi}^{\times} \cdot \left[\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} G\ell\left(a_i, \overline{k}\right)^{(n_{\phi_i})}\right]$.

b) $P$ $k$–rationalizes $\mathcal{Y}$ $\Longrightarrow$ $P$ $k$–rationalizes $\Delta_{\Phi}\left(\prod_{i=1}^{r} Scalar(a_i, K_i)\right)$.

**Proof.**

a) This follows at once from Corollary 2.C.6, ($\Longrightarrow$), by letting $E$ be any Galois extension of $k$, in $\overline{k}$, where $E$ contains both $K_1, \ldots, K_r$ and the $(dim\Phi)^2$ entries of $P \in G\ell\left(dim\Phi, \overline{k}\right)$.

b) This follows at once from Lemma 2.D.1, part (b,i), and Corollary 2.B.2, part (a).

□

**Theorem 2.D.4**

Let $\mathcal{Y} \subseteq Im(\Delta_\Phi)$, where $C_{\overline{k}}(\mathcal{Y}) = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M\left(a_i, \overline{k}\right)^{(n_{\phi_i})}$.

Let $P \in G\ell\left(dim\Phi, \overline{k}\right)$.

**Then:**

a) $P$ $k$-rationalizes $\mathcal{Y}$ $\Longleftrightarrow$ $P \in V_\Phi^\times \cdot \left[\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} G\ell\left(a_i, \overline{k}\right)^{(n_{\phi_i})}\right]$.

b) $P$ $k$-rationalizes $\mathcal{Y}$ $\Longleftrightarrow$ $P$ $k$-rationalizes $\Delta_\Phi\left(\prod_{i=1}^{r} Scalar(a_i, K_i)\right)$.

**Proof.**

a) This follows at once from Corollary 2.C.6, since the condition $C^{-1}\Pi_{\tau,\Phi}\tau(C)\Pi_{\tau,\Phi}^{-1} \in C_{\overline{k}}(\mathcal{Y})$ is vacuous here, and by letting $E$ be any Galois extension of $k$, in $\overline{k}$, where $E$ contains both $K_1, \ldots, K_r$ and the $(dim\Phi)^2$ entries of $P \in G\ell\left(dim\Phi, \overline{k}\right)$.

b) This follows at once from Lemma 2.D.1, part (b,i), and Corollary 2.B.2, part (b).

□

## 2.5 Extension of Main Results, Beyond $\overline{k}$

The main results of the previous section apply to $P \in G\ell\left(dim\Phi, \overline{k}\right)$. By means of Proposition App. 4, of the Appendix, these results (and more) can easily be generalized to include $P \in G\ell(dim\Phi, L)$, where $L$ is *any* extension field of $\overline{k}$.

*Throughout this section,* we let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, where $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ is a field element over $k$. Furthermore, we let $L$ be any extension field of $\overline{k}$.

**Lemma 2.E.1**

Let $n \in \mathbb{Z}^+$, $\mathcal{Z} \subseteq M\left(n, \overline{k}\right)$, $P \in G\ell(n, L)$.

**Then:**

$$P \ k\text{–rationalizes } \mathcal{Z}$$

$$\Longleftrightarrow$$

$$\exists Q \in G\ell\left(n, \overline{k}\right) : \exists C \in C_L^{\times}(\mathcal{Z}): \quad P = QC \text{ and } Q \ k\text{–rationalizes } \mathcal{Z}.$$

**Proof.**

$(\Longrightarrow)$

This follows at once from Proposition App. 4, in the Appendix, with "$\mathcal{A}$" $\equiv \mathcal{Z}$, "$\mathcal{B}$" $\equiv M(n, k)$.

$(\Longleftarrow)$

This is immediate, since $C$ centralizes $\mathcal{Z}$ and $Q$ $k$–rationalizes $\mathcal{Z}$, we have at once:

$$P\mathcal{Z}P^{-1} = QC\mathcal{Z}C^{-1}Q^{-1} = Q\mathcal{Z}Q^{-1} \subseteq M(n, k).$$

□

**Remark**

The forward direction of this lemma shows: "a $k$–rationalization over $L$ can be 'replaced' by a $k$–rationalization over $\overline{k}$".

**Corollary 2.E.2**

Let $\mathcal{Y}, \mathcal{Z} \subseteq Im(\Delta_\Phi)$.

Let $P \in G\ell(dim\Phi, L)$.

**Then:**

a) Suppose: $C_L(\mathcal{Y}) \subseteq C_L(\mathcal{Z})$. Then:

$$P \text{ } k\text{–rationalizes } \mathcal{Y} \implies P \text{ } k\text{–rationalizes } \mathcal{Z}.$$

b) Suppose: $C_L(\mathcal{Y}) = C_L(\mathcal{Z})$. Then:

$$P \text{ } k\text{–rationalizes } \mathcal{Y} \iff P \text{ } k\text{–rationalizes } \mathcal{Z}.$$

**Proof.**

a) Suppose $C_L(\mathcal{Y}) \subseteq C_L(\mathcal{Z})$, and that $P$ $k$–rationalizes $\mathcal{Y}$. So, by Lemma 2.E.1: $P = QC$ and $Q$ $k$–rationalizes $\mathcal{Y}$, where $Q \in G\ell\left(dim\Phi, \bar{k}\right)$ and $C \in C_L^\times(\mathcal{Y})$. Moreover, we observe:

$$\begin{aligned} C_L(\mathcal{Y}) \subseteq C_L(\mathcal{Z}) &\Rightarrow \left[C_L(\mathcal{Y}) \cap M\left(dim\Phi, \bar{k}\right)\right] \subseteq \left[C_L(\mathcal{Z}) \cap M\left(dim\Phi, \bar{k}\right)\right] \\ &\Rightarrow C_{\bar{k}}(\mathcal{Y}) \subseteq C_{\bar{k}}(\mathcal{Z}). \end{aligned}$$

Thus, at once by Corollary 2.B.2: $Q$ $k$–rationalizes $\mathcal{Z}$. Finally, as above: $C \in C_L^\times(\mathcal{Y}) \subseteq C_L^\times(\mathcal{Z})$; so $C$ also centralizes $\mathcal{Z}$. Thus:

$$P\mathcal{Z}P^{-1} = QC\mathcal{Z}C^{-1}Q^{-1} = Q\mathcal{Z}Q^{-1} \subseteq M(n,k).$$

b) This follows immediately from part (a).

□

**Theorem 2.E.3**

Let $\mathcal{Y} \subseteq Im(\Delta_\Phi)$, where $C_L(\mathcal{Y}) \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $P \in G\ell(dim\Phi, L)$.

**Then:**

a) $P$ $k$–rationalizes $\mathcal{Y}$ $\Longrightarrow$ $P \in V_\Phi^\times \cdot \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}\right]$.

b) $P$ $k$–rationalizes $\mathcal{Y}$ $\Longrightarrow$ $P$ $k$–rationalizes $\Delta_\Phi\left(\prod\limits_{i=1}^{r} Scalar(a_i, K_i)\right)$.

**Proof.**

a) Suppose $P$ $k$–rationalizes $\mathcal{Y}$. So, by Lemma 2.E.1, we have: $P = QC$, where $Q$ $k$–rationalizes $\mathcal{Y}$, $Q \in G\ell\left(dim\Phi, \overline{k}\right)$, and $C \in C_L^\times(\mathcal{Y}) \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M^\times(a_i, L)^{(n_{\phi_i})}$. Hence, by Theorem 2.D.3, part (a): $Q = VC'$, where $V \in V_\Phi^\times$, $C' \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} G\ell\left(a_i, \overline{k}\right)^{(n_{\phi_i})}$. Thus: $P = QC = VC'C$, where $V \in V_\Phi^\times$, $C' \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} G\ell\left(a_i, \overline{k}\right)^{(n_{\phi_i})}$, $C \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M^\times(a_i, L)^{(n_{\phi_i})}$. As $L \supseteq \overline{k}$, we have $C'C \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}$ [noting, obviously, that $M^\times(a_i, L) = G\ell(a_i, L)$].

b) This follows at once from Lemma 2.D.1, part (b,i), and Corollary 2.E.2, part (a).

□

**Theorem 2.E.4**

Let $\mathcal{Y} \subseteq Im(\Delta_\Phi)$, where $C_L(\mathcal{Y}) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $P \in G\ell(dim\Phi, L)$.

**Then:**

a) $P$ $k$–rationalizes $\mathcal{Y} \iff P \in V_\Phi^\times \cdot \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}\right]$.

b) $P$ $k$–rationalizes $\mathcal{Y} \iff P$ $k$–rationalizes $\Delta_\Phi\left(\prod\limits_{i=1}^{r} Scalar(a_i, K_i)\right)$.

**Proof.**

a) $(\Longrightarrow)$: This follows from Theorem 2.E.3, part (a).

$(\Longleftarrow)$: Suppose $P = VC$, where $V \in V_\Phi^\times$, $C \in \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}$. By the given on $C_L(\mathcal{Y})$: $C$ centralizes $\mathcal{Y}$. By Theorem 2.D.2: $V$ $k$–rationalizes $\mathcal{Y}$. So, at once: $P\mathcal{Y}P^{-1} = VC\mathcal{Y}C^{-1}V^{-1} = V\mathcal{Y}V^{-1} \subseteq M(dim\Phi, k)$.

b) This follows at once from Lemma 2.D.1, part (b,i), and Corollary 2.E.2, part (b).

$\square$

**Corollary 2.E.5**

Let $\mathcal{Y} \subseteq Im(\Delta_\Phi)$, where $C_L(\mathcal{Y}) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $\mathcal{Y} \subseteq \mathcal{Z} \subseteq M(dim\Phi, L)$.

Let $P \in G\ell(dim\Phi, L)$.

**Then:**

a) $P$ $k$–rationalizes $\mathcal{Y}$ $\iff$ $\exists V \in V_\Phi^\times : \exists C \in C_L^\times(\mathcal{Y})$: $P = VC$.

b) $P$ $k$–rationalizes $\mathcal{Z}$ $\iff$ $\exists V \in V_\Phi^\times : \exists C \in C_L^\times(\mathcal{Y}) : \exists \tilde{\mathcal{Z}} \subseteq M(dim\Phi, L)$:

1) $P = VC,\ \mathcal{Z} = C^{-1}\tilde{\mathcal{Z}}C$;

2) $\mathcal{Y} \subseteq \tilde{\mathcal{Z}} \subseteq M(dim\Phi, L)$;

3) $V\mathcal{Y}V^{-1} = P\mathcal{Y}P^{-1},\ V\tilde{\mathcal{Z}}V^{-1} = P\mathcal{Z}P^{-1} \subseteq M(dim\Phi, k)$.

c) $\mathcal{Z}$ $k$–rationalizable over $L$ $\Longrightarrow$ $\exists \tilde{\mathcal{Z}} \subseteq M(dim\Phi, L)$:

1) $\mathcal{Y} \subseteq \tilde{\mathcal{Z}} \subseteq M(dim\Phi, L)$;

2) $\tilde{\mathcal{Z}} = C\mathcal{Z}C^{-1}$, for some $C \in C_L^\times(\mathcal{Y})$;

3) $\tilde{\mathcal{Z}}$ is $k$–rationalizable over $L$, by some $V \in V_\Phi^\times$.

**Proof.**

a) This is just a restatement of Theorem 2.E.4, part (a).

b) ($\Longrightarrow$):

Let $P \in G\ell(dim\Phi, L)$, where $P$ $k$–rationalizes $\mathcal{Z}$. So, $P\mathcal{Z}P^{-1} \subseteq M(dim\Phi, k)$. As given $\mathcal{Y} \subseteq \mathcal{Z}$, so a fortiori, $P$ $k$–rationalizes $\mathcal{Y}$. So, by part (a) above:

(1) $P = VC$, where $V \in V_\Phi^\times, C \in C_L^\times(\mathcal{Y})$.

Now let $\tilde{\mathcal{Z}} \equiv C\mathcal{Z}C^{-1} \subseteq M(dim\Phi, L)$. Now we simply observe the following.

(1) As $C$ centralizes $\mathcal{Y}$ [by (1) above]:

$$\mathcal{Y} \subseteq \mathcal{Z} \Longrightarrow C\mathcal{Y}C^{-1} \subseteq C\mathcal{Z}C^{-1} \Longrightarrow \mathcal{Y} \subseteq C\mathcal{Z}C^{-1} \Longrightarrow \mathcal{Y} \subseteq \tilde{\mathcal{Z}}.$$

(2) a) Again, as $C$ centralizes $\mathcal{Y}$:

$$P\mathcal{Y}P^{-1} = VC\mathcal{Y}C^{-1}V^{-1} = V\mathcal{Y}V^{-1}.$$

b) By definition of $\tilde{\mathcal{Z}}$:

$$P\mathcal{Z}P^{-1} = VC\mathcal{Z}C^{-1}V^{-1} = V\tilde{\mathcal{Z}}V^{-1}.$$

c) As $P$ $k$–rationalizes $\mathcal{Z}$ [by supposition above], and using the immediately previous result:

$$V\tilde{\mathcal{Z}}V^{-1} = P\mathcal{Z}P^{-1} \subseteq M(dim\Phi, k).$$

This completes the proof of ($\Longrightarrow$).

($\Longleftarrow$):

This follows a fortiori, as by supposition here – item (3) – we already have $P\mathcal{Z}P^{-1} \subseteq M(dim\Phi, k)$.

c) The desired conclusion (c) follows at once from the desired conclusion (b) – proved just above. □

## Remark

The forward direction of part (b) of this corollary shows: "a $k$–rationalization of $\mathcal{Z} \supseteq \mathcal{Y}$, by $P \in G\ell(dim\Phi, L)$, can be 'replaced' by a $k$–rationalization of $\tilde{\mathcal{Z}} \supseteq \mathcal{Y}$, by $V$; where $\tilde{\mathcal{Z}}$ is an $L$-conjugate of $\mathcal{Z}$, and $V \in G\ell\left(dim\Phi, \overline{k}\right)$."

# Chapter 3

# Subsets of Matrices Rationalizable By, or Together With, Certain Specialized Subsets of Matrices

## 3.1 Introduction

In this short, but critical chapter, we focus attention not on the matrices that perform rationalizations, but rather on the subsets of matrices that are rationalizable. In one main result, we fix matrices from a certain class, and ask which subsets of other matrices can be rationalized *by* matrices taken from that particular class. In the next main result, we fix subsets of matrices from a certain class, and ask which other subsets of matrices can be rationalized *together with* those subsets of matrices taken from that particular class.

*Throughout this chapter*, we let $k$ be a perfect field, $L$ be any extension field of $\overline{k}$, and we let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

## 3.2 Main Results

The following theorem gives a critical result and its proof forms a key argument.

**Theorem 3.B.1** (A Key Argument)

Let $V \in V_{\Phi}^{\times}$.

Let $\mathcal{Y} \subseteq \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

**Then:**

$V$ $k$–rationalizes $\mathcal{Y}$ $\iff$ $\mathcal{Y} \subseteq Im(\Delta_{\Phi})$.

**Proof.**

($\Longleftarrow$)

1) This follows immediately by Theorem 2.D.2.

($\Longrightarrow$)

2) Suppose $V$ $k$–rationalizes $\mathcal{Y}$. Therefore:

$$(1) \qquad V\mathcal{Y}V^{-1} \subseteq M(dim\Phi, k).$$

3) Let $E$ be any intermediate field of $\overline{k}/k$, which is a Galois extension of $k$ containing $K_1, \dots, K_r$. As given $V \in V_\Phi^\times$, clearly:

$$(2) \qquad V \in G\ell(dim\Phi, E).$$

Moreover, by (1) and (2), we see: $Y \in \mathcal{Y} \implies VYV^{-1} \in M(dim\Phi, k) \implies Y \in V^{-1}M(dim\Phi, k)V \implies Y \in M(dim\Phi, E)$. Hence:

$$(3) \qquad \mathcal{Y} \subseteq M(dim\Phi, E).$$

4) Let $Y \in \mathcal{Y}$, and let $\tau \in Gal(E/k)$. Therefore, by (1): $\tau(VYV^{-1}) = VYV^{-1}$. Therefore, using (2) and (3): $\tau(V)\tau(Y)\tau(V)^{-1} = VYV^{-1}$. Therefore, by Lemma 1.D.3, part (e):

$$V\Pi_{\tau,\Phi}\tau(Y)\Pi_{\tau,\Phi}^{-1}V^{-1} = VYV^{-1}.$$

Therefore, "cancelling the $V$'s":

$$\Pi_{\tau,\Phi}\tau(Y)\Pi_{\tau,\Phi}^{-1} = Y.$$

Thus, rearranging, and summarizing:

$$(4) \qquad \forall Y \in \mathcal{Y}: \forall \tau \in Gal(E/k): \quad \tau(Y) = \Pi_{\tau,\Phi}^{-1} Y \Pi_{\tau,\Phi}.$$

5) Now we have, by the given, $\mathcal{Y} \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$, and, by (3), $\mathcal{Y} \subseteq M(dim\Phi, E)$, so at once: $\mathcal{Y} \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, E)^{(n_{\phi_i})}$. Hence, $Y \in \mathcal{Y} \implies Y = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.75em\triangle}\limits_{j=1}^{n_{\phi_i}} Y_j^{(i)}$, for some $Y_j^{(i)} \in M(a_i, E)$. Substituting this in (4), and using

the definitions of $\Pi_{\tau,\Phi}$ and $\Pi_{\tau,\phi_i}$, and the properties of $\Pi_{\tau,\phi_i}$ as a block permutation matrix, we get:

$$\begin{aligned}
\forall Y \in \mathcal{Y}\colon \forall \tau \in Gal(E/k)\colon\ & \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} \tau\left(Y_j^{(i)}\right) \\
&= \Pi_{\tau,\Phi}^{-1}\left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n_{\phi_i}} Y_j^{(i)}\right]\Pi_{\tau,\Phi} \\
&= \left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\Pi_{\tau,\phi_i}^{-1}\right]\cdot\left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\left(\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n_{\phi_i}} Y_j^{(i)}\right)\right]\cdot\left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\Pi_{\tau,\phi_i}\right] \\
&= \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\left(\Pi_{\tau,\phi_i}^{-1}\left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n_{\phi_i}} Y_j^{(i)}\right]\Pi_{\tau,\phi_i}\right) \\
&= \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n_{\phi_i}} Y^{(i)}_{p_{\tau,\phi_i}(j)}\right] = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{n_{\phi_i}} Y^{(i)}_{p_{\tau,\phi_i}(j)}.
\end{aligned}$$

Thus, from this:

(5) $$\forall Y \in \mathcal{Y}\colon \forall \tau \in Gal(E/k)\colon\ \tau\left(Y_j^{(i)}\right) = Y^{(i)}_{p_{\tau,\phi_i}(j)}.$$

6) As $\sigma^{(i)}$ enumerates $Iso(K_i/k)$, we may let:

(6) $$b_i \in \{1, \ldots, n_{\phi_i}\},\ \text{ where } \sigma^{(i)}_{b_i} = id_{K_i}.$$

We calculate, using the definition of $p_{\tau,\phi_i}$:

$$\begin{aligned}
p_{\tau,\phi_i}(b_i) &= \left(\sigma^{(i)^{-1}} \circ \mu_{\tau,\phi_i} \circ \sigma^{(i)}\right)(b_i) \\
&= \sigma^{(i)^{-1}}\left(\mu_{\tau,\phi_i}\left(\sigma^{(i)}(b_i)\right)\right) \\
&= \sigma^{(i)^{-1}}\left(\mu_{\tau,\phi_i}(id_{K_i})\right) \\
&= \sigma^{(i)^{-1}}(\tau \circ id_{K_i}) \\
&= \sigma^{(i)^{-1}}(\tau | K_i).
\end{aligned}$$

Thus, we have:

$$(7) \qquad \forall i \in \{1,\ldots,r\}\colon \quad p_{\tau,\phi_i}(b_i) = \sigma^{(i)^{-1}}(\tau|K_i).$$

Letting $j = b_i$ in (5), and using (7), we have:

$$\tau\left(Y_{b_i}^{(i)}\right) = Y_{p_{\tau,\phi_i}(b_i)}^{(i)} = Y_{\sigma^{(i)^{-1}}(\tau|K_i)}^{(i)}.$$

Thus, we have:

$$(8) \qquad \forall Y \in \mathcal{Y}\colon \forall \tau \in Gal(E/k)\colon \quad \tau\left(Y_{b_i}^{(i)}\right) = Y_{\sigma^{(i)^{-1}}(\tau|K_i)}^{(i)}.$$

As $Gal(E/K_i) \subseteq Gal(E/k)$, and using (6), we have from (8):

$$\tau \in Gal(E/K_i) \implies \tau\left(Y_{b_i}^{(i)}\right) = Y_{\sigma^{(i)^{-1}}(\tau|K_i)}^{(i)} = Y_{\sigma^{(i)^{-1}}(id_{K_i})}^{(i)} = Y_{b_i}^{(i)}.$$

As $E/K_i$ is Galois (a fortiori, as $E/k$ is Galois), the previous gives at once that: $Y_{b_i}^{(i)} \in M(a_i, K_i)$. Thus, we now have:

$$(9) \qquad \forall Y \in \mathcal{Y}\colon \forall i \in \{1,\ldots,r\}\colon \quad Y_{b_i}^{(i)} \in M(a_i, K_i).$$

7) Now for $j \in \{1,\ldots,n_{\phi_i}\}$, let $\tau_j^{(i)}$ be an extension of $\sigma_j^{(i)}$ from $K_i$ to $E$. Hence $\tau_j^{(i)} \in Gal(E/k)$, and $\sigma^{(i)^{-1}}\left(\tau_j^{(i)}\middle| K_i\right) = j$. With this, and using (9) and (8), we calculate:

$$\begin{aligned}\sigma_j^{(i)}\left(Y_{b_i}^{(i)}\right) &= \tau_j^{(i)}\left(Y_{b_i}^{(i)}\right)\\ &= Y_{\sigma^{(i)^{-1}}\left(\tau_j^{(i)}\middle|K_i\right)}^{(i)} = Y_j^{(i)}.\end{aligned}$$

Therefore, we have:

$$(10) \qquad \forall Y \in \mathcal{Y}\colon \forall i \in \{1,\ldots,r\}\colon \forall j \in \{1,\ldots,n_{\phi_i}\}\colon \quad Y_j^{(i)} = \sigma_j^{(i)}\left(Y_{b_i}^{(i)}\right).$$

8) Finally, using (10) and (9), and the definition of $\Delta_\Phi$, we see:

$$\begin{aligned} Y &= \mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{j=1}^{n_{\phi_i}} Y_j^{(i)} = \mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}\left(Y_{b_i}^{(i)}\right) \\ &= \Delta_\Phi\left(Y_{b_1}^{(1)},\ldots,Y_{b_r}^{(r)}\right) \in Im(\Delta_\Phi). \end{aligned}$$

Thus, we have:

$$\forall Y \in \mathcal{Y}: \quad Y \in Im(\Delta_\Phi).$$

I.e.,

$$\mathcal{Y} \subseteq Im(\Delta_\Phi).$$

This completes the proof of ($\Longrightarrow$).

□

**Theorem 3.B.2** (A Main Result)

Let $\mathcal{W} \subseteq Im(\Delta_\Phi)$, where $C_L(\mathcal{W}) \subseteq \mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $L' = L$ or $L' = \overline{k}$, and let $\mathcal{W} \subseteq \mathcal{Y} \subseteq \mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{i=1}^{r} M(a_i, L')^{(n_{\phi_i})}$.

(So note that $L'$ is an intermediate field of $L/\overline{k}$.)

**Then:**

$$\mathcal{Y} \text{ is } k\text{–rationalizable over } L$$

$$\Longleftrightarrow$$

$$\exists C \in \mathop{\bigcirc\mkern-14.5mu\triangle}\limits_{i=1}^{r} G\ell(a_i, L')^{(n_{\phi_i})}: \quad \mathcal{Y} \subseteq C^{-1} Im(\Delta_\Phi) C.$$

**Proof.**

($\Longleftarrow$)

Suppose $\mathcal{Y} \subseteq C^{-1}Im(\Delta_\Phi)C$, where $C \in \underset{i=1}{\overset{r}{\bigcirc\!\!\!\!\!\triangle}} G\ell\,(a_i, L')^{(n_{\phi_i})}$. Now let $V \in V_\Phi^\times$, and let $P \equiv VC \in G\ell(dim\Phi, L') \subseteq G\ell(dim\Phi, L)$. Hence, by supposition here, and by Theorem 2.D.2, we have at once:

$$\begin{aligned} P\mathcal{Y}P^{-1} &= VC\mathcal{Y}C^{-1}V^{-1} \\ &\subseteq VCC^{-1}Im(\Delta_\Phi)CC^{-1}V^{-1} \\ &= VIm(\Delta_\Phi)V^{-1} \subseteq M(dim\Phi, k). \end{aligned}$$

Thus, $P$ $k$–rationalizes $\mathcal{Y}$, and, from the above, we recall $P \in G\ell(dim\Phi, L)$.

($\Longrightarrow$)

Suppose $\mathcal{Y}$ is $k$–rationalizable over $L$. Then, as given $L' = L$ or $L' = \overline{k}$, we note at once, by Proposition App. 5 of the Appendix [with "$\mathcal{A}$" $\equiv \mathcal{Y}$], that we also have that $\mathcal{Y}$ is $k$–rationalizable over $L'$. Thus, we may let $P \in G\ell(dim\Phi, L')$, where $P$ $k$–rationalizes $\mathcal{Y}$. As we are given $\mathcal{W} \subseteq \mathcal{Y}$, so, a fortiori, $P$ $k$–rationalizes $\mathcal{W}$. As $L'$ is an intermediate field of $L/\overline{k}$, we calculate elementarily, using the given on $\mathcal{W}$, that:

$$\begin{aligned} C_{L'}(\mathcal{W}) &= C_L(\mathcal{W}) \cap M(dim\Phi, L') \\ &\subseteq \left[\mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] \cap M(dim\Phi, L') \\ &= \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \left[M(a_i, L) \cap M(a_i, L')\right]^{(n_{\phi_i})} \\ &= \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L')^{(n_{\phi_i})}. \end{aligned}$$

These two previous observations, together with the given on $\mathcal{W}$, and by Theorem 2.E.3, part (a) [with "$L$" $\equiv L'$, "$\mathcal{Y}$" $\equiv \mathcal{W}$, and "$P$" $\equiv P$], show at once that: $P = VC$; where $V \in V_{\Phi}^{\times}, C \in \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} G\ell(a_i, L')^{(n_{\phi_i})}$. And, as above, as $P$ $k$–rationalizes $\mathcal{Y}$, we have $P\mathcal{Y}P^{-1} \subseteq M(dim\Phi, k)$, and so now $VC\mathcal{Y}C^{-1}V^{-1} \subseteq M(dim\Phi, k)$. I.e., we have:

(1) $V$ $k$–rationalizes $C\mathcal{Y}C^{-1}$.

Now, as above, as $C \in \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} G\ell(a_i, L')^{(n_{\phi_i})}$, and as given $\mathcal{Y} \subseteq \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L')^{(n_{\phi_i})}$, certainly $C\mathcal{Y}C^{-1} \subseteq \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L')^{(n_{\phi_i})}$. This, with (1), and by Theorem 3.B.1, ($\Longrightarrow$), shows at once that:

$$C\mathcal{Y}C^{-1} \subseteq Im(\Delta_{\Phi}).$$

Thus, summarizing, we have:

$$\mathcal{Y} \subseteq C^{-1} Im(\Delta_{\Phi}) C, \quad \text{where } C \in \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} G\ell\,(a_i, L')^{(n_{\phi_i})}.$$

□

**Corollary 3.B.3**

Suppose $K_1 = k(\beta_1), \ldots, K_r = k(\beta_r)$, for some $\beta_1, \ldots, \beta_r \in \overline{k}$, where the $\beta_i$ are pair-wise non-conjugate over $k$.

Let $M_i$ be any *upper triangular* element of $M(a_i, K_i)$, where all the diagonal elements of $M_i$ are identical and equal to $\beta_i$.

Let $L' = L$ or $L' = \overline{k}$, and let $\mathcal{Y} \subseteq \mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, L'\right)^{\left(n_{\phi_i}\right)}$.

**Then:**

$$\mathcal{Y} \cup \{\Delta_\Phi(M_1, \ldots, M_r)\} \text{ is } k\text{–rationalizable over } L$$

$$\Longleftrightarrow$$

$$\exists C \in \mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} G\ell\left(a_i, L'\right)^{\left(n_{\phi_i}\right)} : \quad \mathcal{Y} \cup \{\Delta_\Phi(M_1, \ldots, M_r)\} \subseteq C^{-1} Im(\Delta_\Phi) C.$$

**Proof.**

By the gi

$$\begin{aligned}\{\Delta_\Phi(M_1, \ldots, M_r)\} &\subseteq \mathcal{Y} \cup \{\Delta_\Phi(M_1, \ldots, M_r)\} \\ \{ \quad &\subseteq \left[\mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, L'\right)^{\left(n_{\phi_i}\right)}\right] \cup Im(\Delta_\Phi) \\ &\subseteq \left[\mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, L'\right)^{\left(n_{\phi_i}\right)}\right] \cup Im(\Delta_\Phi) \\ &\subseteq \left[\mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, L'\right)^{\left(n_{\phi_i}\right)}\right] \cup \left[\mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, \overline{k}\right)^{\left(n_{\phi_i}\right)}\right] \\ &= \mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, L'\right)^{\left(n_{\phi_i}\right)}.\end{aligned}$$

So, summarizing:

$$\{\Delta_\Phi(M_1, \ldots, M_r)\} \subseteq \mathcal{Y} \cup \{\Delta_\Phi(M_1, \ldots, M_r)\} \subseteq \mathop{\bigcirc\mkern-15mu\triangle}_{i=1}^{r} M\left(a_i, L'\right)^{\left(n_{\phi_i}\right)}.$$

With this, and Theorem 3.B.2 [ with "$\mathcal{W}$" $\equiv \{\Delta_\Phi(M_1,\dots,M_r)\}$, and "$\mathcal{Y}$" $\equiv \mathcal{Y} \cup \{\Delta_\Phi(M_1,\dots,M_r)\}$ ], the proof is complete – save for showing that:

$$C_L\left(\Delta_\Phi(M_1,\dots,M_r)\right) \subseteq \bigodot_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})}.$$

But the latter is immediate from the following: the definition of $\Delta_\Phi$, the given about the $M_i$, Proposition App. 8, part (b), of the Appendix; and the given facts that the $\beta_i \in \overline{k}$ are pair-wise non-conjugate over $k$, and that $K_i = k(\beta_i)$, so that $\deg_k(\beta_i) = [K_i{:}\,k] = n_{\phi_i}$ — thus making all the quantities, $\sigma_j^{(i)}(\beta_i)$, distinct.

□

**Remark**

The previous corollary shall be fruitfully applied, in particular, to the following cases of $M_i$:

i) $M_i = \beta_i I_{a_i}$ (so $M_i$ is a scalar matrix).

ii) $M_i = \beta_i I_{a_i} + N_{a_i}$ (so $M_i$ is a basic Jordan block belonging to $\beta_i$).

# Chapter 4

# Rationalizable Subsets of Diagonal Matrices, and of Certain Other Classes of Matrices

## 4.1 Introduction

In this chapter, we apply the results of the previous two chapters, together with some basic results in the Appendix, to subsets of diagonal matrices and to subsets of certain other classes of matrices which include non-diagonal matrices. One main result, among others, will be an exhibition of all rationalizable subsets of diagonal matrices.

Throughout this chapter, $k$ *is a perfect field* and $L$ *is any extension field of* $\overline{k}$.

## 4.2 Rationalizable Subsets of Diagonal Matrices

The main result of this section will be an exhibition of all $k$–rationalizable subsets, of diagonal matrices, over $L$. Two exhibitions will actually be given: the first and principal exhibition (Theorem 4.B.4) is very "strong", the second and alternative exhibition (Corollary 4.B.6) is "weaker" – but will later [Chapter 7] be seen to have its uses.

The following Lemma allows the key inductive step for the proof of the main part of the exhibition result of Theorem 4.B.4.

**Lemma 4.B.1**

Let $\phi = (K, \sigma, a)$ be a field element over $k$.

Let $\Omega = (\omega_1, \ldots, \omega_s)$ be a field setting *over* $K$, with $\omega_j = \left(L_j, \tau^{(j)}, b_j\right)$ a field element *over* $K$.

Suppose that: $\dim \Omega = a \quad \left(\text{so, } \sum_{j=1}^{s} b_j[L_j : K] = a\right)$.

Let $E$ be any intermediate field of $\overline{k}/k$, which is a Galois extension of $k$, containing $L_1, \ldots, L_s$. (So note, a fortiori, $E$ contains $K$ — as all the $L_j$ contain $K$.)

Finally, by the imbedding extension theorem for field extensions, we may let $\tilde{\sigma}_i \in Gal(E/k)$ be an extension of $\sigma_i \in \text{Iso}(K/k)$. And with this, we let $\tilde{\Delta}_\phi$ be the corresponding extension of $\Delta_\phi$, from $M(a, K)$ to $M(a, E)$; i.e., $\tilde{\Delta}_\phi(M) =$

$\bigotimes_{i=1}^{n_\phi} \tilde{\sigma}_i(M)$, for $M \in M(a, E)$. (So clearly, $\tilde{\Delta}_\phi$ is also an imbedding of $k$–algebras.)

**Then:**

$\exists \Pi \in \mathrm{Perm}(\dim \phi, k)$: $\exists \Omega' = (\omega_1', \dots, \omega_s')$ a field setting *over* $k$, with $\omega_j' = \left(L_j, \tau'^{(j)}, b_j\right)$ a field element *over* $k$:

1) a) $\dim \Omega' = \dim \phi$;

   b) $\mathrm{Domain}(\Delta_{\Omega'}) = \mathrm{Domain}(\Delta_{\Omega'})$.

2) $\tilde{\Delta}_\phi \circ \Delta_\Omega = conj_\Pi \circ \Delta_{\Omega'}$.

[Recall, $conj_\Pi$ is the matrix conjugation map: $conj_\Pi(M) \equiv \Pi^{-1} M \Pi$.]

**Proof.**

1) We note that $\phi = (K, \sigma, a)$ is a field element over $k$. In particular, $K$ is a finite extension of $k$, and thus, as $k$ is given to be perfect, so is $K$.

2) For $j \in \{1, \dots, s\}$, let:

$$S_j \equiv \left\{ \tilde{\sigma}_i \circ \tau_\ell^{(j)} \middle| \, (i, \ell) \in \{1, \dots, n_\phi\} \times \left\{1, \dots, n_{\omega_j}\right\} \right\}.$$

(And note, by definition, $n_{\omega_j} = [L_j : K]$.) We claim $S_j = \mathrm{Iso}\left(L_j/k\right)$. Firstly, we note that as $E \supseteq L_j$, $\tilde{\sigma}_i \in Gal(E/k)$, and $\tau_\ell^{(j)} \in \mathrm{Iso}\left(L_j/K\right)$, we clearly have $S_j \subseteq \mathrm{Iso}\left(L_j/k\right)$. Secondly, as $k$ is perfect, we note that $\left|\mathrm{Iso}\left(L_j/k\right)\right| = [L_j : k]$. We now show that $|S_j| = [L_j : k]$, which proves the claim.

3) Suppose:

$$(1) \qquad \widetilde{\sigma}_{i_1} \circ \tau^{(j)}_{\ell_1} = \widetilde{\sigma}_{i_2} \circ \tau^{(j)}_{\ell_2}.$$

In particular, for all $\beta \in K$:

$$\begin{aligned} \widetilde{\sigma}_{i_1}\left(\tau^{(j)}_{\ell_1}(\beta)\right) &= \widetilde{\sigma}_{i_2}\left(\tau^{(j)}_{\ell_2}(\beta)\right). \\ \widetilde{\sigma}_{i_1}(\beta) &= \widetilde{\sigma}_{i_2}(\beta). \qquad [\text{ as } \beta \in K.\ ] \end{aligned}$$

As $\beta$ is arbitrary in $K$: $\widetilde{\sigma}_{i_1}|\,K = \widetilde{\sigma}_{i_2}|\,K$. So, by the given construction of $\widetilde{\sigma}_i$: $\sigma_{i_1} = \sigma_{i_2}$. As $\sigma$ is injective:

$$(2) \qquad i_1 = i_2.$$

Substituting this in (1), and composing on the left by $\widetilde{\sigma}_{i_1}^{-1}$, we have: $\tau^{(j)}_{\ell_1} = \tau^{(j)}_{\ell_2}$. As $\tau^{(j)}$ is injective:

$$(3) \qquad \ell_1 = \ell_2.$$

So, by the definition of $S_j$, and (1), (2), (3) above, we have at once: $|S_j| = n_\phi \cdot n_{\omega_j} = [K : k][L_j : K] = [L_j : k]$. As discussed above in part (2), this proves the claim stated in part (2), and so we have:

$$(4) \qquad S_j = \operatorname{Iso}\left(L_j/k\right).$$

4) By (4) and the definition of $S_j$, we may let $\tau'^{(j)}$ be the enumerator of $\operatorname{Iso}(L_j/k)$ that "spells out" the elements of $S_j$ in "the dictionary order" indicated in $S_j$'s definition. I.e., we may let:

$$\tau'^{(j)}_1, \ldots, \tau'^{(j)}_{[L_j:k]} = \widetilde{\sigma}_1 \circ \tau^{(j)}_1, \ldots, \widetilde{\sigma}_{n_\phi} \circ \tau^{(j)}_{n_{\omega_j}}.$$

Furthermore, we let $\omega'_j \equiv \left(L_j, \tau'^{(j)}, b_j\right)$, a field element *over* $K$; and we let $\Omega' \equiv (\omega'_1, \ldots, \omega'_s)$; a field setting *over* $K$.

5) Using the definitions of $\Omega$, $\tau^{(j)}$, $\Omega'$, $\tau'^{(j)}$, and Lemma 1.D.1, we have some $\Pi \in \mathrm{Perm}(\dim \phi, k)$, so that for any $N_j \in M\left(b_j, L_j\right)$, we have:

$$\begin{aligned}
\left(\widetilde{\Delta}_\phi \circ \Delta_\Omega\right)(N_1, \ldots, N_s) &= \widetilde{\Delta}_\phi\left(\Delta_\Omega\left(N_1, \ldots, N_s\right)\right) \\
&= \widetilde{\Delta}_\phi\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{s}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{\ell=1}^{n_{\omega_j}}\tau_\ell^{(j)}(N_j)\right) \\
&= \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n_\phi}\widetilde{\sigma}_i\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{s}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{\ell=1}^{n_{\omega_j}}\tau_\ell^{(j)}(N_j)\right) \\
&= \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n_\phi}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{s}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{\ell=1}^{n_{\omega_j}}\left(\widetilde{\sigma}_i\tau_\ell^{(j)}\right)(N_j) \\
&= \Pi^{-1}\left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{s}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n_\phi}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{\ell=1}^{n_{\omega_j}}\left(\widetilde{\sigma}_i\tau_\ell^{(j)}\right)(N_j)\right]\Pi \\
&= \Pi^{-1}\left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{s}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{[L_j:k]}\tau_t'^{(j)}(N_j)\right]\Pi \\
&= \Pi^{-1}\left[\Delta_{\Omega'}(N_1, \ldots, N_s)\right]\Pi \\
&= (conj_\Pi \circ \Delta_{\Omega'})(N_1, \ldots, N_s).
\end{aligned}$$

As the $N_j$ are arbitrary in the previous, we have:

$$\widetilde{\Delta}_\phi \circ \Delta_\Omega = conj_\Pi \circ \Delta_{\Omega'}.$$

6) Finally, by the definitions of $\Omega'$ and $\Omega$, and recalling that we are given $\dim \Omega = a$, we easily observe:

$$\begin{aligned}\dim \Omega' &= \sum_{j=1}^{s} \dim \omega_j' = \sum_{j=1}^{s} b_j [L_j : k] \\ &= \sum_{j=1}^{s} b_j [L_j : K][K : k] \\ &= \sum_{j=1}^{s} (\dim \omega_j)\, n_\phi = n_\phi \sum_{j=1}^{s} \dim \omega_j \\ &= n_\phi \cdot \dim \Omega = n_\phi \cdot a = \dim \phi.\end{aligned}$$

$$\mathrm{Domain}(\Delta_{\Omega'}) = \prod_{j=1}^{s} M(b_j, L_j) = \mathrm{Domain}(\Delta_\Omega).$$

□

The following Lemma will be used to establish Lemma 4.B.3.

**Lemma 4.B.2**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

For $i \in \{1, \ldots, r\}$, let $F_i$ be a subfield of $K_i$.

**Then:**

$\exists \Pi \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \operatorname{Perm}(a_i n_{\phi_i}, I_{a_i}, k) : \exists \Omega = (\omega_1, \ldots, \omega_r)$ a field setting over $k$, with $\omega_i$ a field element over $k$:

$$\omega_i = \left(F_i, \gamma^{(i)}, a_i[K_i \colon F_i]\right) \quad \text{and}$$

$\forall (N_1, \ldots, N_r) \in \prod_{i=1}^{r} M(a_i, F_i)$:

$$\Delta_\Phi(N_1, \ldots, N_r) = \Pi^{-1} \Delta_\Omega \left(N_1^{([K_1:F_1])}, \ldots, N_r^{([K_r:F_r])}\right) \Pi.$$

[Recall, for $M$ a matrix and $e \in \mathbb{Z}^+$: $\quad M^{(e)} \equiv \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{e} M$.]

**Proof.**

1) Let $\nu^{(i)}$ be any enumerator for $\operatorname{Iso}(F_i/k)$; and let $\omega_i \equiv \left(F_i, \nu^{(i)}, a_i[K_i : F_i]\right)$ be a field element over $k$, and let $\Omega \equiv (\omega_1, \ldots, \omega_r)$ be a field setting over $k$.

2) As $k$ is perfect, the imbedding extension theorem for fields shows that each imbedding of $\operatorname{Iso}(F_i/k)$ extends to precisely $[K_i : F_i]$ imbeddings of $\operatorname{Iso}(K_i/k)$, and that these form all the imbeddings of $\operatorname{Iso}(K_i/k)$. So, as $\sigma^{(i)}$ is an enumerator of $\operatorname{Iso}(K_i/k)$, the sequence: $\sigma_1^{(i)}\big| F_i, \ldots, \sigma_{n_{\phi_i}}^{(i)}\big| F_i$, is a permutation of the $[K_i : F_i]$-fold repetition of the sequence: $\nu_1^{(i)}, \ldots, \nu_{n_{\omega_i}}^{(i)}$.

3) Using the previous remarks, the fact that $n_{\omega_i} = [F_i : k]$ here (by definition), and Lemma 1.D.1, we have some $\Pi_i \in \operatorname{Perm}(a_i n_{\phi_i}, I_{a_i}, k)$, so that for any $N_i \in M(a_i, F_i)$, we have:

$$\begin{aligned}
\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(N_i) &= \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \left(\sigma_j^{(i)}\middle| F_i\right)(N_i) \\
&= \Pi_i^{-1}\left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\omega_i}} \mathop{\textcircled{$\triangle$}}_{t=1}^{[K_i:F_i]} \nu_j^{(i)}(N_i)\right]\Pi_i \\
&= \Pi_i^{-1}\left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\omega_i}} \left(\nu_j^{(i)}(N_i)\right)^{([K_i:F_i])}\right]\Pi_i \\
&= \Pi_i^{-1}\left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\omega_i}} \nu_j^{(i)}\left(N_i^{([K_i:F_i])}\right)\right]\Pi_i .
\end{aligned}$$

Thus, using the definition of $\Omega$ above, we have:

$$\begin{aligned}
\Delta_\Phi(N_1,\ldots,N_r) &= \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(N_i) \\
&= \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\left[\Pi_i^{-1}\left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\omega_i}} \nu_j^{(i)}\left(N_i^{([K_i:F_i])}\right)\right]\Pi_i\right] \\
&= \Pi^{-1}\Delta_\Omega\left(N_1^{([K_1:F_1])},\ldots,N_r^{([K_r:F_r])}\right)\Pi, \\
&\text{where}\quad \Pi \equiv \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\Pi_i \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k).
\end{aligned}$$

□

The following lemma, Lemma 4.B.3, will be used in the proof of Theorem 4.B.4, ($\Longrightarrow$) — only at the very end, and only to establish (and at once) the conclusion "(iv)" of that Theorem. In this regard, we mention the following two things.

i) Conclusion "(iv)" of Theorem 4.B.4, while nice to have, is something of a "separate extra" in the context of that Theorem. That is to say, the principal result of Theorem 4.B.4 is contained in its conclusions "(i)–(iii)" — and it could well have been presented just that way. In this important and structural sense, Lemma 4.B.3 has nothing to do with the principal result of Theorem 4.B.4, and both Lemma 4.B.3 and conclusion "(iv)" of Theorem 4.B.4 could have been left out here and introduced at a later point. They were included here to get the complete result of Theorem 4.B.4 sooner.

ii) Lemma 4.B.3, and conclusion "(iv)" of Theorem 4.B.4, will be seen to have very nice, and powerful, uses, in later applications in this paper.

The following lemma makes use of the 3-tuple indexing scheme of a field setting, which was defined and discussed in Chapter 1, Section 3, Subsection 7. As there, the set of indices for this scheme is denoted $\mathcal{I}_\Phi$, where $\Phi$ is the field setting it is based on.

**Lemma 4.B.3**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

Let $\mathcal{Z} \subseteq \Delta_\Phi\left(\prod_{i=1}^{r} \text{Scalar}(a_i, K_i)\right)$, where $C_L(\mathcal{Z}) = \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $\mathcal{Z} \subseteq \Delta_\Phi\left(\prod_{i=1}^{r} \text{Scalar}(a_i, K_i)\right)$, where $C_L(\mathcal{Z}) = \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

**Then:**

$$\forall (i,j,t) \in \mathcal{I}_\Phi\colon \quad \sigma_j^{(i)}(K_i) = k\left(\mathcal{Z}_{(i,j,t)}\right).$$

$$[\,\text{Here,}\quad \mathcal{Z}_{(i,j,t)} \equiv \left\{ Z_{(i,j,t)} \,\middle|\, Z \in \mathcal{Z} \right\}.\,]$$

**Proof.**

1) As $\mathcal{Z} \subseteq \Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)\right)$, we certainly have $\mathcal{Z} = \Delta_\Phi(\mathcal{U})$, for some $\mathcal{U} \subseteq \prod_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)$. Furthermore then, if $U \in \mathcal{U}$, then $U = (\alpha_1(U)I_{a_1}, \dots, \alpha_r(U)I_{a_r})$, where $\alpha_1(U) \in K_1, \dots, \alpha_r(U) \in K_r$. Let $\mathcal{U}_i \equiv \{\alpha_i(U) | U \in \mathcal{U}\}$, and so note that $\mathcal{U}_i \subseteq K_i$. Finally, let $F_i \equiv k(\mathcal{U}_i)$. So clearly:

(1) $\quad F_i$ is a subfield of $K_i$, $\quad \mathcal{Z} \subseteq \Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i, F_i)\right)$.

2) From (1), we have at once by Lemma 4.B.2 that:

$$\exists \Pi \in \mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{r} \mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k) \colon \exists \Omega = (\omega_1, \dots, \omega_r), \text{ a field setting over } k:$$

a) $\forall i \in \{1, \dots, r\}\colon \quad \omega_i = \left(F_i, \nu^{(i)}, b_i\right), \; b_i = a_i[K_i : F_i]$;

b) $\forall (N_1, \dots, N_r) \in \prod_{i=1}^{r} M(a_i, F_i)$:

$$\Delta_\Phi(N_1, \dots, N_r) = \Pi^{-1}\Delta_\Omega\left(N_1^{([K_1:F_1])}, \dots, N_r^{([K_r:F_r])}\right)\Pi.$$

3) In particular then, the previous shows that:

$$\alpha_1 \in F_1, \dots, \alpha_r \in F_r \quad \Longrightarrow$$

$$\Delta_\Phi\left(\alpha_1 I_{a_1}, \dots, \alpha_r I_{a_r}\right) = \Pi^{-1}\Delta_\Omega\left((\alpha_1 I_{a_1})^{([K_1:F_1])}, \dots, (\alpha_r I_{a_r})^{([K_r:F_r])}\right)\Pi.$$

Now clearly (just write it out!):

$$(\alpha_i I_{a_i})^{([K_i:F_i])} = \alpha_i I_{a_i[K_i:F_i]} = \alpha_i I_{b_i},$$

where the last equality follows from part (2) above – item (a). Thus, the previous shows:

$$\Delta_\Phi(\alpha_1 I_{a_1}, \dots, \alpha_r I_{a_r}) = \Pi^{-1}\Delta_\Omega\left(\alpha_1 I_{b_1}, \dots, \alpha_r I_{b_r}\right)\Pi.$$

So, as $\alpha_1 \in F_1, \ldots, \alpha_r \in F_r$, we have:

$$\Delta_\Phi\left(\prod_{i=1}^{r}\text{Scalar}(a_i, F_i)\right) \subseteq \Pi^{-1}\Delta_\Omega\left(\prod_{i=1}^{r}\text{Scalar}(b_i, F_i)\right)\Pi. \tag{2}$$

4) From (1) and (2) we have:

$$\mathcal{Z} \subseteq \Delta_\Phi\left(\prod_{i=1}^{r}\text{Scalar}(a_i, F_i)\right) \subseteq \Pi^{-1}\Delta_\Omega\left(\prod_{i=1}^{r}\text{Scalar}(b_i, F_i)\right)\Pi.$$

So, from the previous, together with Lemma 2.D.1, part (b,i), we have:

$$\begin{aligned} C_L(\mathcal{Z}) &\supseteq C_L\left(\Pi^{-1}\Delta_\Omega\left(\prod_{i=1}^{r}\text{Scalar}(b_i, F_i)\right)\Pi\right) \\ &= \Pi^{-1}C_L\left(\Delta_\Omega\left(\prod_{i=1}^{r}\text{Scalar}(b_i, F_i)\right)\right)\Pi \\ &= \Pi^{-1}\left[\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(b_i, L)^{([F_i:k])}\right]\Pi. \end{aligned} \tag{3}$$

Therefore: $$C_L(\mathcal{Z}) \supseteq \Pi^{-1}\left[\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(b_i, L)^{([F_i:k])}\right]\Pi.$$

5) Now, by the given, we have: $C_L(\mathcal{Z}) = \mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(a_i, L)^{\left(n_{\phi_i}\right)}$. This, with (3), shows:

$$\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(a_i, L)^{\left(n_{\phi_i}\right)} \supseteq \Pi^{-1}\left[\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(b_i, L)^{([F_i:k])}\right]\Pi.$$

Therefore:

$$\Pi\left[\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(a_i, L)^{\left(n_{\phi_i}\right)}\right]\Pi^{-1} \supseteq \mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M(b_i, L)^{([F_i:k])}. \tag{4}$$

6) We now observe that the left-hand side of (4) is "invariant" under conjugation by $\Pi$ — in the sense that the conjugation by $\Pi$ may be "dropped" from the left-hand side of (4). We see this directly, as follows.

In part (2) above here, we have $\Pi \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \operatorname{Perm}(a_i n_{\phi_i}, I_{a_i}, k)$, and so $\Pi = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \Pi_i$, for some $\Pi_i \in \operatorname{Perm}(a_i n_{\phi_i}, I_{a_i}, k)$. Thus, $\Pi_i$ is a block permutation matrix, "made up of" $a_i \times a_i$ subblocks that are either $I_{a_i}$ ($a_i \times a_i$ identity-matrix) or $O_{a_i}$ ($a_i \times a_i$ zero-matrix). Consequently, and as described in Chapter 1, Section 2, Subsection 4, Part (d), conjugation by $\Pi_i$ acts on a block diagonal matrix — all of whose subblocks are $a_i \times a_i$ matrices — by permuting these $a_i \times a_i$ subblocks around. I.e., in particular, we have: $M \in M(a_i, L)^{(n_{\phi_i})} \implies \Pi_i M \Pi_i^{-1} \in M(a_i, L)^{(n_{\phi_i})}$. So clearly, applying this result to the entire *set* of such block diagonal matrices, we get:

$$\Pi_i \left[ M(a_i, L)^{(n_{\phi_i})} \right] \Pi_i^{-1} = M(a_i, L)^{(n_{\phi_i})}.$$

Now we calculate, using the previous at the last step:

$$\begin{aligned} \Pi \left[ \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})} \right] \Pi^{-1} &= \left[ \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \Pi_i \right] \left[ \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})} \right] \left[ \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \Pi_i^{-1} \right] \\ &= \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \Pi_i \left[ M(a_i, L)^{(n_{\phi_i})} \right] \Pi_i^{-1} \\ &= \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}. \end{aligned}$$

Putting this in (4), we now get:

$$\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})} \supseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(b_i, L)^{([F_i:k])}. \tag{5}$$

7) Now, "writing out" the sets of matrices on both sides of (5), and comparing the "upper left-hand corners" of the matrices that form these sets, we see at once,

in particular, that:

$$a_1 \geq b_1.$$

So, by part (2) above here – item (a), we get:

$$\begin{aligned} a_1 &\geq a_1[K_1 : F_1]. \\ \text{Therefore:} \qquad 1 &\geq [K_1 : F_1]. \end{aligned}$$

Thus, $[K_1 : F_1] = 1$, and so $K_1 = F_1$.

(6) Therefore: $K_1 = F_1$.

So, furthermore now: $b_1 = a_1[K_1 : F_1] = a_1 \cdot 1 = a_1$, and $[F_1 : k] = [K_1 : k] = n_{\phi_1}$. Therefore:

(7) $a_1 = b_1$ and $n_{\phi_1} = [F_1 : k]$.

8) Now using (7) in (5) clearly allows us to "knock off" the "upper left-hand (= first)" diagonal block from the matrices of the sets of each side of (5) [ write it out! ], and this then gives:

$$\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=2}^{r} M(a_i, L)^{(n_{\phi_i})} \supseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=2}^{r} M(b_i, L)^{([F_i:k])}.$$

So, following the argument in part (7) above, inductively, we find:

(8) $F_i = K_i$, $a_i = b_i$, $n_{\phi_i} = [F_i : k]$; for all $i \in \{1, \ldots, r\}$.

9) Now recall from part (1) here that:

$$F_i = k(\mathcal{U}_i).$$

This, with (8), gives:

$$(9) \qquad K_i = k(\mathcal{U}_i).$$

10) Now recall again, from part (1), the following:

$$\mathcal{Z} = \Delta_\Phi(\mathcal{U}), \quad \mathcal{U} \subseteq \prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i);$$

$$U \in \mathcal{U} \implies U = (\alpha_1(U) I_{a_1}, \ldots, \alpha_r(U) I_{a_r}), \ \alpha_i(U) \in K_i.$$

So clearly, recalling the 3-tuple indexing scheme of a field setting – discussed in Chapter 1, Section 3, Subsection 7, the above shows:

$$Z = \Delta_\Phi(U) \implies Z_{(i,j,t)} = \sigma_j^{(i)}(\alpha_i(U)), \ \text{for all } (i,j,t) \in \mathcal{I}_\Phi.$$

Thus, in particular, we have:

$$\begin{aligned} \mathcal{Z}_{(i,j,t)} &\equiv \left\{ Z_{(i,j,t)} \middle| Z \in \mathcal{Z} \right\} = \left\{ \sigma_j^{(i)}(\alpha_i(U)) \middle| U \in \mathcal{U} \right\} \\ &= \sigma_j^{(i)} \left( \{ \alpha_i(U) | U \in \mathcal{U} \} \right) = \sigma_j^{(i)}(\mathcal{U}_i); \end{aligned}$$

using the definition of $\mathcal{U}_i$ from part (1) here. Hence:

$$(i,j,t) \in \mathcal{I}_\Phi \implies \mathcal{Z}_{(i,j,t)} = \sigma_j^{(i)}(\mathcal{U}_i).$$

This, with (9), shows:

$$k\left(\mathcal{Z}_{(i,j,t)}\right) = k\left(\sigma_j^{(i)}(\mathcal{U}_i)\right) = \sigma_j^{(i)}(k(\mathcal{U}_i)) = \sigma_j^{(i)}(K_i).$$

So, finally:

$$(i,j,t) \in \mathcal{I}_\Phi \implies \sigma_j^{(i)}(K_i) = k\left(\mathcal{Z}_{(i,j,t)}\right).$$

□

**Theorem 4.B.4** (A Main Result)

Let $n \in \mathbb{Z}^{+}$.

Let $\mathcal{Y} \subseteq D(n, L)$.

**Then:**

$$\mathcal{Y} \text{ is } k\text{–rationalizable over } L$$

$$\Longleftrightarrow$$

$$\mathcal{Y} \subseteq D(n, L) \quad \text{and} \quad \exists \Pi \in \operatorname{Perm}(n, k)\colon \exists \Phi = (\phi_1, \ldots, \phi_r), \text{ a field setting over } k;$$

$$\text{with } \phi_i = \left(K_i, \sigma^{(i)}, a_i\right), \text{ a field element over } k\text{:}$$

i) $\dim\Phi = n$;

ii) $\mathcal{Y} \subseteq \Pi^{-1}\Delta_{\Phi}\left(\prod_{i=1}^{r}\operatorname{Scalar}(a_i, K_i)\right)\Pi$;

iii) $C_L(\mathcal{Y}) = C_L\left(\Pi^{-1}\Delta_{\Phi}\left(\prod_{i=1}^{r}\operatorname{Scalar}(a_i, K_i)\right)\Pi\right) = \Pi^{-1}\left[\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]\Pi$;

iv) $\forall (i, j, t) \in \mathcal{I}_{\Phi}\colon \quad \sigma_j^{(i)}(K_i) = k\left((\Pi\mathcal{Y}\Pi^{-1})_{(i,j,t)}\right)$;

$$\text{here, } \quad (\Pi\mathcal{Y}\Pi^{-1})_{(i,j,t)} \equiv \left\{(\Pi Y \Pi^{-1})_{(i,j,t)} \,\middle|\, Y \in \mathcal{Y}\right\}.$$

**Proof.**

($\Longleftarrow$)

1) Let $\mathcal{Z} \equiv \Pi\mathcal{Y}\Pi^{-1}$; so that, in particular, by (ii):

$$\mathcal{Z} \subseteq Im(\Delta_\phi) \subseteq \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.$$

Let $V \in V_\Phi^\times$; so that, at once, by Theorem 3.B.1: $Vk$ = rationalizes $\mathcal{Z}$. Thus, $V\Pi$ certainly $k$-rationalizes $\mathcal{Y}$. Also note that clearly $V \in V_\Phi^\times \subseteq G\ell(n, \overline{k}) \subseteq G\ell(n, L)$.

This completes the proof of ($\Longleftarrow$).

($\Longrightarrow$)

2) Firstly, we make several simple observations. We may let $P \in G\ell(n, L)$ where $P$ $k$-rationalizes $\mathcal{Y}$:

$$P\mathcal{Y}P^{-1} \subseteq M(n, k).$$

a) Suppose $Y \in \mathcal{Y}$. Hence, $Y \in \mathcal{Y} \subseteq D(n, L)$ and $P\mathcal{Y}P^{-1} \subseteq M(n,k) \Longrightarrow PYP^{-1} \in M(n,k) \Longrightarrow$ charpoly($Y$) $\in k[x] \Longrightarrow$ (as $Y$ is diagonal) the diagonal entries of $Y$ are all in $\overline{k}$. Thus: $Y \in \mathcal{Y} \Longrightarrow Y \in D\left(n, \overline{k}\right)$. Thus:

$$\mathcal{Y} \subseteq D\left(n, \overline{k}\right). \tag{1}$$

b) Suppose $\mathcal{Y} \subseteq \text{Scalar}(n, L)$, and suppose $Y \in \mathcal{Y}$. Hence, $Y \in \mathcal{Y} \Longrightarrow Y = \lambda I_n$, for some $\lambda \in L \Longrightarrow$ (as $P\mathcal{Y}P^{-1} \subseteq M(n,k)$) $P\lambda I_n P^{-1} \in M(n,k) \Longrightarrow \lambda I_n \in M(n,k) \Longrightarrow \lambda \in k$. Thus:

$$\mathcal{Y} \subseteq \text{Scalar}(n, L) \quad \Longrightarrow \quad \mathcal{Y} \subseteq \text{Scalar}(n, k).$$

c) Suppose $\mathcal{Y} \subseteq \text{Scalar}(n, L)$. Thus, by the previous, we have $\mathcal{Y} \subseteq \text{Scalar}(n, k)$. Now let $\Pi \equiv I_n$; $r \equiv 1$; $\Phi \equiv (\phi_1)$, with $\phi_1 \equiv (k, \sigma, n)$, where $\sigma$ is any enumerator of $\text{Iso}(k/k) = \{id_k\}$. With these definitions, we compute:

i) $\dim\Phi = \dim\phi_1 = n \cdot [k : k] = n$;

ii)
$$\begin{aligned} \mathcal{Y} &\subseteq \text{Scalar}(n,k) = \Pi^{-1}[\text{Scalar}(n,k)]\Pi \\ &= \Pi^{-1}\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{1} id_k\,(\text{Scalar}(n,k))\right]\Pi \\ &= \Pi^{-1}\left[\Delta_\Phi\left(\prod_{i=1}^{r}\text{Scalar}\left(a_{\phi_i}, K_{\phi_i}\right)\right)\right]\Pi; \end{aligned}$$

iii)
$$\begin{aligned} C_L(\mathcal{Y}) &= M(n,L) \qquad [\text{ as } \mathcal{Y} \subseteq \text{Scalar}(n,L)\ ] \\ &= \mathop{\textcircled{$\triangle$}}_{i=1}^{1} M(n,L)^{(1)} \\ &= \mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(n,L)^{(n_{\phi_i})}\ [\text{ as } n_{\phi_1} = [k:k] = 1\ ] \quad . \end{aligned}$$

The conclusion (iii) of the Theorem follows at once from the previous and Lemma 2.D.1, part (b,i).

The conclusion (iv) of the Theorem follows at once from (ii) & (iii) above, and Lemma 4.B.3 (with "$\mathcal{Z}$" $\equiv \Pi\mathcal{Y}\Pi^{-1}$).

Thus:

$$(2) \qquad \mathcal{Y} \subseteq \mathrm{Scalar}(n, L) \quad \Longrightarrow \quad (\Longrightarrow) \text{ is true for } \mathcal{Y}.$$

3) We now prove $(\Longrightarrow)$, by induction on $n$. For $n = 1$, certainly $D(n, L) = \mathrm{Scalar}(n, L)$, and so we are done here, by (2). Suppose now that $n \geq 2$, and that $(\Longrightarrow)$ is true for $1, \ldots, n-1$. We will show that $(\Longrightarrow)$ is true for $n$. If $\mathcal{Y} \subseteq \mathrm{Scalar}(n, L)$, then we are immediately done here, again, by (2).

4) In view of the previous, we may suppose $\mathcal{Y} \not\subseteq \mathrm{Scalar}(n, L)$, and we may let $P \in G\ell(n, L)$ where $P$ $k$-rationalizes $\mathcal{Y}$. So, for some $Y_0 \in \mathcal{Y}$: $Y_0 \notin \mathrm{Scalar}(n, L)$. Let $f_0 \equiv$ charpoly $(Y_0)$. By observation (2,a) above, we have $f_0 \in k[x]$. Moreover, $f_0$ is certainly monic and $deg(f_0) = n$ (as $\mathcal{Y} \subseteq D(n, L)$). Thus, we may factor $f_0$ into its canonical factorization into monic irreducibles of $k[x]$:

$$f_0 = \prod_{i=1}^{r} p_i^{a_i};$$

for some $r \in \mathbb{Z}^+, a_i \in \mathbb{Z}^+, p_i$ distinct monic irreducibles of $k[x]$.

We next observe that $a_i < n$, for all $i \in \{1, \ldots, r\}$. Certainly we have $a_i \leq n$, for all $i \in \{1, \ldots, r\}$ (as $deg(f_0) = n$), and so if $a_{i_0} = n$, then the fact that $deg(f_0) = n$ clearly forces $deg(p_{i_0}) = 1$ and $r = 1$. Thus $f_0 = p_{i_0}^n$, $deg(p_{i_0}) = 1$. So, $f_0$ has a single root [necessarily, even, in $k$], repeated $n$ times. As $f_0 = \mathrm{charpoly}(Y_0)$, and $Y_0$ is diagonal (as $Y_0 \in \mathcal{Y}$), this forces $Y_0 \in \text{Scalar}\ (n, L)$ – contrary to the selection of $Y_0$ above. Thus:

$$(3) \qquad \forall i \in \{1, \ldots, r\}: \quad a_i < n.$$

5) With the above, we let $\beta_i \in \overline{k}$ be any root of $p_i$, and we let $K_i \equiv k(\beta_i)$. We note then that $p_i = \text{minpoly}_k(\beta_i)$. We let $\phi_i$ be the field element defined as $\phi_i \equiv \left(K_i, \sigma^{(i)}, a_i\right)$, where $\sigma^{(i)}$ is any enumerator of $\text{Iso}(K_i/k)$, and we let $\Phi$ be the field setting defined as $\Phi = (\phi_1, \ldots, \phi_r)$. We note that $n_{\phi_i} = [K_i : k] = [k(\beta_i) : k] = deg\,(\text{minpoly}_k(\beta_i)) = deg(p_i)$, and so

$$\dim \Phi = \sum_{i=1}^{r} \dim \phi_i = \sum_{i=1}^{r} a_i n_{\phi_i} = \sum_{i=1}^{r} a_i deg(p_i) = deg(f_0) = n.$$

Thus:

$$(4) \qquad \dim \Phi = n.$$

6) Now let $M_i \equiv \beta_i I_{a_i} \in \text{Scalar}(a_i, K_i)$, and let $M \equiv (M_1, \ldots, M_r) \in \prod_{i=1}^{r} \text{Scalar}(a_i, K_i)$. As $K_i = k(\beta_i), k$ is perfect, and $\sigma^{(i)}$ enumerates $\text{Iso}(K_i/k)$, clearly $\sigma_1^{(i)}(\beta_i), \ldots, \sigma_{n_{\phi_i}}^{(i)}(\beta_i)$ are all distinct and are precisely the roots of $\text{minpoly}_k(\beta_i) = p_i$. Thus, $\Delta_{\phi_i}(M_i)$ is a diagonal matrix and

$$\begin{aligned}
\text{charpoly}\left(\Delta_{\phi_i}(M_i)\right) &= \text{charpoly}\left(\mathop{\bigcirc\hspace{-0.75em}\triangle}_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(\beta_i) I_{a_i}\right) \\
&= \prod_{j=1}^{n_{\phi_i}} \left(x - \sigma_j^{(i)}(\beta_i)\right)^{a_i} \\
&= \left[\prod_{j=1}^{n_{\phi_i}} \left(x - \sigma_j^{(i)}(\beta_i)\right)\right]^{a_i} = p_i^{a_i}.
\end{aligned}$$

So, finally, $\Delta_\Phi(M)$ is a diagonal matrix and $\mathrm{charpoly}(\Delta_\Phi(M)) = \mathrm{charpoly}\left(\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\Delta_{\phi_i}(M_i)\right) = \prod\limits_{i=1}^{r}\mathrm{charpoly}\left(\Delta_{\phi_i}(M_i)\right) = \prod\limits_{i=1}^{r} p_i^{a_i} = f_0$. Hence, $Y_0$ and $\Delta_\Phi(M)$ are diagonal matrices with the same characteristic polynomial — and hence with the same set of diagonal entries, multiplicity respected, and so they are conjugate by a permutation matrix. Thus:

(5) $\quad \Psi Y_0 \Psi^{-1} = \Delta_\Phi(M), \quad$ for some $\Psi \in \mathrm{Perm}(n,k)$.

7) Now we have from above that $P \in G\ell(n,L)$ where $P$ $k$–rationalizes $\mathcal{Y}$. Let $\mathcal{Z} \equiv \Psi\mathcal{Y}\Psi^{-1} \subseteq D\left(n,\overline{k}\right)$ [by (1)] and let $Q \equiv P\Psi^{-1} \in G\ell(n,L)$. Using (5), clearly $\Delta_\Phi(M) \in \mathcal{Z}$ and $Q$ $k$–rationalizes $\mathcal{Z}$. Thus:

(6) $\quad \mathcal{Z} = \mathcal{Z} \cup \{\Delta_\Phi(M)\} \quad$ is $k$–rationalizable over $L$.

Noting that $\beta_1, \ldots, \beta_r$ are pair-wise non-conjugate over $k$ (as $\beta_i$ is a root of $p_i$, and the $p_i$ are distinct monic irreducibles of $k[x]$), and $K_i = k(\beta_i)$ (by definition here), and, as $\mathcal{Z} \subseteq D\left(n,\overline{k}\right)$ so a fortiori $\mathcal{Z} \subseteq \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} M\left(a_i,\overline{k}\right)^{(n_{\phi_i})}$, we may apply Corollary 3.B.3, which gives at once, with (6), that:

(7) $\quad \mathcal{Z} \subseteq C^{-1} Im(\Delta_\Phi) C, \quad$ for some $C \in \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} G\ell\left(a_i,\overline{k}\right)^{(n_{\phi_i})}$.

8) By (6) and (7), we have:

(8) $\quad \Delta_\Phi(M) \in \mathcal{Z} = C^{-1}\Delta_\Phi(\mathcal{T})C, \quad$ for some $\mathcal{T} \subseteq \prod\limits_{i=1}^{r} M(a_i,K_i)$;

(9) $\quad C = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} C^{(i)}, \quad C^{(i)} = \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} C_j^{(i)}, \quad$ for some (even unique)

$$C^{(i)} \in \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} G\ell\left(a_i,\overline{k}\right), \quad C_j^{(i)} \in G\ell\left(a_i,\overline{k}\right).$$

Now let the following be defined, recalling that $\mathcal{Z} \subseteq D\left(n, \overline{k}\right)$ $\left(\text{and, by (4), recalling that } n = \dim \Phi = \sum\limits_{i=1}^{r} a_i n_{\phi_i}\right)$.

i) For all $Z \in \mathcal{Z}$, express $Z$ in the obvious (and unique) way as:

$$(10) \qquad Z = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} Z^{(i)}, \quad Z^{(i)} = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{j=1}^{n_{\phi_i}} Z_j^{(i)}, \quad \text{where}$$

$$Z^{(i)} \in D\left(a_i n_{\phi_i}, \overline{k}\right), \quad Z_j^{(i)} \in D\left(a_i, \overline{k}\right).$$

ii) For all $i \in \{1, \ldots, r\}, j \in \{1, \ldots, n_{\phi_i}\}$, let:

$$(11) \qquad \begin{aligned} \mathcal{Z}^{(i)} &\equiv \left\{Z^{(i)} \middle| Z \in \mathcal{Z}\right\} \subseteq D\left(a_i n_{\phi_i}, \overline{k}\right); \\ \mathcal{Z}_j^{(i)} &\equiv \left\{Z_j^{(i)} \middle| Z \in \mathcal{Z}\right\} \subseteq D\left(a_i, \overline{k}\right). \end{aligned}$$

iii) For all $i \in \{1, \ldots, r\}$, let: $\mathcal{T}_i \equiv$ the set of $i^{\underline{th}}$ components of $\mathcal{T}$; so that $\mathcal{T}_i \subseteq M(a_i, K_i)$.

iv) For all $i \in \{1, \ldots, r\}$, let $b_i \in \{1, \ldots, n_{\phi_i}\}$ be such that:

$$\sigma_{b_i}^{(i)} = id_{K_i}.$$

[This is OK, as $\sigma^{(i)}$ enumerates $\operatorname{Iso}(K_i/k)$.]

Now with (8),(9), and the above definitions, we clearly have:

$$\mathcal{Z}_j^{(i)} = C_j^{(i)^{-1}} \sigma_j^{(i)}(\mathcal{T}_i) C_j^{(i)}; \quad \text{for } i \in \{1, \ldots, r\}, j \in \{1, \ldots, n_{\phi_i}\}.$$

In particular, letting $j = b_i$ $\left(\text{so that } \sigma_j^{(i)} = id_{K_i}\right)$, we have:

$$\mathcal{Z}_{b_i}^{(i)} = C_{b_i}^{(i)^{-1}} \mathcal{T}_i C_{b_i}^{(i)}; \quad \text{for } i \in \{1, \ldots, r\}.$$

Thus:

$$C_{b_i}^{(i)} \mathcal{Z}_{b_i}^{(i)} C_{b_i}^{(i)^{-1}} = \mathcal{T}_i \subseteq M(a_i, K_i). \tag{12}$$

Hence, as $C_{b_i}^{(i)} \in G\ell\left(a_i, \overline{k}\right)$, (12) shows at once that:

$$\mathcal{Z}_{b_i}^{(i)} \text{ is } K_i\text{-rationalizable over } \overline{k}.$$

We note that $K_i$ is perfect (as $K_i/k$ is finite, and $k$ is perfect) and, clearly, that $\overline{K}_i = \overline{k}$. So, by (3), as $\mathcal{Z}_{b_i}^{(i)} \subseteq D\left(a_i, \overline{k}\right)$ [by (11)], we may apply the induction hypothesis to $\mathcal{Z}_{b_i}^{(i)}$ (with "$k$" $\equiv K_i$ and "$n$"$\equiv a_i$). Thus, this hypothesis gives some $\Pi_i \in \operatorname{Perm}(a_i, K_i) = \operatorname{Perm}(a_i, k)$ (the latter equality being obvious), and some $\Phi_i = (\phi_1^{(i)}, \ldots, \phi_{s_i}^{(i)})$, a field setting *over* $K_i$, with $\phi_j^{(i)} = \left(K_j^{(i)}, \sigma^{(i,j)}, a_j^{(i)}\right)$, a field element *over* $K_i$, where:

$$\text{i)}\quad \dim \Phi_i = \ a_i \qquad \left(\text{i.e., } \sum_{j=1}^{s_i} a_j^{(i)} \left[K_j^{(i)} : K_i\right] = a_i\right); \tag{13}$$

$$\text{ii)}\quad \mathcal{Z}_{b_i}^{(i)} \subseteq \Pi_i^{-1} \Delta_{\Phi_i} \left(\prod_{j=1}^{s_i} \operatorname{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)\right) \Pi_i;$$

$$\begin{aligned} \text{iii)}\quad C_L\left(\mathcal{Z}_{b_i}^{(i)}\right) &= C_L\left(\Pi_i^{-1} \Delta_{\Phi_i} \left(\prod_{j=1}^{s_i} \operatorname{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)\right) \Pi_i\right) \\ &= \Pi_i^{-1} \left[\mathop{\textcircled{\scriptsize$\triangle$}}_{j=1}^{s_i} M\left(a_j^{(i)}, L\right)^{\left(n_{\phi_j^{(i)}}\right)}\right] \Pi_i. \end{aligned} \tag{14}$$

For convenience, for any field setting, $\Omega = (\omega_1, \ldots, \omega_s)$, over any field $F$, with $\omega_i = \left(L_i, \tau^{(i)}, b_i\right)$ a field element over $F$, we let $Im'(\Delta_\Omega) \equiv$

$\Delta_\Omega\left(\prod_{i=1}^{s}\text{Scalar}(b_i, L_i)\right)$. Thus, (ii) and (iii) above show:

$$(15)\qquad \mathcal{Z}_{b_i}^{(i)} = \Pi_i^{-1}\Delta_{\Phi_i}(\mathcal{S}_i)\Pi_i;\quad \text{for some } \Pi_i \in \text{Perm}\left(a_j^{(i)}, k\right),$$

$$\text{and}\quad \mathcal{S}_i \subseteq \prod_{j=1}^{s_i}\text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right);$$

$$(16)\qquad \begin{aligned} C_L\left(\mathcal{Z}_{b_i}^{(i)}\right) &= C_L\left(\Pi_i^{-1}Im'(\Delta_{\Phi_i})\Pi_i\right) \\ &= \Pi_i^{-1}\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{j=1}^{s_i} M\left(a_j^{(i)}, L\right)^{\left(n_{\phi_j^{(i)}}\right)}\right]\Pi_i. \end{aligned}$$

9) Now let $E_i$ be any intermediate field of $\overline{k}/k$, which is a Galois extension of $k$ containing $K_1^{(i)}, \ldots, K_{s_i}^{(i)}$ and containing each of the $a_i^2$ entries of $C_{b_i}^{(i)} \in G\ell\left(a_i, \overline{k}\right)$. $\left(\text{So note, a fortiori, that } E_i \supseteq K_i \text{ — as } K_j^{(i)} \supseteq K_i.\right)$ Furthermore, referring back to $\sigma^{(i)}$ in step (5) above, let $\tilde{\sigma}_j^{(i)} \in \mathcal{G}a\ell(E_i/k)$ be an extension of $\sigma_j^{(i)} \in \text{Iso}(K_i/k)$, and let $\tilde{\Delta}_{\phi_i}$ be the corresponding extension of $\Delta_{\phi_i}$, from $M(a_i, K_i)$ (and so clearly, $\tilde{\Delta}_{\phi_i}$ is also an imbedding of $k$–algebras). Specifically, for $\widetilde{M} \in M(a_i, E_i)$, we have $\tilde{\Delta}_{\phi_i}\left(\widetilde{M}\right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{j=1}^{n_{\phi_i}} \tilde{\sigma}_j^{(i)}\left(\widetilde{M}\right) \in M(a_i, E_i)^{(n_{\phi_i})}$. Again referring to (8),(9), and the definition of $\mathcal{Z}^{(i)}$ in (11), we clearly have: $\mathcal{Z}^{(i)} = C^{(i)^{-1}}\Delta_{\phi_i}(\mathcal{T}_i)C^{(i)}$, for all $i \in \{1, \ldots, r\}$.

This, with (12) and (15), gives:

$$\mathcal{Z}^{(i)} = C^{(i)^{-1}}\Delta_{\phi_i}\left(C_{b_i}^{(i)}\Pi_i^{-1}\Delta_{\Phi_i}(\mathcal{S}_i)\Pi_i C_{b_i}^{(i)^{-1}}\right)C^{(i)}.$$

This, with the $k$–algebra imbedding $\widetilde{\Delta}_{\phi_i}$ defined above, gives:

$$\begin{aligned}
\mathcal{Z}^{(i)} &= C^{(i)^{-1}}\widetilde{\Delta}_{\phi_i}\left(C_{b_i}^{(i)}\Pi_i^{-1}\Delta_{\Phi_i}(\mathcal{S}_i)\Pi_i C_{b_i}^{(i)^{-1}}\right)C^{(i)} \\
&= C^{(i)^{-1}}\left[\widetilde{\Delta}_{\phi_i}\left(C_{b_i}^{(i)}\Pi_i^{-1}\right)\right]\left[\widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right]\left[\widetilde{\Delta}_{\phi_i}\left(\Pi_i C_{b_i}^{(i)^{-1}}\right)\right]C^{(i)} \\
&= C^{(i)^{-1}}\left[\left(\widetilde{\Delta}_{\phi_i}\left(\Pi_i^{-1}C_{b_i}^{(i)}\right)\right)^{-1}\right]\left[\widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right]\left[\widetilde{\Delta}_{\phi_i}\left(\Pi_i C_{b_i}^{(i)^{-1}}\right)\right]C^{(i)}.
\end{aligned}$$

Thus:

$$\mathcal{Z}^{(i)} = Q^{(i)^{-1}}\left[\widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right]Q^{(i)}, \quad \text{where} \tag{17}$$

$$\begin{aligned}
Q^{(i)} &\equiv \widetilde{\Delta}_{\phi_i}\left(\Pi_i C_{b_i}^{(i)^{-1}}\right)C^{(i)} \\
&= \left(\mathop{\bigcirc\kern-0.75em\triangle}_{j=1}^{n_{\phi_i}}\widetilde{\sigma}_j^{(i)}\left(\Pi_i C_{b_i}^{(i)^{-1}}\right)\right)\cdot\left(\mathop{\bigcirc\kern-0.75em\triangle}_{j=1}^{n_{\phi_i}}C_j^{(i)}\right) \in \mathop{\bigcirc\kern-0.75em\triangle}_{j=1}^{n_{\phi_i}} G\ell\left(a_i,\overline{k}\right).
\end{aligned} \tag{18}$$

10) Now with the definitions of $\phi_i, \Phi_i$, and $\widetilde{\Delta}_{\phi_i}$, we have at once by Lemma 4.B.1 (and this is the motivation for Lemma 4.B.1 in this paper!):

$$\widetilde{\Delta}_{\phi_i}\circ\Delta_{\Phi_i} = conj_{\xi_i}\circ\Delta_{\Phi_i'}; \tag{19}$$

for some $\xi_i \in \operatorname{Perm}(a_i n_{\phi_i}, k)$, and some $\Phi_i' = \left(\phi_1^{(i)'},\ldots,\phi_{s_i}^{(i)'}\right)$, a field setting *over* $k$, with $\phi_j^{(i)'} = \left(K_j^{(i)},\sigma^{(i,j)'},a_j^{(i)}\right)$, a field element *over* $k$, and where $\dim\Phi_i' = \dim\phi_i$. Note that the field elements $\phi_j^{(i)}$ and $\phi_j^{(i)'}$, as defined previously, have the same "$K$" and the same "$a$". By (15) we have $\mathcal{S}_i \subseteq \prod_{j=1}^{s_i}\operatorname{Scalar}\left(a_j^{(i)},K_j^{(i)}\right)$, and so (19) and (17) give:

$$\mathcal{Z}^{(i)} = Q^{(i)^{-1}}\xi_i^{-1}\left[\Delta_{\Phi_i'}(\mathcal{S}_i)\right]\xi_i Q^{(i)}. \tag{20}$$

11) Now, by the definition of $\mathcal{Z}^{(i)}$, we clearly have:

$$\mathcal{Z} \subseteq \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} \mathcal{Z}^{(i)}. \tag{21}$$

So now, by (20):

$$\begin{aligned} \mathcal{Z} &\subseteq \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} \left( Q^{(i)^{-1}} \xi_i^{-1} \left[ \Delta_{\Phi_i'}(\mathcal{S}_i) \right] \xi_i Q^{(i)} \right) \\ &= \left( \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} \xi_i Q^{(i)} \right)^{-1} \left( \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} \Delta_{\Phi_i'}(\mathcal{S}_i) \right) \left( \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} \xi_i Q^{(i)} \right). \end{aligned}$$

Letting $U \equiv \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} Q^{(i)} \xi_i \in \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} G\ell\left(a_i n_{\phi_i}, \overline{k}\right)$, so that $U \in G\ell\left(n, \overline{k}\right)$ (by (4)), the previous becomes:

$$\mathcal{Z} \subseteq U^{-1} \left[ \mathop{\triangle\!\!\!\!\!\bigcirc}_{i=1}^{r} \Delta_{\Phi_i'}(\mathcal{S}_i) \right] U, \quad \text{for some } U \in G\ell\left(n, \overline{k}\right). \tag{22}$$

Now, recalling the definitions of the field settings (recall there are $r$ of them) *over* $k$, given by $\Phi_i' = \left(\phi_1^{(i)'}, \ldots, \phi_{s_i}^{(i)'}\right)$, we let $r' \equiv \sum_{i=1}^{r} s_i \in \mathbb{Z}^+$, and let $\Phi' = (\phi_1', \ldots, \phi_{r'}')$ be the field setting *over* $k$, with $\phi_1' = \left(K_1', \sigma^{(1)'}, a_1'\right), \ldots, \phi_{r'}' = \left(K_{r'}', \sigma^{(r')'}, a_{r'}'\right)$ the field elements *over* $k$, defined by the following permutation of the $\phi_j^{(i)'}$:

$$\Phi' = (\phi_1', \ldots, \phi_{r'}') \equiv (\phi_1^{(1)'}, \ldots, \phi_{s_1}^{(1)'}, \ldots\ldots, \phi_1^{(r)'}, \ldots, \phi_{s_r}^{(r)'}).$$

With these definitions, and recalling from (15) that $\mathcal{S}_i \subseteq \prod_{j=1}^{s_i} \text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)$, the result above in (22) gives:

$$\begin{aligned}
\mathcal{Z} &\subseteq U^{-1}\left[\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r}\Delta_{\Phi'_i}(\mathcal{S}_i)\right]U \\
&\subseteq U^{-1}\left[\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r}\mathop{\bigcirc\kern-0.78em\triangle}_{j=1}^{s_i}\Delta_{\phi_j^{(i)\prime}}\left(\mathrm{Scalar}\left(a_j^{(i)},K_j^{(i)}\right)\right)\right]U \\
&= U^{-1}\left[\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r'}\Delta_{\phi'_i}\left(\mathrm{Scalar}\left(a'_i,K'_i\right)\right)\right]U \\
&= U^{-1}\left[\Delta_{\Phi'}\left(\prod_{i=1}^{r'}\mathrm{Scalar}\left(a'_i,K'_i\right)\right)\right]U \\
&= U^{-1}Im'(\Delta_{\Phi'})U.
\end{aligned}$$

Hence:

$$\mathcal{Z} \subseteq U^{-1}Im'(\Delta_{\Phi'})U, \tag{23}$$

for some $U \in G\ell\left(n,\overline{k}\right)$ and some $\Phi'$, a field setting *over* $k$.

Moreover, recalling from step (10) above that $\dim\Phi'_i = \dim\phi_i$, and using (4), we easily calculate:

$$\begin{aligned}
\dim\Phi' &= \sum_{i=1}^{r'}\dim\phi'_i = \sum_{i=1}^{r}\sum_{j=1}^{s_i}\dim\phi_j^{(i)\prime} \\
&= \sum_{i=1}^{r}\dim\Phi'_i = \sum_{i=1}^{r}\dim\phi_i \\
&= \dim\Phi = n.
\end{aligned}$$

Thus:

$$\dim\Phi' = n. \tag{24}$$

12) We now compute $C_L(\mathcal{Z})$. Before doing so, we make several useful observations.

a) From step (6) above, we recall that $M = (M_1, \dots, M_r)$ and $M_i = \beta_i I_{a_i}$. Thus $\Delta_\Phi(M) = \mathop{\bigcirc\mkern-14mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-14mu\triangle}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(\beta_i) I_{a_i}$, and $\Delta_{\phi_i}(M_i) = \mathop{\bigcirc\mkern-14mu\triangle}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(\beta_i) I_{a_i}$. As noted earlier, the quantities $\beta_1, \dots, \beta_r$ are pair-wise non-conjugate over $k$, and $\deg_k(\beta_i) = [k(\beta_i) : k] = [K_i : k] = n_{\phi_i}$. Thus, the quantities, $\sigma_j^{(i)}(\beta_i)$, are all distinct. So, at once by Propositions App. 8, part (b) and App. 9, part (i), of the Appendix, we have:

$$C_L\left(\Delta_\Phi(M)\right) = \mathop{\bigcirc\mkern-14mu\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})},$$

(25) and

$$C_L\left(\Delta_{\phi_i}(M_i)\right) = M(a_i, L)^{(n_{\phi_i})}.$$

b) From (8), we have:

$$(26) \quad \Delta_\Phi(M) \in \mathcal{Z} \subseteq \mathop{\bigcirc\mkern-14mu\triangle}\limits_{i=1}^{r} M\left(a_i, \overline{k}\right)^{(n_{\phi_i})} \qquad [\mathcal{Z} \text{ is even diagonal}].$$

So, in particular, $C_L(\Delta_\Phi(M)) \supseteq C_L(\mathcal{Z})$, and so by (25):

$$C_L(\mathcal{Z}) \subseteq \mathop{\bigcirc\mkern-14mu\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.$$

So, at once by the definition of $\mathcal{Z}_j^{(i)}$, and by Proposition App. 6 of the Appendix, we have:

$$(27) \qquad C_L(\mathcal{Z}) = \mathop{\bigcirc\mkern-14mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-14mu\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\mathcal{Z}_j^{(i)}\right).$$

c) Now recalling (17) and (18), we have:

$$(28) \quad \mathcal{Z}^{(i)} = Q^{(i)^{-1}}\left[\tilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right] Q^{(i)}, \quad \text{and} \quad Q^{(i)} \in \mathop{\bigcirc\mkern-14mu\triangle}\limits_{j=1}^{n_{\phi_i}} G\ell\left(a_i, \overline{k}\right).$$

In particular, we may write:

$$Q^{(i)} = \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} Q_j^{(i)}, \quad \text{for some [even unique]} \quad Q_j^{(i)} \in G\ell\left(a_i, \overline{k}\right). \tag{29}$$

Recalling the definition of $\widetilde{\Delta}_{\phi_i}$ from step (9) above, and using (28) and (29), we see:

$$\begin{aligned}
\mathcal{Z}^{(i)} &= Q^{(i)^{-1}} \left[\widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right] Q^{(i)} \\
&= \left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}}\right] \left[\left\{\widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(S)\right) \middle| S \in \mathcal{S}_i\right\}\right] \left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} Q_j^{(i)}\right] \\
&= \left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}}\right] \left[\left\{\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \left[\widetilde{\sigma}_j^{(i)}\left(\Delta_{\Phi_i}(S)\right)\right] \middle| S \in \mathcal{S}_i\right\}\right] \left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} Q_j^{(i)}\right] \\
&= \left\{\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \left(Q_j^{(i)^{-1}} \left[\widetilde{\sigma}_j^{(i)}\left(\Delta_{\Phi_i}(S)\right)\right] Q_j^{(i)}\right) \middle| S \in \mathcal{S}_i\right\}.
\end{aligned}$$

So clearly now, by definition of $\mathcal{Z}_j^{(i)}$, the previous gives immediately:

$$\begin{aligned}
\mathcal{Z}_j^{(i)} &= \left\{Q_j^{(i)^{-1}} \left[\widetilde{\sigma}_j^{(i)}\left(\Delta_{\Phi_i}(S)\right)\right] Q_j^{(i)} \middle| S \in \mathcal{S}_i\right\} \\
&= Q_j^{(i)^{-1}} \left[\widetilde{\sigma}_j^{(i)}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right] Q_j^{(i)}.
\end{aligned} \tag{30}$$

d) Let $\mathcal{W}^{(i)} \equiv Q^{(i)^{-1}} \left[\widetilde{\Delta}_{\phi_i}\left(Im'\left(\Delta_{\Phi_i}\right)\right)\right] Q^{(i)}$. By (29), and the definition of $\widetilde{\Delta}_{\phi_i}$, we clearly have:

$$\mathcal{W}^{(i)} \subseteq M\left(a_i, \overline{k}\right)^{\left(n_{\phi_i}\right)}. \tag{31}$$

So, for $W^{(i)} \in \mathcal{W}^{(i)}$, we may express $W^{(i)}$ in the obvious [and even unique] way as:

$$W^{(i)} = \mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} W_j^{(i)}, \quad \text{where } W_j^{(i)} \in M\left(a_i, \overline{k}\right);$$

and we let $\mathcal{W}_j^{(i)} \equiv \left\{ W_j^{(i)} \in M\left(a_i, \overline{k}\right) \middle| W^{(i)} \in \mathcal{W}^{(i)} \right\} \subseteq M\left(a_i, \overline{k}\right)$. Now, from (8), we have $\Delta_\Phi(M) \in \mathcal{Z}$, which is the same as $\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \Delta_{\phi_i}(M_i) \in \mathcal{Z}$; and so, by definition of $\mathcal{Z}^{(i)}$: $\Delta_{\phi_i}(M_i) \in \mathcal{Z}^{(i)}$. This, with (28), (15), the definition of $\mathcal{W}^{(i)}$, and (31), shows:

$$\Delta_{\phi_i}(M_i) \in \mathcal{Z}^{(i)} \subseteq \mathcal{W}^{(i)} \subseteq M\left(a_i, \overline{k}\right)^{\left(n_{\phi_i}\right)}.$$

Hence, in particular, $C_L(\Delta_{\phi_i}(M_i)) \supseteq C_L\left(\mathcal{W}^{(i)}\right)$, and so by (25):

$$C_L\left(\mathcal{W}^{(i)}\right) \subseteq M(a_i, L)^{(n_{\phi_i})}.$$

So, at once by the definition of $\mathcal{W}_j^{(i)}$, and by Proposition App. 6 of the Appendix, we have:

$$C_L\left(\mathcal{W}^{(i)}\right) = \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} C_L\left(\mathcal{W}_j^{(i)}\right). \tag{32}$$

e) From the definitions of $\mathcal{W}^{(i)}$ and $\widetilde{\Delta}_{\phi_i}$, we see:

$$\begin{aligned}
\mathcal{W}^{(i)} &= Q^{(i)^{-1}} \left[\widetilde{\Delta}_{\phi_i}\left(Im'\left(\Delta_{\Phi_i}\right)\right)\right] Q^{(i)} \\
&= \left[\mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}}\right] \left[\left\{ \widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}(S)\right) \middle| S \in \prod_{j=1}^{s_i} \mathrm{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right) \right\}\right] \left[\mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)}\right] \\
&= \left[\mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}}\right] \left[\left\{ \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} \left[\widetilde{\sigma}_j^{(i)}\left(\Delta_{\Phi_i}(S)\right)\right] \middle| S \in \prod_{j=1}^{s_i} \mathrm{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right) \right\}\right] \left[\mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)}\right] \\
&= \left\{ \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}} \left[\widetilde{\sigma}_j^{(i)}\left(\Delta_{\Phi_i}(S)\right)\right] Q_j^{(i)} \middle| S \in \prod_{j=1}^{s_i} \mathrm{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right) \right\}.
\end{aligned}$$

So, by the definition of $\mathcal{W}_j^{(i)}$, the previous gives immediately:

(33)

$$\begin{aligned}\mathcal{W}_j^{(i)} &= \left\{ Q_j^{(i)^{-1}} \left[\tilde{\sigma}_j^{(i)} (\Delta_{\Phi_i}(S))\right] Q_j^{(i)} \middle| S \in \prod_{j=1}^{s_i} \text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right) \right\} \\ &= Q_j^{(i)^{-1}} \left[\tilde{\sigma}_j^{(i)} \left(\Delta_{\Phi_i} \left(\prod_{j=1}^{s_i} \text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)\right)\right)\right] Q_j^{(i)} \\ &= Q_j^{(i)^{-1}} \left[\tilde{\sigma}_j^{(i)} \left(Im'(\Delta_{\Phi_i}\right)\right] Q_j^{(i)}.\end{aligned}$$

f) Now let $\mathcal{D}_i \subseteq \prod_{j=1}^{s_i} \text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)$; so, in particular, we have $\Delta_{\Phi_i}(\mathcal{D}_i) \subseteq D(a_i, E_i)$ [as $\dim \Phi_i = a_i$, by (13)]. Now $\tilde{\sigma}_j^{(i)} \in Ga\ell(E_i/k)$, so in particular $\tilde{\sigma}_j^{(i)}$ is injective on $E_i$. Thus, as $E_i \subseteq \overline{k} \subseteq L$, at once by Corollary App. 12, of the Appendix, we have:

$$C_L\left(\tilde{\sigma}_j^{(i)} (\Delta_{\Phi_i}(\mathcal{D}_i))\right) = C_L\left(\Delta_{\Phi_i}(\mathcal{D}_i)\right). \tag{34}$$

We will use this shortly, with $\mathcal{D}_i \equiv \mathcal{S}_i$, and with $\mathcal{D}_i \equiv \prod_{j=1}^{s_i} \text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)$.

g) Let $\Omega = (\omega_1, \ldots, \omega_s)$ be any field setting over $k$, with $\omega_i = \left(L_i, \tau^{(i)}, b_i\right)$ a field element over $k$. The following simple calculation will prove useful. We have:

$$\begin{aligned}
Im'(\Delta_\Omega) &= \Delta_\Omega\left(\prod_{i=1}^{s} \mathrm{Scalar}\,(b_i, L_i)\right)\\
&= \{\Delta_\Omega(T_1,\dots,T_s) \,|\, T_i \in \mathrm{Scalar}\,(b_i, L_i)\}\\
&= \left\{\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{s} \Delta_{\omega_i}(T_i) \,\middle|\, T_i \in \mathrm{Scalar}\,(b_i, L_i)\right\}\\
&= \mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{s} \Delta_{\omega_i}\left(\mathrm{Scalar}\,(b_i, L_i)\right).
\end{aligned}$$

Hence:

$$Im'(\Delta_\Omega) = \mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{s} \Delta_{\omega_i}(\mathrm{Scalar}\,(b_i, L_i)). \tag{35}$$

h) Let $\Omega_1,\dots,\Omega_t$ be field settings over $k$. By (35), clearly $O_{\dim \Omega_i}$, $I_{\dim \Omega_i} \in Im'(\Delta_{\Omega_i})$. Thus, at once, by iterative application of Proposition App. 8, part (a), of the Appendix, we have, in particular:

$$C_L\left(\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{t} Im'(\Delta_{\Omega_i})\right) = \mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{t} C_L\left(Im'(\Delta_{\Omega_i})\right). \tag{36}$$

i) We make our final observation. While it is simple to observe here, *it is the central observation* that permits the calculation, to be done shortly, of the result for $C_L(\mathcal{Z})$. Using (15) and (16), we have:

$$\begin{aligned}
\Pi_i^{-1} C_L\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right) \Pi_i &= C_L\left(\Pi_i^{-1} \Delta_{\Phi_i}(\mathcal{S}_i) \Pi_i\right)\\
&= C_L\left(\mathcal{Z}_{b_i}^{(i)}\right)\\
&= C_L\left(\Pi_i^{-1} Im'(\Delta_{\Phi_i}) \Pi_i\right)\\
&= \Pi_i^{-1} C_L\left(Im'(\Delta_{\Phi_i})\right) \Pi_i.
\end{aligned}$$

Thus, at once:

$$(37) \qquad C_L\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right) = C_L\left(Im'(\Delta_{\Phi_i})\right).$$

j) Finally, we calculate $C_L(\mathcal{Z})$. Using the observations of this step, together with (19) and the definitions of $U$ and $\Phi'$, we calculate:

$$\begin{aligned}
&C_L(\mathcal{Z}) \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\mathcal{Z}_j^{(i)}\right) && \text{[by (27)]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(Q_j^{(i)^{-1}}\left[\widetilde{\sigma_j}^{(i)}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right] Q_j^{(i)}\right) && \text{[by (30)]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}} C_L\left(\widetilde{\sigma_j}^{(i)}\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right)\right) Q_j^{(i)} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}} C_L\left(\Delta_{\Phi_i}(\mathcal{S}_i)\right) Q_j^{(i)} && \text{[by (34)]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}} C_L\left(Im'(\Delta_{\Phi_i})\right) Q_j^{(i)} && \text{[by (37)]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} Q_j^{(i)^{-1}} C_L\left(\tilde{\sigma}_j^{(i)}\left(Im'(\Delta_{\Phi_i})\right)\right) Q_j^{(i)} && \text{[by (34)]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(Q_j^{(i)^{-1}}\left[\tilde{\sigma}_j^{(i)}\left(Im'(\Delta_{\Phi_i})\right)\right] Q_j^{(i)}\right) \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{n_{\phi_i}} C_L\left(\mathcal{W}_j^{(i)}\right) && \text{[by (33)]}
\end{aligned}$$

$$\begin{aligned}
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} C_L\left(\mathcal{W}^{(i)}\right) && \text{[by (32)]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} C_L\left(Q^{(i)^{-1}}\left[\widetilde{\Delta}_{\phi_i}\left(Im'(\Delta_{\Phi_i})\right)\right] Q^{(i)}\right) && \text{[def. } \mathcal{W}^{(i)}\text{]} \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} C_L\left(Q^{(i)^{-1}}\left[\widetilde{\Delta}_{\phi_i}\left(\Delta_{\Phi_i}\left(\prod_{j=1}^{s_i}\text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)\right)\right)\right] Q^{(i)}\right) \\
&= \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} C_L\left(Q^{(i)^{-1}}\left[\xi_i^{-1}\Delta_{\Phi_i'}\left(\prod_{j=1}^{s_i}\text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)\right)\xi_i\right] Q^{(i)}\right) && \text{[by (19)]}
\end{aligned}$$

$$= \mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} C_L\left(Q^{(i)^{-1}}\xi_i^{-1} Im'\left(\Delta_{\Phi_i'}\right)\xi_i Q^{(i)}\right) \qquad \text{[def. } \Phi_i'\text{]}$$

$$= \mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} Q^{(i)^{-1}}\xi_i^{-1} C_L\left(Im'\left(\Delta_{\Phi_i'}\right)\right)\xi_i Q^{(i)}$$

$$= \left(\mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} \xi_i Q^{(i)}\right)^{-1}\left(\mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} C_L\left(Im'\left(\Delta_{\Phi_i'}\right)\right)\right)\left(\mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} \xi_i Q^{(i)}\right)$$

$$= U^{-1}\left(\mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} C_L\left(Im'\left(\Delta_{\Phi_i'}\right)\right)\right)U \qquad \text{[def. U]}$$

$$= U^{-1}C_L\left(\mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} Im'\left(\Delta_{\Phi_i'}\right)\right)U \qquad \text{[by (36)]}$$

$$= U^{-1}C_L\left(\mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r}\mathop{\triangle\kern-0.75em\bigcirc}\limits_{j=1}^{s_i} \Delta_{\phi_j^{(i)\prime}}\left(\text{Scalar}\left(a_j^{(i)}, K_j^{(i)}\right)\right)\right)U$$

$$\text{[by (35) and def. } \Phi_i'\text{]}$$

$$= U^{-1}C_L\left(Im'(\Delta_{\Phi'})\right)U$$

$$\text{[by (35) and def. } \Phi'\text{]}$$

$$= C_L\left(U^{-1}Im'(\Delta_{\Phi'})U\right).$$

Hence:

$$C_L(\mathcal{Z}) = C_L\left(U^{-1}Im'(\Delta_{\Phi'})U\right). \tag{38}$$

13) We now collect together, from (23) and (38), the two main results thus far:

$$\mathcal{Z} \subseteq U^{-1}Im'(\Delta_{\Phi'})U \quad \text{and} \quad C_L(\mathcal{Z}) = C_L\left(U^{-1}Im'(\Delta_{\Phi'})U\right).$$

So clearly:

$$U\mathcal{Z}U^{-1} \subseteq Im'(\Delta_{\Phi'}) \quad \text{and} \quad C_L\left(U\mathcal{Z}U^{-1}\right) = C_L\left(Im'(\Delta_{\Phi'})\right). \tag{39}$$

Now clearly by definition of $Im'(\Delta_{\Phi'})$, and by (24), we have $Im'(\Delta_{\Phi'}) \subseteq D\left(\dim \Phi', \overline{k}\right) = D\left(n, \overline{k}\right)$. So, by (39):

$$(40) \qquad UZU^{-1} \subseteq Im'(\Delta_{\Phi'}) \subseteq D\left(n, \overline{k}\right).$$

So, by (40), (39), and Corollary App. 17, of the Appendix, we have, at once, for some $\Pi \in \mathrm{Perm}(n, k)$:

$$\Pi Z \Pi^{-1} = UZU^{-1} \subseteq Im'(\Delta_{\Phi'}).$$

So now, substituting $\Pi Z \Pi^{-1} = UZU^{-1}$ in (39), we get:

$$\Pi Z \Pi^{-1} \subseteq Im'(\Delta_{\Phi'}) \quad \text{and} \quad C_L\left(\Pi Z \Pi^{-1}\right) = C_L\left(Im'(\Delta_{\Phi'})\right).$$

And hence:

$$(41) \qquad Z \subseteq \Pi^{-1} Im'(\Delta_{\Phi'}) \Pi \quad \text{and} \quad C_L(Z) = C_L\left(\Pi^{-1} Im'(\Delta_{\Phi'}) \Pi\right).$$

14) Now from step (7), we recall that $Z = \Psi \mathcal{Y} \Psi^{-1}$; and from (5), we recall that $\Psi \in \mathrm{Perm}(n, k)$. Thus $\mathcal{Y} = \Psi^{-1} Z \Psi$; and so by (41), letting $\Pi' \equiv \Pi \Psi \in \mathrm{Perm}(n, k)$, we have:

$$(42) \qquad \mathcal{Y} \subseteq \Pi'^{-1} Im'(\Delta_{\Phi'}) \Pi' \quad \text{and} \quad C_L(\mathcal{Y}) = C_L\left(\Pi'^{-1} Im'(\Delta_{\Phi'}) \Pi'\right).$$

Recalling that $\Pi' \in \mathrm{Perm}(n, k)$; and that, by definition of $\Phi'$ and (24), we have that $\Phi'$ is a field setting over $k$, where $\dim \Phi' = n$; we see at once from (42) that we have now proved, in the induction for $\mathcal{Y}$, most of the desired conclusions for $(\Longrightarrow)$. It remains only to complete the desired conclusion (iii); and to prove the desired conclusion (iv), of $(\Longrightarrow)$.

Well, the rest of the conclusion in (iii) follows at once from (42) and Lemma 2.D.1, part (b,i). And the conclusion in (iv) follows at once from (42), from the completed conclusion (iii) [now just proved previously], and Lemma 4.B.3 $\left(\text{with ``}\mathcal{Z}\text{''} \equiv \Pi'\mathcal{Y}\Pi'^{-1}\right)$. This now completes the induction for $\mathcal{Y}$, and so completes the induction proof of $(\Longrightarrow)$.

This completes the proof of the theorem!

□

The following Lemma shows that any field setting can be related, naturally, to a certain "simpler" kind of field setting. This will be used to establish Corollary 4.B.6 — an alternative and "weaker" form of the result in Theorem 4.B.4. This Corollary has meanings of its own, and will have a key use in Chapter 7.

**Lemma 4.B.5**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

Let $\dot{\Phi}$ be the field setting over $k$, defined as follows:

$$\dot{\Phi} \equiv \Big( \underbrace{\dot{\phi}_1, \ldots, \dot{\phi}_1}_{a_1 \text{ times}}, \ldots\ldots, \underbrace{\dot{\phi}_r, \ldots, \dot{\phi}_r}_{a_r \text{ times}} \Big),$$

where $\dot{\phi}_i$ is the field element over $k$, defined as $\dot{\phi}_i \equiv \left(K_i, \sigma^{(i)}, 1\right)$.

**Then:**

1) $\dim \dot{\Phi} = \dim \Phi$;

2) $\exists \Pi \in \underset{i=1}{\overset{r}{\triangle\!\!\!\!\bigcirc}} \operatorname{Perm}(a_i n_{\phi_i}, k) \subseteq \operatorname{Perm}(\dim \Phi, k)$:

   a) $\Delta_\Phi \left( \prod_{i=1}^{r} \operatorname{Scalar}(a_i, K_i) \right) \subseteq \Pi Im\left(\Delta_{\dot{\Phi}}\right) \Pi^{-1} \subseteq D\left(\dim \Phi, \overline{k}\right),$

   b) i) $V_\Phi \Pi \subseteq V_{\dot{\Phi}},$

      ii) $V \in V_\Phi^\times \implies V\Pi$ $k$–rationalizes $Im\left(\Delta_{\dot{\Phi}}\right)$.

**Proof.**

1) We have $\dot{\phi}_i = \left(K_i, \sigma^{(i)}, 1\right)$, and so $\dim \dot{\phi}_i = 1 \cdot [K_i : k] = [K_i : k]$. With this, and the definition of dimension of a field setting, we easily compute:

$$\begin{aligned} \dim \dot{\Phi} &= \sum_{i=1}^{r} \sum_{t=1}^{a_i} \dim \dot{\phi}_i = \sum_{i=1}^{r} \sum_{t=1}^{a_i} [K_i : k] \\ &= \sum_{i=1}^{r} a_i [K_i : k] = \sum_{i=1}^{r} \dim \phi_i = \dim \Phi. \end{aligned}$$

2) For any two positive integers, $a, n$, we define a permutation $p_{(a,n)} \in S_{a \cdot n}$ as follows. Let $x_1, x_2, \ldots, x_{a \cdot n}$ be $a \cdot n$ distinct "letters". Now, as below, re-express this sequence of $a \cdot n$ letters with the following "double-index" notation:

$$(1) \qquad (x_1, x_2, \ldots, x_{a \cdot n}) = \Big(\underbrace{x_1^{(1)}, \ldots, x_a^{(1)}}_{a}, \underbrace{x_1^{(2)}, \ldots, x_a^{(2)}}_{a}, \ldots\ldots, \underbrace{x_1^{(n)}, \ldots, x_a^{(n)}}_{a}\Big).$$

Finally, let $p_{(a,n)} \in S_{a \cdot n}$ be the permutation, defined clearly, as below:

$$(2) \qquad \begin{gathered} \Big(x_{p_{(a,n)}(1)}, x_{p_{(a,n)}(2)}, \ldots, x_{p_{(a,n)}(a \cdot n)}\Big) = \\ \Big(\underbrace{x_1^{(1)}, x_1^{(2)}, \ldots, x_1^{(n)}}_{n}, \underbrace{x_2^{(1)}, x_2^{(2)}, \ldots, x_2^{(n)}}_{n}, \ldots\ldots, \underbrace{x_a^{(1)}, x_a^{(2)}, \ldots, x_a^{(n)}}_{n}\Big). \end{gathered}$$

With this, let $\Pi_{(a,n)}$ be the basic permutation matrix associated with $p_{(a,n)}$, as defined in Chapter 1, Section B, Subsection 4, Part (d):

$$(3) \qquad \Pi_{(a,n)} \equiv \Pi_{a \cdot n}\left(p_{(a,n)}\right) \in \operatorname{Perm}(a \cdot n, k).$$

3) With $\Pi_{(a,n)}$ as defined in (3), and recalling the facts about basic permutation matrices as in Chapter 1, Section B, Subsection 4, Part (d), and, with (1) and (2), we easily make the two observations below.

   a) Let $a, n, N \in \mathbb{Z}^+$. For $j \in \{1, \ldots, n\}, t \in \{1, \ldots, a\}$, let $\vec{A}_t^{(j)} \in M(N \times 1, L)$; i.e., $\vec{A}_t^{(j)}$ is an $N \times 1$ column vector over $L$. Let:

$$(4) \qquad A \equiv \mathop{\bigcirc\!\!\!\!\!\parallel}_{j=1}^{n} \mathop{\bigcirc\!\!\!\!\!\parallel}_{t=1}^{a} \vec{A}_t^{(j)} \in M(N \times an, L).$$

By the above-mentioned part of Chapter 1, and (4), and *the definition of $p_{(a,n)}$ as in (1) and (2),* we see at once:

$$\begin{aligned} A\Pi_{(a,n)} &= \text{“}A,\ \text{where column}(q)\ \textit{has become}\ \text{column}\left(p_{(a,n)}(q)\right)\text{”} \\ &= \text{“}\mathop{\textcircled{$\shortparallel$}}_{j=1}^{n}\mathop{\textcircled{$\shortparallel$}}_{t=1}^{a}\vec{A}_t^{(j)},\ \text{where column}(q)\ \textit{has become}\ \text{column}\left(p_{(a,n)}(q)\right)\text{”} \\ &= \mathop{\textcircled{$\shortparallel$}}_{t=1}^{a}\mathop{\textcircled{$\shortparallel$}}_{j=1}^{n}\vec{A}_t^{(j)}. \end{aligned}$$

I.e.,

$$A\Pi_{(a,n)} = \mathop{\textcircled{$\shortparallel$}}_{t=1}^{a}\mathop{\textcircled{$\shortparallel$}}_{j=1}^{n}\vec{A}_t^{(j)}. \tag{5}$$

By (4) and (5), we summarize:

$$\vec{A}_t^{(j)} \in M(N\times 1, L) \implies \left[\mathop{\textcircled{$\shortparallel$}}_{j=1}^{n}\mathop{\textcircled{$\shortparallel$}}_{t=1}^{a}\vec{A}_t^{(j)}\right]\Pi_{(a,n)} = \left[\mathop{\textcircled{$\shortparallel$}}_{t=1}^{a}\mathop{\textcircled{$\shortparallel$}}_{j=1}^{n}\vec{A}_t^{(j)}\right]. \tag{6}$$

I.e., “ $[\cdots]\Pi_{(a,n)}$ reverses the order of ‘$\textcircled{$\shortparallel$}$-ing’ ”.

b) Referring to the same above-mentioned part of Chapter 1, and following, quite similarly, the above, we also conclude at once:

$$b_t^{(j)} \in L \implies {\Pi_{(a,n)}}^{-1}\left[\mathop{\textcircled{$\triangle$}}_{j=1}^{n}\mathop{\textcircled{$\triangle$}}_{t=1}^{a}\left[b_t^{(j)}\right]\right]\Pi_{(a,n)} = \left[\mathop{\textcircled{$\triangle$}}_{t=1}^{a}\mathop{\textcircled{$\triangle$}}_{j=1}^{n}\left[b_t^{(j)}\right]\right]. \tag{7}$$

I.e., “ ${\Pi_{(a,n)}}^{-1}[\cdots]\Pi_{(a,n)}$ reverses the order of ‘$\textcircled{$\triangle$}$-ing’ ”.

4) With (6) and (7), we now return to the main proof. For $i \in \{1,\ldots,r\}$, we let $\Pi_i \equiv \Pi_{(a_i,n_{\phi_i})} \in \text{Perm}\ (a_i n_{\phi_i}, k)$, and we let:

$$\Pi \equiv \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\Pi_i \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\text{Perm}\ (a_i n_{\phi_i}, k) \subseteq \text{Perm}\left(\sum_{i=1}^{r} a_i n_{\phi_i}, k\right) = \text{Perm}\,(\dim\Phi, k). \tag{8}$$

With this, we make the following two observations.

a) Let $\alpha_1 \in K_1, \dots, \alpha_r \in K_r$. Then we observe:

$$\begin{aligned}
&\Delta_{\Phi}\left(\alpha_1 I_{a_1}, \dots, \alpha_r I_{a_r}\right) \\
&= \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(\alpha_i) I_{a_i} \\
&= \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{a_i} \left[\sigma_j^{(i)}(\alpha_i)\right] \\
&= \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \left(\Pi_i \left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{a_i} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} \left[\sigma_j^{(i)}(\alpha_i)\right]\right] \Pi_i^{-1}\right) && \text{[by (7)]} \\
&= \left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \Pi_i\right] \left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{a_i} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}} \left[\sigma_j^{(i)}(\alpha_i)\right]\right] \left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \Pi_i\right]^{-1} \\
&= \Pi \left[\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{a_i} \Delta_{\dot{\phi}_i}\left([\alpha_i]\right)\right] \Pi^{-1} && \text{[by defs. } \Pi, \dot{\phi}_i] \\
&= \Pi\, \Delta_{\dot{\Phi}}\Big(\underbrace{[\alpha_1], \dots, [\alpha_1]}_{a_1}, \underbrace{[\alpha_2], \dots, [\alpha_2]}_{a_2}, \dots\dots, \underbrace{[\alpha_r], \dots, [\alpha_r]}_{a_r}\Big)\Pi^{-1} && \text{[by def. } \dot{\Phi}] \\
&\in \Pi\, Im\left(\Delta_{\dot{\Phi}}\right) \Pi^{-1}.
\end{aligned}$$

Thus, we have shown:

$$(9) \qquad \Delta_{\Phi}\left(\prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i)\right) \subseteq \Pi\, Im\left(\Delta_{\dot{\Phi}}\right) \Pi^{-1}.$$

Moreover, as $\dot{\phi}_i = \left(K_i, \sigma^{(i)}, 1\right)$, so $M\left(a_{\dot{\phi}_i}, K_{\dot{\phi}_i}\right) = M\left(1, K_i\right)$, and thus clearly $Im\left(\Delta_{\dot{\phi}_i}\right) \subseteq D\left(\dim \dot{\phi}_i, \overline{k}\right)$. Hence, clearly, $Im\left(\Delta_{\dot{\Phi}}\right)$ consists of diagonal matrices, so:

$$Im\left(\Delta_{\dot{\Phi}}\right) \subseteq D\left(\dim \dot{\Phi}, \overline{k}\right) = D\left(\dim \Phi, \overline{k}\right),$$

where the latter equality follows from the result in step (1) here, above.

Thus, as $\Pi$ is a permutation matrix, clearly now:

$$(10) \qquad \Pi Im\left(\Delta_{\dot{\Phi}}\right)\Pi^{-1} \subseteq D\left(\dim\Phi,\bar{k}\right).$$

b) Let $V \in V_{\Phi}$. By definition of $V_{\Phi}$, then:

$$(11) \qquad V = \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(Q_i), \quad \text{for some} \quad Q_i \in M\Big((\dim\Phi)\times a_i, K_i\Big).$$

Now write out $Q_i$ "in columns", clearly, as below:

$$(12) \qquad Q_i = \mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i} \vec{Q}_{i,t}\,; \quad \text{for some} \quad \vec{Q}_{i,t} \in M\Big((\dim\Phi)\times 1, K_i\Big).$$

So, clearly by (11) and (12):

$$(13) \qquad V = \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}}\mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i} \sigma_j^{(i)}\left(\vec{Q}_{i,t}\right).$$

Then we easily observe, using (8), (6), and the definitions of "$V_{N,\phi}$", "$V_{\Phi}$":

$$\begin{aligned}
V\Pi &= \left[\mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}}\mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i} \sigma_j^{(i)}\left(\vec{Q}_{i,t}\right)\right]\left[\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r}\Pi_i\right] \\
&= \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\left(\left[\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}}\mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i} \sigma_j^{(i)}\left(\vec{Q}_{i,t}\right)\right]\Pi_i\right) \\
&= \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\left(\left[\mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i}\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}\left(\vec{Q}_{i,t}\right)\right]\right) \\
&= \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i}\left[\mathop{\textcircled{$\|$}}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}\left(\vec{Q}_{i,t}\right)\right] \\
&\in \mathop{\textcircled{$\|$}}\limits_{i=1}^{r}\mathop{\textcircled{$\|$}}\limits_{t=1}^{a_i} V_{\dim\Phi,\phi_i} = V_{\dot{\Phi}}.
\end{aligned}$$

Thus, we have shown:

$$(14) \qquad V_{\Phi}\Pi \subseteq V_{\dot{\Phi}}.$$

Now, by Theorem 3.B.1, ($\Longleftarrow$) [ with "$\mathcal{Y}$" $\equiv$ $Im(\Delta_{\dot{\Phi}})$ ], we have: $W \in V_{\dot{\Phi}}{}^{\times} \implies W$ $k$–rationalizes $Im(\Delta_{\dot{\Phi}})$. Thus, at once by (14), we have:

(15)

$$V \in V_{\Phi}^{\times} \implies V\Pi \in V_{\dot{\Phi}}{}^{\times} \implies V\Pi \quad k\text{–rationalizes } Im(\Delta_{\dot{\Phi}}).$$

By step (1) here above, (8), (9), (10), (14), and (15), the proof of this lemma is complete.

$\square$

### Corollary 4.B.6

Let $n \in \mathbb{Z}^{+}$.

Let $\mathcal{Y} \subseteq D(n, L)$.

**Then:**

$$\mathcal{Y} \quad \text{is } k\text{–rationalizable over } L$$

$$\Longleftrightarrow$$

$$\mathcal{Y} \subseteq D\left(n, \overline{k}\right) \quad \text{and} \quad \exists \Pi \in \mathrm{Perm}(n, k):$$

$$\exists \Phi = (\phi_1, \ldots, \phi_r), \text{ a field setting over } k; \text{ with}$$

$$\phi_i = \left(K_i, \sigma^{(i)}, a_i\right), \text{ a field element over } k:$$

i) $a_1 = \cdots = a_r = 1$, and $\dim \Phi = n$;

ii) [ identifying $M(1, K_i)$ with $K_i$ ] $\mathcal{Y} \subseteq \Pi^{-1} \Delta_{\Phi} \left( \prod_{i=1}^{r} K_i \right) \Pi$.

**Proof.**

1) ($\Longleftarrow$):

Follows, verbatim, by the simple proof given for Theorem 4.B.4, ($\Longrightarrow$).

2) ($\Longrightarrow$):

Follows at once from Theorem 4.B.4, ($\Longleftarrow$), and Lemma 4.B.5, parts (1) and (2,a) (noting that in that Lemma, by definition, we have $a_{\dot{\phi}_i} = 1$, for all $i$).

$\square$

## 4.3 Rationalizable Subsets of a Certain Class of Matrices.

For convenience, we will call a matrix in Jordan Form *an elementary Jordan matrix,* when each eigenvalue has exactly one basic Jordan block belonging to it. The main result of this section will be a classification of all $k$ – rationalizable subsets of matrices that contain and centralize a given elementary Jordan matrix.

Recall from Chapter 1 that, for $a \in \mathbb{Z}^+$, we let $N_a \in M(a,k)$ be the canonical $a \times a$ nilpotent matrix:

$$N_a = \begin{bmatrix} 0 & 1 & & \bigcirc \\ & & \cdots & \\ & \cdots & & 1 \\ \bigcirc & & & 0 \end{bmatrix}.$$

**Lemma 4.C.1**

Let $F$ be any field, and let $L$ be any extension field of $F$.

Let $n, a \in \mathbb{Z}^+$, where $a \geq 2$.

Let $X \in M(n, F)$, where $X$ is nilpotent with index $a$.

Let $p \in L[x]$, where $p \neq 0$ and $deg(p) \leq a - 1$.

**Then:**

$$p(X) \in M(n, F) \Longrightarrow p \in F[x].$$

**Proof.**

The proof here is elementary, and is given by induction.

1) For $f \in L[x] - \{0\}$, let $\delta(f) \equiv$ the largest power of $x$ that divides $f$: $x^{\delta(f)} \| f$.

So clearly:

$$f \in L[x] - \{0\} \Longrightarrow f = qx^{\delta(f)+1} + \alpha x^{\delta(f)};$$

for some $q \in L[x]$ and $\alpha \in L - \{0\}$.

2) Let $p \in L[x]$ be as given: $p \neq 0, deg(p) \leq a-1$ and $p(X) \in M(n,F)$. Suppose $\delta(p) = a-1$. So clearly, by definition of $\delta$, we now have here:

$$p = \alpha x^{a-1}, \text{ for some } \alpha \in L - \{0\}.$$

Therefore:

$$p(X) = \alpha X^{a-1}.$$

Therefore:

$$\alpha X^{a-1} \in M(n,F). \tag{1}$$

Now we are given $X \in M(n,F)$, and $X^{a-1} \neq O_n$ (as $X$ is given with nilpotence index $a \geq 2$). So, at once, by (1):

$$\alpha \in F.$$

Therefore:

$$p = \alpha x^{a-1} \in F[x]. \tag{2}$$

3) Inductively, we let $0 < m \leq a-1$ and suppose that the desired conclusion of the lemma is true for such $p \in L[x]$ where $m \leq \delta(p) \leq a-1$. We now suppose that $\delta(p) = m-1$, and show that the conclusion is true for $p$. As $\delta(p) = m-1$, we have:

$$p = qx^m + \alpha x^{m-1}; \text{ for some } q \in L[x], \alpha \in L - \{0\}. \tag{3}$$

As $0 < m \leq a-1$, we have $1 \leq a-m \leq a-1$, and so:

$$x^{a-m}p = qx^a + \alpha x^{a-1}.$$

So, using the given that $X^a = O_n$:

$$X^{a-m}p(X) = q(X)X^a + \alpha X^{a-1} = \alpha X^{a-1}.$$

Thus, as given $X, p(X) \in M(n,F)$, we conclude:

$$\alpha X^{a-1} \in M(n,F).$$

So, immediately, as in step (2) above:

$$\alpha \in F. \tag{4}$$

4) Thus, using (3),(4), and the given that $X, p(X) \in M(n,F)$, we have:

$$q(X)X^m = p(X) - \alpha X^{m-1} \in M(n,F). \tag{5}$$

Now if $q \neq 0$, then clearly $\delta(qx^m) \geq m$ (and, certainly, by (3): $deg(qx^m) = deg(p) \leq a-1$, so that $\delta(qx^m) \leq a-1$). This, with (5), allows the induction hypothesis to be applied to $qx^m$, and so here we have at once: $qx^m \in F[x]$. The latter conclusion is certainly also true if $q = 0$. So we now conclude that:

$$qx^m \in F[x]. \tag{6}$$

5) Combining (3),(4), and (6), we have at once:

$$p = qx^m + \alpha x^{m-1} \in F[x].$$

This completes the induction for $p$.

$\square$

**Theorem 4.C.2**

Let $\beta_1, \ldots, \beta_r \in \overline{k}$, where the $\beta_i$ are pair-wise non-conjugate over $k$.

Suppose $\Phi = (\phi_1, \ldots, \phi_r)$ is a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$, where $K_i = k(\beta_i)$.

Let $M_i \equiv \beta_i I_{a_i} + N_{a_i} \in M(a_i, K_i)$.

Suppose $\mathcal{Y} \subseteq M(\dim \Phi, L)$, where $\Delta_\Phi(M_1, \ldots, M_r) \in \mathcal{Y}$ and all elements of $\mathcal{Y}$ commute with $\Delta_\Phi(M_1, \ldots, M_r)$.

**Then:**

1) $\mathcal{Y}$ is $k$–rationalizable over $L$

$$\Longleftrightarrow$$

$$\mathcal{Y} \subseteq \Delta_\Phi\left(\Pi_{i=1}^{r} K_i[N_{a_i}]\right).$$

[Here, $K_i[N_{a_i}] \equiv$ the $K_i$–subalgebra of $M(a_i, K_i)$ generated by $N_{a_i}$.]

2) In particular:

$$\mathcal{Y} \text{ is } k\text{–rationalizable over } L \quad \Longrightarrow$$

$$\text{a)} \quad \mathcal{Y} \subseteq M(\dim \Phi, \overline{k});$$

$$\text{b)} \quad \mathcal{Y} \text{ is commutative;}$$

$$\text{c)} \quad k[\mathcal{Y}] \hookrightarrow \Pi_{i=1}^{r} \tfrac{K_i[x]}{(x^{a_i})}.$$

[ Here, $k[\mathcal{Y}] \equiv$ the $k$–subalgebra of $M(\dim \Phi, \overline{k})$ generated by $\mathcal{Y}$. ]

**Proof.**

($\Longleftarrow$)

1) Let $\mathcal{Y} \subseteq \Delta_\Phi \left( \prod_{i=1}^{r} K_i[N_{a_i}] \right) \subseteq Im(\Delta_\Phi)$. So, at once by Theorem 3.B.1 (and is $L \supseteq \overline{k}$), $\mathcal{Y}$ is $k$–rationalizable over $L$.

($\Longrightarrow$)

2) Let $\mathcal{Y}$ be $k$–rationalizable over $L$. Now by definition of the $M_i$, we have easily:

$$\Delta_\Phi(M_1, \ldots, M_r) = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} \left[ \sigma_j^{(i)}(\beta_i) I_{a_i} + N_{a_i} \right],$$

$$\Delta_{\phi_i}(M_i) = \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} \left[ \sigma_j^{(i)}(\beta_i) I_{a_i} + N_{a_i} \right].$$

We are given that the quantities $\beta_1, \ldots, \beta_r$ are pair-wise non-conjugate over $k$. Moreover, by the given, we also have: $deg_k(\beta_i) = [k(\beta_i) : k] = [K_i : k] = n_{\phi_i}$. Thus, the quantities, $\sigma_j^{(i)}(\beta_i)$, are all distinct. So, at once, by Propositions App. 8, part (b) and App. 9, part (ii) of the Appendix, we have:

$$(1)\qquad \begin{aligned} C_L\left(\Delta_{\Phi}(M_1,\ldots,M_r)\right) &= \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{i=1}^{r} L[N_{a_i}]^{(n_{\phi_i})}, \\ C_L\left(\Delta_{\phi_i}(M_i)\right) &= L[N_{a_i}]^{(n_{\phi_i})}. \end{aligned}$$

In particular:

$$(2)\qquad C_L\left(\Delta_{\Phi}(M_1,\ldots,M_r)\right) \subseteq \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})}.$$

3) So now, given that $\mathcal{Y} \subseteq M(\dim\Phi, L)$ and that $\mathcal{Y}$ centralizes $\Delta_{\Phi}(M_1,\ldots,M_r)$, we have at once by (1) and (2):

$$(3)\qquad \mathcal{Y} \subseteq \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{i=1}^{r} L[N_{a_i}]^{(n_{\phi_i})}.$$

In particular:

$$(4)\qquad \mathcal{Y} \subseteq \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})}.$$

4) Now for $Y \in \mathcal{Y}$, by (4), express $Y$ in the obvious [and even unique] way as:

(5)

$$Y = \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{i=1}^{r} Y^{(i)},\quad Y^{(i)} = \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{j=1}^{n_{\phi_i}} Y_j^{(i)};\ \text{for some } Y^{(i)} \in M(a_i n_{\phi_i}, L), Y_j^{(i)} \in M(a_i, L).$$

5) For all $Y \in \mathcal{Y}$, we have by (3) and (5):

$$(6)\qquad Y_j^{(i)} = P^{(i)}_{Y,j}(N_{a_i});\ \text{for some } P^{(i)}_{Y,j} \in L[x],$$

with $P^{(i)}_{Y,j} = 0$ or $deg(P^{(i)}_{Y,j}) \leq a_i - 1$ (we may take $deg(P^{(i)}_{Y,j}) \leq a_i - 1$ as $(N_{a_i})^{a_i} = O_{a_i}$).

6) By (4) and Theorem 3.B.2 [with "$\mathcal{W}$"$\equiv \{\Delta_\Phi(M_1,\dots,M_r)\}$], and the supposition here that $\mathcal{Y}$ is $k$–rationalizable over $L$, we have at once:

$$\mathcal{Y} \subseteq C^{-1} Im(\Delta_\Phi) C;\ \text{for some } C \in \mathop{\textcircled{$\Delta$}}_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}.$$

Thus:

(7)

$$\mathcal{Y} = C^{-1}\Delta_\Phi(\mathcal{T})C;\ \text{for some } C \in \mathop{\textcircled{$\Delta$}}_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}, \mathcal{T} \subseteq \Pi_{i=1}^{r} M(a_i, K_i).$$

7) As $C \in \mathop{\textcircled{$\Delta$}}_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}$, express C in the obvious [and even unique] way as:

$$(8)\ \ C = \mathop{\textcircled{$\Delta$}}_{i=1}^{r} C^{(i)} = \mathop{\textcircled{$\Delta$}}_{j=1}^{n_{\phi_i}} C_j^{(i)};\ \text{for some } C^{(i)} \in G\ell(a_i n_{\phi_i}, L), C_j^{(i)} \in G\ell(a_i, L).$$

This, with (7) and (5), shows:

$$(9)\qquad Y_j^{(i)} = (C_j^{(i)})^{-1}\sigma_j^{(i)}(T_Y^{(i)})C_j^{(i)};\ \text{for some } T_Y^{(i)} \in M(a_i, K_i).$$

8) Now for $i \in \{1,\dots,r\}$, let $b(i) \in \{1,\dots,n_{\phi_i}\}$ be such that $\sigma_{b(i)}^{(i)} = id_{K_i}$ [this is OK, as $\sigma^{(i)}$ enumerates $\mathrm{Iso}(K_i/k)$]. So, in particular, by (9):

$$Y_{b(i)}^{(i)} = (C_{b(i)}^{(i)})^{-1} T_Y^{(i)} C_{b(i)}^{(i)};\ \text{for some } T_Y^{(i)} \in M(a_i, K_i).$$

Hence:

$$(10)\qquad C_{b(i)}^{(i)} Y_{b(i)}^{(i)} C_{b(i)}^{(i)} = T_Y^{(i)} \in M(a_i, K_i).$$

And, in particular, by (6):

$$(11)\qquad Y_{b(i)}^{(i)} = P_{Y,b(i)}^{(i)}(N_{a_i});\ \text{for some } P_{Y,b(i)}^{(i)} \in L[x],$$

with $P^{(i)}_{Y,b(i)} = 0$ or $\deg\,(P^{(i)}_{Y,b(i)}) \le a_i - 1$.

9) Let $Y_0 \equiv \Delta_\Phi(M_1, \ldots, M_r)$. So, by the given, we have $Y_0 \in \mathcal{Y}$. Clearly, by definition of $Y_0$, we have $(Y_0)^{(i)}_j = \sigma^{(i)}_j(\beta_i)I_{a_i} + N_{a_i}$. Thus, by (9):

(12) $\sigma^{(i)}_j(\beta_i)I_{a_i} + N_{a_i} = (C^{(i)}_j)^{-1}\sigma^{(i)}_j(T^{(i)}_{Y_0})C^{(i)}_j$; for some $T^{(i)}_{Y_0} \in M(a_i, K_i)$.

And also, by (10):

$$(13) \qquad C^{(i)}_{b(i)}(\beta_i I_{a_i} + N_{a_i})C^{(i)^{-1}}_{b(i)} = T^{(i)}_{Y_0} \in M(a_i, K_i).$$

10) Now from (13), as $\beta_i I_{a_i}$ is a scalar matrix, we have:

$$(14) \qquad \beta_i I_{a_i} + C^{(i)}_{b(i)}N_{a_i}C^{(i)^{-1}}_{b(i)} = T^{(i)}_{Y_0} \in M(a_i, K_i).$$

Letting

$$(15) \qquad N'_{a_i} \equiv C^{(i)}_{b(i)}N_{a_i}C^{(i)^{-1}}_{b(i)},$$

using $\beta_i \in K_i$ by the given, and observing that $N'_{a_i} = T^{(i)}_{Y_0} - \beta_i I_{a_i}$ by (14), we conclude at once:

$$(16) \qquad N'_{a_i} \in M(a_i, K_i).$$

11) Substituting (14) into (12), and using (15) and (16), we have:

$$\begin{aligned}
\sigma^{(i)}_j(\beta_i)I_{a_i} + N_{a_i} &= (C^{(i)}_j)^{-1}\sigma^{(i)}_j(\beta_i I_{a_i} + N'_{a_i})C^{(i)}_j \\
&= (C^{(i)}_j)^{-1}\left(\sigma^{(i)}_j(\beta_i)I_{a_i} + \sigma^{(i)}_j(N'_{a_i})\right)C^{(i)}_j \\
&= \sigma^{(i)}_j(\beta_i)I_{a_i} + (C^{(i)}_j)^{-1}\sigma^{(i)}_j(N'_{a_i})C^{(i)}_j.
\end{aligned}$$

Thus, cancelling the "$\sigma_j^{(i)}(\beta_i)I_{a_i}{}'$ s", moving the "$C_j^{(i)}$'s" over to the LHS, and transposing the previous, we have:

(17) $$\sigma_j^{(i)}(N'_{a_i}) = C_j^{(i)} N_{a_i} (C_j^{(i)})^{-1}.$$

12) Now, substituting (11) in (10), we have:

$$C_{b(i)}^{(i)} P_{Y,b(i)}^{(i)}(N_{a_i}) C_{b(i)}^{(i)^{-1}} = T_Y^{(i)} \in M(a_i, K_i).$$

So, as $P_{Y,b(i)}^{(i)}$ is a polynomial over $L$:

$$P_{Y,b(i)}^{(i)}(C_{b(i)}^{(i)} N_{a_i} C_{b(i)}^{(i)^{-1}}) = T_Y^{(i)} \in M(a_i, K_i).$$

Thus, by (15):

(18) $$P_{Y,b(i)}^{(i)}(N_{a_i}{}') \in M(a_i, K_i).$$

The facts in (18),(16), and (11), together with the fact that, by (15), $N'_{a_i}$ is clearly nilpotent with index $a_i$, show at once, using Lemma 4.C.1 (with "$F$" $\equiv K_i$), that:

$$a_i = 1 \quad \text{or} \quad P_{Y,b(i)}^{(i)} = 0 \text{ or } \ P_{Y,b(i)}^{(i)} \in K_i[x].$$
$$\text{Therefore}: a_i = 1 \quad \text{or} \quad P_{Y,b(i)}^{(i)} \in K_i[x].$$

Now if $a_i = 1$, then, by definition, $N_{a_i}$ is the $1 \times 1$ matrix $[0]$: $N_{a_i} = [0]$. So clearly, by (15), we have also $N'_{a_i} = [0]$. So, by (18): $P_{Y,b(i)}^{(i)}([0]) \in M(a_i, K_i)$; hence, $P_{Y,b(i)}^{(i)}(0) \in K_i$. But, by (11), here: $P_{Y,b(i)}^{(i)} = 0$ or $\deg\,(P_{Y,b(i)}^{(i)}) \leq 0$; hence, $P_{Y,b(i)}^{(i)}$ is constant. The previous two conclusions show at once that here: $P^{(i)}_{Y,b(i)} \in K_i \subseteq K_i[x]$. Thus, in particular, if $a_i = 1$, then $P^{(i)}_{Y,b(i)} \in K_i[x]$. This, with the conclusion now immediately above gives at once:

$$P^{(i)}_{Y,b(i)} \in K_i[x]. \tag{19}$$

13) Now we stop to make a simple observation. Let $a \in \mathbb{Z}^+, K/k$ be any extension of fields, and $\sigma \in \mathrm{Iso}(K/k)$. We let $\widehat{\sigma}$ denote the canonical extension of $\sigma$, from $K$ to $K[x]$; i.e., for $f = \sum_{i=0}^{n} \alpha_i x^i \in K[x]$, we let $\widehat{\sigma}(f) \equiv \sum_{i=0}^{n} \sigma(\alpha_i) x^i \in (\sigma(K))[x]$. (So $\widehat{\sigma}$ is clearly also an imbedding of $k$-algebras, but we do not need this.) Finally, let $p \in K[x]$ and $A \in M(a, K)$. With this, and writing $p = \sum_{i=0}^{n} \alpha_i x^i \in K[x]$, we easily calculate:

$$\sigma\left(p(A)\right) = \sigma\left(\sum_{i=0}^{n} \alpha_i A^i\right) = \sum_{i=0}^{n} \sigma(\alpha_i)\sigma(A)^i = \widehat{\sigma}(p)\left(\sigma(A)\right).$$

Thus:

$$p \in K[x], A \in M(a, K) \Longrightarrow \sigma\left(p(A)\right) = \widehat{\sigma}(p)\left(\sigma(A)\right). \tag{20}$$

14) Now using (9),(10),(11),(15),(20),(17), and the fact that $N_{a_i}$ consists of 0 's and 1 's only, we calculate:

$$\begin{aligned}
Y_j^{(i)} &= (C_j^{(i)})^{-1}\sigma_j^{(i)}(T_Y^{(i)})C_j^{(i)} && \text{[by (9)]} \\
&= (C_j^{(i)})^{-1}\sigma_j^{(i)}(C_{b(i)}^{(i)}Y_{b(i)}^{(i)}C_{b(i)}^{(i)^{-1}})C_j^{(i)} && \text{[by (10)]} \\
&= (C_j^{(i)})^{-1}\sigma_j^{(i)}\left(C_{b(i)}^{(i)}P_{Y,b(i)}^{(i)}(N_{a_i})C_{b(i)}^{(i)^{-1}}\right)C_j^{(i)} && \text{[by (11)]} \\
&= (C_j^{(i)})^{-1}\sigma_j^{(i)}\left(P_{Y,b(i)}^{(i)}(C_{b(i)}^{(i)}N_{a_i}C_{b(i)}^{(i)^{-1}})\right)C_j^{(i)} \\
&\qquad\qquad \text{[as } P_{y,b(i)}^{(i)} \text{ is a polynomial over L ]} \\
&= (C_j^{(i)})^{-1}\sigma_j^{(i)}\left(P_{Y,b(i)}^{(i)}(N'_{a_i})\right)C_j^{(i)} && \text{[by (15)]} \\
&= (C_j^{(i)})^{-1}\left[\widehat{\sigma_j^{(i)}}(P_{Y,b(i)}^{(i)})\left(C_j^{(i)}N'_{a_i})\right)\right]C_j^{(i)} \\
&\qquad\qquad \text{by (16), (19), and (20)]} \\
&= \widehat{\sigma_j^{(i)}}(P_{Y,b(i)}^{(i)})\left((C_j^{(i)})^{-1}\sigma_j^{(i)}(N'_{a_i})C_j^{(i)}\right) \\
&\qquad\qquad \text{[ as } \widehat{\sigma_j^{(i)}}(P_{Y,b(i)}^{(i)})\text{[ is a polynomial ]} \\
&= \widehat{\sigma_j^{(i)}}(P_{y,b(i)}^{(i)})(N'_{a_i}) && \text{[ by (17)]} \\
&= \widehat{\sigma_j^{(i)}}(P_{y,b(i)}^{(i)})\left(\sigma_j^{(i)}(N'_{a_i})\right) \\
&\qquad\qquad \text{[as } N_{a_i} \text{ consists of 0's , 1's]} \\
&= \sigma_j^{(i)}\left(P_{Y,b(i)}^{(i)}(N_{a_i})\right) && \text{[by (20)].}
\end{aligned}$$

Therefore:

$$Y_j^{(i)} = \sigma_j^{(i)}\left(P_{Y,b(i)}^{(i)}(N_{a_i})\right).$$

And, again by (19), clearly:

$$P_{Y,b(i)}^{(i)}(N_{a_i}) \in K_i[N_{a_i}] \subseteq M(a_i, K_i).$$

Thus, by the previous two conclusions, by the definition of $\Delta_\Phi$, and by (5), we have:

$$\begin{aligned} Y &= \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} Y_j^{(i)} = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathop{\textcircled{$\triangle$}}\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)} \left( P_{Y,b(i)}^{(i)}(N_{a_i}) \right) \\ &= \Delta_\Phi \left( P_{Y,b(1)}^{(1)}(N_{a_1}), \ldots, P_{Y,b(r)}^{(r)}(N_{a_r}) \right) \\ &\in \Delta_\Phi \left( \prod_{i=1}^{r} K_i[N_{a_i}] \right). \end{aligned}$$

Hence:

$$\mathcal{Y} \subseteq \Delta_\Phi \left( \prod_{i=1}^{r} K_i[N_{a_i}] \right). \tag{21}$$

This completes the proof of the desired conclusion (1).

15) The desired conclusion (2) follows at once from the conclusion (1), ($\Longrightarrow$), just proved above, and the obvious fact that $K_i[N_{a_i}] \approx K_i[x]/(x^{a_i})$, as $k$–algebras, and recalling that $\Delta_\Phi$ is an imbedding of $k$–algebras.

$\square$

# Chapter 5

# Conjugate Parallelism and Rationalizability

## 5.1 Introduction

In this chapter, we present a point of view which allows an alternative, and very succinct, statement of the condition for $k$–rationalizability of subsets of diagonal matrices. This alternative interpretation can be quite illustrative.

The above-mentioned statement is the sole result of this chapter, and follows fairly easily from the definitions of the next section. Because of this, and the fact that this result will not be used afterward, its proof is just briefly sketched here.

*Throughout this chapter, $k$ is a perfect field and $L$ is any extension field of $\overline{k}$.*

## 5.2 Definitions

Here we present a number of definitions which provide the alternative point of view mentioned in Section 1.

### 5.2.1 General Definitions

Let $S$ be a set.

Let $f: S \to \overline{k}$, $g: S \to \overline{k}$.

We let:

a) $k(f) \equiv k(Im(f)) \subseteq \overline{k}$; and we call $k(f)$: *the field of $f$.*

b) $f \sim_k g \overset{def}{\Leftrightarrow} \exists \sigma \in \mathrm{Iso}(k(f)/k)$: $\sigma \circ f = g$;

if $f \sim_k g$, we say *$f$ is $k$-conjugate to $g$* (or, *$g$ is a $k$-conjugate of $f$*).

Clearly, $\sim_k$ is an equivalence relation on $\overline{k}^S$.

### 5.2.2 Definitions for Diagonal Matrices – I

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{Y} \subseteq D(n, \overline{k})$. [For $Y \in \mathcal{Y}$, recall $Y_{ii}$ = the $i^{th}$ diagonal entry of $Y \in \overline{k}$.]

Let $i \in \{1, \ldots, n\}$.

We let:

a) $R^{(i)}_{\mathcal{Y}}\colon \mathcal{Y} \to \bar{k}$ ; $R^{(i)}_{\mathcal{Y}}\colon Y \mapsto Y_{ii}$.

We call $R^{(i)}_{\mathcal{Y}}$: *the $i^{th}$ row-function of $\mathcal{Y}$.*

b) $N_i \equiv \left|\{j \in \{1,\dots,n\} \mid R^{(j)}_{\mathcal{Y}} = R^{(i)}_{\mathcal{Y}}\}\right| \in \{1,\dots,n\}$.

We call $N_i$: *the multiplicity of $R^{(i)}_{\mathcal{Y}}$ in $\mathcal{Y}$.*

c) $K_i \equiv k\left(R^{(i)}_{\mathcal{Y}}\right) \subseteq \bar{k}$.

We call $K_i$: *the $i^{th}$ row-field of $\mathcal{Y}$.*

### 5.2.3 Definitions for Diagonal Matrices – II

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{Y} \subseteq D(n, \bar{k})$.

We say:

a) $\mathcal{Y}$ has *conjugate parallelism over $k$* $\overset{def}{\Longleftrightarrow}$ the set of row-functions of $\mathcal{Y}$ is closed under $k$–conjugation of functions.

b) $\mathcal{Y}$ has *even parallelism over $k$* $\overset{def}{\Longleftrightarrow}$ if two row-functions of $\mathcal{Y}$ are $k$–conjugate, then they have the same multiplicity in $\mathcal{Y}$.

## 5.3 Main Result

The following theorem compares with Theorem 4.B.4, and Corollary 4.B.6. This theorem provides an alternative point of view of the condition for $k$–rationalizability of subsets of diagonal matrices.

**Theorem 5.C.1**

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{Y} \subseteq D(n, L)$.

**Then:**

$$\mathcal{Y} \text{ is } k\text{–rationalizable over } L$$

$$\Longleftrightarrow$$

all row-fields of $\mathcal{Y}$ are *finite extensions* of $k$, and $\mathcal{Y}$ has *even, conjugate parallelism* over $k$.

**Proof.** (Sketch)

$(\Longrightarrow)$

1) This follows virtually at once from Corollary 4.B.6, $(\Longrightarrow)$, and elementary use of field imbeddings.

$(\Longleftarrow)$

2) First, we note that, as the row-fields of $\mathcal{Y}$ are given to be finite extensions of $k$, so clearly $\mathcal{Y} \subseteq D(n, \overline{k})$. Second, we define the following quantities.

a) $r \equiv$

the number of equivalence classes of $\sim_k$, when restricted to the set of row-functions of $\mathcal{Y}$.

b) $K_1, \ldots, K_r \equiv$

any sequence of row-fields of $\mathcal{Y}$, obtained by selecting exactly one row-function from each of the equivalence classes in (a) above.

c) $\sigma^{(1)}, \ldots, \sigma^{(r)} \equiv$

any sequence of enumerators for, resp., $Iso(K_1/k), \ldots, Iso(K_r/k)$.

d) $a_1, \ldots, a_r \equiv$

the multiplicity number of the row-functions within the equivalence classes in (a)–these classes being selected in the sequence from (b). [Multiplicity numbers are constant over a given class here, as $\mathcal{Y}$ is given to have *even* parallelism over $k$.]

e) $\Phi \equiv$

$(\phi_1, \ldots, \phi_r)$, a field setting over $k$, with $\phi_i \equiv \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$.

f) Let $\Pi \in \mathrm{Perm}(n, k)$ be any permutation matrix such that the action of $\mathrm{conj}_\Pi$ on diagonal matrices causes the rows represented in each equivalence class of (a) to be "blocked together", and within these blocks, identical rows are to be "blocked together" and in sequence "corresponding to" the "$\sigma^{(i)}$" selected in (c) above, for that class.

Then, with the quantities as defined above, we easily see:

i) $\dim \Phi = n$;

ii) $\mathcal{Y} \subseteq \Pi^{-1}\Delta_{\Phi}\left(\Pi_{i=1}^{r} \text{ Scalar } (a_i, K_i)\right)\Pi$.

In particular, we have:

$$\mathcal{Y} \subseteq \Pi^{-1} Im(\Delta_{\Phi})\Pi.$$

So clearly, by Theorem 3.B.1, ($\Longleftarrow$), we have:

$$\mathcal{Y} \text{ is } k\text{–rationalizable over } L.$$

$\square$

**Remark**

In the statement of Theorem 5.C.1, the phrase "all row-fields of $\mathcal{Y}$ are finite extensions of $k$", could actually also be dropped. This is a simple field-theoretic consequence of the fact that $\mathcal{Y}$ already has a finite number $[= n]$ of row-functions.

# Chapter 6

# Rationalizable Normalizers of Subsets of Diagonal Matrices

## 6.1 Introduction

In this section, we look at normalizing extensions of the subsets of diagonal matrices previously found to be $k$–rationalizable over $L$. We determine which subsets of these normalizing extensions are themselves $k$–rationalizable over $L$.

*Throughout this chapter, $k$ is a perfect field, and $L$ is any extension field of $\overline{k}$.*

This chapter is somewhat lengthy, and weaves together several results of different nature. The chapter begins by recalling some basic material from Chapter 1, Section 4, on equivalence of field elements and field settings, and by developing some additional, small results in connection with this. After this, a particularly "clean and organized" type of field setting is defined, and is called a **reduced field setting**. The definition may seem to be not only natural, and with no real loss of generality, but will also be seen to make many results clearer and simpler to state. With this definition, a few very technical lemmas are proved. Then, the most key theorem of this chapter, Theorem 6.D.1, is proved. The proof consists of two main "acts", and (at present) is lengthy. Following this, a number of important lemmas are proved. Some of these lemmas contain very key and non-trivial arguments of their own, and some contain results which are due mostly to Theorem 6.D.1. Finally, these critical results are pulled together to form the final exhibitions and conclusions of Theorems 6.F.1 and 6.F.2.

## 6.2 Equivalence of Field Elements, and Notation

Here, we recall from Chapter 1 the definitions of equivalence of field elements and field settings. We then introduce some further notation connected with this, and which will be critically and liberally used throughout this chapter.

### 6.2.1 Recollections from Chapter 1

Recall the following definitions from Chapter 1, Section 4, Subsection 4.

a) Let $\phi = (K, \sigma, a)$, $\theta = (L, \tau, b)$ be two field elements over $k$. Then we recall the following:

$$\phi \sim_k \theta \overset{def}{\Leftrightarrow} K \sim_k L \text{ and } a = b.$$

**Note:** Here, recall that $K \sim_k L$ means that $K$ and $L$ are fields that are conjugate over $k$.

Recall that $\sim_k$ is an equivalence relation on the set of field elements over $k$.

b) Let $\Phi = (\phi_1, \ldots, \phi_r)$, $\Omega = (\omega_1, \ldots, \omega_s)$ be two field settings over $k$. Then we recall the following:

$$\Phi \sim_k \Omega \overset{def}{\Leftrightarrow} r = s \text{ and } \exists p \in S_r \colon \forall i \in \{1, \ldots, r\} \colon \ \phi_i \sim_k \omega_{p(i)}.$$

Recall that $\sim_k$ is an equivalence relation on the set of field settings over $k$.

Additionally, throughout this chapter, we will frequently be using the permutation matrices defined on field elements and field settings, and their properties, as described in Chapter 1, Section 3, Subsections 3 and 6, and Section 4, Subsection 2. We recall from those sections, and list below, the main properties of these matrices that we will be using here. (The fundamental definitions of these matrices will not be recalled or needed here – we will only need the *properties* of these matrices.)

c) Let $\phi = (K, \sigma, a)$ be a field element over $k$. Let $\sigma \in \mathit{Iso}(K/k) \subseteq E \subseteq \overline{k}$, $E$ any intermediate field of $\overline{k}/k$. Let $\tau \in \mathit{Iso}(E/k)$, $\gamma \in \mathit{Gal}(K/k)$. Then we recall the following:

   i) $\Pi_{\tau,\phi}\,,\, \Gamma_{\gamma,\phi} \in \mathrm{Perm}(an_\phi, I_a, k)$;

   ii) $\forall M \in M(a, K) \colon \ \tau\left(\Delta_\phi(M)\right) = \Pi_{\tau,\phi}^{-1} \Delta_\phi(M) \Pi_{\tau,\phi}$,

$$\Delta_{\phi}\left(\gamma(M)\right) = \Gamma_{\gamma,\phi}\Delta_{\phi}(M)\Gamma^{-1}_{\gamma,\phi} = \Gamma^{-1}_{\gamma^{-1},\phi}\Delta_{\phi}(M)\Gamma_{\gamma^{-1},\phi};$$

iii) $\Pi_{\tau,\phi}$ , $\Gamma_{\gamma,\phi}$ commute;

iv) The map $f$ below is an imbedding:

$$f\colon Ga\ell(K/k) \to \mathrm{Perm}(an_{\phi}, I_a, k)$$

$$f\colon \gamma \mapsto \Gamma_{\gamma,\phi}.$$

v) $Ga\ell(\phi) \equiv \{\Gamma_{\gamma,\phi} \in \mathrm{Perm}(an_{\phi}, I_a, k) | \gamma \in Ga\ell(K/k)\} \approx Ga\ell(K/k)$.

d) Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$. Let $\cup_{i=1}^{r} \cup_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(K_i) \subseteq E \subseteq \overline{k}$, $E$ any intermediate field of $\overline{k}/k$. Let $\tau \in Iso(E/k)$, $\vec{\gamma} \equiv (\gamma_1, \ldots, \gamma_r) \in \Pi_{i=1}^{r} Ga\ell(K_i/k)$. Then we recall the following:

i) $\Pi_{\tau,\Phi} \equiv \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \Pi_{\tau,\phi_i} \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k)$;

ii) $\Gamma_{\vec{\gamma},\Phi} \equiv \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \Gamma_{\gamma_i,\phi_i} \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r} \mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k)$;

iii) $\forall B \in Im(\Delta_{\Phi})$: $\tau(B) = \Pi^{-1}_{\tau,\Phi} B \Pi_{\tau,\Phi}$;

iv) $\Pi_{\tau,\Phi}$ and $\Gamma_{\vec{\gamma},\Phi}$ commute;

v) $\forall V \in V_{\Phi}$: $\tau(V) = V\Pi_{\tau,\Phi}$.

### 6.2.2 Definition of Equivalence Classes of a Field Setting

With the recollections in parts (a) and (b) of the previous Subsection in mind, we make the following fundamental definition.

**Definition**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$.

**We let:**

$\Phi/\!\sim_k \equiv$ the set of equivalence classes of $(\phi_1, \ldots, \phi_r)$, under $\sim_k$ (here, $\sim_k$ is the equivalence relation for field elements).

**Note:** Here, we count $\phi_i$ and $\phi_j$ as distinct elements, if $i \neq j$; this will cause no confusion. (What we are working with here, really, is an equivalence relation, $\sim_k$, on the set of *indices,* $\{1, \ldots, r\}$, used for the field elements, $\phi_i$. Technically, we would write $i \sim_k j \overset{def}{\Leftrightarrow} \phi_i \sim_k \phi_j$, and we would break up $\{1, \ldots, r\}$ into equivalence classes; but this would cause confusion! So, we stick with the above approach, its mild abuse understood!)

## 6.2.3 Elementary Lemmas

With the two previous subsections in mind, we give the following two elementary lemmas. The second lemma below will be referred to frequently.

**Lemma 6.B.1**

Let $\phi, \theta$ be two field elements over $k$.

**Then:**

$$\phi \sim_k \theta \Rightarrow a_\phi = a_\theta, n_\phi = n_\theta, \dim\phi = \dim\theta.$$

**Proof.**

Let $\phi = (K, \sigma, a), \theta = (L, \tau, b)$. As given $\phi \sim_k \theta$, we have, by definition, that: $b = a$ and $L \sim_k K$. Thus, at once:

$$a_\phi = a = b = a_\theta, n_\phi = [K\colon k] = [L\colon k] = n_\theta,$$

and so also then, $\dim \phi = a_\phi n_\phi = a_\theta n_\theta = \dim \theta$.

$\square$

**Lemma 6.B.2**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

Let $u \equiv |\Phi/\sim_k|$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\sim_k$, and let $m_h \equiv |[\phi_{i_h}]|$.

**Then:**

1) $u, m_h \in \{1, \ldots, r\}$.

2) $\sum_{h=1}^{u} m_h = r$.

3) $\sum_{h=1}^{u} m_h a_{i_h} [K_{i_h}\colon k] = \dim \Phi$.

**Proof.**

1) As $\Phi = (\phi_1, \ldots, \phi_r)$, so $\Phi$ is a sequence of $r$ field elements. Thus $\Phi/\!\sim_k$, being a partition of $\Phi$, has at most $r$ "blocks" as elements. And thus $[\phi_{i_h}]$, a subset of $\Phi$, has at most $r$ elements. This proves (1).

2) As $(\phi_{i_1}, \ldots, \phi_{i_u})$ is given to be a set of representatives of $\Phi/\!\sim_k$, so $[\phi_{i_1}], \ldots, [\phi_{i_u}]$ is a partition of $\Phi$. Thus, as $\Phi$ consists of $r$ elements, we now have, in particular: $\sum_{h=1}^{u} [\phi_{i_h}]| = |\Phi|$, i.e.; $\sum_{h=1}^{u} m_h = r$. This proves (2).

3) As, by the previous, $[\phi_{i_1}], \ldots, [\phi_{i_u}]$ is a partition of $\Phi$, we certainly have:

$$\dim \Phi = \sum_{i=1}^{r} \dim \phi_i = \sum_{h=1}^{u} \sum_{\phi \in [\phi_{i_h}]} \dim \phi.$$

Now, if $\phi, \phi' \in [\phi_{i_h}]$, then, by definition, $\phi \sim_k \phi'$, and so, by Lemma 6.B.1 above, we have: $\dim \phi = \dim \phi'$. Thus, noting that certainly $\phi_{i_h} \in [\phi_{i_h}]$, we have:

$$\sum_{\phi \in [\phi_{i_h}]} \dim \phi = \sum_{\phi \in [\phi_{i_h}]} \dim \phi_{i_h} = |[\phi_{i_h}]| \dim \phi_{i_h} = m_h \dim \phi_{i_h}.$$

Substituting this in the above gives now:

$$\dim \Phi = \sum_{h=1}^{u} \sum_{\phi \in [\phi_{i_h}]} \dim \phi = \sum_{h=1}^{u} m_h \dim \phi_{i_h}.$$

Finally, at once from the given, we have $\phi_{i_h} = (K_{i_h}, \sigma^{(i_h)}, a_{i_h})$. Thus, by definition: $\dim \phi_{i_h} = a_{i_h} n_{\phi_{i_h}} = a_{i_h} [K_{i_h} \colon k]$. Substituting this in the above proves (3).

□

### 6.2.4 Definition of a Reduced Field Setting

Here, we define a certain class of "nicely structured" field settings. It will be easily observed that any field setting is equivalent to one of these. Thus, essentially, all we will need to study are these field settings – and this is thankful, because they are much easier to work with.

The "nicely structured" field settings will be called *reduced field settings.* In a nutshell, reduced field settings are field settings, $\Phi$, where the field elements are all identical within a given equivalence class of $\Phi/\sim_k$, and where the sequence of field elements in $\Phi$ spells out these equivalence classes in order. Precisely, we have the definition below.

**Definition** (Reduced Field Setting)

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$.

Let $u \equiv |\Phi/\sim_k| \in \{1, \ldots, r\}$.

**We say:**

$$\Phi \text{ is a } \textit{reduced} \text{ field setting over } k \quad \overset{def}{\Leftrightarrow}$$

i) the sequence, $(\phi_1, \ldots, \phi_r)$, can be partitioned into the equivalence classes of $\Phi/\sim_k$:

i.e., for some $1 \le h_1 < h_2 < \cdots < h_u = r$, we have:

$$\Phi = (\phi_1, \ldots, \phi_r) = (\phi_1, \ldots, \phi_{h_1}, \phi_{h_1+1}, \ldots, \phi_{h_2}, \ldots\ldots, \phi_{h_{u-1}+1}, \ldots, \phi_{h_u})$$

and

$$\Phi/\!\sim_k = (\phi_1, \ldots, \phi_r)/\!\sim_k = \left((\phi_1, \ldots, \phi_{h_1}), (\phi_{h_1+1}, \ldots, \phi_{h_2}), \ldots, (\phi_{h_{u-1}+1}, \ldots, \phi_{h_u})\right).$$

ii) within each equivalence class of $\Phi/\!\sim_k$, all field elements are identical:

$$\phi_1 = \cdots = \phi_{h_1}, \phi_{h_1+1} = \cdots = \phi_{h_2}, \ldots, \phi_{h_{u-1}+1} = \cdots = \phi_{h_u}.$$

In short, $\Phi = (\phi_1, \ldots, \phi_r)$ is a reduced field setting over $k$, when $\Phi$ is of the form:

$$\Phi = (\phi_{i_1}, \ldots, \phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_2}, \ldots\ldots, \phi_{i_u}, \ldots, \phi_{i_u}),$$

for some pair-wise non-conjugate over $k$ field elements

$$\phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_u} \in (\phi_1, \ldots, \phi_r).$$

(Certainly here, we note that we must necessarily have: $1 = i_1 < i_2 < \cdots < i_u = r$. We will not need this.) The following useful lemma expands upon these latter remarks.

**Lemma 6.B.3**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$.

Let $u \equiv |\Phi/\!\sim_k| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/\!\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$, and let $m_h \equiv |[\phi_{i_h}]|$.

**Then:**

1) a) $m_1 + m_2 + \ldots + m_u = r$;

b)
$$\begin{aligned}\Phi &= (\phi_1, \ldots, \phi_r)\\ &= (\phi_1, \ldots, \phi_{m_1}, \phi_{m_1+1}, \ldots, \phi_{m_1+m_2}, \ldots\ldots,\\ &\qquad \phi_{m_1+m_2+\cdots+m_{u-1}+1}, \ldots, \phi_{m_1+m_2+\cdots+m_u}\Big)\\ &= \left(\underbrace{\phi_{i_1}, \ldots, \phi_{i_1}}_{m_1}, \underbrace{\phi_{i_2}, \ldots, \phi_{i_2}}_{m_2}, \ldots, \underbrace{\phi_{i_u}, \ldots, \phi_{i_u}}_{m_u}\right).\end{aligned}$$

c)
$$\begin{aligned}\Phi/{\sim_k} &= (\phi_1, \ldots, \phi_r)/{\sim_k}\\ &= ((\phi_1, \ldots, \phi_{m_1}), (\phi_{m_1+1}, \ldots, \phi_{m_1+m_2}), \ldots,\\ &\qquad (\phi_{m_1+m_2+\cdots+m_{u-1}+1}, \ldots, \phi_{m_1+m_2+\cdots+m_u})\Big)\\ &= \left(\underbrace{(\phi_{i_1}, \ldots, \phi_{i_1})}_{m_1}, \underbrace{(\phi_{i_2}, \ldots, \phi_{i_2})}_{m_2}, \ldots, \underbrace{(\phi_{i_u}, \ldots, \phi_{i_u})}_{m_u}\right).\end{aligned}$$

2) a) If $f$ is a function on the field settings $\phi_1, \ldots, \phi_r$, where $f(\phi_i)$ is a subset of matrices, then:

$$\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} f(\phi_i) = \mathop{\bigcirc\kern-0.78em\triangle}_{h=1}^{u} f(\phi_{i_h})^{(m_h)}.$$

b) If $g$ is a function on the field settings $\phi_1, \ldots, \phi_r$, where $g(\phi_i)$ is an element of a ring, then:

$$\sum_{i=1}^{r} g(\phi_i) = \sum_{h=1}^{u} m_h \cdot g(\phi_{i_h}).$$

**Proof.**

1) As $\Phi$ is given reduced, we have, from part (i) of the definition 'reduced', that, for some $1 \leq h_1 < h_2 < \cdots < h_u = r$:

$$(1) \qquad \Phi = (\phi_1, \ldots, \phi_r) = (\phi_1, \ldots, \phi_{h_1}, \phi_{h_1+1}, \ldots, \phi_{h_2}, \ldots\ldots, \phi_{h_{u-1}+1}, \ldots, \phi_{h_u}),$$

and

$$(2) \qquad \Phi/\!\sim_k = (\phi_1, \ldots, \phi_r)/\!\sim_k = \left( \underbrace{(\phi_1, \ldots, \phi_{h_1})}_{E_1}, \underbrace{(\phi_{h_1+1}, \ldots, \phi_{h_2})}_{E_2}, \ldots, \underbrace{(\phi_{h_{u-1}+1}, \ldots, \phi_{h_u})}_{E_u} \right).$$

Now, as $(\phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_u})$ is given as a *subsequence* of $(\phi_1, \ldots, \phi_r)$, and is also given as a set of representatives of $\Phi/\!\sim_k$, we see clearly at once, from (1), and from (2), that:

$$(3) \qquad \phi_{i_1} \in E_1, \phi_{i_2} \in E_2, \ldots, \phi_{i_u} \in E_u.$$

As $E_1, E_2, \ldots, E_u$ are equivalence classes of $\Phi/\!\sim_k$ (by (2)), the previous shows at once that:

$$(4) \qquad [\phi_{i_1}] = E_1, [\phi_{i_2}] = E_2, \ldots, [\phi_{i_u}] = E_u.$$

As we are given $m_h = |[\phi_{i_h}]|$, the previous shows at once that also:

$$(5) \qquad m_1 = |E_1|, m_2 = |E_2|, \ldots, m_u = |E_u|.$$

Now by (2), we have at once:

$$(6) \qquad |E_1| = h_1, |E_2| = h_2 - h_1, \dots, |E_u| = h_u - h_{u-1}.$$

This, with (5), gives easily:

(7)

$$h_1 = m_1, h_2 = m_1+m_2, \dots, h_k = m_1+m_2+\cdots+m_k, \dots, h_u = m_1+m_2+\cdots+m_u.$$

And, the last equation of the previous, with the earlier-mentioned fact that $h_u = r$, shows at once:

$$(8) \qquad m_1 + m_2 + \cdots + m_u = r.$$

Finally, by part (ii) of the definition of 'reduced', with (2), (3) and (5), we have that:

$$(9) \qquad E_\ell = \left( \underbrace{\phi_{i_\ell}, \dots, \phi_{i_\ell}}_{m_\ell} \right); \quad \ell \in \{1, \dots, u\}.$$

Thus, by (2), we have:

$$(10) \qquad \left(\phi_{h_{\ell-1}+1}, \dots, \phi_{h_\ell}\right) = \left( \underbrace{\phi_{i_\ell}, \dots, \phi_{i_\ell}}_{m_\ell} \right); \quad \ell \in \{1, \dots, u\}.$$

Hence, by (8), and by substituting (7) and (10) into (1) and (2), we have proved the desired conclusion (1).

2) From desired conclusion (1,b), just proved above, we have:

$$(11) \qquad \Phi = (\phi_1, \dots, \phi_r) = \left( \underbrace{\phi_{i_1}, \dots, \phi_{i_1}}_{m_1}, \underbrace{\phi_{i_2}, \dots, \phi_{i_2}}_{m_2}, \dots\dots, \underbrace{\phi_{i_u}, \dots, \phi_{i_u}}_{m_u} \right).$$

The desired conclusions in (2) follow easily from (11) above. With function $f$ as defined in desired conclusion (2,a), we calculate at once, using (11):

$$\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} f(\phi_i) = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} \mathop{\bigcirc\kern-0.78em\triangle}\limits_{j=1}^{m_h} f(\phi_{i_h}) = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} f(\phi_{i_h})^{(m_h)}.$$

Similarly, with $g$, we calculate, using (11):

$$\sum_{i=1}^{r} g(\phi_i) = \sum_{h=1}^{u} \sum_{j=1}^{m_h} g(\phi_{i_h}) = \sum_{h=1}^{u} m_h \cdot g(\phi_{i_h}).$$

□

## 6.3 Fundamental Propositions

In this section, we present four fundamental propositions. The first two produce reduced field settings, and show "reduced" is no real loss of generality. The last two are useful, but perhaps technical, lemmas.

The following lemma shows that any field setting is equivalent to a reduced one.

**Lemma 6.C.1**

Let $\Phi$ be a field setting over $k$.

**Then:**

$\exists\tilde{\Phi}$, a *reduced* field setting over $k$: $\tilde{\Phi} \sim_k \Phi$.

**Proof.**

1) Let $\Phi = (\phi_1, \dots, \phi_r)$, where $\phi_i$ is a field element over $k$. Let $u \equiv |\Phi/{\sim_k}\ |$ and let the subsequence $(\phi_{i_1}, \phi_{i_2}, \dots, \phi_{i_u}) \subseteq (\phi_1, \dots, \phi_r)$ be a set of representatives of $\Phi/{\sim_k}$. Furthermore, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/{\sim_k}$, and let $m_h \equiv |[\phi_{i_h}]|$. With this, we may let $[\phi_{i_h}] = \left(\phi_{i_h}^{(1)}, \phi_{i_h}^{(2)}, \dots, \phi_{i_h}^{(m_h)}\right)$, where $\phi_{i_h}^{(1)} = \phi_{i_h}$. Now, as $(\phi_{i_1}, \phi_{i_2}, \dots, \phi_{i_u})$ is a set of representatives of $\Phi/{\sim_k}$, so $[\phi_{i_1}], [\phi_{i_2}], \dots, [\phi_{i_u}]$ partition [as a set, not as a sequence] $\Phi = (\phi_1, \dots, \phi_r)$. With the previous two sentences, we see at once that, for some $p \in S_r$, we have:

$$(1)\quad \left(\phi_{i_1}^{(1)}, \dots, \phi_{i_1}^{(m_1)}, \phi_{i_2}^{(1)}, \dots, \phi_{i_2}^{(m_2)}, \dots\dots, \phi_{i_u}^{(1)}, \dots, \phi_{i_u}^{(m_u)}\right) = \left(\phi_{p(1)}, \dots, \phi_{p(r)}\right).$$

2) Now let $\tilde{\Phi} = (\theta_1, \dots, \theta_s)$ be the field setting over $k$, where the $\theta_i$ are defined by:

$$(2)\qquad \tilde{\Phi} = (\theta_1, \dots, \theta_s) = (\underbrace{\phi_{i_1}, \dots, \phi_{i_1}}_{m_1}, \underbrace{\phi_{i_2}, \dots, \phi_{i_2}}_{m_2}, \dots\dots, \underbrace{\phi_{i_u}, \dots, \phi_{i_u}}_{m_u}).$$

3) Comparing the LHS of (1) and the RHS of (2), above, we see that both of these sequences have the same number of field elements. Thus, comparing now the RHS of (1) and the LHS of (2), we observe at once that we must have: $r = s$. (This also follows by Lemma 6.B.2, part (2), but we do not need this.) Furthermore, let $i \in \{1, \dots, r\}$. Then by (1), for some $h \in \{1, \dots, u\}$ and $j \in \{1, \dots, m_h\}$, we see:

$$(3)\qquad \phi_{p(i)} = \phi_{i_h}^{(j)}.$$

These same "positions" in the corresponding field settings in (2) (recall from the above: $r = s$) yield at once:

$$(4) \qquad \theta_i = \phi_{i_h}.$$

Now, by step (1) above, we have $\phi_{i_h}, \phi_{i_h}^{(j)} \in [\phi_{i_h}]$. Thus:

$$(5) \qquad \phi_{i_h} \sim_k \phi_{i_h}^{(j)}.$$

Hence, at once by (3), (4) and (5), we have:

$$\theta_i = \phi_{i_h} \sim_k \phi_{i_h}^{(j)} = \phi_{p(i)}.$$

I.e.,

$$\theta_i \sim_k \phi_{p(i)}.$$

As $r = s$ and $p \in S_r$, the previous shows, by definition, that $\tilde{\Phi} \sim_k \Phi$.

4) It remains to show that $\tilde{\Phi}$ is reduced. This is clear, at once, from (2), because we are given $(\phi_{i_1}, \phi_{i_2}, \dots, \phi_{i_u})$ is a set of representatives of $\Phi/\!\sim_k$, and so, in particular, $(\phi_{i_1}, \phi_{i_2}, \dots, \phi_{i_u})$ are pair-wise $\sim_k$ –inequivalent, and then so, by (2), the equivalence classes of $\tilde{\Phi}/\!\sim_k$ are: $(\underbrace{\phi_{i_1}, \dots, \phi_{i_1}}_{m_1}), (\underbrace{\phi_{i_2}, \dots, \phi_{i_2}}_{m_2}), \dots, (\underbrace{\phi_{i_u}, \dots, \phi_{i_u}}_{m_u})$.

$\square$

The theorem below is a sharper version of Theorem 4.B.4 – the main result which exhibits the $k$–rationalizable (over $L$ ) subsets of diagonal matrices. This new theorem shows that "a reduced field setting may always be used", and is perhaps the sharpest version of the above-mentioned main result. This theorem follows fairly easily from Lemma 6.C.1 here, and it will be used towards the end of this chapter.

**Theorem 6.C.2**

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{Y} \subseteq D(n, L)$.

**Then:**

$\mathcal{Y}$ is $k$–rationalizable over $L$ $\Leftrightarrow$

$\mathcal{Y} \subseteq D(n, \overline{k})$ and $\exists \Pi \in \mathrm{Perm}(n, k)$: $\exists \Phi = (\phi_1, \ldots, \phi_r)$, a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$, a field element over $k$:

1) $\dim \Phi = n$;
2) $\mathcal{Y} \subseteq \Pi^{-1} \Delta_\Phi \left( \prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i) \right) \Pi$;
3) $C_L(\mathcal{Y}) = \Pi^{-1} \left[ \mathop{\triangle\kern-0.75em\bigcirc}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})} \right] \Pi$;
4) $\forall (i, j, t) \in \mathcal{I}_\Phi$: $\sigma_j^{(i)}(K_i) = k\left( \{ Z_{(i,j,t)} | Z \in \Pi \mathcal{Y} \Pi^{-1} \} \right)$.

**Proof.**

($\Leftarrow$)

1) This follows immediately, and a fortiori, from Theorem 4.B.4, ($\Leftarrow$).

($\Rightarrow$)

2) Supposing that $\mathcal{Y}$ is $k$–rationalizable over $L$, from Theorem 4.B.4, ($\Rightarrow$), we have immediately:

   a) $\mathcal{Y} \subseteq D(n, \overline{k})$;

   b) $\exists \Psi \in \mathrm{Perm}(n,k)$: $\exists \Lambda = (\lambda_1, \ldots, \lambda_s)$, a field setting over $k$, with $\lambda_i = (L_i, \tau^{(i)}, b_i)$, a field element over $k$:

      i) $\dim \Lambda = n$,

      ii) $\mathcal{Y} \subseteq \Psi^{-1} \Delta_\Lambda \left( \prod\limits_{i=1}^{s} \mathrm{Scalar}(b_i, L_i) \right) \Psi$,

      iii) $C_L(\mathcal{Y}) = \Psi^{-1} \left[ \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{s} M(b_i, L)^{(n_{\lambda_i})} \right] \Psi$.

3) Now, by Lemma 6.C.1, we have:

$$\Phi \sim_k \Lambda,$$

for some *reduced* field setting over $k$, call it $\Phi$. We may let $\Phi = (\phi_1, \ldots, \phi_r)$, with field element $\phi_i = (K_i, \sigma^{(i)}, a_i)$.

4) Now as $\Phi \sim_k \Lambda$, by Lemma 1.D.5, parts (1) and (2,b,iii), we have, in particular, that:

   a) $\dim \Phi = \dim \Lambda$;

   b) $\exists \xi \in \mathrm{Perm}(n,k)$: $\Delta_\Phi \left( \prod\limits_{i=1}^{r} \mathrm{Scalar}(a_i, K_i) \right) = \xi \Delta_\Lambda \left( \prod\limits_{i=1}^{s} \mathrm{Scalar}(b_i, L_i) \right) \xi^{-1}$.

5) By (4,a) and (2,b,i) above, we have $\dim \Phi = n$. This proves the desired conclusion (1). By (4,b) above, we have, trivially:

$$(2)\qquad \Psi^{-1}\Delta_\Lambda\left(\prod_{i=1}^{s}\mathrm{Scalar}(b_i, L_i)\right)\Psi = (\xi\Psi)^{-1}\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)\right)(\xi\Psi).$$

So, letting $\Pi \equiv \xi\Psi$, we see that (2,b,ii) above and (2) give the desired conclusion (2). Finally, using Lemma 2.D.1, part (b,i), twice, together with (2,b,iii) above and (2), we calculate easily:

$$\begin{aligned}
C_L(\mathcal{Y}) &= \Psi^{-1}\left[\mathop{\textcircled{$\scriptstyle\triangle$}}_{i=1}^{s} M(b_i, L)^{(n_{\lambda_i})}\right]\Psi \\
&= C_L\left(\Psi^{-1}\Delta_\Lambda\left(\prod_{i=1}^{s}\mathrm{Scalar}(b_i, L_i)\right)\Psi\right) \\
&= C_L\left(\Pi^{-1}\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)\right)\Pi\right) \\
&= \Pi^{-1}\left[\mathop{\textcircled{$\scriptstyle\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]\Pi.
\end{aligned}$$

This proves the desired conclusion (3). Lastly, the desired conclusion in (4) follows at once from the desired conclusions (2) and (3) (just proved above), by Lemma 4.B.3 (with "$\mathcal{Z}$"$\equiv \Pi\mathcal{Y}\Pi^{-1}$). This completes the proof of the theorem.

□

The following powerful lemma shows that a matrix that normalizes a subset of diagonal matrices may be "replaced" by a single permutation matrix.

**Lemma 6.C.3**

Let $n \in \mathbb{Z}^{+}$.

Let $\mathcal{Y} \subseteq D(n, L)$.

Let $N \in M^{\times}(n, L)$ $[= G\ell(n, L)]$.

**Then:**

$$N^{-1}\mathcal{Y}N = \mathcal{Y} \quad \text{(i.e., } N \text{ normalizes } \mathcal{Y}) \quad \Leftrightarrow$$

$$\exists \Pi \in \mathrm{Perm}(n, k) \colon \exists C \in C_L^{\times}(\mathcal{Y}) \colon \; N = C\Pi \text{ and } \Pi^{-1}\mathcal{Y}\Pi = \mathcal{Y}.$$

**Proof.**

$(\Rightarrow)$

1) This follows, at once and in particular, from Proposition App. 16, of the Appendix.

$(\Leftarrow)$

2) Suppose $N = C\Pi$, $\Pi^{-1}\mathcal{Y}\Pi = \mathcal{Y}$, where $C \in C_L^{\times}(\mathcal{Y})$. Thus:

$$\begin{aligned} N^{-1}\mathcal{Y}N &= \Pi^{-1}C^{-1}\mathcal{Y}C\Pi \\ &= \Pi^{-1}\mathcal{Y}\Pi \qquad [\text{as } C \in C_L^{\times}(\mathcal{Y})] \\ &= \mathcal{Y} \quad [\text{by supposition above}]. \end{aligned}$$

$$\text{Therefore} \quad N^{-1}\mathcal{Y}N = \mathcal{Y}. \qquad \square$$

The following lemma refers to the "3-tuple indexing scheme" of a field setting, of Chapter 1, Section 3, Subsection 7. This lemma is perhaps very particular, and will be used in the proof of Theorem 6.D.1.

**Lemma 6.C.4**

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $\mathcal{Z} \subseteq D(n, L)$, where $C_L(\mathcal{Z}) = \mathop{\bigcirc\kern-0.9em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $(i_1, j_1, t_1), (i_2, j_2, t_2) \in \mathcal{I}_\Phi$ (the "3-tuple indexing scheme" of $\Phi$).

**Then:**

$$[\forall Z \in \mathcal{Z}\colon\ Z_{(i_1,j_1,t_1)} = Z_{(i_2,j_2,t_2)}] \quad \Leftrightarrow \quad i_1 = i_2 \text{ and } j_1 = j_2.$$

**Proof.**

Here, the field setting $\Phi$ is introduced, but only its "dimensions" – $a_i, n_{\phi_i}$ – are really taken for use.

The conclusion follows elementarily, and at once, from these items: given $C_L(\mathcal{Z}) = \mathop{\bigcirc\kern-0.9em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$, together with Proposition App. 10 of the Appendix (on centralizers of diagonal subsets), we immediately determine the set "$T(\mathcal{Z})$" (as in the Appendix there), and then the definition of "$T(\mathcal{Z})$" (as also in the Appendix there), together with the definition of the 3-tuple indexing scheme, $\mathcal{I}_\Phi$, immediately (if not verbatim) gives the desired result.

□

## 6.4 The Critical Theorem on Rationalizable Normalizers of Subsets of Diagonal Matrices

The theorem proved next, and the sole result of this section, is the critical theorem here on rationalizable normalizers of diagonal subsets. The theorem essentially determines the permutation matrices which normalize a diagonal subset. While more is needed for the later, more complete results, this result will be seen to be the critical key (among some other important keys) for our work on normalizers.

The proof of the theorem is long, and fundamentally divides into two logical parts. The first part determines "an equivalent algebraic effect" that the above-mentioned permutation matrices must have on a diagonal subset, and the second part uses this to generate the structure and content of these permutation matrices. The second part is really the heart of the theorem, and shows how the Galois groups of the field elements naturally arise in the body of the normalizers.

The remaining results of this chapter, some of which are major, do require some key non-trivial arguments of their own. At the same time, virtually all of the main results of this chapter are critically founded, for their complete statements, in the sole theorem of this section – Theorem 6.D.1.

**Theorem 6.D.1** [A Key Argument]

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/{\sim_k}| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/{\sim_k}$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/{\sim_k}$, and let $m_h \equiv |[\phi_{i_h}]|$.

Let $\mathcal{Z} \subseteq \Delta_\Phi\left(\Pi_{i=1}^r \mathrm{Scalar}(a_i, K_i)\right)$, where $C_L(\mathcal{Z}) = \mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $\Pi \in \mathrm{Perm}(n, k)$.

**Then:**

$$\Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z} \quad \Rightarrow$$

$$\Pi \in \left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathrm{Perm}(a_i, k)^{(n_{\phi_i})}\right] \cdot \left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} Gal(\phi_{i_h})^{(m_h)} \cdot \mathrm{Perm}(a_{i_h}[K_{i_h}\colon k]m_h, I_{a_{i_h}[K_{i_h}:k]}, k)\right].$$

**Proof.**

1) We suppose that $\Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z}$.

2) The rest of the proof divides itself into two logical parts, with overviews given below, as follows.

**Part I** (Does not use the fact that $\Phi$ is reduced – is valid for any $\Phi$.)

Here, we essentially determine a "complete algebraic effect" that the map $conj_\Pi$ has on the elements of $\mathcal{Z}$. By the given on $\mathcal{Z}$, for $Z \in \mathcal{Z}$, we may write $Z = \Delta_\Phi(\alpha_1 I_{a_1}, \ldots, \alpha_r I_{a_r})$, for some $\alpha_1 \in K_1, \ldots, \alpha_r \in K_r$. With this expression for $Z$, the above-mentioned effect of $conj_\Pi$, on $Z \in \mathcal{Z}$, may be broken down into two parts (the same for all $Z \in \mathcal{Z}$), as follows:

i) firstly, $conj_\Pi$ permutes the "$\alpha_i I_{a_i}$'s" around – and only within indices $i$ corresponding to $k$–equivalent field elements; i.e., "$conj_\Pi$ permutes the '$\alpha_i I_{a_i}$'s ' within the equivalence classes of $\Phi/\!\!\sim_k$".

ii) secondly, and lastly, $conj_\Pi$ replaces each "$\alpha_i I_{a_i}$" with a particular $k$–conjugate of itself (i.e., with "$\tau(\alpha_i) I_{a_i}$", for some particular $\tau \in Iso(K_i/k)$).

This "algebraic effect" is a consequence that is largely due, "merely", to the given on $C_L(\mathcal{Z})$. Although the ideas behind this part of the proof are few and relatively simple, the details in expressing them here seem tedious at times.

**Part II** (Does use the fact that $\Phi$ is reduced – is quite important that $\Phi$ be reduced here.)

Here, we show how the "algebraic effect" developed in Part I lets us determine the specific structure and content of the permutation matrix, $\Pi$. Here, it is very convenient – and important – that $\Phi$ be reduced. We are essentially led to conclude that, up to a centralizing (of $\mathcal{Z}$) permutation matrix, $\Pi$ is a product of two permutation matrices: one, a block-diagonal join of elements of the Galois groups of the field elements of $\Phi$, and the other, a block-diagonal join of "large" permutation matrices, which permute certain of these Galois groups of field elements.

This completely determines the values for $\Pi$.

### Part I

i) We have $\Pi \in \mathrm{Perm}(n,k)$. So $\Pi = \Pi_n(p)$, for some $p \in S_n$ (recall the definition of $\Pi_n$ in Section 1.2.4, Part (d)). Thus, $conj_\Pi$ permutes the diagonal entries of $n \times n$ diagonal matrices, according to $p$:

$$\Pi^{-1}\begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{bmatrix}\Pi = \begin{bmatrix} d_{p(1)} & & \\ & \ddots & \\ & & d_{p(n)} \end{bmatrix}.$$

It will be most useful here to index the diagonal entries of elements of $D(n,L)$ using the "3-tuple indexing scheme of $\Phi$", $\mathcal{I}_\Phi$, as described in Section 1.3.7. We have $\mathcal{I}_\Phi \equiv \cup_{i=1}^{r}\left(\{i\} \times \{1,\ldots,n_{\phi_i}\} \times \{1,\ldots,a_i\}\right) \subseteq \mathbb{Z}^3$; and for $(i,j,t) \in \mathcal{I}_\Phi$, $D \in D(n,L)$, we have $D_{(i,j,t)}$ is "the $(i,j,t)^{th}$–diagonal entry of $D$"; i.e., we have:

$$D \in D(n,L) \Rightarrow D = \mathop{\bigcirc\kern-0.8em\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\kern-0.8em\triangle}\limits_{j=1}^{n_{\phi_i}}\mathop{\bigcirc\kern-0.8em\triangle}\limits_{t=1}^{a_i} D_{(i,j,t)}. \tag{1}$$

Let $conj_\Pi$ act by making the diagonal entry in position $(i,j,t)$ become the diagonal entry that was formerly in position $(f(i,j,t), g(i,j,t), h(i,j,t))$, for some functions $f, g, h$. I.e.,

(2) $$D \in D(n,L) \;\Rightarrow\; \Pi^{-1}D\Pi = \mathop{\textcircled{$\scriptstyle\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\scriptstyle\triangle$}}_{j=1}^{n_{\phi_i}}\mathop{\textcircled{$\scriptstyle\triangle$}}_{t=1}^{a_i} D_{(f(i,j,t),g(i,j,t),h(i,j,t))}.$$

Clearly, the functions $f, g, h$, completely determine the action of $conj_{\Pi}$, and so completely determine $\Pi$ itself. Furthermore, because $conj_{\Pi}$ *permutes* the diagonal entries of diagonal matrices, the map $P$ spelled out below is *bijective*:

(3) $$\begin{aligned} &P\colon \mathcal{I}_{\Phi} \xrightarrow{bij} \mathcal{I}_{\Phi} \\ &P\colon (i,j,t) \mapsto \left(f(i,j,t), g(i,j,t), h(i,j,t)\right). \end{aligned}$$

ii) For $Y \in \Delta_{\Phi}\left(\Pi_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)\right)$, we may clearly write:

$$Y = \Delta_{\Phi}\left(\alpha_1(Y)I_{a_1}, \ldots, \alpha_r(Y)I_{a_r}\right);$$

for some functions $\alpha_i\colon \Delta_{\Phi}\left(\Pi_{i=1}^{r}\ \mathrm{Scalar}\ (a_i, K_i)\right) \to K_i$. (The $\alpha_i$ are unique, and are "projection" functions; but we shall not need this.) With the $\alpha_i$, and the definition of $\Delta_{\Phi}$, we have, with the 3-tuple index notation:

(5)

$$Y \in \Delta_{\Phi}\left(\Pi_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)\right) \;\Rightarrow\; Y_{(i,j,t)} = \sigma_j^{(i)}(\alpha_i(Y)); \text{ for all } (i,j,t) \in \mathcal{I}_{\Phi}.$$

iii) Now let $Z \in \mathcal{Z}$. So $Z \in \Delta_{\Phi}\left(\Pi_{i=1}^{r}\mathrm{Scalar}(a_i, K_i)\right)$, and so by (1) and (5):

$$Z = \mathop{\textcircled{$\scriptstyle\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\scriptstyle\triangle$}}_{j=1}^{n_{\phi_i}}\mathop{\textcircled{$\scriptstyle\triangle$}}_{t=1}^{a_i} \sigma_j^{(i)}(\alpha_i(Z)).$$

Now as $\Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z}$ by original supposition in step (1) above, we thus also have $\Pi^{-1}Z\Pi \in \mathcal{Z}$, and hence the previous equation applies equally well with

"$Z$" $\equiv \Pi^{-1}Z\Pi$. Thus also:

$$(6)\qquad \Pi^{-1}Z\Pi = \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{a_i}\sigma_j^{(i)}\left(\alpha_i(\Pi^{-1}Z\Pi)\right).$$

However, again using the fact that $Z \in \Delta_\Phi\left(\Pi_{i=1}^{r}\text{ Scalar }(a_i, K_i)\right)$ ,by (2) and (5), we then have:

$$(7)\qquad \Pi^{-1}Z\Pi = \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{r}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{j=1}^{n_{\phi_i}}\mathop{\bigcirc\mkern-15mu\triangle}\limits_{t=1}^{a_i}\sigma_{g(i,j,t)}^{(f(i,j,t))}\left(\alpha_{f(i,j,t)}(Z)\right).$$

Hence, comparing (6) and (7), we conclude at once:

$$(8)\qquad \forall Z \in \mathcal{Z}\colon \forall(i,j,t) \in \mathcal{I}_\Phi\colon\ \sigma_{g(i,j,t)}^{(f(i,j,t))}(\alpha_{f(i,j,t)}(Z)) = \sigma_j^{(i)}\left(\alpha_i(\Pi^{-1}Z\Pi)\right).$$

The previous is a key, and fundamental, equation here, from which much will follow.

iv) We now look at (8) to develop several critical invariances. For $i \in \{1,\ldots,r\}$, let $b(i) \in \{1,\ldots,n_{\phi_i}\}$ such that $\sigma_{b(i)}^{(i)} = id_{K_i}$. (This is OK, as $\sigma^{(i)}$ enumerates $Iso(K_i/k)$.) So in (8):

$$\forall Z \in \mathcal{Z}\colon \forall i \in \{1,\ldots,r\}\colon \forall t \in \{1,\ldots,a_i\}\colon$$

$$\sigma_{g(i,b(i),t)}^{(f(i,b(i),t))}\left(\alpha_{f(i,b(i),t)}(Z)\right) = id_{K_i}\left(\alpha_i(\Pi^{-1}Z\Pi)\right) = \alpha_i(\Pi^{-1}Z\Pi).$$

Thus, in particular (letting $t = 1,\ldots,a_i$ in the previous):

$$\forall Z \in \mathcal{Z}\colon \forall i \in \{1,\ldots,r\}\colon$$

$$\sigma_{g(i,b(i),1)}^{(f(i,b(i),1))}\left(\alpha_{f(i,b(i),1)}(Z)\right) = \cdots = \sigma_{g(i,b(i),a_i)}^{(f(i,b(i),a_i))}\left(\alpha_{f(i,b(i),a_i)}(Z)\right).$$

And so, using (5) (with "$i$"$= f(i,b(i),1)$, "$j$" $= g(i,b(i),1)$, "$t$"$= 1$):

$$\forall Z \in \mathcal{Z}: \forall i \in \{1,\ldots,r\}:$$

$$Z_{(f(i,b(i),1),g(i,b(i),1),1)} = \cdots = Z_{(f(i,b(i),a_i),g(i,b(i),a_i),1)}.$$

Now from the given in this Theorem (esp., the given about $C_L(\mathcal{Z})$), we may apply Lemma 6.C.4 to $\mathcal{Z}$. This Lemma, together with the previous result, gives at once:

$$(9) \qquad \forall i \in \{1,\ldots,r\}: \qquad f(i,b(i),1) = \cdots = f(i,b(i),a_i)$$

and

$$g(i,b(i),1) = \cdots = g(i,b(i),a_i).$$

v) The invariance in (9) suggests the following definition – which will soon be seen to be quite useful. For $i \in \{1,\ldots,r\}$, we let:

$$(10) \qquad F(i) \equiv f(i,b(i),1) \text{ and } G(i) \equiv g(i,b(i),1).$$

So, in particular (observing, by (3), that $(F(i),G(i),1) \in \mathcal{I}_\Phi$):

$$(11) \qquad F(i) \in \{1,\ldots,r\} \text{ and } G(i) \in \{1,\ldots,n_{\phi_{F(i)}}\}.$$

The above definitions, together with (9), give at once:

$$\forall i \in \{1,\ldots,r\}: \forall t \in \{1,\ldots,a_i\}: \; F(i) = f(i,b(i),t) \text{ and } G(i) = g(i,b(i),t).$$

This gives, in (3):

$$\forall i \in \{1,\ldots,r\} \colon \forall t \in \{1,\ldots,a_i\} \colon$$

$$P\left((i,b(i),t)\right) = \left(f(i,b(i),t), g(i,b(i),t), h(i,b(i),t)\right) = \left(F(i), G(i), h(i,b(i),t)\right).$$

This will now allow us, in particular, to compare $a_i$ and $a_{F(i)}$. As $P$ maps into $\mathcal{I}_\Phi$, the latter result shows, in particular:

$$h(i,b(i),t) \in \{1,\ldots,a_{F(i)}\}.$$

Now fix $i \in \{1,\ldots,r\}$. The previous two results give, in particular:

$$P\left(\{i\} \times \{b(i)\} \times \{1,\ldots,a_i\}\right) \subseteq \{F(i)\} \times \{G(i)\} \times \{1,\ldots,a_{F(i)}\}.$$

Now since $P$ is *bijective* by (3), taking cardinalities in the previous containment gives at once:

$$a_i \leq a_{F(i)}. \tag{12}$$

vi) The definitions of $F(i)$ and $G(i)$, together with (8), also give the following:

$$\forall Z \in \mathcal{Z} \colon \forall i \in \{1,\ldots,r\} \colon$$

$$\sigma^{(F(i))}_{G(i)}\left(\alpha_{F(i)}(Z)\right) = \sigma^{(i)}_{b(i)}\left(\alpha_i(\Pi^{-1}Z\Pi)\right) =$$

$$id_{K_i}\left(\alpha_i(\Pi^{-1}Z\Pi)\right) = \alpha_i\left(\Pi^{-1}Z\Pi\right).$$

Thus:

$$\forall Z \in \mathcal{Z} \colon \forall i \in \{1,\ldots,r\} \colon\ \sigma^{(F(i))}_{G(i)}\left(\alpha_{F(i)}(Z)\right) = \alpha_i(\Pi^{-1}Z\Pi). \tag{13}$$

This is a key consequence of (8), and a very important fact. Among other things, (13) will now allow us to compare the fields $K_i$ and $K_{F(i)}$. Using (5) in (13) (and observing that $\alpha_i(\Pi^{-1}Z\Pi) = \sigma^{(i)}_{b(i)}(\alpha_i(\Pi^{-1}Z\Pi))$; and letting "$Y$"$\equiv Z, \Pi^{-1}Z\Pi$; and using "$t$"$\equiv 1$), we have:

$$\forall Z \in \mathcal{Z}: \forall i \in \{1,\ldots,r\}:\ Z_{(F(i),G(i),1)} = (\Pi^{-1}Z\Pi)_{(i,b(i),1)}.$$

Thus, in particular:

$$\begin{aligned} &\forall i \in \{1,\ldots,r\}: \\ &k\left(\{Z_{(F(i),G(i),1)} | Z \in \mathcal{Z}\}\right) = k\left(\{(\Pi^{-1}Z\Pi)_{(i,b(i),1)} | Z \in \mathcal{Z}\}\right) \\ = \ &k\left(\{Z_{(i,b(i),1)} | Z \in \mathcal{Z}\}\right) \text{ [as by supposition here: } \Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z}]. \end{aligned}$$

Hence:

$$\forall i \in \{1,\ldots,r\}:\ k\left(\{Z_{(F(i),G(i),1)} | Z \in \mathcal{Z}\}\right) = k\left(\{Z_{(i,b(i),1)} | Z \in \mathcal{Z}\}\right).$$

Now from the given in this Theorem, we may apply Lemma 4.B.3 to $\mathcal{Z}$. This lemma, together with the previous result, gives at once:

$$\forall i \in \{1,\ldots,r\}:\ \sigma^{(F(i))}_{G(i)}(K_{F(i)}) = \sigma^{(i)}_{b(i)}(K_i) = id_{K_i}(K_i) = K_i.$$

Thus:

$$\text{(14)} \qquad \forall i \in \{1,\ldots,r\}:\ \sigma^{(F(i))}_{G(i)}(K_{F(i)}) = K_i.$$

And so also, in particular:

$$\text{(15)} \qquad \forall i \in \{1,\ldots,r\}:\ K_i \sim_k K_{F(i)} \text{ and } n_{\phi_i} = n_{\phi_{F(i)}}.$$

vii) We now show that the function $F$, defined in (10) and (11), is bijective. Let $i_1, i_2 \in \{1, \ldots, r\}$ and suppose that $F(i_1) = F(i_2)$. So, trivally:

$$\forall Z \in \mathcal{Z}\colon\ Z_{(F(i_1),G(i_1),1)} = Z_{(F(i_2),G(i_1),1)}.$$

Thus, by (5):

$$\forall Z \in \mathcal{Z}\ :\sigma_{G(i_1)}^{(F(i_1))}\left(\alpha_{F(i_1)}(Z)\right) = \sigma_{G(i_1)}^{(F(i_2))}\left(\alpha_{F(i_2)}(Z)\right).$$

And hence, by (13):

$$(16) \qquad \forall Z \in \mathcal{Z}\colon\ \sigma_{i_1}(\Pi^{-1}Z\Pi) = \sigma_{G(i_1)}^{(F(i_2))}\left(\sigma_{G(i_2)}^{(F(i_2))}\right)^{-1}\left(\alpha_{i_2}(\Pi^{-1}Z\Pi)\right).$$

Now let $\eta \equiv \sigma_{G(i_1)}^{(F(i_2))} \circ \left(\sigma_{G(i_2)}^{(F(i_2))}\right)^{-1}$. So, by (14), together with the supposition here that $F(i_1) = F(i_2)$, we have the diagram:

$$\begin{tikzcd} K_{i_2} \arrow[r, "\left(\sigma_{G(i_2)}^{(F(i_2))}\right)^{-1}", "iso"'] & K_{F(i_2)} = K_{F(i_1)} \arrow[r, "\sigma_{G(i_1)}^{(F(i_1))}", "iso"'] & K_{i_1}. \end{tikzcd}$$

Thus, $\eta\colon K_{i_2} \xrightarrow{iso} K_{i_1}$. In particular, then, $\eta \in Iso(K_{i_2}/k)$, and so $\eta = \sigma_J^{(i_2)}$, for some $J \in \{1, \ldots, n_{\phi_{i_2}}\}$. Thus, we may rewrite (16) as:

$$\forall Z \in \mathcal{Z}\colon\ \alpha_{i_1}(\Pi^{-1}Z\Pi) = \sigma_J^{(i_2)}\left(\alpha_{i_2}(\Pi^{-1}Z\Pi)\right).$$

Hence, as by supposition here $\Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z}$, the previous shows:

$$\forall Z \in \mathcal{Z}\colon\ \alpha_{i_1}(Z) = \sigma_J^{(i_2)}\left(\alpha_{i_2}(Z)\right).$$

As $\sigma_{b(i_1)}^{(i_1)} = id_{K_{i_1}}$, we now have:

$$\forall Z \in \mathcal{Z}\colon \sigma_{b(i_1)}^{(i_1)}\left(\alpha_{i_1}(Z)\right) = \sigma_J^{(i_2)}\left(\alpha_{i_2}(Z)\right).$$

So, by (5), we have:

$$\forall Z \in \mathcal{Z}\colon\ Z_{(i_1,b(i_1),1)} = Z_{(i_2,J,1)}.$$

As before, applying Lemma 6.C.4 to $\mathcal{Z}$, in the previous, we get at once:

$$i_1 = i_2 \text{ and } b(i_1) = J.$$

So, in particular:

$$i_1 = i_2.$$

Thus:

$$F \text{ is injective.}$$

Now as $F\colon \{1,\dots,r\} \to \{1,\dots,r\}$ by (10) and (11), the previous result gives at once that $F$ is bijective; and so, in fact, $F \in S_r$. Thus:

$$F \in S_r. \tag{17}$$

This fact forms a principal part of the conclusion we will soon state as the result of this Part I, and will be a key part in the work of Part II.

viii) Among other things, (17) will now allow us to compare $a_i$ and $a_{F(i)}$ better. Using (17) and (15) we can strengthen (12), as follows:

$$\begin{aligned}\textstyle\sum_{i=1}^r a_i n_{\phi_i} &= \textstyle\sum_{i=1}^r a_{F(i)} n_{\phi_{F(i)}} [\text{by } (17)]\\ &= \textstyle\sum_{i=1}^r a_{F(i)} n_{\phi_i} [\text{by } (15)].\end{aligned}$$

So, subtracting, we get:

$$\sum_{i=1}^r (a_i - a_{F(i)}) n_{\phi_i} = 0.$$

Now certainly $n_{\phi_i} \in \mathbb{Z}^+$, and by (12) we see $a_i - a_{F(i)} \leq 0$. Thus, the previous equation above gives at once:

$$a_i - a_{F(i)} = 0, \text{ for all } i \in \{1, \ldots, r\}.$$

Thus:

$$\forall i \in \{1, \ldots, r\}\colon\ a_i = a_{F(i)}. \tag{18}$$

This last key fact allows us to form a main conclusion here, and then to complete Part I.

ix) By (15) and (18), we have immediately:

$$\forall i \in \{1, \ldots, r\}\colon\ K_i \sim_k K_{F(i)} \text{ and } a_i = a_{F(i)}.$$

Thus, by definition:

$$\forall i \in \{1, \ldots, r\}\colon\ \phi_i \sim_k \phi_{F(i)}. \tag{19}$$

Thus, $F \in S_r$ "permutes" $(\phi_1, \ldots, \phi_r)$, and within the equivalence classes of $\Phi/\!\sim_k$ only. I.e., each $E \in \Phi/\!\sim_k$ is "invariant" under $F$.

x) Before stating our complete conclusion for Part I, we use (14) more fully, and define an important quantity. By (14), we have:

$$\forall i \in \{1, \ldots, r\}\colon\ \sigma^{(F(i))}_{G(i)}\colon K_{F(i)} \xrightarrow{iso} K_i.$$

As $F \in S_r$, we may let "$i$"$\equiv F^{-1}(i)$ in the previous result, and this gives:

$$\forall i \in \{1, \ldots, r\}\colon\ \sigma^{(i)}_{G(F^{-1}(i))}\colon K_i \xrightarrow{iso} K_{F^{-1}(i)}. \tag{20}$$

With this, we make the following definition:

(20′) $$\text{for } i \in \{1,\ldots,r\}, \text{ we let: } \gamma_i \equiv \sigma^{(i)}_{G(F^{-1}(i))}.$$

As $\sigma^{(i)}$ enumerates $Iso(K_i/k)$, we note from this definition that $\gamma_i \in Iso(K_i/k)$.

With this note, and (20) and (20′), we summarize:

(21) $$\forall i \in \{1,\ldots,r\}\colon \gamma_i \in Iso(K_i/k), \gamma_i = \sigma^{(i)}_{G(F^{-1}(i))}, \gamma_i\colon K_i \xrightarrow{iso} K_{F^{-1}(i)}.$$

Letting "$i$"$\equiv F(i)$ in (21), we find:

(21′) $$\begin{aligned} \forall i \in \{1,\ldots,r\}\colon\ & \gamma_{F(i)} \in Iso(K_{F(i)}/k), \\ & \gamma_{F(i)} = \sigma^{(F(i))}_{G(i)}, \\ & \gamma_{F(i)}\colon K_{F(i)} \xrightarrow{iso} K_i. \end{aligned}$$

With the above, we now combine several results to form a main conclusion.

Letting $Z \in \mathcal{Z}$, we now observe:

$$\Pi^{-1}Z\Pi = \Delta_\Phi\Big(\alpha_1(\Pi^{-1}Z\Pi)I_{a_1}, \dots, \alpha_r(\Pi^{-1}Z\Pi)I_{a_r}\Big)$$

[as $\Pi^{-1}Z\Pi \in \mathcal{Z}$, and then using (4) with "$Y$" $\equiv \Pi^{-1}Z\Pi$]

$$= \Delta_\Phi\Big(\sigma_{G(1)}^{(F(1))}\left(\alpha_{F(1)}(Z)\right) I_{a_1}, \dots, \sigma_{G(r)}^{(F(r))}\left(\alpha_{F(r)}(Z)\right) I_{a_r}\Big)$$

[by (13)]

$$= \Delta_\Phi\Big(\sigma_{G(1)}^{(F(1))}\left(\alpha_{F(1)}(Z)\right) I_{aF(1)}, \dots, \sigma_{G(r)}^{(F(r))}\left(\alpha_{F(r)}(Z)\right) I_{aF(r)}\Big)$$

[by (18)]

$$= \Delta_\Phi\Big(\gamma_{F(1)}\left(\alpha_{F(1)}(Z)\right) I_{aF(1)}, \dots, \gamma_{F(r)}\left(\alpha_{F(r)}(Z)\right) I_{aF(r)}\Big)$$

[by (21′)].

Therefore:

(22)

$$\forall Z \in \mathcal{Z}\colon\ \Pi^{-1}Z\Pi = \Delta_\Phi\left(\gamma_{F(1)}\left(\alpha_{F(1)}(Z)\right) I_{aF(1)}, \dots, \gamma_{F(r)}\left(\alpha_{F(r)}(Z)\right) I_{a_{F(r)}}\right).$$

This important conclusion essentially finishes our work in Part I; we now state our complete conclusions for Part I below. We have shown, from (17),(21), (22), and (19), that:

(23)

$$\exists F \in S_r\colon \forall i \in \{1,\ldots,r\}\colon \exists \gamma_i \in Iso(K_i/k), \gamma_i\colon K_i \xrightarrow{iso} K_{F^{-1}(i)}\colon$$

a)$\forall Z \in \mathcal{Z}$:

$$\Pi^{-1} Z \Pi = \Delta_\Phi\Big(\gamma_{F(1)}\big(\alpha_{F(1)}(Z)\big)\, I_{a_{F(1)}}, \ldots, \gamma_{F(r)}\big(\alpha_{F(r)}(Z)\big)\, I_{a_{F(r)}}\Big);$$

b) $\forall i \in \{1,\ldots,r\}$: $\phi_{F(i)} \sim_k \phi_i$.

(I.e., $F$ "permutes" the field elements of $\Phi$ only *within* the equivalence classes of $\Phi/\!\sim_k$). The above result forms an "equivalent algebraic effect" for the action of $conj_\Pi$ on the elements of $\mathcal{Z}$. This completes "Part I". (Note that *all of the results of Part I above are valid for arbitrary* $\Phi$ *– reduced or not.* This is because we never referred to this particular property of $\Phi$ in all of Part I.)

## Part II

We now use the results of Part I – esp, the effect of $conj_\Pi$ on the elements of $\mathcal{Z}$, as in (23) – to generate the structure and content of the permutation matrix, $\Pi$. *Here, we will make use of the fact that* $\Phi$ *is reduced.*

xi) Now, immediately making use of the fact that $\Phi$ is reduced (in particular, the fact that all field elements in any equivalence class of $\Phi/\!\sim_k$ are identical) – we have at once, by (19), that:

(24) $$\forall i \in \{1,\ldots,r\}\colon\ \phi_{F(i)} = \phi_i.$$

Thus, in particular, we have:

$$(24') \qquad \forall i \in \{1, \ldots, r\}\colon\ K_{F(i)} = K_i.$$

Letting "$i$"$\equiv F^{-1}(i)$ in the previous, we have now:

$$\forall i \in \{1, \ldots, r\}\colon\ K_i = K_{F^{-1}(i)}.$$

This, with (21), gives:

$$\gamma_i \in Iso(K_i/k) \text{ and } \gamma_i\colon K_i \xrightarrow{iso} K_i.$$

Thus, at once, $\gamma_i \in Ga\ell(K_i/k)$. Hence:

$$(24'') \qquad \forall i \in \{1, \ldots, r\}\colon\ \gamma_i \in Ga\ell(K_i/k).$$

xi′) We introduce some notation that will simplify conclusion (23,a). For $i \in \{1, \ldots r\}$, and $Z \in \mathcal{Z}$, we let:

$$(25) \qquad S_i(Z) \equiv \gamma_i(\alpha_i(Z)) I_{a_i} \in \text{ Scalar } (a_i, K_i).$$

(Note that, as $\alpha_i(Z) \in K_i$ by construction of $\alpha_i$, and, as $\gamma_i \in Ga\ell(K_i/k)$ by (24′′), so $\gamma_i(\alpha_i(Z)) \in K_i$, and so, in fact, $S_i(Z) \in$ Scalar $(a_i, K_i)$.) With this, we have from (23,a) that:

$$\begin{aligned}
Z \in \mathcal{Z} \ &\Rightarrow \Pi^{-1} Z \Pi = \Delta_\Phi \left(\gamma_{F(1)}\left(\alpha_{F(1)}(Z)\right) I_{a_{F(1)}}, \ldots, \gamma_{F(r)}\left(\alpha_{F(r)}(Z)\right) I_{a_{F(r)}}\right) \\
&= \Delta_\Phi \left(S_{F(1)}(Z), \ldots, S_{F(r)}(Z)\right) \text{ [by (25)]} \\
&= \mathop{\textcircled{$\Delta$}}_{i=1}^{r} \Delta_{\phi_i} \left(S_{F(i)}(Z)\right) \text{ [by def. } \Delta_\Phi\text{]} \\
&= \mathop{\textcircled{$\Delta$}}_{i=1}^{r} \Delta_{\phi_{F(i)}} \left(S_{F(i)}(Z)\right) \text{ [by (24) ].}
\end{aligned}$$

Therefore:

$$(25') \qquad \forall Z \in \mathcal{Z}\colon\ \Pi^{-1}Z\Pi = \mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{r} \Delta_{\phi_{F(i)}}\left(S_{F(i)}(Z)\right).$$

xii) Now we are given that $\Phi$ is a *reduced* field setting, and we have the quantities $u, (\phi_{i_1}, \ldots, \phi_{i_u}), [\phi_{i_h}], m_h$ as defined in the given of this theorem. Thus, at once, by Lemma 6.B.3, part (1,b), we have [and letting the subsequences $E_1, E_2, \ldots, E_u$ be defined as in the following]:

$$(26) \qquad (\phi_1, \ldots, \phi_r) = \left(\underbrace{\phi_1, \ldots, \phi_{m_1}}_{E_1}, \underbrace{\phi_{m_1+1}, \ldots, \phi_{m_1+m_2}}_{E_2}, \cdots\cdots, \underbrace{\phi_{m_1+m_2+\ldots+m_{u-1}+1}, \cdots, \phi_{m_1+m_2+\cdots+m_u}}_{E_u}\right).$$

Furthermore, by part (1,c) of that same Lemma, we have:

$$(27) \qquad \Phi/{\sim_k} = \left(\underbrace{(\phi_1, \ldots, \phi_{m_1})}_{E_1}, \underbrace{\phi_{m_1+1}, \ldots, \phi_{m_1+m_2}}_{E_2}, \cdots\cdots, \underbrace{(\phi_{m_1+m_2+\ldots+m_{u-1}+1}, \cdots, \phi_{m_1+m_2+\cdots+m_u})}_{E_u}\right);$$

$$(28) \qquad \text{and } E_h = \underbrace{(\phi_{i_h}, \ldots, \phi_{i_h})}_{m_h}.$$

It will be convenient to re-express the subsequences, $E_h$, defined in (26), by a double-index notation. As, by (26), we clearly note that $|E_h| = m_h$, we will let:

$$(29) \qquad E_h = (\phi_1^{(h)}, \ldots, \phi_{m_h}^{(h)}).$$

(So, also then $(\phi_1^{(h)}, \ldots, \phi_{m_h}^{(h)}) = (\phi_{m_1+\ldots+m_{h-1}+1}, \ldots, \phi_{m_1+\ldots+m_h})\ \underbrace{(\phi_{i_h}, \ldots, \phi_{i_h})}_{m_h}$.)

Substituting (29) into (26), and with (27), we have:

$$(30)\qquad (\phi_1, \ldots, \phi_r) = \left( \underbrace{\phi_1^{(1)}, \ldots, \phi_{m_1}^{(1)}}_{E_1}, \underbrace{\phi_1^{(2)}, \ldots, \phi_{m_2}^{(2)}}_{E_2}, \ldots\ldots, \underbrace{\phi_1^{(u)}, \ldots, \phi_{m_u}^{(u)}}_{E_u} \right);$$

(31) and the equivalence classes of $\Phi/\!\!\sim_k$ are : $E_1, E_2, \ldots, E_u$.

Now, by (17) and (19), the sequence, $(\phi_{F(1)}, \ldots, \phi_{F(r)})$, is the sequence, $(\phi_1, \ldots, \phi_r)$, where the field elements, $\phi_i$, have been permuted *within* the equivalence classes of $\Phi/\!\!\sim_k$ – i.e., by (31), within the $E_1, E_2, \ldots, E_u$. I.e., from (30), we have:

(32)

$$(\phi_{F(1)}, \ldots, \phi_{F(r)}) =$$

$$\left(\phi^{(1)}_{p^{(1)}(1)}, \ldots, \phi^{(1)}_{p^{(1)}(m_1)}, \phi^{(2)}_{p^{(2)}(1)}, \ldots, \phi^{(2)}_{p^{(2)}(m_2)}, \ldots\ldots, \phi^{(u)}_{p^{(u)}(1)}, \ldots, \phi^{(u)}_{p^{(u)}(m_u)}\right);$$

for some permutations $p^{(1)} \in S_{m_1}, p^{(2)} \in S_{m_2}, \ldots, p^{(u)} \in S_{m_u}$.

xiii) Now let $M_1 \in M(a_1, K_1), \ldots, M_r \in M(a_r, K_r)$. Apply the same double-indexing to $M_1, \ldots, M_r$, as in (30), and write:

(33)

$$(M_1, \ldots, M_r) = \left(M_1^{(1)}, \ldots, M_{m_1}^{(1)}, M_1^{(2)}, \ldots, M_{m_2}^{(2)}, \ldots\ldots, M_1^{(u)}, \ldots, M_{m_u}^{(u)}\right).$$

Now given the way that $F$ permutes the indices $\{1, \ldots, r\}$ – as represented in

(32) with the double-index notation, we have, clearly, with (33), that:

(34)

$$(M_{F(1)}, \ldots, M_{F(r)}) =$$

$$\left(M^{(1)}_{p^{(1)}(1)}, \ldots, M^{(1)}_{p^{(1)}(m_1)}, M^{(2)}_{p^{(2)}(1)}, \ldots, M^{(2)}_{p^{(2)}(m_2)}, \ldots\ldots, M^{(u)}_{p^{(u)}(1)}, \ldots, M^{(u)}_{p^{(u)}(m_u)}\right).$$

So, clearly, using (32) and (34):

$$\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \Delta_{\phi_{F(i)}}(M_{F(i)}) = \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathop{\textcircled{$\triangle$}}_{j=1}^{m_h} \Delta_{\phi^{(h)}_{p^{(h)}(j)}}(M^{(h)}_{p^{(h)}(j)}). \tag{35}$$

xiv) We now note the following. By (29) and (28):

$$E_h = (\phi^{(h)}_1, \ldots, \phi^{(h)}_{m_h}) = \underbrace{(\phi_{i_h}, \ldots, \phi_{i_h})}_{m_h}.$$

Thus:

$$\forall \phi^{(h)}_j \in E_h\colon \quad \phi^{(h)}_j = \phi_{i_h}.$$

So, in particular:

$$\forall \phi^{(h)}_j \in E_h\colon \quad \dim \phi^{(h)}_j = \dim \phi_{i_h}.$$

And so:

$$\Delta_{\phi^{(h)}_{p^{(h)}(j)}}(M^{(h)}_{p^{(h)}(j)}) \in M(\dim \phi^{(h)}_{p^{(h)}(j)}, L) = M(\dim \phi_{i_h}, L); \tag{36}$$

$$\mathop{\textcircled{$\triangle$}}_{j=1}^{m_h} \Delta_{\phi^{(h)}_{p^{(h)}(j)}}(M^{(h)}_{p^{(h)}(j)}) \in \mathop{\textcircled{$\triangle$}}_{j=1}^{m_h} M(\dim \phi_{i_h}, L) = M(\dim \phi_{i_h}, L)^{(m_h)}.$$

xv) Now recall from (32) that $p^{(h)} \in S_{m_h}$. This, with (36), and the facts inSection 1.2.4, Part (d) on block permutation matrices, shows:

$$\mathop{\textcircled{$\triangle$}}_{j=1}^{m_h} \Delta_{\phi^{(h)}_{p^{(h)}(j)}}(M^{(h)}_{p^{(h)}(j)}) = (\Psi^{(h)})^{-1} \left[\mathop{\textcircled{$\triangle$}}_{j=1}^{m_h} \Delta_{\phi^{(h)}_j}(M^{(h)}_j)\right] \Psi^{(h)}; \tag{37}$$

where $\Psi^{(h)}$ is the $(\dim \phi_{i_h} \times \dim \phi_{i_h})$-block permutation matrix:

(38) $$\Psi^{(h)} \equiv \widehat{\Pi}_{m_h}(p^{(h)}, I_{dim\phi_{i_h}}) \in \text{Perm }(m_h \text{dim } \phi_{i_h}, I_{dim\phi_{i_h}}, k).$$

xvi) Continuing now from (35), with (37) and (38), we have:

$$\begin{aligned}
\mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \Delta_{\phi_{F(i)}}(M_{F(i)}) &= \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \mathop{\triangle\!\!\!\!\bigcirc}\limits_{j=1}^{m_h} \Delta_{\phi^{(h)}_{p^{(h)}(j)}} (M^{(h)}_{p^{(h)}(j)}) \\
&= \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \left[ (\Psi^{(h)})^{-1} \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{j=1}^{m_h} \Delta_{\phi^{(h)}_j}(M^{(h)}_j) \right] \Psi^{(h)} \right] \\
&= \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \Psi^{(h)} \right]^{-1} \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \mathop{\triangle\!\!\!\!\bigcirc}\limits_{j=1}^{m_h} \Delta_{\phi^{(h)}_j}(M^{(h)}_j) \right] \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \Psi^{(h)} \right] \\
&= \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \Psi^{(h)} \right]^{-1} \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \Delta_{\phi_i}(M_i) \right] \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \Psi^{(h)} \right] \quad \text{[by (30) and (33)]} \\
&= \Psi^{-1} \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \Delta_{\phi_i}(M_i) \right] \Psi;
\end{aligned}$$

where $\Psi \equiv \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \Psi^{(h)} \in \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \text{Perm}(m_h \text{dim}\, \phi_{i_h}, I_{\dim \phi_{i_h}}, k)$. We summarize these conclusions below.

(39)

i) $\Psi \equiv \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \Psi^{(h)} \equiv \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \widehat{\Pi}_{m_h}(p^{(h)}, I_{\dim \phi_{i_h}}) \in \mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \text{Perm}(m_h \text{dim}\, \phi_{i_h}, I_{\dim \phi_{i_h}}, k)$;

ii) $\forall M_1 \in M(a_1, K_1), \ldots, M_r \in M(a_r, K_r)$:

$$\mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \Delta_{\phi_{F(i)}}(M_{F(i)}) = \Psi^{-1} \left[ \mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \Delta_{\phi_i}(M_i) \right] \Psi.$$

xvii) Combining (25′) and (39,ii) (with "$M_i$"$\equiv S_i(Z)$), and, in the last step, using Lemma 1.D.3, part (c) (recalling the definition of $\Gamma_{\overline{\gamma},\Phi}$ in Section 1.3.6), we have at once:

(40)

$$
\begin{aligned}
\forall Z \in \mathcal{Z}\colon\quad \Pi^{-1} Z \Pi &= \mathop{\text{\textcircled{$\scriptstyle\triangle$}}}_{i=1}^{r} \Delta_{\phi_{F(i)}}\Big(S_{F(i)}(Z)\Big) \\
&= \Psi^{-1}\left[\mathop{\text{\textcircled{$\scriptstyle\triangle$}}}_{i=1}^{r} \Delta_{\phi_i}\Big(S_i(Z)\Big)\right]\Psi \\
&= \Psi^{-1}\Delta_{\Phi}\Big(S_1(Z),\ldots,S_r(Z)\Big)\Psi \qquad \text{[by definition } \Delta_{\Phi}] \\
&= \Psi^{-1}\Delta_{\Phi}\Big(\gamma_1(\alpha_1(Z))I_{a_1},\ldots,\gamma_r(\alpha_r(Z))I_{a_r}\Big)\Psi \\
&\qquad\qquad\qquad\qquad \text{[by definition } S_i(Z) \text{ in (25)]} \\
&= \Psi^{-1}\Gamma^{-1}_{\overrightarrow{\gamma^{-1}},\Phi}\,\Delta_{\Phi}\Big(\alpha_1(Z)I_{a_1},\ldots,\alpha_r(Z)I_{a_r}\Big)\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi,
\end{aligned}
$$

where $\overrightarrow{\gamma^{-1}} \equiv (\gamma_1^{-1},\ldots,\gamma_r^{-1})$. Thus, continuing, we have:

$$
\begin{aligned}
\forall Z \in \mathcal{Z}\colon\quad \Pi^{-1} Z \Pi &= \Psi^{-1}\Gamma^{-1}_{\overrightarrow{\gamma^{-1}},\Phi}\,\Delta_{\Phi}\Big(\alpha_1(Z)I_{a_1},\ldots,\alpha_r(Z)I_{a_r}\Big)\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi \\
&= \left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right)^{-1}\Delta_{\Phi}\Big(\alpha_1(Z)I_{a_1},\ldots,\alpha_r(Z)I_{a_r}\Big)\left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right) \\
&= \left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right)^{-1} Z \left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right) \qquad \text{[by (4)].}
\end{aligned}
$$

So, we have now:

$$
\forall Z \in \mathcal{Z}\colon\quad \Pi^{-1} Z \Pi = \left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right)^{-1} Z \left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right).
$$

Thus, at once:

$$
\Pi\left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right)^{-1} \in C_L(\mathcal{Z}).
$$

So, by the given on $C_L(\mathcal{Z})$:

$$
(41) \qquad \Pi\left(\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\,\Psi\right)^{-1} = C, \quad \text{for some } C \in \mathop{\text{\textcircled{$\scriptstyle\triangle$}}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.
$$

Now as $\Pi, \Gamma_{\overrightarrow{\gamma^{-1}}}$, and $\Psi$ are permutation matrices, $C$ above must also be a permutation matrix. This, with (41), gives clearly:

$$C \in \left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] \cap \mathrm{Perm}(n,k) = \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}.$$

Thus:

$$C \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}.$$

Using this in (41) gives:

$$\Pi = C\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}\Psi, \quad \text{and } C \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}. \tag{42}$$

xviii) Now recalling the definition of $\Gamma_{\overrightarrow{\gamma^{-1}},\Phi}$ here from (40) and fromSection 1.3.6, and recalling the definition of the Galois group of a field element from Section 1.4.3, we have:

$$\begin{aligned} \Gamma_{\overrightarrow{\gamma^{-1}},\Phi} &\equiv \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \Gamma_{\gamma_i^{-1},\phi_i} \\ &\in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \{\Gamma_{\gamma,\phi_i} \in \mathrm{Perm}(a_i n_{\phi_i}, I_{a_i}, k) \mid \gamma \in \mathit{Ga\ell}(K_i/k)\} \\ &= \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathit{Ga\ell}(\phi_i). \end{aligned}$$

Thus:

$$\Gamma_{\overrightarrow{\gamma^{-1}},\Phi} \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathit{Ga\ell}(\phi_i). \tag{43}$$

Now, at once, by Lemma 6.B.3, part (2,a) [with "*f*"$\equiv$ *Gaℓ*], we have:

$$\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \mathit{Ga\ell}(\phi_i) = \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathit{Ga\ell}(\phi_{i_h})^{(m_h)}. \tag{44}$$

Thus, by (43) and (44), we have:

$$\Gamma_{\overrightarrow{\gamma^{-1}},\Phi} \in \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathit{Ga\ell}(\phi_{i_h})^{(m_h)}. \tag{45}$$

xix) Finally, by (42), with (45), and the first part of (39), we have at once:

$$\begin{aligned}\Pi &= C\Gamma^{\Psi}_{\overrightarrow{\gamma^{-1}},\Phi} \\ &\in \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\mathrm{Perm}(a_i,k)^{(n_{\phi_i})}\right]\cdot\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u}\mathit{Ga}\ell(\phi_{i_h})^{(m_h)}\right]\cdot\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u}\mathrm{Perm}(m_h\mathrm{dim}\,\phi_{i_h},I_{\mathrm{dim}\,\phi_{i_h}},k)\right] \\ &= \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\mathrm{Perm}(a_i,k)^{(n_{\phi_i})}\right]\cdot\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u}\mathit{Ga}\ell(\phi_{i_h})^{(m_h)}\mathrm{Perm}(m_h\mathrm{dim}\,\phi_{i_h},I_{\mathrm{dim}\,\phi_{i_h}},k)\right].\end{aligned}$$

Hence, substituting $\dim\phi_{i_h} = a_{i_h}[K_{i_h}\colon k]$ [as given that $\phi_i = (K_i,\sigma^{(i)},a_i)$], we conclude:

$$\Pi \in \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r}\mathrm{Perm}(a_i,k)^{(n_{\phi_i})}\right]\cdot\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u}\mathit{Ga}\ell(\phi_{i_h})^{(m_h)}\mathrm{Perm}(a_{i_h}[K_{i_h}\colon k]m_h, I_{a_{i_h}[K_{i_h}:k]},k)\right].$$

This completes "Part II"; and the proof of the theorem!!

□

# 6.5 Main Results

## 6.5.1 Introduction

In this section, we obtain the main results about the rationalizable normalizers of subsets of rationalizable diagonal matrices. There are five lemmas to be shown here; only the last one makes use of the key Theorem 6.D.1. The first two lemmas show structural and group-theoretic properties of some of the subsets of matrices connected with a reduced field setting, these lemmas do not study rationalizability questions. The third lemma shows a main commutativity result, and contains a key argument. The last two lemmas show main rationalizability results, and both contain key arguments.

### 6.5.2 Main Lemmas

The previous theorem shows some of the importance of the Galois groups and permutation groups connected with a reduced field setting. The following lemma exhibits some basic and technical properties of some of these and other "objects" connected with a reduced field setting.

**Lemma 6.E.1**

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \dots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/\sim_k| \in \{1, \dots, r\}$, let the subsequence $(\phi_{i_1}, \dots, \phi_{i_u}) \subseteq (\phi_1, \dots, \phi_r)$ be a set of representatives of $\Phi/\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\sim_k$, and let $m_h \equiv \left|[\phi_{i_h}]\right|, n_h \equiv n_{\phi_{i_h}} = [K_{i_h} \colon k]$.

Additionally, let $G_h \equiv \mathcal{Gal}(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

**Then:**

1) a) $\mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})} = \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} M(a_{i_h}, L)^{(n_h m_h)}$;

b) $\left[\mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} M(a_{i_h}, L)^{(n_h m_h)}\right] \cap \left[\mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)\right] = \{I_n\}$;

c) $C, C' \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} M^{\times}(a_i, L)^{(n_{\phi_i})}$; $\Pi, \Pi' \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k) \Rightarrow$

$[C\Pi = C'\Pi' \Leftrightarrow C = C' \text{ and } \Pi = \Pi']$.

2) a) $\left[\mathrm{Perm}(a_{i_h} n_h, I_{a_{i_h}}, k)^{(m_h)}\right] \cdot \left[\mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)\right] \subseteq$

$\mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)$;

b) $\mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \subseteq \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)$;

c) $\Pi \in \mathrm{Perm}(n, k)$, $\Pi' \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{i=1}^{r} \mathrm{Perm}(a_i, k)^{(n_{\phi_i})}$, $\tilde{\Pi} \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \Rightarrow$

$[\Pi = \Pi'\tilde{\Pi} \Rightarrow$ this representation of $\Pi$, as $\Pi' \cdot \tilde{\Pi}$, is unique];

d) $\Pi \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)$, $\Pi'$ and $\tilde{\Pi}$ as in (c) previously $\Rightarrow$

$[\Pi = \Pi'\tilde{\Pi} \Rightarrow \Pi = \tilde{\Pi}$, and so, in particular, $\Pi \in \mathop{\bigcirc\kern-0.78em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h]$.

**Proof.**

1) a) This follows at once from Lemma 6.B.3, part (2,a), by letting $f(\phi_i) \equiv M(a_{\phi_i}, L)^{(n_{\phi_i})}$, noting that $a_{\phi_i} = a_i$ here, and observing easily, that:

$$\begin{aligned} \left(M(a_{i_h}, L)^{(n_{\phi_{i_h}})}\right)^{(m_h)} &= \left(M(a_{i_h}, L)^{(n_h)}\right)^{(m_h)} \\ &= M(a_{i_h}, L)^{(n_h m_h)}. \end{aligned}$$

b) To prove (1,b), we calculate, as below, making several simple, but necessary, observations. We have:

$$\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{h=1}^{u} M(a_{i_h}, L)^{(n_h m_h)}\right] \cap \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)\right]$$

$$= \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{h=1}^{u} \underbrace{M(a_{i_h}, L)^{(n_h m_h)}}_{\text{see note 1}} \cap \underbrace{\mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)}_{\text{see note 2}}\right] \qquad \text{[clearly]}$$

$$= \mathop{\bigcirc\!\!\!\!\!\!\triangle}_{h=1}^{u} \{I_{a_{i_h}}\}^{(n_h m_h)} \qquad \text{[clearly, by notes below]}$$

$$= \mathop{\bigcirc\!\!\!\!\!\!\triangle}_{h=1}^{u} \{I_{a_{i_h} n_h m_h}\} \qquad \text{[clearly]}$$

$$= \left\{I_{\sum_{h=1}^{u} a_{i_h} n_h m_h}\right\} \qquad \text{[clearly]}$$

$$= \{I_n\} \quad \text{[by Lemma 6.B.2, part (3), and the given here that } \dim \Phi = n\text{].}$$

<u>note 1:</u> elements are all block-diagonal, and all diagonal subblocks are $(a_{i_h} \times a_{i_h})$.

<u>note 2:</u> elements have all [canonical] $(a_{i_h} \times a_{i_h})$ subblocks equal to $I_{a_{i_h}}$ or $O_{a_{i_h}}$.

c) The conclusion in (1,c) follows at once from these clear facts:

i) $C\Pi = C'\Pi' \Rightarrow (C')^{-1}C = \Pi'\Pi^{-1}$;

ii) $\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{r} M^{\times}(a_i, L)^{(n_{\phi_i})}$, $\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)$ are groups;

iii) conclusions (1,b) and (1,a), just proved above.

2) a) To prove (2,a), we calculate, as below, making a few simple, but necessary, observations. We have:

$$\left[\underbrace{\mathrm{Perm}(a_{i_h}n_h, I_{a_{i_h}}, k)^{(m_h)}}_{\text{see note 3}}\right] \cdot \left[\underbrace{\mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}n_h}, k)}_{\text{see note 4}}\right]$$

$\subseteq$ the set of $(a_{i_h} \times a_{i_h})$–block permutation matrices, of dimension $a_{i_h}n_hm_h$

[clearly, by notes below]

$= \mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k)$ [by definition].

note 3: elements are all block-diagonal, and each of the $m_h$ diagonal subblocks is $(a_{i_h}n_h \times a_{i_h}n_h)$ and has all [canonical] $(a_{i_h} \times a_{i_h})$ subblocks equal to $I_{a_{i_h}}$ or $O_{a_{i_h}}$.

note 4: each element here, when multiplied on the right of a given matrix, permutes the [canonical] $(a_{i_h}n_h)$ column blocks of that matrix as whole entities.

Thus:

$$\left[\mathrm{Perm}(a_{i_h}n_h, I_{a_{i_h}}, k)^{(m_h)}\right] \cdot \left[\mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}n_h}, k)\right] \subseteq \mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k).$$

b) From Section 6.2.1, item (c,v), we see:

$$G_h \equiv \mathcal{G}a\ell(\phi_{i_h}) \subseteq \mathrm{Perm}(a_{i_h}n_h, I_{a_{i_h}}, k).$$

This, and the definition of $P_h$ in the given, together with the conclusion (2,a) just proved above, shows the desired conclusion (2,b), at once.

c) The desired conclusion in (2,c) here follows at once from the conclusions

(2,b) and (1,c) just proved above, noting obviously that:

$$\Pi' \in \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r} \mathrm{Perm}(a_i, k)^{(n_{\phi_i})} \subseteq \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r} M^{\times}(a_i, \overline{k})^{(n_{\phi_i})}.$$

d) The desired conclusion in (2,d) follows at once from the observation: $\Pi = \Pi'\widetilde{\Pi} \Rightarrow I_n\Pi = \Pi'\widetilde{\Pi}$, and from the use here of conclusion (1,c) just proved above [with "$C$"$\equiv I_n$, "$C'$"$\equiv \Pi'$, "$\Pi$"$\equiv \Pi$, "$\Pi'$"$\equiv \widetilde{\Pi}$], also noting the conclusion (2,b) just proved above.

□

The first conclusion in the following lemma is proved by a key argument, and this conclusion forms a first, and critical, partial converse to the result of the previous main Theorem 6.D.1. The remainder of the conclusions here are concerned with several important structural connections, and isomorphisms, between the groups $G_h, P_h$, and $I_m^{\times}(\Delta_{\Phi})$ – as defined in the lemma below (and identical to those defined in the previous Lemma 6.E.1).

**Lemma 6.E.2**

Let $n \in \mathbb{Z}^{+}$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/\!\sim_k| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/\!\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$, and let $m_h \equiv |[\phi_{i_h}]|, n_h \equiv n_{\phi_{i_h}} = [K_{i_h} : k]$.

Additionally, let $G_h \equiv \mathcal{G}al(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

For each $\phi_i$, let $\mathcal{N}_{\phi_i} \subseteq M(a_{\phi_i}, K_{\phi_i}) = M(a_i, K_i)$. Suppose that each $\mathcal{N}_{\phi_i}$ is "closed" under $\mathcal{G}al(K_i/k)$: $\forall \gamma \in \mathcal{G}al(K_i/k)$: $\gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i}$.

**Then:**

1) $\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$ normalizes $\Delta_\Phi\left(\Pi_{i=1}^{r} \mathcal{N}_{\phi_i}\right)$.

2) a) $\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$ normalizes $Im(\Delta_\Phi)$, and $\Delta_\Phi\left(\Pi_{i=1}^{r} \mathrm{Scalar}(a_i, K_i)\right)$;

   b) $\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \cap Im(\Delta_\Phi) = \{I_n\}$.

3) a) $P_h$ normalizes $G_h^{(m_h)}$;

   b) $P_h \cap G_h^{(m_h)} = \{I_{a_{i_h} n_h m_h}\}$.

4) a) $\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$ is a group, and is isomorphic to

$$\prod_{h=1}^{u} \left[\mathcal{G}al(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right];$$

   b) $Im^{\times}(\Delta_\Phi)\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$ is a group, and is isomorphic to

$$\left[\prod_{i=1}^{r} \mathcal{G}\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u} \left[\mathcal{G}al(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right]\right];$$

   c) $Im^{\times}(\Delta_\Phi)\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \rhd Im^{\times}(\Delta_\Phi)$, and

$$Im^{\times}(\Delta_\Phi)\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \Big/ Im^{\times}(\Delta_\Phi) \approx \prod_{h=1}^{u} \left[\mathcal{G}al(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right];$$

   d) i) $\sum_{i=1}^{r} a_i [K_i : k] = \sum_{h=1}^{u} a_{i_h} [K_{i_h} : k] m_h = n$;

      ii) $\sum_{h=1}^{u} m_h = r$.

**Proof.**

1) a) We make an initial observation. We are given that $\mathcal{N}_{\phi_i} \subseteq M(a_i, K_i)$, and $\mathcal{N}_{\phi_i}$ is closed under $Gal(K_i/k)$:

$$\forall\gamma \in Gal(K_i/k):\ \ \gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i}.$$

Hence, for $\gamma \in Gal(K_i/k)$: $\gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i}$;

and so:

$$\gamma^2(\mathcal{N}_{\phi_i}) \subseteq \gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i}.$$

So, iterating, we have for all $s \in \mathbb{Z}^+$:

$$\gamma^s(\mathcal{N}_{\phi_i}) \subseteq \gamma^{s-1}(\mathcal{N}_{\phi_i}) \subseteq \cdots \subseteq \gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i}.$$

But $\gamma \in Gal(K_i/k)$, and so $\gamma$ has finite order: $\gamma^J = id_{K_i}$, for some $J \in \mathbb{Z}^+$ (e.g., $J \equiv |Gal(K_i/k)|$). Letting $s \equiv J$ in the above chain of inclusions, we have, in particular:

$$\gamma^J(\mathcal{N}_{\phi_i}) \subseteq \gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i};$$

$$id_{K_i}(\mathcal{N}_{\phi_i}) \subseteq \gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i};$$

$$\mathcal{N}_{\phi_i} \subseteq \gamma(\mathcal{N}_{\phi_i}) \subseteq \mathcal{N}_{\phi_i}.$$

Thus:

$$\gamma(\mathcal{N}_{\phi_i}) = \mathcal{N}_{\phi_i}.$$

Hence:

$$\forall\gamma \in Gal(K_i/k):\ \ \gamma(\mathcal{N}_{\phi_i}) = \mathcal{N}_{\phi_i}. \tag{1}$$

b) Now let:

$$\Pi \in \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] = \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{h=1}^{u} \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} G_h\right] \cdot P_h\right].$$

Thus, by definitions of $G_h$ and $P_h$:

$$\Pi = \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{h=1}^{u} \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right] \cdot \Psi_h\right], \tag{2}$$

for some $\gamma_j^{(h)} \in Ga\ell(K_{i_h}/k)$ and $\Psi_h \in \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

c) Now, using the definition of $\Delta_\Phi$, and by Lemma 6.B.3, part (2,a), with $f(\phi_i) \equiv \mathcal{N}_{\phi_i}$, we note the following:

$$\Delta_\Phi\left(\Pi_{i=1}^{r} \mathcal{N}_{\phi_i}\right) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} \Delta_{\phi_i}(\mathcal{N}_{\phi_i}) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{h=1}^{u} \left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}. \tag{3}$$

e) Now we make the calculation below.

$$\begin{aligned}
&\left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]^{-1} \cdot \left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)} \cdot \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right] \\
&\quad = \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]^{-1} \cdot \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right] \cdot \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right] \\
&\quad = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \left[\Gamma^{-1}_{\gamma_j^{(h)},\phi_{i_h}} \Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}}) \Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right] \\
&\quad = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Delta_{\phi_{i_h}}\left(\gamma_j^{(h)^{-1}}(\mathcal{N}_{\phi_{i_h}})\right);
\end{aligned}$$

where the last equality follows from Section 6.2.1, item (c,ii). Now from (2) we have $\gamma_j^{(h)} \in Ga\ell(K_{i_h}/k)$ (and thus so also is $\gamma_j^{(h)^{-1}}$), and so at once by (1) we have $\gamma_j^{(h)^{-1}}(\mathcal{N}_{\phi_{i_h}}) = \mathcal{N}_{\phi_{i_h}}$. Using this, the last expression above becomes:

$$\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Delta_{\phi_{i_h}}\left(\gamma_j^{(h)^{-1}}(\mathcal{N}_{\phi_{i_h}})\right) = \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{j=1}^{m_h} \Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}}) = \left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}.$$

Thus, the above equalities now show:

$$\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]^{-1}\cdot\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}\cdot\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]=\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}.$$

Using the previous result, we clearly see:

$$\begin{aligned}&\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{h=1}^{u}\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]\right]^{-1}\cdot\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{h=1}^{u}\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}\right]\cdot\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{h=1}^{u}\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]\right]\\&\quad=\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{h=1}^{u}\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]^{-1}\cdot\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}\cdot\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]\\&\quad=\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{h=1}^{u}\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}.\end{aligned}$$

This, together with (3), thus shows at once:

$$(4)\qquad\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{h=1}^{u}\left[\mathop{\bigcirc\kern-0.75em{\scriptstyle\triangle}}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]\right]\text{ normalizes }\Delta_{\Phi}\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right).$$

f) Now recall from (2) that $\Psi_h\in\mathrm{Perm}(a_{i_h}n_hm_h,I_{a_{i_h}n_h},k)$. Thus $\Psi_h$ is an $(a_{i_h}n_h\times a_{i_h}n_h)$–block permutation matrix. Thus, by recalling the basic properties of such matrices, as described in Section 1.2.4, Part (d), we see that the map $conj_{\Psi_h}$ acts on the elements of $M(a_{i_h}n_h,L)^{(m_h)}$ by permuting all the $m_h$ diagonal subblocks, of these elements, as whole units. In particular, we thus see:

$$(5)\qquad\mathcal{M}\subseteq M(a_{i_h}n_h,L)\Rightarrow\Psi_h^{-1}\left[\mathcal{M}^{(m_h)}\right]\Psi_h=\mathcal{M}^{(m_h)}.$$

Thus, letting $\mathcal{M}\equiv\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\subseteq M(\dim\phi_{i_h},\overline{k})=M(a_{i_h}n_h,\overline{k})$, we have at once:

$$\Psi_h^{-1}\left[\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}\right]\Psi_h=\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}.$$

Using the previous, we easily have:

$$\begin{aligned}\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\Psi_h\right]^{-1}\cdot\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}\right]\cdot\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\Psi_h\right]&\\ =\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\Psi_h^{-1}\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}\Psi_h\right]&\\ =\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\left[\Delta_{\phi_{i_h}}(\mathcal{N}_{\phi_{i_h}})\right]^{(m_h)}.&\end{aligned}$$

This, together with (3), thus shows at once:

$$\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\Psi_h\right]\text{ normalizes }\Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right).\tag{6}$$

g) Now (4) and (6), together, show at once:

$$\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]\right]\cdot\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\Psi_h\right]\text{ normalizes }\Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right).$$

Hence:

$$\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{j=1}^{m_h}\Gamma_{\gamma_j^{(h)},\phi_{i_h}}\right]\cdot\Psi_h\right]\text{ normalizes }\Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right).$$

Thus, by (2):

$$\Pi\text{ normalizes }\Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right).$$

Therefore, as $\Pi$ is an arbitrary element of $\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}G_h^{(m_h)}\cdot P_h\right]$, we conclude:

$$\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u}G_h^{(m_h)}\cdot P_h\right]\text{ normalizes }\Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right).\tag{7}$$

This completes the proof of the desired conclusion (1).

2) a) i) For each $\phi_i$, here let $\mathcal{N}_{\phi_i}\equiv M(a_i,K_i)$. Clearly now, $\mathcal{N}_{\phi_i}$ is "closed" under $Ga\ell(K_i/k)$. Thus, at once by conclusion (1) just proved above,

we have:

$$\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \text{ normalizes}$$

$$\Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right) = \Delta_\Phi\left(\Pi_{i=1}^{r}M(a_i,K_i)\right) = Im(\Delta_\Phi).$$

ii) Similarly to (i) above, for each $\phi_i$, now let $\mathcal{N}_{\phi_i} \equiv \text{Scalar}(a_i, K_i)$. Clearly again, $\mathcal{N}_{\phi_i}$ is "closed" under $Ga\ell(K_i/k)$. Thus, at once, as above, we have:

$$\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \text{ normalizes } \Delta_\Phi\left(\Pi_{i=1}^{r}\mathcal{N}_{\phi_i}\right) = \Delta_\Phi\left(\Pi_{i=1}^{r}\text{Scalar}(a_i,K_i)\right).$$

b) The desired conclusion in (2,b) follows at once from Lemma 6.E.1, parts (2,b), (1,a) and (1,b), and the definition of $\Delta_\Phi$, as follows:

$$\begin{aligned}
&\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \cap Im(\Delta_\Phi) \\
&\qquad \subseteq \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} \text{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k)\right] \cap \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{i=1}^{r} M(a_i,\overline{k})^{(n_{\phi_i})}\right] \\
&\qquad = \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} \text{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k)\right] \cap \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} M(a_{i_h},\overline{k})^{(n_hm_h)}\right] \\
&\qquad = \{I_n\}.
\end{aligned}$$

Clearly also $I_n \in \left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \cap Im(\Delta_\Phi)$ (all entries in the latter are groups, or $k$–algebras, themselves). Thus:

$$\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \cap Im(\Delta_\Phi) = \{I_n\}.$$

This completes the proof of desired conclusion (2).

3) a) Let $\Psi \in P_h \equiv \mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}n_h}, k)$. Then, exactly as was argued to establish (5), we have:

$$\mathcal{M} \subseteq M(a_{i_h}n_h, L) \Rightarrow \Psi^{-1}\mathcal{M}^{(m_h)}\Psi = \mathcal{M}^{(m_h)}.$$

Now recall from the definition of $G_h$, that:

$$(8) \qquad G_h \subseteq \mathrm{Perm}(a_{i_h}n_h, I_{a_{i_h}}, k) \subseteq M(a_{i_h}n_h, L).$$

So, letting $\mathcal{M} \equiv G_h$ in the second-to-last previous result, we now have:

$$\Psi^{-1}G_h^{(m_h)}\Psi = G_h^{(m_h)}.$$

Thus, as $\Psi$ is an arbitrary element of $P_h$, we conclude at once:

$$P_h \text{ normalizes } G_h^{(m_h)}.$$

b) We now calculate, using (8):

$$\begin{aligned} P_h \cap G_h^{(m_h)} &\subseteq \left[\underbrace{\mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}n_h}, k)}_{\text{see note 5}}\right] \cap \left[\underbrace{M(a_{i_h}n_h, L)}_{\text{see note 6}}\right]^{(m_h)} \\ &= \{I_{a_{i_h}n_h}\}^{(m_h)} \qquad \text{[clearly, by above captions]} \\ &= \{I_{a_{i_h}n_hm_h}\} \qquad \text{[clearly].} \end{aligned}$$

note 5: elements have all (canonical) $a_{i_h}n_h \times a_{i_h}n_h$ subblocks equal to $\mathrm{I}_{a_{i_h}n_h}$ or $\mathrm{O}_{a_{i_h}n_h}$.

note 6: elements are all block-diagonal, and all diagonal subblocks are $a_{i_h}n_h \times a_{i_h}n_h$.

As in step (2,b) above, clearly $I_{a_{i_h} n_h m_h} \in P_h \cap G_h^{(m_h)}$ (both $P_h$ and $G_h$ are groups). Thus:

$$P_h \cap G_h^{(m_h)} = \{I_{a_{i_h} n_h m_h}\}.$$

This completes the proof of desired conclusion (3).

4) a) By the desired conclusion (3,a) just proved above, and elementary group theory, we have that $G_h^{(m_h)} \cdot P_h$ is a group. Thus clearly so is $\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h$. Now recall, from Sec. 6.2.1, item $(c, v)$, that $G_h \equiv Ga\ell(\phi_{i_h}) \approx Ga\ell(K_{i_h}/k)$, and, by definition of $P_h$ and basic properties of permutation matrices, that $P_h \approx S_{m_h}$ (symmetric group on $m_h$ letters). So clearly we see $G_h^{(m_h)} \approx Ga\ell(K_{i_h}/k)^{m_h}$. This, together with conclusions (3,a),(3,b) just proved above, and elementary group theory, show at once:

$$G_h^{(m_h)} \cdot P_h \approx Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}.$$

Thus, clearly:

$$\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \approx \left[\prod_{h=1}^{u} [Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]\right].$$

b) Using conclusions (2,a),(2,b) just proved above, and arguing similarly to step (4,a) above, we have at once:

$$Im^{\times}(\Delta_{\Phi}) \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \text{ is a group, and}$$

$$(9) \qquad Im^{\times}(\Delta_{\Phi}) \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \approx Im^{\times}(\Delta_{\Phi}) \rtimes \left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right].$$

Now recalling that $\Delta_\Phi$ is an imbedding of $k$–algebras, and recalling the definition of $\Delta_\Phi$, we clearly have $Im^\times(\Delta_\Phi) \approx \Pi_{i=1}^{r} G\ell(a_i, K_i)$. This, together with conclusion (4,a) just proved above, when applied in (9), gives at once:

$$Im^\times(\Delta_\Phi)\left[\mathop{\triangle\kern-0.85em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \approx \left[\prod_{i=1}^{r} G\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u} [Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]\right].$$

c) The former part of conclusion (2,a) just proved above shows, essentially immediately, that:

$$\left[\mathop{\triangle\kern-0.85em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \text{ normalizes } Im^\times(\Delta_\Phi).$$

Both of the conclusions in (4,c) follow immediately from this previous result, from conclusions (2,b) and (4,a) just proved above, and from elementary group theory (specifically, from the elementary fact that if $H, K$ are subgroups of $G$, and $K$ normalizes $H$, then $HK$ is a subgroup of $G, HK \rhd H$ and $HK/H \approx K/(H \cap K)$).

d) The conclusions in (4,d) follow immediately from Lemma 6.B.2, and the given here that $\dim \Phi = n$.

This completes the proof of desired conclusion (4).

□

The statement of the following lemma refers to the permutation matrices "$\Pi_{\tau,\Phi}$" recalled in Sec. 6.2.1, part (d). This lemma establishes the commutativity of all the permutation matrices, $\Pi_{\tau,\Phi}$, with "almost" any permutation matrix that normalizes a $k$–rationalizable diagonal subset of matrices that is "canonically" connected to the field setting $\Phi$.

**Lemma 6.E.3**

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/\!\sim_k| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/\!\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$, and let $m_h \equiv |[\phi_{i_h}]|, n_h \equiv n_{\phi_{i_h}} = [K_{i_h} \colon k]$.

Additionally, let $G_h \equiv \mathcal{G}a\ell(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

Let $\mathcal{Z} \subseteq \Delta_\Phi\,(\Pi_{i=1}^{r}\mathrm{Scalar}(a_i, K_i))$, where $C_L(\mathcal{Z}) = \mathop{\bigtriangleup\kern-0.85em\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$. Let $\tilde{\Pi} \in \mathop{\bigtriangleup\kern-0.85em\bigcirc}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)$. Suppose $\tilde{\Pi}$ normalizes $\mathcal{Z}$. Let $E$ be any intermediate field of $\overline{k}/k$ where $\bigcup_{i=1}^{r}\bigcup_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(K_i) \subseteq E \subseteq \overline{k}$.

**Then:**

$$\forall \tau \in Iso(E/k)\colon\ \tilde{\Pi} \text{ commutes with } \Pi_{\tau,\Phi}.$$

**Proof.**

1) As given $\tilde{\Pi}$ normalizes $\mathcal{Z}$, we have:

$$(1) \qquad \tilde{\Pi}^{-1}\mathcal{Z}\tilde{\Pi} = \mathcal{Z}.$$

Thus, in particular:

$$(2) \qquad \forall Z \in \mathcal{Z} \colon \exists \tilde{Z} \in \mathcal{Z} \colon \; \tilde{\Pi}^{-1}Z\tilde{\Pi} = \tilde{Z}.$$

2) Let $\tau \in Iso(E/k)$. Now as $\mathcal{Z} \subseteq Im(\Delta_{\Phi})$, and all $\sigma_j^{(i)}(K_i) \subseteq E$, we may apply $\tau$ to elements of $\mathcal{Z}$. Thus, applying $\tau$ to (2), we have:

$$\forall Z \in \mathcal{Z} \colon \; \tau(\tilde{\Pi}^{-1}Z\tilde{\Pi}) = \tau(\tilde{Z}).$$

Thus:

$$\begin{aligned} \tau(\tilde{\Pi})^{-1}\tau(\mathcal{Z})\tau(\tilde{\Pi}) &= \tau(\tilde{Z}), && \text{[as } \tau \text{ is an isomorphism]} \\ \tilde{\Pi}^{-1}\tau(\mathcal{Z})\tilde{\Pi} &= \tau(\tilde{Z}), && \text{[as } \tilde{\Pi} \text{ consists only of 0's and 1's]} \\ \tilde{\Pi}^{-1}\left(\Pi_{\tau,\Phi}^{-1}Z\Pi_{\tau,\Phi}\right)\tilde{\Pi} &= \Pi_{\tau,\Phi}^{-1}\tilde{Z}\Pi_{\tau,\Phi}; \end{aligned}$$

where the latter follows from Sec 6.2.1, part (d), item (iii) (itself being an important fact recalled directly from Chapter 1), and from the given that $Z, \tilde{Z} \in \mathcal{Z}$ and so $Z, \tilde{Z} \in Im(\Delta_{\Phi})$. So we now have:

$$\forall Z \in \mathcal{Z} \colon \; \tilde{\Pi}^{-1}(\Pi_{\tau,\Phi}^{-1}Z\Pi_{\tau,\Phi})\tilde{\Pi} = \Pi_{\tau,\Phi}^{-1}\tilde{Z}\Pi_{\tau,\Phi}.$$

Thus:

$$(\tilde{\Pi}^{-1}\Pi_{\tau,\Phi}^{-1})Z(\Pi_{\tau,\Phi}\tilde{\Pi}) = \Pi_{\tau,\Phi}^{-1}\left(\tilde{\Pi}^{-1}Z\tilde{\Pi}\right)\Pi_{\tau,\Phi}, \qquad \text{[by (2) above].}$$

Hence:

$$\forall Z \in \mathcal{Z}\colon\ (\tilde{\Pi}^{-1}\Pi^{-1}_{\tau,\Phi})Z(\Pi_{\tau,\Phi}\tilde{\Pi}) = (\Pi^{-1}_{\tau,\Phi}\tilde{\Pi}^{-1})Z(\tilde{\Pi}\Pi_{\tau,\Phi}).$$

3) As the previous equation is true for all $Z \in \mathcal{Z}$, it thus shows, at once:

$$(3)\qquad \Pi_{\tau,\Phi}\tilde{\Pi} = B\tilde{\Pi}\Pi_{\tau,\Phi},\ \text{for some } B \in C_L(\mathcal{Z}).$$

We now examine $B$, and show $B = I_n$.

4) By (3) we have $B \in C_L(\mathcal{Z})$, and so by the given on $C_L(\mathcal{Z})$ we have:

$$(4)\qquad B \in \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.$$

But also by (3):

$$(5)\qquad B = \Pi_{\tau,\Phi}\tilde{\Pi}\Pi^{-1}_{\tau,\Phi}\tilde{\Pi}^{-1}.$$

Now by the given on $\tilde{\Pi}$, we have:

$$(6)\qquad \tilde{\Pi} \in \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{h=1}^{u} \text{Perm}\ (a_{i_h} n_h m_h, I_{a_{i_h}}, k).$$

Now by definition of $\Pi_{\tau,\Phi}$ (again as recalled in Sec. 6.2), we have:

$$\Pi_{\tau,\Phi} = \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r} \Pi_{\tau,\phi_i}.$$

Now as $\Phi$ is given to be reduced, the previous, together with Lemma 6.B.3, part (2,a) [with $f(\phi_i) \equiv \{\Pi_{\tau,\phi_i}\}$], gives at once:

$$\begin{aligned}\Pi_{\tau,\Phi} &= \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{i=1}^{r} \Pi_{\tau,\phi_i} = \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{h=1}^{u} \Pi^{(m_h)}_{\tau,\phi_{i_h}} \\ &= \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{h=1}^{u}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{m_h} \Pi_{\tau,\phi_{i_h}} \\ &\in \mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{h=1}^{u}\mathop{\bigcirc\hspace{-0.9em}\triangle}\limits_{j=1}^{m_h} \text{Perm}(a_{i_h} n_h, I_{a_{i_h}}, k);\end{aligned}$$

where the last fact follows at once from the definition of $\Pi_{T,\phi_{i_h}}$. Thus, we have now:

$$\begin{aligned}\Pi_{T,\Phi} &\in \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \underbrace{\mathop{\textcircled{$\triangle$}}_{j=1}^{m_h} \mathrm{Perm}(a_{i_h}n_h, I_{a_{i_h}}, k)}_{\text{see note 7}} \\ &\subseteq \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathrm{Perm}\ (a_{i_h}n_hm_h, I_{a_{i_h}}, k) \qquad \text{[clearly, by above caption].}\end{aligned}$$

<u>note 7:</u> elements are $(a_{i_h} \times a_{i_h})$–block permutation matrices of dimension $a_{i_h}n_hm_h$.

Hence:

$$\Pi_{T,\Phi} \in \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k). \tag{7}$$

So, (5),(6), and (7) show at once:

$$B \in \mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k). \tag{8}$$

And thus, by (4) and (8):

$$B \in \left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] \cap \left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} \mathrm{Perm}(a_{i_h}n_hm_h, I_{a_{i_h}}, k)\right].$$

And so at once, by Lemma 6.E.1, parts (1,a) and (1,b), the previous gives:

$$B = I_n. \tag{9}$$

5) Now putting (9) in (3), we have:

$$\Pi_{T,\Phi}\tilde{\Pi} = \tilde{\Pi}\Pi_{T,\Phi}.$$

Thus, as $\tau$ was an arbitrary element of $Iso(E/k)$, the previous gives:

$$\forall \tau \in Iso(E/k)\colon\ \tilde{\Pi} \text{ commutes with } \Pi_{\tau,\Phi}.$$

□

The statement of the following lemma refers to the subsets of matrices, "$V_\Phi$", defined for any field setting, $\Phi$, in Sec. 1.3.6, item (a). This lemma provides some rationalizability results which allow some "sufficiency" results for rationalizable normalizers of some rationalizable diagonal subsets.

**Lemma 6.E.4**

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/{\sim_k}| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/{\sim_k}$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/{\sim_k}$, and let $m_h \equiv |[\phi_{i_h}]|, n_h \equiv n_{\phi_{i_h}} = [K_{i_h}\colon k]$.

Additionally, let $G_h \equiv Ga\ell(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

Let $E$ be any intermediate field of $\overline{k}/k$ where $\bigcup_{i=1}^{r} \bigcup_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(K_i) \subseteq E \subseteq \overline{k}$.

**Then:**

1) $\mathcal{A} \subseteq C_k(\{\Pi_{\tau,\Phi} \in \mathrm{Perm}(n,k) | \tau \in Iso(E/k)\}) \subseteq M(n,k), V \in V_\Phi^\times \quad \Longrightarrow$

   $Im(\Delta_\Phi) \cdot \mathcal{A}$ is $k$–rationalizable by $V$.

2) $Im(\Delta_\Phi) \cdot \left[ \mathop{\bigcirc\kern-0.85em\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right]$ is $k$–rationalizable by any $V \in V_\Phi^\times$; in particular, it is $k$–rationalizable over $\overline{k}$.

**Proof.**

1) Let $\mathcal{A} \subseteq C_k(\{\Pi_{\tau,\Phi} \in \mathrm{Perm}(n,k) | \tau \in Iso(E/k)\}) \subseteq M(n,k)$, and $V \in V_\Phi^\times$.

   Thus, by definition of $\mathcal{A}$:

   (1) $\quad \mathcal{A} \subseteq M(n,k)$ and $\forall A \in \mathcal{A}$: $\forall \tau \in Iso(E/k)$: $A$ commutes with $\Pi_{\tau,\Phi}$.

   We show that $V$ $k$–rationalizes $Im(\Delta_\Phi) \cdot \mathcal{A}$; i.e., that:

$$V Im(\Delta_\Phi) \mathcal{A} V^{-1} \subseteq M(n,k).$$

   a) We observe, using the given on $E$, that:

      i) $Im(\Delta_\Phi) \subseteq M(n,E)$, by definition of $\Delta_\Phi$;

      ii) $\mathcal{A} \subseteq M(n,E)$, a fortiori, as $\mathcal{A} \subseteq M(n,k)$;

      iii) $V \in M(n,E)$, by definition of $V_\Phi$.

      Hence, we conclude:

$$(2) \qquad V Im(\Delta_\Phi) \mathcal{A} V^{-1} \subseteq M(n,E).$$

b) Let $B \in Im(\Delta_\Phi)$, and $A \in \mathcal{A}$. Let $\tau \in Iso(E/k)$, and *abbreviate* $\Pi_{\tau,\Phi}$ *by* $\Pi_\tau$. As $\tau \in Iso(E/k)$, by (2) we may calculate:

$$\begin{aligned}\tau(VBAV^{-1}) &= \tau(V)\tau(B)\tau(A)\tau(V)^{-1}, && \text{[as } \tau \text{ is an isomorphism]}\\ &= (V\Pi_\tau)(\Pi_\tau^{-1}B\Pi_\tau)\tau(A)(\Pi_\tau^{-1}V^{-1});\end{aligned}$$

where the last equation follows by the results in Sec 6.2.1, part (d), items (iii) and (v). Thus, continuing, we have:

$$\begin{aligned}\tau(VBAV^{-1}) &= (V\Pi_\tau)(\Pi_\tau^{-1}B\Pi_\tau)\tau(A)(\Pi_\tau^{-1}V^{-1})\\ &= (V\Pi_\tau)(\Pi_\tau^{-1}B\Pi_\tau)A(\Pi_\tau^{-1}V^{-1})\\ &\qquad \text{[as } A \in \mathcal{A} \subseteq M(n,k) \text{ and } \tau|k = id_k\text{]}\\ &= VB\Pi_\tau A\Pi_\tau^{-1}V^{-1}\\ &= VBAV^{-1}\\ &\qquad \text{[as by (1), } A \text{ commutes with } \Pi_\tau(=\Pi_{\tau,\Phi})\text{]}.\end{aligned}$$

Therefore:

$$\tau(VBAV^{-1}) = VBAV^{-1}.$$

Thus, we conclude:

$$\forall \tau \in Iso(E/k)\colon\ \tau(VBAV^{-1}) = VBAV^{-1}.$$

Thus, by basic field theory (as $k$ is given perfect!), we conclude:

$$VBAV^{-1} \in M(n,k).$$

Thus, as $B, A$ are arbitrary elements, resp., of $Im(\Delta_\Phi), \mathcal{A}$, the previous shows at once:

$$VIm(\Delta_\Phi)\mathcal{A}V^{-1} \subseteq M(n,k).$$

Therefore, $V$ $k$–rationalizes $Im(\Delta_\Phi) \cdot \mathcal{A}$.

2) Let $\widetilde{\Pi} \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h$. So certainly, $\widetilde{\Pi} \in \mathrm{Perm}(n,k)$. Now we use the previous three lemmas of this section, easily, to make the following observations about $\widetilde{\Pi}$:

i) by Lemma 6.E.1, part (2,b):

$$\widetilde{\Pi} \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k);$$

ii) by Lemma 6.E.2, part (2,a):

$$\widetilde{\Pi} \text{ normalizes } \Delta_\Phi \left(\Pi_{i=1}^{r} \mathrm{Scalar}(a_i, K_i)\right);$$

iii) thus, by (ii) here, and by Lemma 6.E.3 (with "$\mathcal{Z}$"$\equiv \Delta_\Phi$ $(\Pi_{i=1}^{r}\mathrm{Scalar}(a_i, K_i))$, and using Lemma 2.D.1, part (b,i)):

$$\forall \tau \in Iso(E/k)\text{: } \widetilde{\Pi} \text{ commutes with } \Pi_{\tau,\Phi}.$$

So, summarizing, we have, in particular:

$$\widetilde{\Pi} \in \mathrm{Perm}(n,k) \text{ and } \forall \tau \in Iso(E/k)\text{: } \widetilde{\Pi} \text{ commutes with } \Pi_{\tau,\Phi}.$$

Hence, by definition, in particular:

$$\widetilde{\Pi} \in C_k \left(\{\Pi_{\tau,\Phi} \in \mathrm{Perm}(n,k) | \tau \in Iso(E/k)\}\right).$$

Thus, as $\widetilde{\Pi}$ is an arbitrary element of $\mathop{\bigcirc\mkern-15mu\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h$, the previous gives:

$$\mathop{\bigcirc\mkern-15mu\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \subseteq C_k \left(\{\Pi_{\tau,\Phi} \in \mathrm{Perm}(n,k) | \tau \in Iso(E/k)\}\right).$$

This, together with the conclusion (1) of this lemma just proved above (and using "$\mathcal{A}$"$\equiv \mathop{\textcircled{$\Delta$}}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h$), gives at once: $Im(\Delta_\Phi) \cdot \left[\mathop{\textcircled{$\Delta$}}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$ is $k$–rationalizable by any $V \in V_\Phi^\times$; in particular, it is thus $k$–rationalizable over $\overline{k}$.

□

The lemma below contains one of the key, and simple, arguments of this chapter. The result of the lemma basically exhibits the normalizers of rationalizable diagonal subsets, where the normalizer is rationalizable by some element of "$V_\Phi^\times$".

**Lemma 6.E.5** [Key Argument]

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/\!\sim_k| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/\!\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$, and let $m_h \equiv |[\phi_{i_h}]|, n_h \equiv n_{\phi_{i_h}} = [K_{i_h} \colon k]$.

Additionally, let $G_h \equiv \mathcal{G}a\ell(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

Let $\mathcal{Z} \subseteq \Delta_\Phi\,(\Pi_{i=1}^r \mathrm{Scalar}(a_i, K_i))$, where $C_L(\mathcal{Z}) = \mathop{\textcircled{$\Delta$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $\tilde{\Pi}(\mathcal{Z}) \equiv \left\{ \tilde{\Pi} \in \mathop{\textcircled{$\Delta$}}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k) \,\middle|\, \tilde{\Pi} \text{ normalizes } \mathcal{Z} \right\} \subseteq \mathrm{Perm}(n, k)$.

Let $\mathcal{M} \subseteq M^{\times}(n, L)$, where $\mathcal{M}$ normalizes $\mathcal{Z}$.

Suppose $\mathcal{M}$ is $k$–rationalizable over $L$, by some $V \in V_{\Phi}^{\times}$.

**Then:**

1) $\mathcal{M} \subseteq Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z})$.

2) $Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z})$ is $k$–rationalizable by any $V \in V_{\Phi}^{\times}$.

**Proof.**

1) a) Let $E$ be any intermediate field of $\overline{k}/k$, where $\bigcup\limits_{i=1}^{r}\bigcup\limits_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(K_i) \subseteq E \subseteq \overline{k}$. Let $M \in \mathcal{M}$. So, given that $\mathcal{M}$ normalizes $\mathcal{Z}$, we have:

$$M^{-1}\mathcal{Z}M = \mathcal{Z}. \tag{1}$$

This, with the critical Lemma 6.C.3 (with "$\mathcal{Y}$"$\equiv \mathcal{Z}$,"$\mathcal{N}$"$\equiv M$), gives:

$$M = C\Pi;\ \text{for some } C \in C_L^{\times}(\mathcal{Z}),\ \Pi \in \mathrm{Perm}(n, k),$$

where

$$\Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z}.$$

As $\Pi^{-1}\mathcal{Z}\Pi = \mathcal{Z}$, we have by the critical Theorem 6.D.1: $\Pi = \Pi'\tilde{\Pi}$, for some $\Pi' \in \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} \mathrm{Perm}(a_i, k)^{(n_{\phi_i})}, \tilde{\Pi} \in \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h$. So, by the given on $C_L(\mathcal{Z})$, clearly $\Pi' \in C_L^{\times}(\mathcal{Z})$. And, by Lemma 6.E.1, part (2,b), we have $\tilde{\Pi} \in \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k)$. Thus, from these remarks, we have that $\Pi$

normalizes $\mathcal{Z}$ and $\Pi'$ centralizes $\mathcal{Z}$, and so we observe:

$$\begin{aligned}\mathcal{Z} &= \Pi^{-1}\mathcal{Z}\Pi = \tilde{\Pi}^{-1}\Pi'^{-1}\mathcal{Z}\Pi'\tilde{\Pi} \\ &= \tilde{\Pi}^{-1}(\Pi'^{-1}\mathcal{Z}\Pi')\tilde{\Pi} = \tilde{\Pi}^{-1}\mathcal{Z}\tilde{\Pi}.\end{aligned}$$

Thus $\tilde{\Pi}$ normalizes $\mathcal{Z}$; and so, also, by the definition in the given, we have $\tilde{\Pi} \in \tilde{\Pi}(\mathcal{Z})$. Finally, from these remarks, we have from Lemma 6.E.3, immediately:

$$\text{(2)} \qquad \forall \tau \in Iso(E/k)\text{: } \tilde{\Pi} \text{ commutes with } \Pi_{\tau,\Phi}.$$

Thus:

$$M = C\Pi = C(\Pi'\tilde{\Pi}) = B\tilde{\Pi}, \text{ where } B = C\Pi';$$

$$\text{and so} \quad B \in C_L^\times(\mathcal{Z}); \text{ as } C, \Pi' \in C_L^\times(\mathcal{Z}).$$

So, summarizing, we have:

$$\text{(3)} \qquad M = B\tilde{\Pi}; \;\; B \in C_L^\times(\mathcal{Z}), \tilde{\Pi} \in \tilde{\Pi}(\mathcal{Z}).$$

b) By the given, $\mathcal{M}$ is $k$–rationalizable by some $V \in V_\Phi^\times$. Thus:

$$V\mathcal{M}V^{-1} \subseteq M(n,k), \text{ for some } V \in V_\Phi^\times.$$

Now let $M \in \mathcal{M}$. Thus, a fortiori by the previous:

$$VMV^{-1} \in M(n,k).$$

Hence:

$$\text{(4)} \qquad VMV^{-1} = F, \text{ for some } F \in M(n,k).$$

c) By (4) and (3), we have:

$$(5) \qquad V B \tilde{\Pi} V^{-1} = F.$$

We note the following. The previous gives:

$$B = V^{-1} F V \tilde{\Pi}^{-1}.$$

By supposition on the field $E$, in step (1) above, we clearly have: $V \in M(n, E)$ (by definition of $V_\Phi$), $F \in M(n, E)$ (a fortiori, as $F \in M(n, k)$). These facts, together with the previous equation, show: $B \in M(n, E)$. Now furthermore, by (3), we have $B \in C_L^\times(\mathcal{Z})$. Thus, $B \in C_L^\times(\mathcal{Z}) \cap M(n, E)$; and so by the given on $C_L(\mathcal{Z})$, we have:

$$B \in \left[ \mathop{\bigcirc\kern-0.8em\triangle}\limits_{i=1}^{r} M^\times(a_i, L)^{(n_{\phi_i})} \right] \cap M(n, E).$$

Thus, clearly:

$$B \in \mathop{\bigcirc\kern-0.8em\triangle}\limits_{i=1}^{r} M^\times(a_i, E)^{(n_{\phi_i})}.$$

So, from (5) and (4), and the previous, we have:

$$(6) \qquad V B \tilde{\Pi} V^{-1} = F; \; B \in \mathop{\bigcirc\kern-0.8em\triangle}\limits_{i=1}^{r} M^\times(a_i, E)^{(n_{\phi_i})}, \; F \in M(n, k).$$

d) Let $\tau \in Iso(E/k)$. Applying $\tau$ to (6), we have:

$$\tau(V B \tilde{\Pi} V^{-1}) = \tau(F).$$

Thus:

$$\tau(V)\tau(B)\tau(\widetilde{\Pi})\tau(V)^{-1} = \tau(F)$$

[as $\tau$ is an isomorphism; and, as above, as $V, B, \widetilde{\Pi} \in M(n, E)$]

$$\tau(V)\tau(B)\widetilde{\Pi}\tau(V)^{-1} = F$$

[as $\widetilde{\Pi}, F \in M(n,k)$ and $\tau|k = id_k$]

$$(V\Pi_{\tau,\Phi})\tau(B)\widetilde{\Pi}(\Pi^{-1}_{\tau,\Phi}V^{-1}) = F;$$

where the last equation follows by the results in Sec 6.2.1, part (d), item (v). So we now have:

$$V\Pi_{\tau,\Phi}\tau(B)\widetilde{\Pi}\Pi^{-1}_{\tau,\Phi}V^{-1} = F.$$

Thus, by (6):

$$V\Pi_{\tau,\Phi}\tau(B)\widetilde{\Pi}\Pi^{-1}_{\tau,\Phi}V^{-1} = VB\widetilde{\Pi}V^{-1}.$$

Hence, "cancelling" $V, V^{-1}$ in the previous:

$$\Pi_{\tau,\Phi}\tau(B)\widetilde{\Pi}\Pi^{-1}_{\tau,\Phi} = B\widetilde{\Pi}.$$

Hence, by (2):

$$\Pi_{\tau,\Phi}\tau(B)\Pi^{-1}_{\tau,\Phi}\widetilde{\Pi} = B\widetilde{\Pi}.$$

Hence, "cancelling" $\widetilde{\Pi}$ in the previous:

$$\Pi_{\tau,\Phi}\tau(B)\Pi^{-1}_{\tau,\Phi} = B.$$

Thus, we conclude:

$$\tau(B) = \Pi^{-1}_{\tau,\Phi}B\Pi_{\tau,\Phi}. \tag{7}$$

e) Summarizing, from (6) and (7), we have, in particular:

$$B \in \mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{r} M^{\times}(a_i, E)^{(n_{\phi_i})} \text{ and } \forall\tau \in Iso(E/k)\colon\ \tau(B) = \Pi_{\tau,\Phi}^{-1} B \Pi_{\tau,\Phi}.$$

The situation in (8) is precisely that encountered in the proof of Theorem 3.B.1, ($\Rightarrow$). That same key argument, given there for that situation, shows here, precisely, that from (8), we can deduce that $B \in Im(\Delta_{\Phi})$. Therefore, $B \in Im(\Delta_{\Phi})$. Additionally, by (3), we have that $B$ is invertible. Thus now, in fact:

$$B \in Im^{\times}(\Delta_{\Phi}). \tag{9}$$

f) Finally, combining (3) and (9), we have:

$$M = B\tilde{\Pi} \in Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z}).$$

As $M$ was taken to be an arbitrary element of $\mathcal{M}$, we conclude at once:

$$\mathcal{M} \subseteq Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z}).$$

2) Here, we show that $Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z})$ is $k$–rationalizable by any $V \in V_{\Phi}^{\times}$.

a) From the definition of $\tilde{\Pi}(\mathcal{Z})$, and Lemma 6.E.3, we have immediately:

i) $\tilde{\Pi}(\mathcal{Z}) \subseteq \mathrm{Perm}(n,k)$;

ii) $\tilde{\Pi} \in \tilde{\Pi}(\mathcal{Z}) \Rightarrow \forall\tau \in Iso(E/k)\colon$ $\tilde{\Pi}$ commutes with $\Pi_{\tau,\Phi}$.

b) Let $\mathcal{A} \equiv \tilde{\Pi}(\mathcal{Z})$. Thus, at once by the observations (i) and (ii) immediately above, we have, in particular:

$$\mathcal{A} \subseteq C_k\left(\{\Pi_{\tau,\Phi} \in \mathrm{Perm}(n,k) | \tau \in Iso(E/k)\}\right) \subseteq M(n,k).$$

This, and Lemma 6.E.4, part (1), give at once: $Im(\Delta_\Phi) \cdot \mathcal{A}$ is $k$–rationalizable by any $V \in V_\Phi^\times$. Hence, a fortiori, the same is clearly true for $Im^\times(\Delta_\Phi) \cdot \mathcal{A}$, and here, by our definition just above, we have $\mathcal{A} = \tilde{\Pi}(\mathcal{Z})$.

□

## 6.6 Main Theorems

This section contains the principal results of this chapter. By pulling together the lemmas of the previous section, and several earlier results, a unified and concise picture of the rationalizable normalizers of rationalizable diagonal subsets is achieved. This picture is what the two, and main, theorems of this section show.

In this section, the notation defined in Chapter 1 for the normalizer of a subset of matrices, recall $\mathcal{N}_F(\mathcal{A})$, is used often.

**Theorem 6.F.1**

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \dots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/{\sim_k}| \in \{1, \dots, r\}$, let the subsequence $(\phi_{i_1}, \dots, \phi_{i_u}) \subseteq (\phi_1, \dots, \phi_r)$ be a set of representatives of $\Phi/{\sim_k}$, et $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/{\sim_k}$, and let $m_h \equiv |[\phi_{i_h}]|, n_h \equiv n_{\phi_{i_h}} = [K_{i_h} : k]$.

Additionally, let $G_h \equiv Ga\ell(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

Let $\mathcal{Z} \subseteq \Delta_\Phi\,(\Pi_{i=1}^{r}\mathrm{Scalar}(a_i, K_i))$, where $C_L(\mathcal{Z}) = \mathop{\triangle\kern-0.75em\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

Let $\mathcal{M} \subseteq \mathcal{N}_L(\mathcal{Z}) \subseteq M^\times(n, L)$, where $\mathcal{M}$ is $k$–rationalizable over $L$, by some $V \in V_\Phi^\times$.

Let $\langle\mathcal{M}\rangle \equiv$ the subgroup generated by $\mathcal{M}$ in $M^\times(n, L)$;

so also $\langle\mathcal{M}\rangle \subseteq M^\times(n, L)$.

**Then:**

1) a) $\mathcal{M} \subseteq Im^\times(\Delta_\Phi)\left[\mathop{\triangle\kern-0.75em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \subseteq M^\times(n, \overline{k})$.

b) $Im^\times(\Delta_\Phi)\left[\mathop{\triangle\kern-0.75em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$ may not necessarily normalize $\mathcal{Z}$, but nevertheless remains $k$–rationalizable by any $V \in V_\Phi^\times$.

2) a) $\langle\mathcal{M}\rangle \subseteq Im^\times(\Delta_\Phi)\left[\mathop{\triangle\kern-0.75em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \subseteq M^\times(n, \overline{k})$.

b) $\langle\mathcal{M}\rangle \hookrightarrow \left[\prod_{i=1}^{r} G\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u}\,[Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]\right]$; and

$\sum_{i=1}^{r} a_i[K_i\colon k] = \sum_{h=1}^{u} a_{i_h}[K_{i_h}\colon k]m_h = n,\ \ \sum_{h=1}^{u} m_h = r.$

c) $\langle\mathcal{M}\rangle$ normalizes $Im^\times(\Delta_\Phi)$; and

$Im^\times(\Delta_\Phi)\langle\mathcal{M}\rangle/Im^\times(\Delta_\Phi) \hookrightarrow \prod_{h=1}^{u}\,[Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]$; and

$\sum_{h=1}^{u} a_{i_h}[K_{i_h}\colon k]m_h = n,\ \ \sum_{h=1}^{u} m_h = r.$

**Proof.**

1) a) From the given, we have at once by Lemma 6.E.5:

$$(1)\qquad \begin{aligned} &\text{i)}\ \ \mathcal{M} \subseteq Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z}), \\ &\text{ii)}\ \ Im^{\times}(\Delta_{\Phi}) \cdot \tilde{\Pi}(\mathcal{Z}) \text{ is } k\text{-rationalizable by any } V \in V_{\Phi}^{\times}; \end{aligned}$$

where $\tilde{\Pi}(\mathcal{Z})$ is as defined by Lemma 6.E.5:

$$\tilde{\Pi}(\mathcal{Z}) \equiv \left\{ \tilde{\Pi} \in \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k) \middle| \tilde{\Pi} \text{ normalizes } \mathcal{Z} \right\} \subseteq \mathrm{Perm}(n, k).$$

Now let $\tilde{\Pi} \in \tilde{\Pi}(\mathcal{Z})$. Thus, by definition of $\tilde{\Pi}(\mathcal{Z})$:

$$(2)\qquad \tilde{\Pi}^{-1} \mathcal{Z} \tilde{\Pi} = \mathcal{Z} \text{ and } \tilde{\Pi} \in \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{h=1}^{u} \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h}}, k).$$

From the former part of (2), and *by Theorem 6.D.1*, we have at once:

$$\tilde{\Pi} = \Psi' \tilde{\Psi}, \text{ for some } \Psi' \in \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{i=1}^{r} \mathrm{Perm}(a_i, k)^{(n_{\phi_i})},\ \tilde{\Psi} \in \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h.$$

This, together with the latter part of (2), and Lemma 6.E.1, part (2,d), give at once, in particular:

$$\tilde{\Pi} \in \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h.$$

As $\tilde{\Pi}$ is an arbitrary element of $\tilde{\Pi}(\mathcal{Z})$, the previous shows at once:

$$(3)\qquad \tilde{\Pi}(\mathcal{Z}) \subseteq \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h.$$

Thus, (1) and (3) together give (with the latter containment below being immediate from the definitions of $\Delta_{\Phi}, G_h$, and $P_h$):

$$\mathcal{M} \subseteq Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\bigcirc\hspace{-0.78em}\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \subseteq M^{\times}(n, \bar{k}).$$

This proves the desired conclusion (1,a).

b) The desired conclusion in (1,b) follows from the given, verbatim, by Lemma 6.E.4, part (2).

2) a) By the conclusion (1,a) just proved above, we have now:

$$\mathcal{M} \subseteq Im^{\times}(\Delta_{\Phi})\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \subseteq M^{\times}(n,\overline{k}).$$

Now $M^{\times}(n,\overline{k})$ is certainly a group itself, and, by Lemma 6.E.2, part (4,b), so is $Im^{\times}(\Delta_{\Phi})\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right]$. Thus, at once by the above containments, and the definition of $\langle\mathcal{M}\rangle$ in the given, we have:

$$(4)\qquad \langle\mathcal{M}\rangle \subseteq Im^{\times}(\Delta_{\Phi})\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} G_h^{(m_h)} \cdot P_h\right] \subseteq M^{\times}(n,\overline{k}).$$

This proves the desired conclusion (2,a).

b) The desired conclusion in (2,b) follows immediately from (4), and Lemma 6.E.2, parts (4,b) and (4,d).

c) The desired conclusion in (2,c) follows at once from (4), from Lemma 6.E.2, part (4,c), and from elementary group theory (specifically, if $H, K_1, K_2$ are subgroups of $G$, and $K_1 \subseteq K_2 \rhd H$, then $HK_1/H \hookrightarrow HK_2/H$), and also from a repetition of part of the second part of the conclusion (2,b) just proved above.

□

**Theorem 6.F.2**

Let $n \in \mathbb{Z}^+$.

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a *reduced* field setting over $k$, with $\phi_i = (K_i, \sigma^{(i)}, a_i)$ a field element over $k$, and where $\dim \Phi = n$.

Let $u \equiv |\Phi/\!\sim_k| \in \{1, \ldots, r\}$, let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be a set of representatives of $\Phi/\!\sim_k$, let $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$, and let $m_h \equiv |[\phi_{i_h}]|$, $n_h \equiv n_{\phi_{i_h}} = [K_{i_h}\!: k]$.

Additionally, let $G_h \equiv \mathcal{G}a\ell(\phi_{i_h})$, and $P_h \equiv \mathrm{Perm}(a_{i_h} n_h m_h, I_{a_{i_h} n_h}, k)$.

Let $\mathcal{Z}_0 \equiv \Delta_\Phi \, (\Pi_{i=1}^{r} \mathrm{Scalar}(a_i, K_i))$.

Let $\mathcal{M} \subseteq \mathcal{N}_L(\mathcal{Z}_0) \subseteq M^\times(n, L)$, where $\mathcal{M}$ is $k$–rationalizable over $L$, by some $V \in V_\Phi^\times$.

Let $\langle \mathcal{M} \rangle \equiv$ the subgroup generated by $\mathcal{M}$ in $M^\times(n, L)$;

so also $\langle \mathcal{M} \rangle \subseteq M^\times(n, L)$.

**Then**:

1) a) $\mathcal{M} \subseteq Im^\times(\Delta_\Phi) \left[ \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \subseteq M^\times(n, \overline{k})$.

b) $Im^\times(\Delta_\Phi) \left[ \mathop{\bigcirc\!\!\!\!\!\!\triangle}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \subseteq M^\times(n, \overline{k})$ *does* normalize $\mathcal{Z}_0$, and is $k$–rationalizable by any $V \in V_\Phi^\times$.

2) $\quad \langle \mathcal{M} \rangle \subseteq Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \subseteq \mathcal{N}_{\bar{k}}(\mathcal{Z}_0) \subseteq M^{\times}(n, \bar{k}).$

I.e., $\mathcal{Z}_0$ possesses a greatest "$k$–rationalizable by some $V \in V_{\Phi}^{\times}$" normalizer in $M^{\times}(n, L)$, namely:

$$Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right].$$

3) $\quad$ a) $Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \approx \left[ \prod_{i=1}^{r} G\ell(a_i, K_i) \right] \rtimes \left[ \prod_{h=1}^{u} [Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}] \right];$

$$\text{and} \qquad \sum_{i=1}^{r} a_i [K_i : k] = \sum_{h=1}^{u} a_{i_h} [K_{i_h} : k] m_h = n, \ \sum_{h=1}^{u} m_h = r.$$

b) $\quad Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \rhd Im^{\times}(\Delta_{\Phi})$; and

$$Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \Big/ Im^{\times}(\Delta_{\Phi}) \approx \prod_{h=1}^{u} [Ga\ell(K_{i_h}/k)^{m_h} \rtimes S_{m_h}];$$

and $\sum_{h=1}^{u} a_{i_h} [K_{i_h} : k] m_h = n, \ \sum_{h=1}^{u} m_h = r.$

**Proof.**

By Lemma 2.D.1, part (b,i), we have:

$$(1) \qquad C_L(\mathcal{Z}_0) = \mathop{\triangle\kern-0.9em\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.$$

This, in Theorem 6.F.1, part (1,a) (with "$\mathcal{Z}$"$\equiv \mathcal{Z}_0$), gives the desired conclusion in (1,a) here, immediately. Also, by part (1,b) of that same theorem, we have:

$$(2) \qquad Im^{\times}(\Delta_{\Phi}) \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \text{ is } k\text{–rationalizable by any } V \in V_{\Phi}^{\times}.$$

Now, by Lemma 6.E.2, part (2,a), and the definition of $\mathcal{Z}_0$ in the given, we have:

$$(3) \qquad \left[ \mathop{\triangle\kern-0.9em\bigcirc}\limits_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \text{ normalizes } \mathcal{Z}_0.$$

Now clearly $Im^{\times}(\Delta_{\Phi}) \subseteq \bigotimes_{i=1}^{r} M^{\times}(a_i, \overline{k})^{(n_{\phi_i})}$, and so by (1): $Im^{\times}(\Delta_{\Phi}) \subseteq C_L(\mathcal{Z}_0)$. Thus, a fortiori:

$$(4) \qquad Im^{\times}(\Delta_{\Phi}) \text{ normalizes } \mathcal{Z}_0.$$

So, at once, by (3) and (4):

$$(5) \qquad Im^{\times}(\Delta_{\Phi}) \left[ \bigotimes_{h=1}^{u} G_h^{(m_h)} \cdot P_h \right] \text{ normalizes } \mathcal{Z}_0.$$

Together, (2) and (5) prove the desired conclusion in (1,b) here. The desired conclusion in (2) here follows at once using (1) in Theorem 6.F.1, part (2,a) (with "$\mathcal{Z}$"$\equiv \mathcal{Z}_0$), together with (5) above. The desired conclusions in (3) both follow, verbatim, from Lemma 6.E.2, parts (4,b), (4,c) and (4,d).

□

# Chapter 7

# Applications to Diagonalizable Matrix Subalgebras

## 7.1 Introduction

In this chapter, we apply many of our previous results to the study of the matrix subalgebras and subgroups of $M(n,k)$, $k$ a perfect field. The results here include some of the main results of this paper. In a sense, the results here form one of the sets of principal goal results that motivated this paper.

The main results here are classification in nature. They classify, and explicitly exhibit, some fundamental subalgebras and subgroups of $M(n,k)$, and their centralizers and normalizers in $M(n,k)$.

*Throughout this chapter, $k$ is a perfect field, and $L$ is any extension field of $\overline{k}$.*

## 7.2 Preliminary Lemmas

In this section we will frequently be using Theorem 3.B.1 — a key theorem, and one with a single conclusion statement. We will also very frequently be referring to the sets $V_\Phi$ — a set of matrices defined for a field setting $\Phi$, as described in Chapter 1, Section C, part (6). Finally, we will quite frequently be using Proposition App. 18, of the Appendix. It might be valuable to recall for oneself now those results and those definitions.

We introduce some notation that will make many statements from here on in easier to state.

**Definition**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

**We let:**

$$Im'(\Delta_\Phi) \equiv \Delta_\Phi\left(\prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i)\right) \subseteq M\left(n, \overline{k}\right).$$

Clearly, we note: $Im'(\Delta_\Phi) \subseteq D\left(n, \overline{k}\right)$, $Im'(\Delta_\Phi) \subseteq Im(\Delta_\Phi)$.

The following lemma summarizes the results concerning the centralizers and normalizers *over* $L$, of some of the key matrix subalgebras we have worked with.

**Lemma 7.B.1** (Key $L$-centralizers and $L$-normalizers)

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

Let $V \in V_{\Phi}^{\times}$.

**Then:**

1) a) $C_L\left(V Im'(\Delta_\Phi) V^{-1}\right) = V \left[\mathop{\triangle\hspace{-0.9em}\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$,

b) $C_L\left(V Im(\Delta_\Phi) V^{-1}\right) = V \left[\mathop{\triangle\hspace{-0.9em}\bigcirc}\limits_{i=1}^{r} \mathrm{Scalar}(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$;

2) a) $C_L^2\left(V Im'(\Delta_\Phi) V^{-1}\right) = V \left[\mathop{\triangle\hspace{-0.9em}\bigcirc}\limits_{i=1}^{r} \mathrm{Scalar}(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$,

b) $C_L^2\left(V Im(\Delta_\Phi) V^{-1}\right) = V \left[\mathop{\triangle\hspace{-0.9em}\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$;

3) a) $V Im'(\Delta_\Phi) V^{-1} \subseteq C_L\left(V Im(\Delta_\Phi) V^{-1}\right)$,

b) $V Im(\Delta_\Phi) V^{-1} \subseteq C_L\left(V Im'(\Delta_\Phi) V^{-1}\right)$;

4) If $\Phi$ is a *reduced* field setting and the subsequence $(\phi_i, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ is a set of representatives of $\Phi/\!\sim_k$ [and letting $[\phi_{i_h}]$ be the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$], then, furthermore:

$$\mathcal{N}_L\left(V Im'(\Delta_\Phi) V^{-1}\right) = V \left[\mathop{\triangle\hspace{-0.9em}\bigcirc}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}\right] \cdot$$

$$\left(\mathop{\triangle\hspace{-0.9em}\bigcirc}\limits_{h=1}^{u} Ga\ell(\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}\left(a_{i_h}[K_{i_h} : k]\,|[\phi_{i_h}]|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right) V^{-1}.$$

**Proof.**

1) By Lemma 2.D.1, parts (b,i) & (b,iii), we have:

$$(1) \qquad C_L\left(Im'(\Delta_\Phi)\right) = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})};$$

$$(2) \qquad C_L\left(Im(\Delta_\Phi)\right) = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \text{Scalar}(a_i, L)^{(n_{\phi_i})}.$$

Thus, the desired conclusions in (1,a) & (1,b) follow immediately.

2) By inductive use of Proposition App. 8 (with the fact that any field contains more than 1 element), and then a quick use of Proposition App. 9, we easily see:

(3)

$$C_L\left(\mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \text{Scalar}(a_i, L)^{(n_{\phi_i})}\right) = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \left[C_L(\text{Scalar}(a_i, L))\right]^{(n_{\phi_i})} = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})};$$

$$(4) \quad C_L\left(\mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right) = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \left[C_L(M(a_i, L))\right]^{(n_{\phi_i})} = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \text{Scalar}(a_i, L)^{(n_{\phi_i})}.$$

So, by (1) & (4):

$$\begin{aligned} C_L^2\left(Im'(\Delta_\Phi)\right) &= C_L\left(C_L\left(Im'(\Delta_\Phi)\right)\right) \\ &= C_L\left(\mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right) = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} \text{Scalar}(a_i, L)^{(n_{\phi_i})}. \end{aligned}$$

Similarly, by (2) & (3), we find $C_L^2(Im(\Delta_\Phi)) = \mathop{\textcircled{$\scriptstyle\triangle$}}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$. These last two results show the desired conclusions in (2,a) & (2,b).

3) Clearly, by the definitions of $Im'(\Delta_\Phi)$ & $Im(\Delta_\Phi)$, we have:

$$(5)\qquad Im'(\Delta_\Phi) \subseteq \mathop{\triangle\kern-0.85em\bigcirc}\limits_{i=1}^{r} \text{Scalar}(a_i, L)^{(n_{\phi_i})};$$

$$(6)\qquad Im'(\Delta_\Phi) \subseteq \mathop{\triangle\kern-0.85em\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.$$

From (2) & (5), we see the desired conclusion in (3,a) immediately. Similarly, (1) & (6) give conclusion (3,b).

4) Now suppose here, as in the desired conclusion (4), that $\Phi$ is a *reduced* field setting, and the subsequence $(\phi_i, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ is a set of representatives of $\Phi/\!\sim_k$ [with $[\phi_{i_h}]$ the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$]. Now let $N \in G\ell(n, L)$. By (1) above, and Lemma 8.C.4 (with "$\mathcal{Y}$" $\equiv Im'(\Delta_\Phi)$), we have:

$$(7)\qquad \begin{gathered} N \quad \text{normalizes} \quad Im'(\Delta_\Phi) \\ \Longleftrightarrow \\ N = C\Pi; \quad \text{for some} \\ C \in \mathop{\triangle\kern-0.85em\bigcirc}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}, \quad \text{and} \\ \Pi \in \text{Perm}(n, k), \ \text{ where } \Pi \text{ normalizes } Im'(\Delta_\Phi). \end{gathered}$$

I.e., we have:

$$(8)\qquad N_L\left(Im'(\Delta_\Phi)\right) = \left[\mathop{\triangle\kern-0.85em\bigcirc}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}\right] \cdot \mathcal{B},$$

where $\mathcal{B} \equiv \{\Pi \in \text{Perm}(n, k) \,|\, \Pi \text{ normalizes } Im'(\Delta_\Phi)\}$. We note, clearly:

$$(9)\qquad \mathcal{B} = N_L\left(Im'(\Delta_\Phi)\right) \cap \text{Perm}(n, k).$$

5) Now as $\Phi$ is reduced here, we may apply Theorem 6.B.2 (note there "$\mathcal{Y}_0$" $\equiv$ $Im'(\Delta_\Phi)$), with "$\mathcal{M}$" $\equiv \mathcal{B}$ (as $\mathcal{B} \subseteq \mathrm{Perm}(n,k)$, $\mathcal{B}$ is certainly $k$–rationalizable over $L$ — by $I_n$, and clearly $I_n \in V_\Phi^\times$). By conclusion (2,a) of that Theorem, with $m_k$, $G_k$, & $P_n$, as defined there, we have immediately that:

(11)

$$\langle\mathcal{B}\rangle \subseteq Im^\times(\Delta_\Phi)\underbrace{\left[\overset{u}{\underset{h=1}{\bigcircledtriangle}} \mathcal{G}a\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)}\cdot\mathrm{Perm}\left(a_{i_h}\left[K_{i_h}:k\right]|[\phi_{i_k}]|\,,I_{a_{i_h}[K_{i_h}:k]},k\right)\right]}_{\mathcal{G}}$$

$$\subseteq N_{\bar{k}}\left(Im'(\Delta_\Phi)\right).$$

I.e., more succinctly:

$$\langle\mathcal{B}\rangle \subseteq Im^\times(\Delta_\Phi)\cdot\mathcal{G} \subseteq N_{\bar{k}}\left(Im'(\Delta_\Phi)\right).$$

Thus, a fortiori:

$$\mathcal{B} \subseteq Im^\times(\Delta_\Phi)\cdot\mathcal{G} \subseteq N_L\left(Im'(\Delta_\Phi)\right).$$

Thus, in particular:

$$\mathcal{B} \cap \mathrm{Perm}(n,k) \subseteq \left[Im^\times(\Delta_\Phi)\cdot\mathcal{G}\right] \cap \mathrm{Perm}(n,k) \subseteq \mathcal{N}_L\left(Im'(\Delta_\Phi)\right) \cap \mathrm{Perm}(n,k).$$

Thus, as $\mathcal{B} \subseteq \mathrm{Perm}(n,k)$, and by (9), at once:

$$\mathcal{B} \subseteq \left[Im^\times(\Delta_\Phi)\cdot\mathcal{G}\right] \cap \mathrm{Perm}(n,k) \subseteq \mathcal{B}.$$

I.e.:

(12) $$\mathcal{B} = \left[Im^\times(\Delta_\Phi)\cdot\mathcal{G}\right] \cap \mathrm{Perm}(n,k).$$

Now, by definition of $\mathcal{G}$ in (11), clearly $\mathcal{G} \subseteq \mathrm{Perm}(n,k)$. So, as $\mathrm{Perm}(n,k)$ is a group, trivially we see: $[Im^{\times}(\Delta_{\Phi}) \cdot \mathcal{G}] \cap \mathrm{Perm}(n,k) = [Im^{\times}(\Delta_{\Phi}) \cap \mathrm{Perm}(n,k)] \cdot \mathcal{G}$. This, in (12), gives now:

$$\mathcal{B} = \left[Im^{\times}(\Delta_{\Phi}) \cap \mathrm{Perm}(n,k)\right] \cdot \mathcal{G}. \tag{13}$$

6) Now clearly by definition of $\Delta_{\Phi}$, we have: $Im^{\times}(\Delta_{\Phi}) \subseteq \mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}$. So, in particular, $Im^{\times}(\Delta_{\Phi}) \cap \mathrm{Perm}(n,k) \subseteq \mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}$. As $\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}$ is clearly a group, trivially we see:

$$\left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right] \cdot \left[Im^{\times}(\Delta_{\Phi}) \cap \mathrm{Perm}(n,k)\right] = \left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right].$$

This, with (8) & (13), shows, clearly:

$$\begin{aligned}
\mathcal{N}_L\left(Im'(\Delta_{\Phi})\right) &= \left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right] \cdot \mathcal{B} \\
&= \left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right] \cdot \left([Im^{\times}(\Delta_{\Phi}) \cap \mathrm{Perm}(n,k)] \cdot \mathcal{G}\right) \\
&= \left(\left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right] \cdot \left([Im^{\times}(\Delta_{\Phi}) \cap \mathrm{Perm}(n,k)]\right)\right) \cdot \mathcal{G} \\
&= \left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right] \cdot \mathcal{G}.
\end{aligned}$$

I.e.:

$$\mathcal{N}_L\left(Im'(\Delta_{\Phi})\right) = \left[\mathop{\bigcirc\hspace{-0.85em}\triangle}\limits_{i=1}^{r} G\ell(a_i,L)^{(n_{\phi_i})}\right] \cdot \mathcal{G}. \tag{14}$$

With the definition of $\mathcal{G}$ in (11), and using the fact that $V \in V_{\Phi}^{\times} \subseteq G\ell(n,L)$, the desired conclusion in (4) follows immediately from (14) above. $\square$

The following lemma summarizes the results concerning the centralizers and normalizers *over* $k$, of some of the key matrix subalgebras we have worked with.

**Lemma 7.B.2** (Key $k$–centralizers and $k$–normalizers)

Let $\Phi = (\phi_1, \dots \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

Let $V \in V_\Phi^\times$.

**Then:**

1) $VIm'(\Delta_\Phi)V^{-1} \subseteq VIm(\Delta_\Phi)V^{-1} \subseteq M(n,k)$;

i.e., $V$ $k$–rationalizes $Im'(\Delta_\Phi)$, and $Im(\Delta_\Phi)$.

2) a) $C_k\left(VIm'(\Delta_\Phi)V^{-1}\right) = VIm(\Delta_\Phi)V^{-1}$;

b) $C_k\left(VIm(\Delta_\Phi)V^{-1}\right) = VIm'(\Delta_\Phi)V^{-1}$.

3) a) $C_k^2\left(VIm'(\Delta_\Phi)V^{-1}\right) = VIm'(\Delta_\Phi)V^{-1}$;

b) $C_k^2\left(VIm(\Delta_\Phi)V^{-1}\right) = VIm(\Delta_\Phi)V^{-1}$.

4) If $\Phi$ is a *reduced* field setting and the subsequence $(\phi_{i}, \dots, \phi_{i_u}) \subseteq (\phi_1, \dots, \phi_r)$ is a set of representatives of $\Phi/\!\sim_k$ [and letting $[\phi_{i_h}]$ be the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$], then, furthermore:

$$\mathcal{N}_k\left(VIm'(\Delta_\Phi)V^{-1}\right) = V\left[\Delta_\Phi\left(\prod_{i=1}^{r} G\ell(a_i, K_i)\right)\right] \cdot$$

$$\left[\mathop{\bigcirc\!\!\!\!\!\triangle}_{h=1}^{u} Ga\ell\left(\phi_{i_h}\right)^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}\left(a_{i_h}\left[K_{i_h} : k\right]\left|[\phi_{i_h}]\right|, I_{a_{i_h}\left[K_{i_h}:k\right]}, k\right)\right] V^{-1}.$$

**Proof.**

1) By definition of $Im'(\Delta_\Phi)$, we clearly have $Im'(\Delta_\Phi) \subseteq Im(\Delta_\Phi)$, and so:

$$VIm'(\Delta_\Phi)V^{-1} \subseteq UIm(\Delta_\Phi)U^{-1}.$$

Now by Theorem 3.B.1 (with "$\mathcal{Y}$"$= Im(\Delta_\Phi)), (E)$, we ahve at once that $Uk -$ rationalizes $Im(\Delta_\Phi)$ - i.e., $UIm(\Delta_\Phi U^{-1} \subseteq M(n,k)$. This, with the above result gives:

$$UIm'(\Delta_\Phi)U^{-1} \subseteq UIm(\Delta_\Phi)U^{-1} \subseteq M(n,k).$$

This proves the desired conclusion (1).

2) To prove the desired conclusion (2,a), we make the trivial observation that:

$$C_k(VIm'(\Delta_\Phi)V^{-1}) = C_L(VIm'(\Delta_\Phi)V^{-1}) \cap M(n,k).$$

Thus, by Lemma 7.B.1, part (1,a), we now have:

$$C_k(VIm'(\Delta_\Phi)V^{-1}) = V\left[\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})}\right]V^{-1} \cap M(n,k).$$

Hence:

$$\begin{aligned}
&B \in C_k(VIm'(\Delta_\Phi)V^{-1}) \Leftrightarrow \\
&B \in V\left[\mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})}\right]V^{-1} \text{ and } B \in M(n,k) \Leftrightarrow \\
&V^{-1}BV \in \mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})} \text{ and } V(V^{-1}BV)V^{-1} \in M(n,k) \Leftrightarrow \\
&V^{-1}BV \in \mathop{\bigcirc\kern-0.78em\triangle}_{i=1}^{r} M(a_i,L)^{(n_{\phi_i})} \text{ and } Vk - - \text{ rationalizes } V^{-1}BV \Leftrightarrow \\
&V^{-1}BV \in Im(\Delta_\Phi).
\end{aligned}$$

where the last, and critical, result follows at once by Theorem 3.B.1 (with "$\mathcal{Y}$"$\equiv$ $\{V^{-1}BV\}$) [and with noting the obvsious fact that $Im(\Delta_\Phi) \subseteq \mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$].

The previous thus shows:

$$B \in C_K(VIm'(\Delta_\Phi)V^{-1}) \Leftrightarrow B \in VIm(\Delta_\Phi)V^{-1}.$$

I.e.,

$$C_k(VIm'(\Delta_\Phi)V^{-1}) = VIm(\Delta_\Phi)V^{-1}.$$

This proves the desired conclusion (2,a).

3) To prove the desired conclusion (2,b), we again start with the trivial observations:

$$C_K(VIm(\Delta_\Phi)V^{-1}) = C_L(VIm(\Delta_\Phi)V^{-1}) \cap M(n,k).$$

Again, using here 7.B.1, but now part (1,b), we now have:

$$C_K(VIm(\Delta_\Phi)V^{-1}) = V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{Scalar } (a_i, L)^{(n_{\phi_i})}\right] V^{-1} \cap M(n,k).$$

Hence:

$$\begin{aligned}
&B \in C_K(VIm(\Delta_\Phi)V^{-1}) \Leftrightarrow \\
&B \in V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{Scalar } (a_i, L)^{(n_{\phi_i})}\right] V^{-1} \text{ and } B \in M(n,k) \Leftrightarrow \\
&V^{-1}BV \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{Scalar } (a_i, L)^{(n_{\phi_i})} \text{ and } V(V^{1}BV)V^{-1} \in M(n,k) \Leftrightarrow \\
&V^{-1}BV \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{Scalar } (a_i, L)^{(n_{\phi_i})} \text{ and } Vk -- \text{ rationalizes } V^{-1}BV.
\end{aligned}$$

As $\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{Scalar } (a_i, L)^{(n_{\phi_i})} \subseteq \mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$, we can argue as with part (2) above, and thus continue the above chain of equivalences as:

$$B \in C_k(VIm(\Delta_\Phi)V^{-1}) \Leftrightarrow$$

$$V^{-1}BV \in \mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})} \text{ and } V^{-1}BV \in Im(\Delta_\Phi).$$

Therefore,

$$(1)\quad B \in C_k(VIm(\Delta_\Phi)V^{-1}) \Leftrightarrow V^{-1}BV \in Im(\Delta_\Phi) \cap \left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})}\right].$$

4) Now suppose $V^{-1}BV \in Im(\Delta_\Phi) \cap \left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})}\right]$. Thus:

$$(2)\quad V^{-1}BV = \Delta_\Phi(M_1, \ldots, M_r) = \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \sigma_j^{(i)}(M_i); \text{ for some } M_i \in M(a_i, K_i);$$

and

$$V^{-1}BV = \mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathop{\textcircled{$\triangle$}}_{j=1}^{n_{\phi_i}} \lambda_{i,j} I_{a_i}; \text{ for some } \lambda_{i,j} \in L.$$

Equating these two results for $V^{-1}BV$, we read off at once [trivially checking (noting) that both $\sigma_j^{(i)}(M_i)$ and $\lambda_{i,j}I_{a_i}$ are matrices of the same dimension — $a_i \times a_i$]:

$$(3)\qquad \sigma_j^{(i)}(M_i) = \lambda_{i,j} I_{a_i}; \text{ for all } i, j.$$

By (2), we have $M_i \in M(a_i, K_i)$, and so now (3) shows that $\lambda_{i,j} \in \sigma_j^{(i)}(K_i)$. I.e., we have $\lambda_{i,j} = \sigma_j^{(i)}(\alpha_i)$, for some $\alpha_i \in K_i$. Putting this back into (3), we find:

$$\sigma_j^{(i)}(M_i) = \sigma_j^{(i)}(\alpha_i) I_{a_i}; \alpha_i \in K_i$$

$$\sigma_j^{(i)}(M_i) = \sigma_j^{(i)}(\alpha_i I_{a_i}); \alpha_i \in K_i.$$

As $\sigma_j^{(i)}$ is an imbedding, and so a fortiori is injective, the last equation above gives now:

$$M_i = \alpha_i I_{a_i}; \alpha_i \in K_i$$

$$M_i \in \text{ Scalar } (a_i \in K_i).$$

Thus, by (2):

$$V^{-1}BV = \Delta_\Phi(M_1, \ldots, M_r) \in \Delta_\Phi\,(\Pi_{i=1}^{r} \text{ Scalar } (a_i, K_i)) \equiv Im'(\Delta_\Phi).$$

Therefore

$$V^{-1}BV \in Im'(\Delta_\Phi).$$

And, hence, by supposition here, we conclude:

$$Im(\Delta_\Phi) \cap \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})}\right] \subseteq Im'(\Delta_\Phi). \tag{4}$$

5) As certainly $Im'(\Delta_\Phi) \subseteq Im(\Delta_\Phi)_r$ and clearly $Im'(\Delta_\Phi) \subseteq \mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r}$ Scalar $(a_i, L)^{(n_{\phi_i})}$, we obviously have:

$$Im'(\Delta_\Phi) \subseteq Im(\Delta_\Phi) \cap \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})}\right].$$

Combining this with (4), we have:

$$Im(\Delta_\Phi) \cap \left[\mathop{\bigcirc\!\!\!\!\!\triangle}\limits_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})}\right] = Im'(\Delta_\Phi).$$

Combining this with (1), we have:

$$B \in C_k(VIm(\Delta_\Phi)V^{-1}) \Leftrightarrow V^{-1}BV \in Im'(\Delta_\Phi).$$

$$B \in C_k(VIm(\Delta_\Phi)V^{-1}) \Leftrightarrow BV \in Im'(\Delta_\Phi)V^{-1}.$$

I.e.,

$$C_k(VIm(\Delta_\Phi)V^{-1}) = V \in Im'(\Delta_\Phi)V^{-1}.$$

This proves the desired conclusion (2,b).

6) The desired conclusion in (3,a)&(3,b) follow at once from those of (2,a)&(2,b), as follows:

$$\begin{aligned} C_k^2(VIm'(\Delta_\Phi)V^{-1}) &= C_k\left(C_k(VIm'(\Delta_\Phi)V^{-1})\right) \\ &= C_k\left(VIm(\Delta_\Phi)V^{-1}\right);\ \text{by } (2,a) \\ &= VIm'(\Delta_\Phi)V^{-1};\ \text{by } (2,b). \end{aligned}$$

Similarly for $C_k^2(VIm(\Delta_\Phi)V^{-1})$.

7) Now suppose here, as in the desired conclusion (4), that $\Phi$ is a *reduced* field setting, and the subsequence $(\phi_i,\ldots,\phi_{i_u}) \subseteq (\phi_1,\ldots,\phi_r)$ is a set of representatives of $\Phi/\sim_k$ [with $[\phi_{i_h}]$ the equivalence class of $\Phi/\sim_k$]. Now let:

$$\mathcal{N} \equiv \mathcal{N}_k(VIm'(\Delta_\Phi)V^{-1}) \subseteq G\ell(n,k); \tag{5}$$

$$\mathcal{M} \equiv V^{-1}\mathcal{N}V \subseteq G\ell\left(n,\overline{k}\right) \subseteq G\ell(n,L). \tag{6}$$

So clearly we note (using $V \in G\ell\left(n,\overline{k}\right) \subseteq G\ell(n,L)$):

$$\begin{aligned} \mathcal{M} = V^{-1}\mathcal{N}V &= V^{-1}\mathcal{N}_k(VIm'(\Delta_\Phi)V^{-1})V \subseteq V^{-1}\mathcal{N}_L(VIm'(\Delta_\Phi)V^{-1})V \\ &= \mathcal{N}_L(V^{-1}VIm'(\Delta_\Phi)V^{-1}V) = \mathcal{N}_L(Im'(\Delta_\Phi)). \end{aligned}$$

Additively, we clearly note:

$$V\mathcal{M}V^{-1} = \mathcal{N} \subseteq M(n,k).$$

Summarizing the above two notes, we have:

(7) $\mathcal{M} \subseteq \mathcal{N}_L(Im'(\Delta_\Phi))$, $V$ $k$-rationalizes $\mathcal{M}$ and $V \in V_\Phi^\times$.

Now as $\Phi$ is reduced here, we may apply Theorem 8.b.2. to (7) (note there "$\mathcal{Z}_0$"$\equiv$ $Im'(\Delta_\Phi)$). By conclusion (2,a) and (1,b) of that Theorem, as applied to (7), and with $m_k, G_k \& P_k$ as defined in that Theorem, we have immediately that:

(8)

$$\langle \mathcal{M} \rangle \subseteq Im^\times(\Delta_\Phi) \underbrace{\left[ \mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u} G\ell(\phi_{i_h})^{(\|[\phi_{i_h}]\|)} \cdot \mathrm{Perm}(a_{i_h}[K_{i_h}\colon k] \| [\phi_{i_h}] \|, I_{a_{i_h}[K_{i_h}:k]}, k) \right]}_{\mathcal{G}}$$

$$\subseteq \mathcal{N}_{\overline{k}}(Im'(\Delta_\Phi));$$

(9) $Im^\times(\Delta_\Phi) \cdot \mathcal{G}$ is k-rationalizable by $V$.

Rewriting (8), we have:

$$\langle \mathcal{M} \rangle \subseteq Im^\times(\Delta_\Phi) \cdot \mathcal{G} \subseteq \mathcal{N}_{\overline{k}}(Im'(\Delta_\Phi)) \subseteq G\ell\left(n, \overline{k}\right).$$

As $V \in V_\Phi^\times \subseteq G\ell\left(n, \overline{k}\right)$, we have:

$$V \langle \mathcal{M} V^{-1} \subseteq V(Im^\times(\Delta_\Phi) \cdot \mathcal{G})U^{-1} \subseteq \mathcal{N}_{\overline{k}}(Im'(\Delta_\Phi)) \subseteq G\ell\left(n, \overline{k}\right).$$

Again, using $V \in G\ell\left(n, \overline{k}\right)$, we have now:

$$V \langle \mathcal{M} V^{-1} \subseteq V(Im^\times(\Delta_\Phi) \cdot \mathcal{G})U^{-1} \subseteq \mathcal{N}_{\overline{k}}(V Im'(\Delta_\Phi)) \subseteq G\ell\left(n, \overline{k}\right).$$

By (6) we have $V\mathcal{M}V^{-1} = \mathcal{N}$, and by (5) we have that $\mathcal{N}$ is already a subgroup, and so the previous gives:

$$\mathcal{N} \subseteq V(Im^{\times}(\Delta_{\Phi}) \cdot \mathcal{G})V^{-1} \subseteq \mathcal{N}_{\overline{k}}(V Im'(\Delta_{\Phi})V^{-1}) \subseteq G\ell\left(n, \overline{k}\right).$$

So, certainly:

$$\begin{aligned} &\mathcal{N} \cap M(n,k) \subseteq [V(Im^{\times}(\Delta_{\Phi}) \cdot \mathcal{G})V^{-1}] \cap M(n,k) \subseteq \\ &\mathcal{N}_{\overline{k}}(V Im'(\Delta_{\Phi})V^{-1}) \cap M(n,k) \subseteq G\ell(n,k). \end{aligned} \tag{10}$$

Now by (5) we certainly have $\mathcal{N} \subseteq M(n,k)$, by (9) we have $V(Im^{\times}(\Delta_{\Phi}) \cdot \mathcal{G})V^{-1} \subseteq M(n,k)$, and clearly (with (5)) we have $\mathcal{N}_{\overline{k}}(V Im'(\Delta_{\Phi})V^{-1}) \cap M(n,k) = \mathcal{N}_k(V Im'(\Delta_{\Phi})V^{-1}) = \mathcal{N}$. Using these in (10), we now have:

$$\mathcal{N} \subseteq V(Im^{\times}(\Delta_{\Phi}) \cdot \mathcal{G})V^{-1} \subseteq \mathcal{N} \subseteq G\ell(n,k).$$

Therefore,

$$\mathcal{N} = V(Im^{\times}(\Delta_{\Phi}) \cdot \mathcal{G})V^{-1}. \tag{11}$$

With the definitions of $\mathcal{N}$ in (5) and of $\mathcal{G}$ in (8), and trivially noting (as $\Delta_{\Phi}$ is an imbedding of k-algebras) that

$$Im^{\times}(\Delta_{\Phi}) \equiv [\Delta_{\Phi}(\Pi_{i=1}^{r} M(a_i, K_i))]^{\times} = \Delta_{\Phi}(\Pi_{i=1}^{r} G\ell(a_i, K_i)),$$

the desired conclusion in (4) of this Lemma follows immediately from (11) above.

□

The following lemma summarizes *connections* between the centralizers *over* $k$ and the centralizers *over* $L$, and between the normalizers *over* $k$ and the normalizers *over* $L$, of a key class of subsets of matrices with which we have been working.

**Lemma 7.B.3**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

Let $V \in V_\Phi^\times$.

Suppose $\mathcal{A} \subseteq VIm'(\Delta_\Phi)V^{-1} \subseteq M\left(\dim\Phi, \overline{k}\right)$.

**Then:**

1) $\mathcal{A} \subseteq M(\dim\Phi, k)$.

2) The following four statements are equivalent:

   a) $C_k^2(\mathcal{A}) = VIm'(\Delta_\Phi)V^{-1}$;

   b) $C_k(\mathcal{A}) = VIm(\Delta_\Phi)V^{-1}$;

   c) $C_L^2(\mathcal{A}) = V\left[\mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r} \mathrm{Scalar}(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$;

   d) $C_L(\mathcal{A}) = V\left[\mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$.

3) If $\Phi$ is a *reduced* field setting and the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ is a set of representatives of $\Phi/\!\sim_k$ [and letting $[\phi_{i_h}]$ be the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$], then, furthermore:

any of the four equivalent statements in (2) above $\Longrightarrow$

$$\text{a) } \mathcal{N}_k(\mathcal{A}) \subseteq V\left[\Delta_\Phi\left(\prod_{i=1}^{r} G\ell(a_i, K_i)\right)\right] \cdot$$

$$\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(\|[\phi_{i_h}]\|)} \cdot \mathrm{Perm}\left(a_{i_h}\,[K_{i_h} : k]\,\|[\phi_{i_h}]\|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right] V^{-1};$$

$$\text{b) } \mathcal{N}_L(\mathcal{A}) \subseteq V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}\right] \cdot$$

$$\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(\|[\phi_{i_h}]\|)} \cdot \mathrm{Perm}\left(a_{i_h}\,[K_{i_h} : k]\,\|[\phi_{i_h}]\|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right] V^{-1}.$$

**Proof.**

1) The desired conclusion in (1) here follows at once from Lemma 7.B.2, conclusion (1).

2) We will establish the desired conclusion in (2) here by means of the following logical sequences:

$$(a) \Longleftrightarrow (b), \quad (c) \Longleftrightarrow (d), \quad (d) \Longleftrightarrow (b).$$

i) $(a) \Longrightarrow (b)$

So suppose: $C_k^2(\mathcal{A}) = VIm'(\Delta_\Phi)V^{-1}$. Now, using Proposition App. 18, part (3), of the Appendix, and then Lemma 7.B.2, part (2,a), we calculate easily:

$$\begin{aligned} C_k(\mathcal{A}) &= C_k^3(\mathcal{A}) = C_k(C_k^2(\mathcal{A})) \\ &= C_k(VIm'(\Delta_\Phi)V^{-1}) = VIm(\Delta_\Phi)V^{-1}. \end{aligned}$$

ii) $(b) \Longrightarrow (a)$

So, suppose: $C_k(\mathcal{A}) = VIm(\Delta_\Phi)V^{-1}$. Now, using Lemma 7.B.2, part (2,b), we calculate at once:

$$C_k^2(\mathcal{A}) = C_k(C_k(\mathcal{A})) = C_k(VIm(\Delta_\Phi)V^{-1}) = VIm'(\Delta_\Phi)V^{-1}.$$

iii) $(c) \Longrightarrow (d)$

So, suppose: $C_L^2(\mathcal{A}) = V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} \text{ Scalar } (a_i, L)^{(n_{\phi_i})}\right]V^{-1}$. Now, by Lemma 7.B.1, part (2,a), we thus have:

$$C_L^2(\mathcal{A}) = C_L^2(VIm'(\Delta_\Phi)V^{-1}).$$

Therefore: $$C_L^2(\mathcal{A}) = C_L(C_L^2(VIm'(\Delta_\Phi)V^{-1}).$$

Therefore: $$C_L^3(\mathcal{A}) = C_L^3(VIm'(\Delta_\Phi)V^{-1}).$$

Thus, by Proposition App. 18, part (3), of the Appendix:

$$C_L(\mathcal{A}) = C_L(VIm'(\Delta_\Phi)V^{-1}).$$

Hence, by Lemma 7.B.1, part (1,a), we have:

$$C_L(\mathcal{A}) = V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]V^{-1}.$$

iv) $(d) \Longrightarrow (c)$

So, suppose: $C_L^2(\mathcal{A}) = V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]V^{-1}$. Now, by Lemma 7.B.1, part (1,a), we thus have:

$$C_L(\mathcal{A}) = C_L(VIm'(\Delta_\Phi)V^{-1}).$$

Therefore: $$C_L(C_L(\mathcal{A})) = C_L(C_L(VIm'(\Delta_\Phi)V^{-1})).$$

Therefore: $$C_L^2(\mathcal{A}) = C_L^2(VIm'(\Delta_\Phi)V^{-1}).$$

Hence, by Lemma 7.B.1, part (2,a), we have:

$$C_L^2(\mathcal{A}) = V\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{r} \text{Scalar } (a_i, L)^{(n_{\phi_i})}\right] V^{-1}.$$

v) $(d) \Longrightarrow (b)$

So, suppose: $C_L(\mathcal{A}) = V\left[\mathop{\bigcirc\!\!\!\!\!\!\triangle}_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right] V^{-1}$. Now, by Lemma 7.B.1, part (1,a), we thus have:

$$C_L(\mathcal{A}) = C_L(VIm'(\Delta_\Phi)V^{-1}).$$

Therefore: $C_L(\mathcal{A}) \cap M(n,k) = C_L(VIm'(\Delta_\Phi)V^{-1}) \cap M(n,k)$.

Now, using the trivial but useful observation that $C_L(\mathcal{X}) \cap M(n,k) = C_k(\mathcal{X})$, for any $\mathcal{X} \subseteq M(n,k)$, the previous result simplifies at once to give:

$$C_k(\mathcal{A}) = C_k(VIm'(\Delta_\Phi)V^{-1}).$$

Hence, by Lemma 7.B.2, part (2,a), we have:

$$C_k(\mathcal{A}) = VIm(\Delta_\Phi)V^{-1}.$$

vi) $(b) \Longrightarrow (d)$

So, suppose: $C_k(\mathcal{A}) = VIm(\Delta_\Phi)V^{-1}$. Now, by Lemma 7.B.2, parts (1) & (2,a), we thus have:

$$VIm'(\Delta_\Phi)V^{-1} \subseteq M(n,k) \text{ and } C_k(\mathcal{A}) = C_k(VIm'(\Delta_\Phi)V^{-1}).$$

Hence, immediately, by Proposition App. 19 of the Appendix, we have:

$$C_L(\mathcal{A}) = C_L(VIm'(\Delta_\Phi)V^{-1}).$$

And so, by Lemma 7.B.1, part (1,a), we have at once

$$C_L(\mathcal{A}) = V\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]V^{-1}.$$

3) To prove the desired conclusions in (3), we take, as there, that $\Phi$ is a *reduced* field setting with the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ a set of representatives of $\Phi/\sim_k$, and we suppose that any of the four equivalent statements in conclusion (2) here is true. These four statements being equivalent, we conclude, in particular, that statement (2,d) is true. Thus, we have:

$$C_L(\mathcal{A}) = V\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]V^{-1}. \tag{1}$$

To prove the conclusion in (3,a), we see that with $\Phi$ as above, and with (1), and for convenience letting $u \equiv \dim\Phi$, we may apply Theorem 6.B.1, directly, with $\mathcal{Z} \equiv V^{-1}\mathcal{A}V$ and with $\mathcal{M} \equiv V^{-1}\mathcal{N}_k(\mathcal{A})V$. (We easily check, by the given on $\mathcal{A}$, that $\mathcal{Z} \subseteq Im'(\Delta_\Phi)$, and that $\mathcal{M}$ is certainly $k$–rationalizable over $L$ by $V \in V_\Phi^\times$, and that clearly $\mathcal{M} \equiv V^{-1}\mathcal{N}_k(\mathcal{A})V \subseteq V^{-1}\mathcal{N}_L(\mathcal{A})V = \mathcal{N}_L(V^{-1}\mathcal{A}V) = \mathcal{N}_L(\mathcal{Z}) \subseteq M^\times(n, L)$. Here, at once, by conclusion (1,a) of that Theorem, and with $M_h, G_h \& P_h$ as defined in that Theorem, we have immediately that:

$$\mathcal{M} \subseteq Im^\times(\Delta_\Phi)\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} \mathcal{G}a\ell\,(\phi_{i_h})^{|[\phi_{i_h}]|} \cdot \mathrm{Perm}(a_{i_h}[K_{i_h}\!:k]|, I_{a_{i_h}l[K_{i_h}:k]}, k)\right].$$

Finally, replacing $\mathcal{M}$ in the previous with its definition, $\mathcal{M} \equiv V^{-1}\mathcal{N}_k(\mathcal{A})V$, we immediately have the desired conclusion in (3,a).

To prove the conclusion in (3,b), we will need here to refer only to much earlier results — Lemma 6.C.4 and Theorem 6.E.1. (Actually, this present result could have been extracted back then, but we didn't need it there.) We first note that by Lemma 6.C.4 (with "$\mathcal{Y}$"$\equiv \mathcal{Z} = V^{-1}(\mathcal{A})V \subseteq Im'(\Delta_\Phi) \subseteq D(n, L)$), we have (starting things more compactly here):

$$(2) \qquad \mathcal{N}_L(\mathcal{Z}) = C_L^\times(\mathcal{Z}) \cdot (\mathcal{N}_L(\mathcal{Z}) \cap \mathrm{Perm}(n,k)).$$

Now, with $\Phi$ as above, and with (1) and the definition of $\mathcal{Z}$ above, we may apply Theorem 6.E.1, directly, and with $M_h$ as defined in that Theorem, we conclude at once (again, stating things more compactly here):

$$(3) \qquad \begin{aligned} &\mathcal{N}_L(\mathcal{Z}) \cap \mathrm{Perm}(n,k) \subseteq \left[\mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}\right] \cdot \\ &\left[\mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \mathcal{G}a\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}(a_{i_h}[K_{i_h}\colon k]|[\phi_{i_h}]|, I_{a_{i_h}[K_{i_h}:k]}, k)\right]. \end{aligned}$$

Combining (2) & (3), we have:

$$(4) \qquad \begin{aligned} &\mathcal{N}_L(\mathcal{Z}) \subseteq C_L^\times(\mathcal{Z}) \cdot \left[\mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}\right] \cdot \\ &\left[\mathop{\triangle\!\!\!\!\bigcirc}\limits_{h=1}^{u} \mathcal{G}a\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}(a_{i_h}[K_{i_h}\colon k]|[\phi_{i_h}]|, I_{a_{i_h}[K_{i_h}:k]}, k)\right]. \end{aligned}$$

Now from (1), and the definition of $\mathcal{Z} \equiv V^{-1}(\mathcal{A})V$, we have :

$$C_L(\mathcal{Z}) = C_L(V^{-1}\mathcal{A}V) = V^{-1}C_L(\mathcal{A})V = \mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}.$$

Hence:

$$(5) \qquad C_L^\times(\mathcal{Z}) = \mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}.$$

Furthermore, we see from (5) that $\mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}$ is a subgroup of $C_L^\times(\mathcal{Z})$.

Hence:

$$(6) \qquad C_L^\times(\mathcal{Z}) \cdot \left[\mathop{\triangle\!\!\!\!\bigcirc}\limits_{i=1}^{r} \mathrm{Perm}(a_i,k)^{(n_{\phi_i})}\right] = C_L^\times(\mathcal{Z}).$$

Thus, putting (6) into (4), and using (5), we conclude at once:

(7)

$$\mathcal{N}_L(\mathcal{Z}) \subseteq \left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r} G\ell(a_i, k)^{(n_{\phi_i})}\right] \cdot$$

$$\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}(a_{i_h}[K_{i_h}\colon k]|[\phi_{i_h}]|, I_{a_{i_h}[K_{i_h}:k]}, k)\right].$$

Finally, using $\mathcal{Z} \equiv V^{-1}\mathcal{A}V$, and so $\mathcal{N}_L(\mathcal{Z}) = V^{-1}\mathcal{N}_L(\mathcal{A})V$, the above result in (7) gives us at once the desired conclusion in (3,b). This completes the proof of the conclusions in (3).

□

The following Lemma summarizes, in one place, basic results about field settings in general. Some of these results have been recorded in various earlier places. We will frequently refer to this Lemma because it has all these basic results in once place.

**Lemma 7.B.4**

Let $\Phi = (\phi_1, \ldots, \phi_r)$ be a field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ a field element over $k$.

Let $u \equiv |\Phi/\sim_k| \in \{1, \ldots, r\}$.

Let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be any set of representatives of $\Phi/\sim_k$, with $[\phi_{i_h}] \equiv$ the equivalence class of $\phi_{i_h}$ in $\Phi/\sim_k$ .

Let $\mathcal{Y} \subseteq Im'(\Delta_{\Phi})$, where $C_L(\mathcal{Y}) = \mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$.

**Then:**

1) a) $\sum\limits_{h=1}^{u} a_{i_h}\,[K_{i_h} : k]\,|[\phi_{i_h}]| = \sum\limits_{i=1}^{r} a_i[K_i : k] = \dim \Phi$;

b) $\sum\limits_{h=1}^{u} |[\phi_{i_h}]| = r$.

2) a) $\Delta_{\Phi}\left(\prod\limits_{i=1}^{r} \mathrm{Scalar}(a_i, K_i)\right) \approx \prod\limits_{i=1}^{r} K_i$;

b) $\Delta_{\Phi}\left(\prod\limits_{i=1}^{r} M(a_i, K_i)\right) \approx \prod\limits_{i=1}^{r} M(a_i, K_i)$;

c) If $\Phi$ is a *reduced* field setting, then:

i) $\Delta_{\Phi}\left(\prod\limits_{i=1}^{r} G\ell(a_i, K_i)\right) \cdot$

$$\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}\left(a_{i_k}\,[K_{i_h} : k]\,|[\phi_{i_h}]|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right]$$

$$\approx \left[\prod_{i=1}^{r} G\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u} \left[Ga\ell\,(K_{i_h}/k)^{|[\phi_{i_h}]|} \rtimes S_{|[\phi_{i_h}]|}\right]\right],$$

ii) $\Delta_{\Phi}\left(\prod\limits_{i=1}^{r} G\ell(a_i, K_i)\right) \cdot$

$$\frac{\left[\mathop{\bigcirc\hspace{-0.75em}\triangle}\limits_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm}\left(a_{i_k}\,[K_{i_h} : k]\,|[\phi_{i_h}]|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right]}{\Delta_{\Phi}\left(\prod\limits_{i=1}^{r} G\ell(a_i, K_i)\right)}$$

$$\approx \prod_{h=1}^{u} \left[Ga\ell\,(K_{i_h}/k)^{|[\phi_{i_h}]|} \rtimes S_{|[\phi_{i_h}]|}\right].$$

3) As given $\mathcal{Y} \subseteq Im'(\Delta_\Phi)$, so we see $\mathcal{Y}$ is a set of diagonal matrices.

   Then, using the 3-tuple index notation, $\mathcal{I}_\Phi$, for $\Phi$, we have:

$$\forall (i,j,t) \in \mathcal{I}_\Phi: \quad k\left(\left\{Y_{(i,j,t)} \middle| Y \in \mathcal{Y}\right\}\right) = \sigma_j^{(i)}(K_i).$$

4) Suppose: $\quad Q \in G\ell(n,L) \quad$ and $\quad Q$ $k$–rationalizes $\mathcal{Y}$.

   Then we have:

   a) $Q$ actually $k$–rationalizes all of $Im'(\Delta_\Phi)$, even all of $Im(\Delta_\Phi)$.

   b) $Q$ may be "point-wise replaced" by some $V \in V_\Phi^\times$:

$$\exists V \in V_\Phi^\times : \forall Z \in Im'(\Delta_\Phi): \quad QZQ^{-1} = VZV^{-1}.$$

$$\text{I.e.:} \quad conj_{Q^{-1}} | Im'(\Delta_\Phi) = conj_{V^{-1}} | Im'(\Delta_\Phi);$$

$$\text{in particular,} \quad QIm'(\Delta_\Phi)Q^{-1} = VIm'(\Delta_\Phi)V^{-1}.$$

**Proof.**

1) The conclusions in (1) follow at once from the given, by Lemma 6.B.2, parts (3)&(2), and with the definition of dim$\Phi$.

2) The conclusions in (2,a) & (2,b) follow at once from the fact that $\Delta_\Phi$ is an imbedding of $k$–algebras, and that, clearly, Scalar$(a_i, K_i) \approx K_i$.

3) The conclusions in (2,c) follow at once from Lemma 6.F.2, parts (4,b)&(4,c); noting, clearly, that $Im^\times(\Delta_\Phi) = \left(\Delta_\Phi\left(\Pi_{i=1}^r M(a_i,K_i)\right)\right)^\times = \Delta_\Phi\left(\Pi_{i=1}^r G\ell(a_i,K_i)\right)$, as $\Delta_\Phi$ is an imbedding of $k$–algebras.

4) The conclusion in (3) follows immediately from the given (esp., the given on $\mathcal{Y}$), by Lemma 4.B.3 (there, with "$\mathcal{Z}$"$\equiv \mathcal{Y}$).

5) The conclusions in (4) follow as follows. As, by supposition here, $Q$ $k$–rationalizes $\mathcal{Y}$, and as, by the given on $\mathcal{Y}$, $C_L(\mathcal{Y}) = C_L(Im'(\Delta_\Phi)) = \bigotimes_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}$, we may apply the much earlier Corollary 2.E.2, part (a), at once (with "$\mathcal{Z}$"$\equiv Im'(\Delta_\Phi)$, "$P$"$\equiv Q$), and we find: $Q$ $k$–rationalizes $Im'(\Delta_\Phi)$. This proves conclusion (4,a).

Now from the previous, we now have that $Q \in G\ell(\dim\Phi, L)$ and $Q$ $k$–rationalizes $Im'(\Delta_\Phi)$. Hence, at once, by much earlier Theorem 2.E.4 (with "$\mathcal{Y}$"$\equiv Im'(\Delta_\Phi)$), part (a, $\Rightarrow$), we have:

$$Q = VC,$$

for some $V \in V_\Phi^\times$ and $C \in \bigotimes_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}$. Thus clearly $C \in C_L^\times(Im'(\Delta_\Phi))$, and so for all $Z \in Im'(\Delta_\Phi)$ we have at once:

$$QZQ^{-1} = VCZC^{-1}V^{-1} = VZV^{-1}.$$

This proves conclusion (4,b).

This completes the proof of the conclusions in (4), and so completes the proof of this lemma.

□

## 7.3 Diagonalizable Subsets of $M(n,k)$, Main Results

In this section, we give our results concerning the diagonalizable subsets of $M(n,k)$. These are some of the main results of this paper, and they include exhibitions and classifications of all the diagonalizable subsets of $M(n,k)$, of their centralizers in $M(n,k)$, and inclusions for their normalizers in $M(n,k)$.

The same is achieved for all the subsets of $M(n,k)$ which are second centralizers (i.e., $C_k^2(\cdots)$) of some diagonalizable (over $L$) subset of $M(n,k)$, and, furthermore, for those subsets, their normalizers in $M(n,k)$ are exactly determined. (These subsets are a particular class of diagonalizable subset of $M(n,k)$ — see Corollary 7.C.3, part (2).)

Finally, the same is achieved for all the *maximal* diagonalizable (over $L$) subsets of $M(n,k)$ — see Corollary 7.C.5, ($\Longrightarrow$), part (1).

Other results are also given.

The following Theorem exhibits all diagonalizable subsets of $M(n,k)$, exhibits their centralizers in $M(n,k)$, and exhibits inclusions for their normalizers in $M(n,k)$. It also gives several other key results about these subsets.

This is one of the very main results of this paper.

**Theorem 7.C.1** (Diagonalizable Subsets of $M(n,k)$;

Centralizers and Normalizers —Exhibition)

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{A} \subset M(n,k)$.

**Then:**

$$\mathcal{A} \text{ is a diagonalizable (over } L\text{) subset of } M(n,k)$$

$$\Longleftrightarrow$$

$\exists \Phi = (\phi_1, \dots, \phi_r)$, a reduced field setting over $k$; with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$; and with the subsequence $(\phi_{i_1}, \dots, \phi_{i_u}) \subseteq (\phi_1, \dots, \phi_r)$ being any set of representatives of $\Phi/{\sim_k}$ [letting $[\phi_{i_h}]$ be the equivalence class of $\phi_h$ in $\Phi/{\sim_k}$]:

$\exists V \in V_\Phi^\times$:

1) $\dim \Phi = n$.

2) a) $\displaystyle\sum_{h=1}^{u} a_{i_h} [K_{i_h} : k] \, |[\phi_{i_h}]| = \sum_{i=1}^{r} a_i [K_i : k] = n$;

   b) $\displaystyle\sum_{h=1}^{u} |[\phi_{i_h}]| = r$.

3) a) $\displaystyle\mathcal{A} \subseteq V \Delta_\Phi \left( \prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i) \right) V^{-1}$;

   b) i) $\displaystyle C_k^2(\mathcal{A}) = C_k^2 \left( V \Delta_\Phi \left( \prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i) \right) V^{-1} \right)$

$$= V \Delta_\Phi \left( \prod_{i=1}^{r} \mathrm{Scalar}(a_i, K_i) \right) V^{-1},$$

$$\text{ii)}\quad C_L^2(\mathcal{A}) = C_L^2\left(V\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i,K_i)\right)V^{-1}\right)$$

$$= V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r}\mathrm{Scalar}(a_i,L_i)^{(n_{\phi_i})}\right]V^{-1};$$

$$\text{c)}\quad\text{i)}\quad C_k(\mathcal{A}) = C_k\left(V\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i,K_i)\right)V^{-1}\right)$$

$$= V\Delta_\Phi\left(\prod_{i=1}^{r}M(a_i,K_i)\right)V^{-1},$$

$$\text{ii)}\quad C_L(\mathcal{A}) = C_L\left(V\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i,L_i)\right)V^{-1}\right)$$

$$= V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r}M(a_i,L)^{(n_{\phi_i})}\right]V^{-1};$$

$$\text{d)}\quad\text{i)}\quad \mathcal{N}_k(\mathcal{A}) \subseteq \mathcal{N}_k\left(V\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i,K_i)\right)V^{-1}\right)$$

$$= V\left[\Delta_\Phi\left(\prod_{i=1}^{r}G\ell(a_i,K_i)\right)\right]\cdot$$

$$\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u}\mathcal{G}a\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)}\cdot\mathrm{Perm}\left(a_{i_h}\,[K_{i_h}:k]\,|[\phi_{i_h}]|\,,I_{a_{i_h}[K_{i_h}:k]},k\right)\right]V^{-1},$$

$$\text{ii)}\quad \mathcal{N}_L(\mathcal{A}) \subseteq \mathcal{N}_L\left(V\Delta_\Phi\left(\prod_{i=1}^{r}\mathrm{Scalar}(a_i,K_i)\right)V^{-1}\right)$$

$$= V\left[\mathop{\textcircled{$\triangle$}}_{i=1}^{r}G\ell(a_i,L)^{(n_{\phi_i})}\right]\cdot$$

$$\left[\mathop{\textcircled{$\triangle$}}_{h=1}^{u}\mathcal{G}a\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)}\cdot\mathrm{Perm}\left(a_{i_h}\,[K_{i_h}:k]\,|[\phi_{i_h}]|\,,I_{a_{i_h}[K_{i_h}:k]},k\right)\right]V^{-1}.$$

4) Observing, by (3,a) above, that $V^{-1}\mathcal{A}V \subseteq D(n,L)$, and using $\mathcal{I}_\Phi$, the 3-tuple index notation for $\Phi$, we have:

$$\forall(i,j,t)\in\mathcal{I}_\Phi:\quad k\left(\left\{Y_{(i,j,t)}\,\middle|\,Y\in V^{-1}\mathcal{A}V\right\}\right) = \sigma_j^{(i)}(K_i).$$

**Proof.**

($\Longleftarrow$)

1) This direction is immediate because we have, by supposition in this direction, that conclusion (3,a) holds: $\mathcal{A} \subseteq V Im'(\Delta_\Phi) V^{-1}$. Thus, $V^{-1}(\mathcal{A})V \subseteq Im'(\Delta_\Phi)$, and, as $Im'(\Delta_\Phi)$ is a set of diagonal matrices, clearly $\mathcal{A}$ is a diagonalizable (over $L$) subset of $M(n,k)$.

($\Longrightarrow$)

2) So, suppose $\mathcal{A}$ is a diagonalizable (over $L$) subset of $M(n,k)$. So, we may let $P \in G\ell(n,L)$ diagonalize $\mathcal{A}$:

$$P \in G\ell(n,L) \quad \text{and} \quad P^{-1}\mathcal{A}P \subseteq D(n,L).$$

Now let $\mathcal{Y} \equiv P^{-1}\mathcal{A}P \subseteq D(n,L)$. So, by construction, and supposition that $\mathcal{A} \subseteq M(n,k)$, we have that $P$ $k$–rationalizes $\mathcal{Y}$. In particular, $\mathcal{Y}$ is a $k$–rationalizable (over $L$) subset of $D(n,L)$. Thus, by Theorem 8.C.3, ($\Longrightarrow$), we have at once that (stating things compactly):

$$\exists \Pi \in \mathrm{Perm}(n,k):$$

$\exists \Phi = (\phi_1, \ldots, \phi_r)$, a *reduced* field setting over $k$, with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$:

(1) i) $\dim \Phi = k$;

(2) ii) $\mathcal{Y} \subseteq \Pi^{-1} Im'(\Delta_\Phi)\Pi$;

(3) iii) $C_L(\mathcal{Y}) = \Pi^{-1}\left[\overset{r}{\underset{i=1}{\bigcirc\!\!\!\!\triangle}} M(a_i, L)^{(n_{\phi_i})}\right]\Pi.$

By virtue of Lemma 2.D.1, part (b,i), we can rewrite (3) above as:

(3′) iii′) $C_L(\mathcal{Y}) = \Pi^{-1} C_L\left(Im'(\Delta_\Phi)\right)\Pi.$

Now, as above, we have that $\Phi$ is a reduced field setting over $k$. As for any field setting, we may let the subsequence $(\phi_{i_1}, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be any set of representatives of $\Phi/\!\sim_k$ (and we will let $[\phi_{i_h}]$ denote the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$). Then, by Lemma 7.B.4, parts (1,a) & (1,b), together with result (1) above, we have at once the desired conclusions (1) & (2) of the theorem.

3) Now, using the above definition of $\mathcal{Y}$ ( $\equiv P^{-1}\mathcal{A}P$), in (2) & (3'), we have easily:

(6) $\left(P\Pi^{-1}\right)^{-1}\mathcal{A}\left(P\Pi^{-1}\right) \subseteq Im'(\Delta_\Phi)$;

(7) $C_L\left(\left(P\Pi^{-1}\right)^{-1}\mathcal{A}\left(P\Pi^{-1}\right)\right) = C_L\left(Im'(\Delta_\Phi)\right).$

Now, by (6) & (7), we may apply Lemma 7.B.4, part (4,b) (with "$\mathcal{Y}$" $\equiv$ $\left(P\Pi^{-1}\right)^{-1}\mathcal{A}\left(P\Pi^{-1}\right)$, and "$Q$"$\equiv P\Pi^{-1}$; so that $Q$ certainly $k$-rationalizes

$\mathcal{Y}$ — as, by the given, we have here that $\mathcal{A} \subseteq M(n,k)$, and we find:

$$\exists V \in V_\Phi^\times: \quad \left(P\Pi^{-1}\right) Im'(\Delta_\Phi) \left(P\Pi^{-1}\right)^{-1} = V Im'(\Delta_\Phi) V^{-1}.$$

This, in (6) & (7), gives easily:

$$(8) \qquad \mathcal{A} \subseteq \left(P\Pi^{-1}\right) Im'(\Delta_\Phi) \left(P\Pi^{-1}\right)^{-1} = V Im'(\Delta_\Phi) V^{-1};$$

$$(9) \quad C_L(\mathcal{A}) = C_L\left(\left(P\Pi^{-1}\right) Im'(\Delta_\Phi) \left(P\Pi^{-1}\right)^{-1}\right) = C_L\left(V Im'(\Delta_\Phi) V^{-1}\right).$$

The results above in (8) & (9), together with Lemma 7.B.1, part (1,a), prove the conclusions (3,a) & (3,c,ii) of the theorem. With these two conclusions established, the remaining conclusions in (3) follow verbatim from Lemma 7.B.3, parts (2) & (3), and from Lemma 7.B.2 and Lemma 7.B.1.

4) Finally, using (8) & (9), we see we may apply Lemma 7.B.4, part (3) (with "$\mathcal{Y}$"$\equiv V^{-1}\mathcal{A}V$), and we conclude at once:

$$\forall (i,j,t) \in \mathcal{I}_\Phi: \quad k\left(\left\{Y_{(i,j,t)} \middle| Y \in V^{-1}\mathcal{A}V\right\}\right) = \sigma_j^{(i)}(K_i).$$

This proves conclusion (4) of the theorem, and so completes the proof of $(\Longrightarrow)$.

□

The following corollary classifies all diagonalizable subalgebras of $M(n,k)$, classifies their centralizers in $M(n,k)$, and gives imbeddings for their normalizers in $M(n,k)$. It also gives several other key results about these subalgebras.

This, too, is one of the very main results of this paper.

**Corollary 7.C.2** (Diagonalizable Subsets of $M(n,k)$;

Centralizers and Normalizers —Classification)

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{A} \subseteq M(n,k)$.

**Then:**

$\mathcal{A}$ is a diagonalizable (over $L$) subalgebra of $M(n,k)$

$$\Longrightarrow$$

$\exists r \in \{1,\ldots,n\}$:

$\exists K_1,\ldots,K_r$ intermediate fields of $\overline{k}/k$ and finite extensions of $k$:

$\exists a_1,\ldots,a_r \in \{1,\ldots,n\}$:

$\exists u \in \{1,\ldots,r\}: \exists 1 \leq i_1 < i_2 < \ldots < i_u \leq r: \exists m_1,\ldots,m_u \in \{1,\ldots,r\}$:

1) a) $\sum_{h=1}^{u} a_{i_h}[K_{i_h} : k]m_h = \sum_{i=1}^{r} a_i[K_i : k] = n;$

b) $\sum_{h=1}^{u} m_h = r.$

2) a) $\mathcal{A} \hookrightarrow \prod_{i=1}^{r} K_i;$

b) $C_k^2(\mathcal{A}) \approx \prod_{i=1}^{r} K_i;$

c) $C_k(\mathcal{A}) \approx \prod_{i=1}^{r} M(a_i, K_i);$

d) $\mathcal{N}_k(\mathcal{A}) \hookrightarrow \left[\prod_{i=1}^{r} G\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u} \left[Ga\ell\,(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right]\right];$

e) $\mathcal{N}_k(\mathcal{A})/C_k^{\times}(\mathcal{A}) \hookrightarrow \prod_{h=1}^{u} \left[Ga\ell\,(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right].$

(Recall, here, $S_{m_h}$ is the symmetric group on $m_h$ letters.)

**Proof.**

This corollary follows at once from the previous Theorem 7.C.1, as below.

So, suppose $\mathcal{A}$ is a diagonalizable (over $L$) subalgebra of $M(n,k)$. Then, by Theorem 7.C.1, $(\Longrightarrow)$, we may let $\Phi$, $V$, and properties (1)–(4) be as in the conclusion of that Theorem. Then, respectively, by conclusions (2), (3,a), (3,b,i), (3,c,i), (3,d,i) of that Theorem, together, respectively, with conclusions (1), (2,a), (2,b), (2,c) of Lemma 7.B.4, and the obvious facts that $conj_V$, $\Delta_\Phi$, are imbeddings of $k$-algebras, and that clearly $\mathcal{N}_k(\mathcal{A})/C_k^{\times}(\mathcal{A}) \approx (V^{-1}\mathcal{N}_k(\mathcal{A})V) \,/\, \left(V^{-1}C_k^{\times}(\mathcal{A})V\right)$, and letting $m_h \equiv |[\phi_{i_h}]|$, we have at once, respectively, the desired conclusions (1), (2,a), (2,b), (2,c), (2,d) & (2,e) of this Corollary. □

The following Corollary gives some qualitative facts about diagonalizable subsets of $M(n,k)$ and their centralizers in $M(n,k)$.

**Corollary 7.C.3**

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{A} \subseteq M(n,k)$.

Suppose $\mathcal{A}$ is a diagonalizable (over $L$) subset of $M(n,k)$.

**Then:**

1) $\mathcal{A} \subseteq C_k^2(\mathcal{A}) \subseteq C_k(\mathcal{A}) \subseteq M(n,k)$;

2) $C_k^2(\mathcal{A})$ is a diagonalizable (over $\overline{k}$) subalgebra of $M(n,k)$.

**Proof.**

1) By Proposition App. 18, of the Appendix, we have (for *any* subset $\mathcal{A} \subseteq M(n,k)$):

$$\mathcal{A} \subseteq C_k^2(\mathcal{A}). \tag{1}$$

Additionally, as $\mathcal{A}$ is diagonalizable, certainly $\mathcal{A}$ is abelian, and so clearly:

$$\mathcal{A} \subseteq C_k(\mathcal{A}).$$

Thus, again using Proposition App. 18, of the Appendix, the previous gives:

$$C_k(\mathcal{A}) \supseteq C_k\left(C_k(\mathcal{A})\right).$$

I.e.,

$$C_k(\mathcal{A}) \supseteq C_k^2(\mathcal{A}).$$

Hence, combining (1) & (2), we have at once:

$$\mathcal{A} \subseteq C_k^2(\mathcal{A}) \subseteq C_k(\mathcal{A}) \subseteq M(n,k).$$

This proves conclusion (1).

(We note that the above is also known to be true, immediately, from Theorem 7.C.1, ($\Longrightarrow$), parts (3,a), (3,b,i) & (3,c,i).)

2) The conclusion in (2) here is seen to be true, immediately, from Theorem 7.C.1, ($\Longrightarrow$), part (3,b,i), and recalling that $\Delta_\Phi \left( \prod_{i=1}^{r} \text{Scalar}(a_i, K_i) \right)$ is a set of diagonal matrices.

□

The following Theorem concerns those subsets of $M(n,k)$ which are second centralizers (i.e, $C_k^2(\cdots)$) of some diagonalizable (over $L$) subset of $M(n,k)$. This Theorem exhibits all such subsets, exhibits their centralizers in $M(n,k)$, and exhibits their normalizers in $M(n,k)$. It also gives some other key results about these subsets.

**Theorem 7.C.4**

Let $n \in \mathbb{Z}^{+}$.

Let $\mathcal{A} \subseteq M(n,k)$.

**Then:**

$$\exists \mathcal{B} \subseteq M(n,k),\ \mathcal{B} \text{ a diagonalizable (over } L) \text{ subset: } \mathcal{A} = C_k^2(\mathcal{B})$$

$$\Longleftrightarrow$$

1) a) $\mathcal{A} = C_k^2(\mathcal{A})$;

b) If $\mathcal{A} = C_k^2(\mathcal{B})$, then $C_k(\mathcal{A}) = C_k(\mathcal{B})$.

2) $\exists \Phi = (\phi_1, \ldots, \phi_r)$, a reduced field setting over $k$; with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$;

with the subsequence $(\phi_i, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ being any set of representatives of $\Phi/\!\sim_k$ [letting $[\phi_{i_h}]$ denote the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$]:

$\exists V \in V_\Phi$:

a) $\dim \Phi = n$;

b) i) $\sum_{h=1}^{u} a_{i_h} [K_{i_h} : k] \, |[\phi_{i_h}]| = \sum_{i=1}^{r} a_i [K_i : k] = n$,

ii) $\sum_{h=1}^{u} |[\phi_{i_h}]| = r$;

c) i) $\mathcal{A} = V \Delta_\Phi \left( \prod_{i=1}^{r} \operatorname{Scalar}(a_i, K_i) \right) V^{-1}$,

$$\text{ii) } \alpha) \ C_k(\mathcal{A}) = V\Delta_\Phi\left(\prod_{i=1}^{r} M(a_i, K_i)\right)V^{-1},$$

$$\beta) \ C_L(\mathcal{A}) = V\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} M(a_i, L)^{(n_{\phi_i})}\right]V^{-1};$$

$$\text{iii) } \alpha) \ C_k^2(\mathcal{A}) = V\Delta_\Phi\left(\prod_{i=1}^{r} \text{Scalar}(a_i, K_i)\right)V^{-1},$$

$$\beta) \ C_L^2(\mathcal{A}) = V\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} \text{Scalar}(a_i, L_i)^{(n_{\phi_i})}\right]V^{-1};$$

$$\text{iv) } \alpha) \ \mathcal{N}_k(\mathcal{A}) = V\left[\Delta_\Phi\left(\prod_{i=1}^{r} G\ell(a_i, K_i)\right)\right]\cdot$$

$$\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)}\cdot \text{Perm}\left(a_{i_h}\,[K_{i_h} : k]\,|[\phi_{i_h}]|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right]V^{-1},$$

$$\beta) \ \mathcal{N}_L(\mathcal{A}) = V\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{r} G\ell(a_i, L)^{(n_{\phi_i})}\right]\cdot$$

$$\left[\mathop{\bigcirc\kern-0.75em\triangle}\limits_{h=1}^{u} Ga\ell\,(\phi_{i_h})^{(|[\phi_{i_h}]|)}\cdot \text{Perm}\left(a_{i_h}\,[K_{i_h} : k]\,|[\phi_{i_h}]|\,, I_{a_{i_h}[K_{i_h}:k]}, k\right)\right]V^{-1}.$$

d) Observing, by (2,c,i) above, that $V^{-1}\mathcal{A}V \subseteq D(n, L)$, and using $\mathcal{I}_\Phi$, the 3-tuple index notation for $\Phi$, we have:

$$\forall (i,j,t) \in \mathcal{I}_\Phi\colon \quad k\left(\left\{Y_{(i,j,t)}\middle| Y \in V^{-1}\mathcal{A}V\right\}\right) = \sigma_j^{(i)}(K_i).$$

**Proof.**

$(\Longleftarrow)$

1) This direction is immediate, because we have, by supposition in this direction, that conclusions (1) and (2,c,i) hold. The former is that: $\mathcal{A} = C_k^2(\mathcal{A})$, and the latter shows that: $\mathcal{A}$ is diagonalizable (over $L$) [ in fact, by

$V$ ]. With this, we may let: $\mathcal{B} = \mathcal{A}$, and we have thus at once completed the proof of ($\Longleftarrow$).

($\Longrightarrow$)

2) So, suppose: $\mathcal{A} = C_k^2(\mathcal{B})$; for some $\mathcal{B}$, a diagonalizable (over $L$) subset of $M(n,k)$. Using Proposition App. 18, of the Appendix, we have at once the following two calculations:

$$\begin{aligned} C_k^2(\mathcal{A}) &= C_k^2\left(C_k^2(\mathcal{B})\right) = C_k\left(C_k^3(\mathcal{B})\right) = C_k\left(C_k(\mathcal{B})\right) = C_k^2(\mathcal{B}) = \mathcal{A}; \\ C_k(\mathcal{A}) &= C_k\left(C_k^2(\mathcal{B})\right) = C_k^3(\mathcal{B}) = C_k(\mathcal{B}). \end{aligned}$$

This proves conclusion (1) of the Theorem.

Now, as $\mathcal{B}$ is a diagonalizable (over $L$) subset of $M(n,k)$; by Theorem 7.C.1, ($\Longrightarrow$) (with "$\mathcal{A}$" $\equiv \mathcal{B}$), we may at once let $\Phi$, $V$, and properties (1)–(4) be as in the conclusion of that Theorem. Conclusions (1) and (2) of that Theorem give, verbatim, the desired conclusions (2,a) and (2,b) of this Theorem. Now, by conclusion (3,b,i) of that Theorem (remembering that it takes place with "$\mathcal{A}$" $\equiv \mathcal{B}$), we have: $C_k^2(\mathcal{B}) = V\mathrm{Im}'\left(\Delta_\Phi\right)V^{-1}$. This, together with our starting supposition here that: $\mathcal{A} = C_k^2(\mathcal{B})$, gives at once:

$$(1) \qquad \mathcal{A} = V\mathrm{Im}'\left(\Delta_\Phi\right)V^{-1}.$$

This proves conclusion (2,c,i) of this Theorem.

This single fact in (1), alone, by Lemmas 7.B.1 and 7.B.2 (and with $\Phi$ being reduced), shows at once the remaining desired conclusions in part (2,c) of this Theorem. Finally, from conclusion (4) of the above-mentioned application of Theorem 7.C.1, ($\Longrightarrow$) (with "$\mathcal{A}$" $\equiv \mathcal{B}$), we have at once:

$$(2) \qquad \forall (i,j,t) \in \mathcal{I}_\Phi\colon \quad k\left(\left\{Y_{(i,j,t)} \middle| Y \in V^{-1}\mathcal{B}V\right\}\right) = \sigma_j^{(i)}(K_i).$$

Additionally, by conclusion (3,a) of that Theorem, we have: $\mathcal{B} \subseteq V\mathrm{Im}'(\Delta_\Phi)V^{-1}$. This, with (1), gives at once:

$$\mathcal{B} \ \subseteq \mathcal{A} \ = V\mathrm{Im}'(\Delta_\Phi)V^{-1}.$$

Therefore:

$$V^{-1}\mathcal{B}V \ \subseteq V^{-1}\mathcal{A}V \ = \mathrm{Im}'(\Delta_\Phi).$$

So clearly:

$\forall (i,j,t) \in \mathcal{I}_\Phi$:

$$\begin{aligned} k\left(\left\{Y_{(i,j,t)} \middle| Y \in V^{-1}\mathcal{B}V\right\}\right) \ &\subseteq k\left(\left\{Y_{(i,j,t)} \middle| Y \in V^{-1}\mathcal{A}V\right\}\right) \\ &= k\left(\left\{Y_{(i,j,t)} \middle| Y \in \mathrm{Im}'(\Delta_\Phi)\right\}\right). \end{aligned}$$

So, now by (2):

$$\begin{aligned} (3) \qquad \forall (i,j,t) \in \mathcal{I}_\Phi\colon \quad \sigma_j^{(i)}(K_i) \ &\subseteq k\left(\left\{Y_{(i,j,t)} \middle| Y \in V^{-1}\mathcal{A}V\right\}\right) \\ &= k\left(\left\{Y_{(i,j,t)} \middle| Y \in \mathrm{Im}'(\Delta_\Phi)\right\}\right). \end{aligned}$$

And, by the definitions of $\mathcal{I}_\Phi$ and $\mathrm{Im}'(\Delta_\Phi)$, we have, certainly:

$$k\left(\left\{Y_{(i,j,t)} \middle| Y \in \mathrm{Im}'(\Delta_\Phi)\right\}\right) = \sigma_j^{(i)}(K_i).$$

(In fact, equality in the latter is clear, too; but we do not need it.)

The previous, in (3), gives at once:

$$k\left(\left\{Y_{(i,j,t)}\middle| Y\in V^{-1}\mathcal{A}V\right\}\right)=\sigma_j^{(i)}(K_i).$$

This proves conclusion (2,d) of this Theorem.

This completes the proof of ($\Longrightarrow$), and so completes the proof of the entire Theorem.

$\square$

The following Corollary also concerns those subsets of $M(n,k)$ which are second centralizers (i.e, $C_k^2(\cdots)$) of some diagonalizable (over $L$) subset of $M(n,k)$. This Corollary classifies all such subsets of $M(n,k)$, classifies their centralizers in $M(n,k)$, and classifies their normalizers in $M(n,k)$. It also gives some other key results about these subsets.

**Corollary 7.C.5**

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{A} \subseteq M(n,k)$.

**Then:**

$$\exists \mathcal{B} \subseteq M(n,k),\ \mathcal{B} \text{ a diagonalizable (over } L\text{) subset: } \mathcal{A} = C_k^2(\mathcal{B})$$

$$\Longrightarrow$$

$\exists r \in \{1,\dots,n\}$:

$\exists K_1,\dots,K_r$ intermediate fields of $\overline{k}/k$ and finite extensions of $K$:

$\exists a_1,\dots,a_r \in \{1,\dots,n\}$:

$\exists u \in \{1,\dots,r\}$: $\exists 1 \leq i_1 < i_2 < \dots < i_u \leq r$: $\exists m_1,\dots,m_u \in \{1,\dots,r\}$:

1) a) $\sum_{h=1}^{u} a_{i_h}\,[K_{i_h} : k]\,m_h = \sum_{i=1}^{r} a_i[K_i : k] = n$;

   b) $\sum_{h=1}^{u} m_h = r$.

2) a) $\mathcal{A} \approx \prod_{i=1}^{r} K_i$;

   b) $C_k(\mathcal{A}) \approx \prod_{i=1}^{r} M(a_i, K_i)$;

   c) $C_k^2(\mathcal{A}) \approx \prod_{i=1}^{r} K_i$;

d) $\mathcal{N}_k(\mathcal{A}) \approx \left[\prod_{i=1}^{r} G\ell(a_i, K_i)\right] \rtimes \left[\prod_{h=1}^{u} [Ga\ell\,(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]\right]$;

e) $\mathcal{N}_k(\mathcal{A})/C_k^{\times}(\mathcal{A}) \approx \prod_{h=1}^{u} [Ga\ell\,(K_{i_h}/k)^{m_h} \rtimes S_{m_h}]$.

(Recall, here, $S_{m_h}$ is the symmetric group on $m_h$ letters.)

**Proof.**

This Corollary follows at once from the previous Theorem 7.C.4. So, suppose: $\mathcal{A} = C_k^2(\mathcal{B})$; for some $\mathcal{B}$, a diagonalizable (over $L$) subset of $M(n,k)$. Then, by Theorem 7.C.4, ($\Longrightarrow$), we may let $\Phi$, $V$, and properties (2,a)–(2,c) be as in the conclusion of that Theorem. Then, by conclusions (2,b), (2,c,ii,$\alpha$), (2,c,iii,$\alpha$), (2,c,iv,$\alpha$) of that Theorem, together, respectively, with conclusions (1), (2,a), (2,b), (2,c) of Lemma 7.B.4, and the obvious facts that $conj_V$, $\Delta_\Phi$, are imbeddings of $k$-algebras, and that clearly $\mathcal{N}_k(\mathcal{A})/C_k^{\times}(\mathcal{A}) \approx (V^{-1}\mathcal{N}_k(\mathcal{A})V)\,/\,\left(V^{-1}C_k^{\times}(\mathcal{A})V\right)$, and letting $m_h \equiv |[\phi_{i_h}]|$, we have at once, respectively, the desired conclusions (1), (2,a), (2,b), (2,c), (2,d) & (2,e) of this Corollary.

□

The following four results concern the maximal diagonalizable subsets of $M(n,k)$ — i.e., the diagonalizable subsets of $M(n,k)$ which admit no proper diagonalizable extension in $M(n,k)$. The first Theorem gives a characterization of these by four equivalent statements. The second result exhibits all such subsets, and exhibits their centralizers and normalizers in $M(n,k)$, as well as gives some other key results here. The third result classifies all such subsets, and classifies their centralizers and normalizers in $M(n,k)$, as well as gives some other key results here. The last result is a qualitative one that shows, in short, that every such diagonalizable subset is contained in a maximal such.

**Theorem 7.C.6** (Maximal Diagonalizable Subsets — Characterization)

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{M} \subset M(n,k)$.

**Then:**

The following four statements are equivalent:

1) $\mathcal{M}$ is a maximal diagonalizable (over $L$) subset of $M(n,k)$;

2) $\mathcal{M}$ is a diagonalizable (over $L$) subset of $M(n,k)$, and $\mathcal{M} = C_k(\mathcal{M})$;

3) $\exists \Phi = (\phi_1, \ldots, \phi_r)$, a field setting over $k$, which may be taken to be reduced; with

$\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$:

$\exists V \in V_\Phi^\times$:

a) i) $a_1 = a_2 = \cdots = a_r = 1$,

ii) $\dim \Phi = n$;

b) $\mathcal{M} = V\Delta_\Phi\left(\prod_{i=1}^{r} K_i\right)V^{-1}$.

[ In the latter, we have identified $M(1, K_i)$ with $K_i$. ]

4) $\exists\Phi = (\phi_1, \ldots, \phi_r)$, a field setting over $k$, which may be taken to be reduced; with

$\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$:

$\exists P \in G\ell(n, L)$:

a) i) $a_1 = a_2 = \cdots = a_r = 1$,

ii) $\dim \Phi = n$;

b) $\mathcal{M} = P\Delta_\Phi\left(\prod_{i=1}^{r} K_i\right)P^{-1}$.

[ In the latter, we have identified $M(1, K_i)$ with $K_i$. ]

**Proof.**

1) We will prove this Theorem via the logical sequence:

$$(2) \implies (1) \implies (4) \implies (3) \implies (2).$$

2) (2) $\implies$ (1)

We suppose $\mathcal{M}$ is a diagonalizable (over $L$) subset of $M(n,k)$, and $\mathcal{M} = C_k(\mathcal{M})$. To show $\mathcal{M}$ is a maximal diagonalizable (over $L$) subset of $M(n,k)$, we suppose $\mathcal{M} \subseteq \mathcal{M}' \subseteq M(n,k)$, where $\mathcal{M}'$ is diagonalizable (over $L$). As $\mathcal{M}'$ is diagonalizable, certainly $\mathcal{M}'$ is abelian; and as $\mathcal{M} \subseteq \mathcal{M}'$, we have certainly, in particular, that $\mathcal{M}' \subseteq C_k(\mathcal{M})$. But by supposition here, we have $\mathcal{M} = C_k(\mathcal{M})$. Thus, we have now $\mathcal{M} \subseteq \mathcal{M}' \subseteq C_k(\mathcal{M}) = \mathcal{M}$; hence, $\mathcal{M}' = \mathcal{M}$, and thus we have that $\mathcal{M}$ is maximal, as desired.

3) (1) $\implies$ (4)

We suppose $\mathcal{M}$ is a maximal diagonalizable (over $L$) subset of $M(n,k)$. As $\mathcal{M}$ is diagonalizable, by Theorem 7.C.1, we have at once:

$$(1) \qquad \mathcal{M} \subseteq V\mathrm{Im}'(\Delta_\Phi)V^{-1};$$

for some reduced field setting $\Phi$, some $V \in V_\Phi^\times$, and where $\dim \Phi = n$.

Now let $\dot{\Phi}$ be the field setting constructed from $\Phi$, as defined much earlier in Lemma 4.B.5. From the definition of reduced field setting, we see virtually immediately that if $\Phi$ is reduced, then so also is $\dot{\Phi}$. Thus, here, $\dot{\Phi}$ is reduced. Furthermore, from Lemma 4.B.5, and using the above-mentioned fact that $\dim \Phi = n$, we have the following:

$$(2) \qquad \dim \dot{\Phi} = \dim \Phi = n;$$

$$\text{(3)} \qquad \operatorname{Im}'(\Delta_{\Phi}) \subseteq \Pi \operatorname{Im}(\Delta_{\dot\Phi})\,\Pi^{-1} \subseteq M(n,k);$$

$$\text{(4)} \qquad V\Pi \quad k\text{-rationalizes} \quad \operatorname{Im}(\Delta_{\dot\Phi});$$

for some $\Pi \in \operatorname{Perm}(n,k)$.

Combining (1), (3), and (4), we have:

$$\text{(5)} \qquad \mathcal{M} \subseteq (V\Pi)\operatorname{Im}(\Delta_{\dot\Phi})\,(V\Pi)^{-1} \subseteq M(n,k).$$

Now the above field setting, $\dot\Phi$, which is constructed in Lemma 4.B.5, is clearly one of the form:

$$\dot\Phi = (\omega_1, \ldots, \omega_s) \ ;$$

where $\omega_i = \left(L_i, \tau^{(i)}, b_i\right)$ is a field element over $k$, <u>where</u> $\underline{\underline{b_i = 1}}$. With this, we see:

$$\text{(6)} \qquad \operatorname{Im}(\Delta_{\dot\Phi}) = \Delta_{\dot\Phi}\left(\prod_{i=1}^{s} M(1, L_i)\right);$$

and so, by definition of $\Delta_{\dot\Phi}$, and the fact that the elements of $M(1, L_i)$ are all $1 \times 1$ matrices, the previous shows at once, in particular, that:

$\operatorname{Im}(\Delta_{\dot\Phi})$ is a set of diagonal matrices.

This, with (5), shows immediately that $(V\Pi)\operatorname{Im}(\Delta_{\dot\Phi})\,(V\Pi)^{-1}$ is a diagonalizable subset of $M(n,k)$ — in fact, it is diagonalized by $V\Pi \in G\ell\left(n, \overline{k}\right)$. But now, by supposition here, $\mathcal{M}$ is a maximal such diagonal subset — and so, immediately, by (5), we have:

$$\mathcal{M} = (V\Pi)\mathrm{Im}\,(\Delta_{\dot{\Phi}})\,(V\Pi)^{-1}\,. \tag{7}$$

Now, finally, letting $P \equiv V\Pi \in G\ell\left(n,\bar{k}\right) \subseteq G\ell(n,L)$, and using (6), the previous result gives:

$$\mathcal{M} = P\Delta_{\dot{\Phi}}\left(\prod_{i=1}^{s} M(1,L_i)\right)P^{-1}\,. \tag{8}$$

As $P \in G\ell(n,L)$, as (2) shows $\dim\dot{\Phi} = n$, as mentioned earlier we have $\dot{\Phi}$ is a reduced field setting, and identifying $M(1,L_i)$ with $L_i$, the result in (8) completes the proof here of (1) $\Longrightarrow$ (4).

4) <u>(4) $\Longrightarrow$ (3)</u>

Suppose $\Phi$ and $P$ are as in conclusion (4); so, we have:

$$\mathcal{M} = P\,\Delta_{\Phi}\left(\prod_{i=1}^{r} K_i\right)P^{-1} = P\,\Delta_{\Phi}\left(\prod_{i=1}^{r} M(1,K_i)\right)P^{-1}; \quad P \in G\ell(n,L).$$

As obviously $M(1,K_i) = \mathrm{Scalar}(1,K_i)$, the previous shows:

$$\mathcal{M} = P\,\Delta_{\Phi}\left(\prod_{i=1}^{r} \mathrm{Scalar}(1,K_i)\right)P^{-1} = P\,\mathrm{Im}'\,(\Delta_{\Phi})\,P^{-1}. \tag{9}$$

With this, we may apply Lemma 7.B.4, part (4) (with $\Phi$ as above, "$\mathcal{Y}$" $\equiv$ $\mathrm{Im}'\,(\Delta_{\Phi})$, "Q" $\equiv P$), at once; and we obtain:

$$P\,\mathrm{Im}'\,(\Delta_{\Phi})\,P^{-1} = V\,\mathrm{Im}'\,(\Delta_{\Phi})\,V^{-1}, \quad \text{for some } V \in V_{\Phi}^{\times}.$$

Substituting this into (9) completes the proof of (4) $\Longrightarrow$ (3).

5) (3) $\Longrightarrow$ (2)

Suppose $\Phi$ and $V$ are as in conclusion (3); so, we have:

$$\mathcal{M} = V\,\Delta_\Phi\left(\prod_{i=1}^{r} K_i\right)V^{-1} = V\,\Delta_\Phi\left(\prod_{i=1}^{r} M(1,K_i)\right)V^{-1}\,; \quad \text{for some } V \in V_\Phi^\times .$$

As in step (3) above, we clearly have: $M(1,K_i) = \text{Scalar}(1,K_i)$; and so immediately we have: $\operatorname{Im}(\Delta_\Phi) = \operatorname{Im}'(\Delta_\Phi)$. With this, the above result gives now:

$$\text{(10)} \qquad \mathcal{M} = V \operatorname{Im}'(\Delta_\Phi)\, V^{-1}, \quad \text{for some } V \in V_\Phi^\times .$$

As $\operatorname{Im}'(\Delta_\Phi)$ is a set of diagonal matrices, clearly (10) shows that $\mathcal{M}$ is a diagonalizable subset of $M(n,k)$ — in fact, it is diagonalized by $V \in G\ell\left(n,\overline{k}\right)$. Moreover, by Lemma 7.B.2, part (2,a), we have at once from (10) that:

$$C_k(\mathcal{M}) = C_k\left(V \operatorname{Im}'(\Delta_\Phi)\, V^{-1}\right) = V \operatorname{Im}(\Delta_\Phi)\, V^{-1}, \quad \text{for some } V \in V_\Phi^\times .$$

But, as mentioned above, we have here that: $\operatorname{Im}(\Delta_\Phi) = \operatorname{Im}'(\Delta_\Phi)$. This, in the previous result, gives at once:

$$C_k(\mathcal{M}) = V \operatorname{Im}'(\Delta_\Phi)\, V^{-1}, \quad \text{for some } V \in V_\Phi^\times .$$

Finally, (10), together with the previous result, gives:

$$\mathcal{M} = C_k(\mathcal{M}).$$

This, together with the above-mentioned result that $\mathcal{M}$ is a diagonalizable subset of $M(n,k)$, completes the proof of (3) $\Longrightarrow$ (2).

As discussed in step (1) above, this completes the proof of this Theorem.

□

**Corollary 7.C.7** (Maximal Diagonalizable Subsets — Exhibition)

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{M} \subseteq M(n,k)$.

**Then:**

$\mathcal{M}$ is a maximal diagonalizable (over $L$) subset of $M(n,k)$

$$\Longleftrightarrow$$

1) $\mathcal{M} = C_k(\mathcal{M}) = C_k^2(\mathcal{M})$;

2) $\exists \Phi = (\phi_1, \ldots, \phi_r)$, a field setting over $k$ (which may be taken to be reduced); with $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$, a field element over $k$;

with the subsequence $(\phi_i, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ being any set of representatives of $\Phi/\!\sim_k$ [letting $[\phi_{i_h}]$ denote the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$]:

$\exists V \in V_\Phi^\times$:

a) i) $a_1 = \cdots = a_r = 1$,

ii) $\dim \Phi = n$;

b) i) $\sum_{h=1}^{u} [K_{i_h} : k]\, |[\phi_{i_h}]| = \sum_{i=1}^{r} [K_i : k] = n$,

ii) $\sum_{h=1}^{u} |[\phi_{i_h}]| = r$;

c) i) $\mathcal{M} = V \, \Delta_\Phi \left( \prod_{i=1}^{r} K_i \right) V^{-1}$,

ii) $\alpha$) $C_k(\mathcal{M}) = V \, \Delta_\Phi \left( \prod_{i=1}^{r} K_i \right) V^{-1}$,

$\beta$) $C_L(\mathcal{M}) = V \, D(n, L) \, V^{-1}$;

iii) $\alpha$) $C_k^2(\mathcal{M}) = V \, \Delta_\Phi \left( \prod_{i=1}^{r} K_i \right) V^{-1}$,

$\beta$) $C_L^2(\mathcal{M}) = V \, D(n, L) \, V^{-1}$;

iv) $\alpha$) $\mathcal{N}_k(\mathcal{M}) = V \left[ \Delta_\Phi \left( \prod_{i=1}^{r} K_i^{\times} \right) \right] \cdot$

$$\left[ \underset{h=1}{\overset{u}{\bigcirc\!\!\!\!\!\!\triangle}} \, \mathit{Ga}\ell \, (\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm} \left( [K_{i_h} : k] \, |[\phi_{i_h}]| \, , I_{[K_{i_h} : k]}, k \right) \right] V^{-1} ,$$

$\beta$) $\mathcal{N}_L(\mathcal{M}) = V \, D \, (n, L^{\times}) \cdot$

$$\left[ \underset{h=1}{\overset{u}{\bigcirc\!\!\!\!\!\!\triangle}} \, \mathit{Ga}\ell \, (\phi_{i_h})^{(|[\phi_{i_h}]|)} \cdot \mathrm{Perm} \left( [K_{i_h} : k] \, |[\phi_{i_h}]| \, , I_{[K_{i_h} : k]}, k \right) \right] V^{-1} .$$

d) Observing, by (2,c,i) above, that: $V^{-1} \mathcal{M} V \subseteq D(n, L)$, and using $\mathcal{I}_\Phi$, the 3-tuple index notation for $\Phi$, we have:

$$\forall (i, j, t) \in \mathcal{I}_\Phi\text{:} \quad k \left( \left\{ Y_{(i,j,t)} \middle| \, Y \in V^{-1} \mathcal{M} V \right\} \right) = \sigma_j^{(i)}(K_i).$$

<u>Note:</u> In all parts of (2,c) above, we have identified $M(1, K_i)$ with $K_i$, and $M^{\times}(1, K_i)$ with $K_i^{\times}$.

**Proof.**

($\Longleftarrow$)

1) Suppose statements (1), (2,a)–(2,d) are true. Thus, we may take $\Phi$ and $V$ as there, and we may suppose that properties in (2,a) and (2,c,i) are true. This shows that statement (3) of Theorem 7.C.6 is true. Hence, as Theorem 7.C.6 is a list of equivalent statements, we conclude that statement (1) of that Theorem is true. But this is exactly what we wanted to show here.

($\Longrightarrow$)

2) Suppose $\mathcal{M}$ is a maximal diagonalizable (over $L$) subset of $M(n,k)$. Then statement (1) of Theorem 7.C.6 is true, and so, as above, we conclude statement (3) of that Theorem is true. So, we may take $\Phi$ and $V$ as there, and so we have:

(1) $\Phi = (\phi_1, \dots, \phi_r)$ is a reduced field setting over $k$;

(2) $\phi_i = \left(K_i, \sigma^{(i)}, a_i\right)$ is a field element over $k$;

(3) $V \in V_\Phi^\times$;

(4) $a_1 = \cdots = a_r = 1$;

(5) $\dim \Phi = n$;

(6) $\mathcal{M} = V \Delta_\Phi \left(\prod_{i=1}^{r} K_i\right) V^{-1}$;

[ where $M(1, K_i)$ has been identified with $K_i$ ] .

Furthermore, we may let:

(7) the subsequence $(\phi_i, \ldots, \phi_{i_u}) \subseteq (\phi_1, \ldots, \phi_r)$ be any set of representatives of $\Phi/\!\sim_k$;

[ where $[\phi_{i_h}]$ denotes the equivalence class of $\phi_{i_h}$ in $\Phi/\!\sim_k$ ].

The above proves immediately our desired conclusions (2,a) and (2,c,i).

Now as a result of (4), we have clearly: $M(1, K_i) = \mathrm{Scalar}(1, K_i)$, and so at once we have here: $\mathrm{Im}\,(\Delta_\Phi) = \mathrm{Im}'\,(\Delta_\Phi)$. This observation, together with rewriting (6) as: $\mathcal{M} = V\,\mathrm{Im}\,(\Delta_\Phi)\,V^{-1}$; and using (1) & (7) above, with Lemma 7.B.2, parts (2,b), (3,b), and (4), at once shows our desired conclusions (2,c,ii,$\alpha$), (2,c,iii,$\alpha$), (2,c,iv,$\alpha$). Similarly, with Lemma 7.B.1, parts (1,b), (2,b), and (4) ( and trivially noting that: $\mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} M(1, L)^{(n_{\phi_i})} = \mathop{\textcircled{$\triangle$}}\limits_{i=1}^{r} \mathrm{Scalar}(1, L)^{(n_{\phi_i})} = D(N, L)$; where $N \equiv \sum\limits_{i=1}^{r} n_{\phi_i} = \sum\limits_{i=1}^{r} (1 \cdot n_{\phi_i}) = \sum\limits_{i=1}^{r} (a_i \cdot n_{\phi_i}) = \dim \Phi = n$ [by (5)] ), we obtain at once our desired conclusions (2,c,ii,$\beta$), (2,c,iii,$\beta$), (2,c,iv,$\beta$).

The desired conclusions in (2,b) and (2,d) now follow at once from Lemma 7.B.4 ( with, using (6) and the above, "Y" $\equiv V^{-1} \mathcal{M} V = \mathrm{Im}\,(\Delta_\Phi) = \mathrm{Im}'\,(\Delta_\Phi)$ ), parts (1) and (3), followed by substituting: $a_1 = \cdots = a_r = 1$, as given in (4) above.

Finally, we note that our desired conclusion in (1) follows at once from the already proved conclusions (2,c,i), (2,c,ii,$\alpha$), (2,c,iii,$\alpha$) above. (It also follows at once from the supposition here that $\mathcal{M}$ is maximal diagonalizable, together with statements (1) and (2) of Theorem 7.C.6.)

This completes the proof of $(\Longrightarrow)$, and so completes the proof of the Corollary itself.

$\square$

**Corollary 7.C.8** (Maximal Diagonalizable Subsets — Classification)

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{M} \subseteq M(n,k)$.

**Then:**

$\mathcal{M}$ is a maximal diagonalizable (over $L$) subalgebra of $M(n,k)$

$$\Longrightarrow$$

1) $\mathcal{M}$ is a maximal abelian subalgebra of $M(n,k)$;

2) $\exists r \in \{1,\ldots,n\}$:

$\exists K_1,\ldots,K_r$ intermediate fields of $\overline{k}/k$ and finite extensions of $k$:

$\exists u \in \{1,\ldots,r\}$:

$\exists 1 \leq i_1 < i_2 < \ldots < i_u \leq r$: $\exists m_1,\ldots,m_u \in \{1,\ldots,r\}$:

a) i) $\sum_{h=1}^{u} [K_{i_h} : k]\, m_h = \sum_{i=1}^{r} [K_i : k] = n$,

ii) $\sum_{h=1}^{u} m_h = r$;

b) i) $\mathcal{M} \approx \prod_{i=1}^{r} K_i$,

ii) $C_k(\mathcal{M}) \approx \prod_{i=1}^{r} K_i$,

iii) $C_k^2(\mathcal{M}) \approx \prod_{i=1}^{r} K_i$,

iv) $\mathcal{N}_k(\mathcal{M}) \approx \left[\prod_{i=1}^{r} K_i^{\times}\right] \rtimes \left[\prod_{h=1}^{u} \left[Gal\,(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right]\right]$,

v) $\mathcal{N}_k(\mathcal{M})/C_k^{\times}(\mathcal{M}) \approx \prod_{h=1}^{u} \left[Gal\,(K_{i_h}/k)^{m_h} \rtimes S_{m_h}\right]$.

(Recall, here, $S_{m_h}$ is the symmetric group on $m_h$ letters.)

**Proof.**

This Corollary follows at once from the previous Corollary 7.C.7. So, suppose $\mathcal{M}$ is a maximal diagonalizable (over $L$) subalgebra of $M(n,k)$. Then, by Corollary 7.C.7, ($\Longrightarrow$), we may let $\Phi$, $V$, and properties (2,a)–(2,c) be as in the conclusion of that Corollary. Then, respectively, by conclusions (2,b), (2,c,i), (2,c,ii,$\alpha$), (2,c,iii,$\alpha$), (2,c,iv,$\alpha$) of that Corollary; together, respectively, with conclusions (1), (2,a), (2,b), (2,c) of Lemma 7.B.4; and the obvious facts that $conj_V$, $\Delta_\Phi$, are imbeddings of $k$-algebras; and that clearly: $\mathcal{N}_k(\mathcal{M})/C_k^\times(\mathcal{M}) \approx (V^{-1}\mathcal{N}_k(\mathcal{M})V) \,/\, \left(V^{-1}C_k^\times(\mathcal{M})V\right)$; and letting $m_h \equiv |[\phi_{i_h}]|$; we have at once, respectively, the desired conclusions (2,a), (2,b,i), (2,b,ii), (2,b,iii), (2,b,iv) & (2,b,v) of this Corollary.

Finally, the desired conclusion (1) of this Corollary follows at once from our initial supposition here on $\mathcal{M}$, together with Theorem 7.C.6, parts (1) and (2).

$\square$

We mention that the following, final Corollary can be proved slickly and "implicitly" by Zorn's Lemma, or "explicitly" by means of Theorem 7.C.1, Lemma 4.B.5, and Theorem 7.C.6. We omit the straightforward proofs here.

**Corollary 7.C.9**

Let $n \in \mathbb{Z}^+$.

Let $\mathcal{A} \subseteq M(n,k)$.

Suppose $\mathcal{A}$ is a diagonalizable (over $L$) subset of $M(n,k)$.

**Then:**

$\exists \mathcal{M} \subseteq M(n,k)$: $\mathcal{M} \supseteq \mathcal{A}$

and

$\mathcal{M}$ is a maximal diagonalizable (over $L$) subset of $M(n,k)$.

# Appendix

## A. Matrices

**Proposition App. 1**

Let $n \in \mathbb{Z}^+$. Let $k$ be any field. Let $P \in G\ell(n,k)$.

**Then:**

$\forall b \in \{1, \ldots, n\}$:

every subset of $b$ columns of $P$ (consecutive or not) contains some $b \times b$ submatrix of rows (not necessarily consecutive), which is an *invertible* matrix.

**Proof.**

As $P \in G\ell(n,k)$, its columns are linearly independent over $k$; and so, a fortiori, every subset of $b$ columns is linearly independent over $k$ — and thus the $n \times b$ submatrix it forms (not necessarily of consecutive columns), has rank $b$. As for any matrix: (column rank) = (row rank), all such $n \times b$ submatrices of $P$ thus have *row* rank $b$. As the span of such a row space thus has dimension $b$, it must contain $b$ (not necessarily consecutive) linearly independent rows. This $b \times b$ subblock of rows (not necessarily consecutive), is thus invertible, and so can be taken as the above-desired submatrix.

□

## B. Ideal Theory and Matrix Applications

**Lemma App. 2** (A Key Argument)

Let $k$ and $E$ be any fields.

Suppose $\phi\colon \overline{k} \hookrightarrow E$ is an imbedding of fields.

Let $n \in \mathbb{Z}^{+}$.

Let $I$ be any *proper* ideal of $\overline{k}[x_1, \ldots, x_n]$.

**Then:**

$\exists$ map $\widehat{\phi}\colon \overline{k}[x_1, \ldots, x_n] \big/ I \longrightarrow E$, such that:

1) $\widehat{\phi}$ is a homomorphism of rings;

2) $\widehat{\phi}\big|\overline{k} = \phi$.

I.e., $\phi$ can be homomorphically extended from $\overline{k}$ to $\overline{k}[x_1, \ldots, x_n] \big/ I$.

[ Note: as $I$ is a proper ideal, $\overline{k}$ is canonically imbedded in $\overline{k}[x_1, \ldots, x_n] \big/ I$. ]

**Proof.**

The Little Nullstellensatz will be used to prove this. Though it is not necessary to use it, it provides a fast and elementary proof.

1) Let $\tilde{\phi}\colon \overline{k}[x_1,\ldots,x_n] \longrightarrow E[x_1,\ldots,x_n]$ be the canonical ring-homomorphic extension of $\phi$ — i.e., replace coefficients of elements of $\overline{k}[x_1,\ldots,x_n]$ with their images under $\phi$.

2) As $I$ is a *proper* ideal of $\overline{k}[x_1,\ldots,x_n]$, we may let $M$ be a maximal ideal of $\overline{k}[x_1,\ldots,x_n]$ that contains $I$:

$$I \subseteq M \subset \overline{k}[x_1,\ldots,x_n], \quad M \text{ a maximal ideal.}$$

3) By the Little Nullstellensatz, $M$ has a zero in $\overline{k}^{\,n}$:

$$\exists\, \vec{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \overline{k}^{\,n}\colon \quad \vec{\alpha} \text{ is a zero of } M.$$

4) Now define the map $\widehat{\phi}$ below:

$$\widehat{\phi}\colon \overline{k}[x_1,\ldots,x_n]\big/ I \longrightarrow E;$$

$$\widehat{\phi}\colon f + I \longmapsto \tilde{\phi}(f)\big(\phi(\alpha_1),\ldots,\phi(\alpha_n)\big) \quad \Big[= \tilde{\phi}(f)\big(\phi(\vec{\alpha})\big)\Big].$$

5) It is easy to check that $\widehat{\phi}$ is well-defined:

$$\begin{aligned} f+I=g+I \; &\Longrightarrow f-g \in I \subseteq M \\ &\Longrightarrow (f-g)(\vec{\alpha}) = 0 \\ &\Longrightarrow f(\vec{\alpha}) = g(\vec{\alpha}) \quad \big[\in \overline{k}\,\big] \\ &\Longrightarrow \phi\big(f(\vec{\alpha})\big) = \phi\big(g(\vec{\alpha})\big) \quad \big[\text{by given: } \overline{k} = \text{domain}(\phi)\,\big] \\ &\Longrightarrow \big(\tilde{\phi}(f)\big)\big(\phi(\vec{\alpha})\big) = \big(\tilde{\phi}(g)\big)\big(\phi(\vec{\alpha})\big) \quad [\text{ see note below }] \\ &\Longrightarrow \widehat{\phi}(f) = \widehat{\phi}(g). \end{aligned}$$

Therefore: $\widehat{\phi}$ is well-defined.

[ Note (refered to in above implication sequence): for any $h \in \overline{k}[x_1, \dots, x_n]$ and with $h$ written out in its canonical form, as $\phi$ is a homomorphism, we see at once: $\phi\big(h\,(\vec{\alpha})\big) = \big(\tilde{\phi}(h)\big)\,\big(\phi\,(\vec{\alpha})\big)$. ]

6) It is also easy to check that $\widehat{\phi}$ is a ring homomorphism — either by direct verification, or immediately, by observing that:

$\widehat{\phi} = (\text{"eval–@–}\vec{\alpha}\text{"}) \circ \tilde{\phi}$; making $\widehat{\phi}$ a composition of 2 ring homomorphisms.

7) Lastly, by the definition of $\tilde{\phi}$, it is immediate that $\widehat{\phi}\big|\overline{k} = \phi$:

$\alpha \in \overline{k}$ $\Big[$ so $\alpha$ "is" a constant polynomial of $\overline{k}[x_1, \dots, x_n]$ $\Big]$ $\Longrightarrow$

$$\widehat{\phi}(\alpha) = \tilde{\phi}(\alpha)\big(\phi(\alpha)\big) = \phi(\alpha).$$

□

**Corollary App. 3**

Let $k$ be any field.

Let $A$ be a finitely-generated, commutative $\overline{k}$–algebra; $A \neq \{0\}$.

**Then:**

$\exists$ map $\phi: A \longrightarrow \overline{k}$, such that:

1) $\phi$ is a homomorphism of $\overline{k}$–algebras;

2) $\phi\big|\overline{k} = id_{\overline{k}}$ .

**Proof.**

1) $A$ a finitely-generated commutative $\overline{k}$–algebra $\Longrightarrow$

$A = \overline{k}[\theta_1, \ldots, \theta_n]$; for some $\theta_1, \ldots, \theta_n \in A \Longrightarrow$

$\overline{k}[x_1, \ldots, x_n] \big/ I \approx A$; by the canonical isomorphism, say $\eta$, where:

$\eta$: $x_i + I \longmapsto \theta_i$, and $\eta\big|\overline{k} = \mathrm{id}_{\overline{k}}$ [ as $A \neq \{0\}$ ].

Furthermore, as $A \neq \{0\}$, we have that $I$ is a proper ideal of $\overline{k}[x_1, \ldots, x_n]$.

2) Now let: $\phi \equiv \mathrm{id}_{\overline{k}}$, $E \equiv \overline{k}$.

Certainly then: $\phi$: $\overline{k} \hookrightarrow E$, is an imbedding of fields.

3) Thus, by the previous Lemma App. 2, at once: $\phi$ can be ring-homomorphically extended to $\overline{k}[x_1, \ldots, x_n] \big/ I$:

$$\widehat{\phi}: \overline{k}[x_1, \ldots, x_n] \big/ I \longrightarrow E; \quad \widehat{\phi} \text{ is a ring homomorphism;} \quad \widehat{\phi}\big|\overline{k} = \phi.$$

And we note then, as $\phi \equiv \mathrm{id}_{\overline{k}}$, and $\widehat{\phi}\big|\overline{k} = \phi$, so $\widehat{\phi}\big|\overline{k} = \mathrm{id}_{\overline{k}}$.

4) So we now have the sequence of homomorphisms and isomorphisms, each of which is the identity on $\overline{k}$:

$$A \xrightarrow[\text{iso.}]{\eta^{-1}} \overline{k}[x_1,\dots,x_n]\big/ I \xrightarrow[\text{homo.}]{\widehat{\phi}} \overline{k} = E; \qquad \eta^{-1}\big|\overline{k} = \widehat{\phi}\big|\overline{k} = \mathrm{id}_{\overline{k}};$$

$$\text{and thus:} \qquad A \xrightarrow[\text{homo.}]{\widehat{\phi}\circ\eta^{-1}} E; \qquad \left(\widehat{\phi}\circ\eta^{-1}\right)\Big|\overline{k} = \mathrm{id}_{\overline{k}}.$$

Thus, letting $\phi \equiv \widehat{\phi}\circ\eta^{-1}$, we have the desired result.

□

**Proposition App. 4**

Let $n \in \mathbb{Z}^+$.

Let $k$ be any field.

Let $L$ be any extension field of $\overline{k}$.

Let $\mathcal{A}, \mathcal{B} \subseteq M\left(n, \overline{k}\right)$.

Suppose: $P \in G\ell(n, L)$ and $P\mathcal{A}P^{-1} \subseteq \mathcal{B}$. Write: $P = (p_{i,j})$.

**Then:**

a) $\exists C \in C_L(\mathcal{A})\colon \exists Q = (q_{i,j}) \in G\ell\left(n, \overline{k}\right)$:

i) $P = QC$;

ii) $\forall (i,j) \in \{1, \ldots, n\}^2\colon \qquad p_{i,j} \in \overline{k} \quad \Longrightarrow \quad q_{i,j} = p_{i,j}.$

b) For any $Q \in G\ell\left(n, \overline{k}\right)$ occuring in (a) above:

i) $\forall A \in \mathcal{A}\colon \quad PAP^{-1} = QAQ^{-1}$;

ii) $Q\mathcal{A}Q^{-1} \subseteq \mathcal{B}$.

**Proof.**

1) Let $L' \equiv \overline{k}\,[\text{ the } n^2 \text{ entries of } P\,]$. Thus, $L'$ is a finitely-generated, commutative $\overline{k}$–algebra. As $P$ is given invertible, not all entries of $P$ are 0, and so $L' \neq \{0\}$; and so also: $\overline{k} \subseteq L'$.

Thus, by the previous Corollary App. 3, we have some map $\phi$:

$$\phi\colon L' \xrightarrow{\overline{k}\text{-algebra homo.}} \overline{k}, \qquad \text{and} \qquad \phi \big| \overline{k} = \mathrm{id}_{\overline{k}}.$$

2) Now by definition of $L'$, and the given, we clearly have:

$$P \in G\ell(n, L') \quad \text{and} \quad \mathcal{A}, \mathcal{B} \subseteq M(n, L') \qquad \left[\text{ as } \overline{k} \subseteq L',\ \text{from Step (1)}\right].$$

Now let:

$$Q \equiv \phi(P); \quad \text{and so } Q \subseteq M\left(n, \overline{k}\right).$$

As $P$ is invertible, and $\phi$ is a $k$–algebra homomorphism, certainly $Q$ is invertible. Thus:

$$Q \in G\ell\left(n, \overline{k}\right).$$

3) As given $P\mathcal{A}P^{-1} \subseteq \mathcal{B}$:

$$\forall A \in \mathcal{A} \colon \exists B \in \mathcal{B} \colon \qquad PAP^{-1} = B.$$

As $\phi$ is a homomorphism on $L'$, and $\overline{k} \subseteq L'$ (as in Step (1) above), and $P \in G\ell(n, L')$ (in the first line of Step (2) above), we have:

$$\phi(P)\phi(A)\phi(P)^{-1} = \phi(B).$$

As $\phi \big| \overline{k} = \mathrm{id}_{\overline{k}}$, and given $\mathcal{A}$, $\mathcal{B} \subseteq M\left(n, \overline{k}\right)$, we now have:

$$\phi(P)\, A\, \phi(P)^{-1} = B.$$

Thus, by definition of $Q$ in Step (2), we have:

$$QAQ^{-1} = B.$$

Thus, from the first line of this Step, we have at once:

$$QAQ^{-1} = PAP^{-1}.$$

Hence, as $A$ is arbitrary in $\mathcal{A}$, $Q \in G\ell\left(n, \overline{k}\right)$, $P \in G\ell(n, L)$, and $\overline{k} \subseteq L' \subseteq L$ (by Step (1), and by construction of $L'$), the previous gives at once:

$$P^{-1}Q \in \mathcal{C}_L(\mathcal{A}).$$

Thus:

$$P = QC, \qquad \text{for some } C \in \mathcal{C}_L(\mathcal{A}).$$

This, with the last line of Step (2) above, establishes desired result (a,i).

4) As $Q \equiv \phi(P)$, and $\phi\big|\overline{k} = \mathrm{id}_{\overline{k}}$, at once:

$$(p_{i,j}) \in \overline{k} \quad \Longrightarrow \quad (q_{i,j}) \in \overline{k}.$$

This establishes desired result (a,ii).

5) For any $Q$ occuring in part (a) of the given, we have: $P = QC$, and $C \in \mathcal{C}_L(\mathcal{A})$. As $C$ then commutes with all elements of $\mathcal{A}$, the desired result (b,i) follows immediately, and the desired result (b,ii) follows immediately from this result (b,i) and the last line of the given.

□

**Corollary App. 5**

Let $n \in \mathbb{Z}^+$.

Let $k$ be any field.

Let $L$ be any extension field of $\overline{k}$.

Let $\mathcal{A} \subseteq M\left(n, \overline{k}\right)$.

**Then:**

$$\mathcal{A} \text{ is } k\text{–rationalizable over } L \iff \mathcal{A} \text{ is } k\text{–rationalizable over } \overline{k}.$$

**Proof.**

($\Longleftarrow$) Immediate, as given $\overline{k} \subseteq L$.

($\Longrightarrow$) Immediate from the previous Proposition App. 4, by letting:

$$P \in G\ell(n, L), \quad \text{where } P \;\; k\text{–rationalizes } \mathcal{A}, \qquad \text{and} \quad \mathcal{B} \equiv M\left(n, \overline{k}\right);$$

then taking any $Q$ from part (a) of that Proposition, and then using part (b,ii) of that Proposition.

□

## C. Centralizers of Block-Diagonal Matrices

### Proposition App. 6

Let $F$ be any field.

Let $L$ be any extension field of $F$.

Let $n \in \mathbb{Z}^+$; $b_1, \ldots, b_n \in \mathbb{Z}^+$.

Let $\mathcal{Y} \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} M(b_i, F)$ ; and, for all $Y \in \mathcal{Y}$, express $Y$ in the obvious [and unique] way as:

$$Y = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} Y^{(i)}, \quad \text{where} \quad Y^{(i)} \in M(b_i, F).$$

Let $\mathcal{Y}^{(i)} \equiv \left\{ Y^{(i)} \middle| Y \in \mathcal{Y} \right\} \subseteq M(b_i, F)$.

Suppose: $\mathcal{C}_L(\mathcal{Y}) \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} M(b_i, L)$.

**Then:**

$$\mathcal{C}_L(\mathcal{Y}) = \mathcal{C}_L\left( \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)} \right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left( \mathcal{Y}^{(i)} \right).$$

**Proof.**

1) By definition of $\mathcal{Y}^{(i)}$, we certainly have:

$$\mathcal{Y} \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)}.$$

As $\mathcal{C}_L$ is clearly an inclusion-reversing operator, the previous gives:

$$\mathcal{C}_L(\mathcal{Y}) \supseteq \mathcal{C}_L\left( \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)} \right).$$

2) Now let $C \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left( \mathcal{Y}^{(i)} \right)$, and write $C$ in the obvious [and unique] way as:

$$C = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} C_i, \qquad \text{for some} \quad C_i \in \mathcal{C}_L\left( \mathcal{Y}^{(i)} \right) \subseteq M(b_i, L)$$

[ the latter is true as: $\mathcal{Y}^{(i)} \subseteq M(b_i, F)$ and $F \subseteq L$ ].

From the previous on $C_i$, certainly $C_i$ commutes with all elements of $\mathcal{Y}^{(i)}$, and so clearly:

$$\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} C_i \quad \text{commutes with all elements of} \quad \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)}.$$

Thus:

$$\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} C_i \in \mathcal{C}_L\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)}\right).$$

Hence, as the LHS of the previous is $C$ (as given above), and $C$ is arbitrary, we have:

$$\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left(\mathcal{Y}^{(i)}\right) \subseteq \mathcal{C}_L\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)}\right).$$

Combining the previous with the last line of Step (1), we have:

$$\mathcal{C}_L(\mathcal{Y}) \supseteq \mathcal{C}_L\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)}\right) \supseteq \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left(\mathcal{Y}^{(i)}\right).$$

[Note that the previous is obtained independently of any restrictions on $\mathcal{C}_L(\mathcal{Y})$ — thus giving the Remark that follows this Proposition.]

3) Now let $D \in \mathcal{C}_L(\mathcal{Y})$. So $D$ commutes with all the elements of $\mathcal{Y}$. Now, by the given on $\mathcal{C}_L(\mathcal{Y})$, we may write $D$ in the obvious [and unique] way as:

$$D = \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} D_i, \qquad \text{for some} \quad D_i \in M(b_i, L).$$

Now let $Y \in \mathcal{Y}$. So, as in the given, we may write $Y$ in the obvious [and unique] way as:

$$Y = \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} Y_i, \qquad \text{for some} \quad Y_i \in \mathcal{Y}^{(i)} \subseteq M(b_i, L).$$

Thus:

$$D \text{ commutes with } Y \quad \Longrightarrow \quad \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} D_i \quad \text{commutes with} \quad \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} Y_i.$$

As the latter two block-diagonal matrices each have $n$ blocks, with the same successive dimensions $[b_1, \ldots, b_n]$, we have at once:

$$D_i \text{ commutes with } Y_i.$$

As $Y$ is arbitrary, and by the construction of $\mathcal{Y}^{(i)}$, we have at once: $D_i$ commutes with all elements of $\mathcal{Y}^{(i)}$. Thus:

$$D_i \in \mathcal{C}_L\left(\mathcal{Y}^{(i)}\right).$$

Thus:

$$D = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} D_i \in \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left(\mathcal{Y}^{(i)}\right).$$

As $D$ is arbitrary (as taken above), we thus have:

$$\mathcal{C}_L(\mathcal{Y}) \subseteq \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left(\mathcal{Y}^{(i)}\right).$$

This, together with the result at the end of Step (2), gives at once:

$$\mathcal{C}_L(\mathcal{Y}) = \mathcal{C}_L\left(\mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{Y}^{(i)}\right) = \mathop{\bigcirc\kern-0.75em\triangle}\limits_{i=1}^{n} \mathcal{C}_L\left(\mathcal{Y}^{(i)}\right).$$

□

**Remark**

For the general case of $\mathcal{Y}$ as above — where we do not make any suppositions on $C_L(\mathcal{Y})$, as pointed out at the end of Step (2) of the above Proof, we always have the following weaker facts:

$$C_L(\mathcal{Y}) \supseteq C_L\left(\mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} \mathcal{Y}^{(i)}\right) \supseteq \mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} C_L\left(\mathcal{Y}^{(i)}\right).$$

**Corollary App. 7**

Let $F$ be any field.

Let $L$ be any extension field of $F$.

Let $n \in \mathbb{Z}^+$; $\quad b_1, \ldots, b_n \in \mathbb{Z}^+$.

For $i \in \{1, \ldots, n\}$, let: $\mathcal{X}_i \subseteq M(b_i, F)$.

Suppose: $\quad C_L\left(\mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} \mathcal{X}_i\right) \subseteq \mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} M(b_i, L)$.

**Then:**

$$C_L\left(\mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} \mathcal{X}_i\right) = \mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} C_L(\mathcal{X}_i).$$

**Proof.**

This follows immediately from Proposition App. 6, by letting: "$\mathcal{Y}$" $\equiv \mathop{\bigcirc\hspace{-0.75em}\triangle}_{i=1}^{n} \mathcal{X}_i$, and then noting at once that: "$\mathcal{Y}^{(i)}$" $= \mathcal{X}_i$.

$\square$

**Proposition App. 8**

Let $F$ be any field.

Let $L$ be any extension field of $F$.

Let $n \in \mathbb{Z}^+$; $b_1, \ldots, b_n \in \mathbb{Z}^+$.

Let $\mathcal{X}_i \subseteq M(b_i, F)$.

Suppose $A_i \in \mathcal{X}_i$; and pair-wise, $A_1, \ldots, A_n$ have no common eigenvalues (i.e., $i \neq j \implies A_i, A_j$ have no common eigenvalues).

**Then:**

a) $C_L\left(\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{n} \mathcal{X}_i\right) = \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{n} C_L(\mathcal{X}_i) \subseteq \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{n} M(b_i, L)$.

b) In particular: $C_L\left(\mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{n} A_i\right) = \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{n} C_L(A_i) \subseteq \mathop{\text{\textcircled{$\triangle$}}}_{i=1}^{n} M(b_i, L)$.

**Proof.**

1) We prove (b) first; (a) will then to be shown to follow almost immediately.

2) To prove (b), it suffices to prove it for $n = 2$; the general result then follows at once inductively. I.e., we wish to show:

(1)

$$A \subseteq M(b_1, F),\ B \subseteq M(b_2, F) \quad \text{and} \quad A,\ B \text{ have no common eigenvalues}$$

$$\implies$$

$$C_L\left(A \mathbin{\text{\textcircled{$\triangle$}}} B\right) = C_L(A) \mathbin{\text{\textcircled{$\triangle$}}} C_L(B).$$

3) Furthermore, to prove (1), it is clear that we may suppose that $A$ is upper triangular. [ $A$ can be conjugated into that form by an invertible matrix over $F$, and so certainly then, by an invertible matrix over $L$. ]

I.e., it suffices to show:

$$(2)\qquad \begin{gathered} T \subseteq M(b_1, F),\ T \text{ upper triangular}, \quad B \subseteq M(b_2, F); \\ T,\ B \text{ have no common eigenvalues} \\ \Longrightarrow \\ \mathcal{C}_L\left(T \mathbin{\bigcirc\mkern-15mu\triangle} B\right) = \mathcal{C}_L(T) \mathbin{\bigcirc\mkern-15mu\triangle} \mathcal{C}_L(B). \end{gathered}$$

4) Now let $M \in \mathcal{C}_L\left(T \mathbin{\bigcirc\mkern-15mu\triangle} B\right)$. Write $M$ as:

$$(3)\qquad M = \begin{array}{c c} & \begin{array}{cc} b_1 & b_2 \end{array} \\ \begin{array}{c} b_1 \\ b_2 \end{array} & \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \end{array}; \qquad \text{where } P,\ Q,\ R,\ S \text{ are all matrices over } L.$$

As $M \in \mathcal{C}_L\left(T \mathbin{\bigcirc\mkern-15mu\triangle} B\right)$, we have:

$$\begin{pmatrix} P & Q \\ R & S \end{pmatrix} \begin{pmatrix} T & \\ & B \end{pmatrix} = \begin{pmatrix} T & \\ & B \end{pmatrix} \begin{pmatrix} P & Q \\ R & S \end{pmatrix}.$$

Thus, by (2) and (3): the submatrix dimensions within all the matrices of the previous equation are "compatible", and so we now have at once:

$$(4)\qquad PT = TP, \quad QB = TQ, \quad RT = BR, \quad SB = BS.$$

5) The first and last equations in (4) show at once:

$$(5)\qquad P \in \mathcal{C}_L(T), \qquad S \in \mathcal{C}_L(B).$$

6) Now consider the second equation in (4):

$$(6) \qquad QB = TQ.$$

Recalling that $T$ is upper triangular, and $T \subseteq M(b_1, F)$, we may let the diagonal entries of $T$ be, in order: $t_1, \ldots, t_{b_1} \in F$.

Now define the following notation for temporary use:

$$(7) \qquad \text{For any matrix } M: \quad \overline{\rho}(M) \equiv \text{the last row of } M.$$

Thus, with this definition, and the definition of the $t_i$ above, we have at once from equation (6):

$$\overline{\rho}(Q)\, B = t_{b_1} \cdot \overline{\rho}(Q).$$

Taking the transpose of both sides of the previous, we get:

$$B^T\, \overline{\rho}(Q)^T = t_{b_1} \cdot \overline{\rho}(Q)^T.$$

Thus:

$$\overline{\rho}(Q)^T = 0 \qquad \text{or} \qquad t_{b_1} \text{ is an eigenvalue of } B^T.$$

Hence $\left[\text{as } \det(\lambda I - X) = \det(\lambda I - X)^T = \det\left(\lambda I - X^T\right)\right]$:

$$\overline{\rho}(Q)^T = 0 \qquad \text{or} \qquad t_{b_1} \text{ is an eigenvalue of } B.$$

As $t_{b_1}$ is a diagonal entry (even the last one) of $T$, and $T$ is upper triangular, so $t_{b_1}$ is an eigenvalue of $T$. This is in contradiction with the latter part of the previous result. Hence, we have the former part of the previous result:

$$\overline{\rho}(Q)^T = 0.$$

Thus:

$$\overline{p}(Q) = 0.$$

Hence, by definition of $\overline{p}$, we have now:

(8) the last row of $Q$ is: $0$.

7) Now taking the result in (8), substituting it into the equation in (6), and following the identical argument in the previous Step — but now for the second-to-last row of $Q$, we find the same way:

(9) the second-to-last row of $Q$ is: $0$.

Continuing to argue this way (or inductively), we see:

all rows of $Q$ are: $0$.

I.e.:

$$Q = 0. \tag{10}$$

8) Now return to (4), and consider its third equation:

$$RT = BR.$$

Analyzing this exactly as in Step (6) above — but now with $\overline{p}$ meaning *the first column* of any matrix, we conclude exactly as in Step (7) above, that:

$$R = 0. \tag{11}$$

9) Now looking back at (3), and combining this with (10) and (11), we have at once:

$$M = P \mathbin{\bigcirc\mkern-15mu\triangle} S\,.$$

Thus, by (5), we have:

$$M \in \mathcal{C}_L(P) \mathbin{\bigcirc\mkern-15mu\triangle} \mathcal{C}_L(S)\,.$$

So, as $M$ is arbitray in $\mathcal{C}_L\left(T \mathbin{\bigcirc\mkern-15mu\triangle} B\right)$, we have:

$$\mathcal{C}_L\left(T \mathbin{\bigcirc\mkern-15mu\triangle} B\right) \subseteq \mathcal{C}_L(P) \mathbin{\bigcirc\mkern-15mu\triangle} \mathcal{C}_L(S)\,.$$

As the reverse inclusion of the previous is trivially true, we have at once:

$$\mathcal{C}_L\left(T \mathbin{\bigcirc\mkern-15mu\triangle} B\right) = \mathcal{C}_L(P) \mathbin{\bigcirc\mkern-15mu\triangle} \mathcal{C}_L(S)\,.$$

Thus: we have shown (2). As discussed above, this shows (1), which, as also discussed above, shows (b).

Thus we have now proved (b).

10) Now (a) follows fairly easily from (b).

As:

$$\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} A_i \in \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{X}_i\,,$$

and the centralizer operator in inclusion–reversing, we have, together with the now–proved result (b):

$$C_L\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} \mathcal{X}_i\right) \subseteq C_L\left(\mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} A_i\right) = \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} C_L(A_i) \subseteq \mathop{\bigcirc\mkern-15mu\triangle}\limits_{i=1}^{n} M(b_i, L).$$

So, in particular:

$$\mathcal{C}_L\left(\mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{X}_i\right) \subseteq \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} M(b_i, L). \tag{12}$$

11) Now let:

$$M \in \mathcal{C}_L\left(\mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{X}_i\right). \tag{13}$$

So, by (12):

$$M = \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} M_i\ ; \qquad \text{for some} \quad M_i \in M(b_i, L).$$

Thus, by the given on $M$, and the previous, we have:

$$\mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} M_i \qquad \text{commutes with all elements of} \qquad \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{X}_i.$$

Writing the previous out, and as the dimensions of $M_i$ are the same as those of the elements of $\mathcal{X}_i$, we have at once:

$$M_i \in \mathcal{C}_L(\mathcal{X}_i).$$

Thus:

$$\mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} M_i \in \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{C}_L(\mathcal{X}_i).$$

Hence:

$$M \in \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{C}_L(\mathcal{X}_i).$$

As $M$ was taken arbitrarily in (13), we have now:

$$\mathcal{C}_L\left(\mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{X}_i\right) \subseteq \mathop{\bigcirc\kern-0.85em\triangle}\limits_{i=1}^{n} \mathcal{C}_L(\mathcal{X}_i).$$

As the reverse inclusion of the previous is trivially true, we now have at once:

$$C_L\left(\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{n} \mathcal{X}_i\right) = \mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{n} C_L(\mathcal{X}_i)\,.$$

This proves (a).

This now completes the proof of this Proposition.

□

**Proposition App. 9**

Let $F$ be any field.

Let $L$ be any extension field of $F$.

Let $n \in \mathbb{Z}^+$, and $\lambda \in F$.

**Then:**

i) $C_L(\lambda I_n) = C_L\big(L[\lambda I_n]\big) = C_L\big(\mathrm{Scalar}(n, L)\big) = M(n, L)$.

ii) $C_L(N_n) = C_L\big(L[N_n]\big) = L[N_n]$.

iii) $C_L(M(n, F)) = C_L\big(L[M(n, F)]\big) = C_L(M(n, L)) = \mathrm{Scalar}(n, L)$.

**Proof.**

Clearly, within each of the desired results (i)–(iii), all equalities are immediate, except possibly the last equality. These last equalities we show below.

1) As the center of $M(n, L)$ is $\text{Scalar}(n, L)$, (iii) follows at once. The same fact gives (i) at once.

2) Here we show first: $\mathcal{C}_L(N_n) = L[N_n]$. Then, in (ii), as mentioned above, the other equality was immediate before this.

Let: $C \in \mathcal{C}_L(N_n)$. Thus: $CN_n = N_nC$. Recalling, as in Chapter 1, that $N_n$ is the canonical $n \times n$ nilpotent matrix; we see $CN_n$ is $C$, with its columns shifted to the right by 1, and all 0's in column 1. Similarly, $N_nC$ is $C$, with its rows shifted up by 1, and all 0's in row $n$. Equating these two matrices, element-wise, we see at once that: the first column of $C$ is all 0's, except possibly for the $(1,1)$–entry. Similarly, at once, the last row of $C$ is all 0's, except possibly for the $(n,n)$–entry. Now with this about $C$, we look again at the above equation: $CN_n = N_nC$, analyze it similarly, and then iteratively find that $C$ must be upper triangular. Now with this further information about $C$, we look again at the above equation: $CN_n = N_nC$, and equate the $(1,n)$–entries. At once, this shows that the $(1,n-1)$ and $(2,n)$–entries of $C$ are identical — i.e., the next-to-last upper diagonal of $C$ consists of identical entries. With this, we again look at the above equation, analyze it similarly, and then iteratively find that each upper diagonal, and the main diagonal, of $C$, consist of their own identical entries. As $C$ is upper triangular, this now shows at once that: $C \in L[N_n]$.

$\square$

# D. Subsets of Diagonal Matrices

In this section, we let $F$ be any field and $L$ any extension field of $F$.

We let $n \in \mathbb{Z}^+$.

Recall the following simple notation pertaining to diagonal matrices, as discussed in Chapter 1. For $Y \in D(n,F)$ and $i \in \{1,\ldots,n\}$, we let $Y_{ii} \in F$ be the $i^{th}$ diagonal entry of $Y$.

a) **Definition**

Let $\mathcal{Y} \subseteq D(n,F)$.

Then we let:

$$T(\mathcal{Y}) \equiv \left\{ (i,j) \in \{1,\ldots,n\}^2 \,\middle|\, \forall Y \in \mathcal{Y}\colon\ Y_{ii} = Y_{jj} \right\} \subseteq \{1,\ldots,n\}^2.$$

b) **Results**

i) **Proposition App. 10a**

Let $\mathcal{Y} \subseteq D(n,F)$.

**Then:**

$$C_L(\mathcal{Y}) = \left\{ M = (m_{ij}) \in M(n,L) \,\middle|\, \forall (i,j) \notin T(\mathcal{Y})\colon\ m_{ij} = 0 \right\}.$$

**Proof.**

1) Let $Y \in \mathcal{Y}$, and let $M \in M(n,L)$. As $Y$ is diagonal: $MY$ is $M$, with its columns multiplied, respectively, by the corresponding diagonal entries of $Y$; and $YM$ is $M$, with its rows multiplied, respectively, by the corresponding diagonal entries of $Y$. With this, consider the equation: $MY = YM$, and equate all $n^2$ matrix entries. If $Y_{ii} = Y_{jj}$, then the above shows immediately that the equation is satisfied at the $(i,j)$–entry. If $Y_{ii} \neq Y_{jj}$, then the above shows immediately that the equation is satisfied at the $(i,j)$–entry precisely when: $m_{ij} = 0$. I.e., by definition of the operator $T$ above:

$$MY = YM \iff$$

$$M \in \left\{ M = (m_{ij}) \in M(n,L) \,\middle|\, \forall (i,j) \notin T\big(\{Y\}\big):\ m_{ij} = 0 \right\} .$$

Thus:

$$C_L\big(\{Y\}\big) = \left\{ M = (m_{ij}) \in M(n,L) \,\middle|\, \forall (i,j) \notin T\big(\{Y\}\big):\ m_{ij} = 0 \right\}.$$

2) Thus, at once by the previous (using DeMorgan's Law in the third equality below):

$$\begin{aligned}
\mathcal{C}_L(\mathcal{Y}) &= \textstyle\bigcap_{Y\in\mathcal{Y}} \mathcal{C}_L\big(\{Y\}\big) \\
&= \textstyle\bigcap_{Y\in\mathcal{Y}} \Big\{M=(m_{ij})\in M(n,L)\,\Big|\,\forall (i,j)\notin T\big(\{Y\}\big):\ m_{ij}=0\Big\} \\
&= \Big\{M=(m_{ij})\in M(n,L)\,\Big|\,\forall (i,j)\notin \textstyle\bigcup_{Y\in\mathcal{Y}} T\big(\{Y\}\big):\ m_{ij}=0\Big\} \\
&= \Big\{M=(m_{ij})\in M(n,L)\,\Big|\,\forall (i,j)\notin T\Big(\textstyle\bigcup_{Y\in\mathcal{Y}}\{Y\}\Big):\ m_{ij}=0\Big\} \\
&= \Big\{M=(m_{ij})\in M(n,L)\,\Big|\,\forall (i,j)\notin T(\mathcal{Y}):\ m_{ij}=0\Big\}.
\end{aligned}$$

Note that the fourth equality above is easily seen:

$$\begin{aligned}
(i,j)\in \textstyle\bigcup_{Y\in\mathcal{Y}} T\big(\{Y\}\big) &\iff \forall Y\in\mathcal{Y}:\ (i,j)\in T\big(\{Y\}\big) \\
&\iff \forall Y\in\mathcal{Y}:\ Y_{ii}=Y_{jj} \\
&\iff \forall Y\in \textstyle\bigcup_{Y\in\mathcal{Y}}\{Y\}:\ Y_{ii}=Y_{jj} \quad \text{[trivially]} \\
&\iff Y\in T\Big(\textstyle\bigcup_{Y\in\mathcal{Y}}\{Y\}\Big).
\end{aligned}$$

□

ii) **Proposition App. 10b**

Let $\mathcal{Y}\subseteq D(n,F)$.

**Then:**

$T(\mathcal{Y})$ is an equivalence relation on $\{1,\ldots,n\}$.

**Proof.**

Recall the definition of $T(\mathcal{Y})$:

$$T(\mathcal{Y}) \equiv \Big\{(i,j)\in\{1,\ldots,n\}^2\,\Big|\,\forall Y\in\mathcal{Y}:\ Y_{ii}=Y_{jj}\Big\}\subseteq\{1,\ldots,n\}^2.$$

We see at once that $T(\mathcal{Y})$ is reflexive, symmetric, and transitive. □

### iii) Corollary App. 11

Let $\mathcal{Y} \subseteq D(n, F)$.

By Proposition App. 10b, of this Appendix, we may let the set, $\{1, \ldots, n\}$, have $m \in \{1, \ldots, n\}$ equivalence classes under $T(\mathcal{Y})$ $\Big[$ i.e., $m \equiv \big|\{1, \ldots, n\}/T(\mathcal{Y})\big| \in \{1, \ldots, n\}\Big]$.

We let the cardinalities of the above $m$ equivalence classes be (including multiplicity): $b_1, \ldots, b_m \in \mathbb{Z}^+$.

**Then:**

$$\exists\, \Pi \in \mathrm{Perm}(n, F):$$

$$\mathcal{Y} \subseteq \Pi^{-1} \left[\mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{m} \mathrm{Scalar}(b_i, L)\right] \Pi \qquad \text{and} \qquad \mathcal{C}_L(\mathcal{Y}) = \Pi^{-1} \left[\mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{m} M(b_i, L)\right] \Pi.$$

**Proof.**

1) Let the sequence $(1, \ldots, n)$ be permuted so the resulting sequence lists the equivalence classes of $(1, \ldots, n)$ under $T(\mathcal{Y})$, consecutively; say:

(1) $(1,\dots,n)$ is permuted to

$$\left( \underbrace{\underbrace{i_{c_1},\dots,i_{c_2-1}}\,\underbrace{i_{c_2},\dots,i_{c_3-1}},\dots\dots,\underbrace{i_{c_{m-1}},\dots,i_{c_m-1}}}_{\text{the equivalence classes under } T(\mathcal{Y})} \right);$$

where the $c_j$ "measure" the size of the equivalence classes:

$$c_1 = 1,\ (c_2 - c_1) = b_2,\ \dots\dots,\ (c_{m-1} - c_m) = b_m$$

$$\left[\text{i.e.,}\quad c_1 \equiv 1;\quad c_j \equiv \sum_{t=1}^{m} b_j\,,\ \text{for } j \in \{2,\dots,m\}\right].$$

2) Let $p \in S_n$ be the permutation on $\{1,\dots,n\}$ that achieves the above change on $\{1,\dots,n\}$, and, using the notation of Chapter 1, let $\Pi \equiv \Pi_n(p) \in G\ell(n,L)$ be the basic permutation matrix of $p$.

Thus, conjugation of a diagonal matrix by $\Pi$ has the same permutational change on the location of its diagonal entries, as the change above has on the location of the entries of $\{1,\dots,n\}$.

3) Now let $Y \in \mathcal{Y}$. Then $\Pi Y \Pi^{-1}$ is $Y$, with its diagonal entries permuted as above — i.e., now located following the above order of the equivalence classes of $(1,\dots,n)$ under $T(\mathcal{Y})$.

By the definition of the operator $T$, for each equivalence class of $T(\mathcal{Y})$, the diagonal entries of $Y$ in the locations of that class, *are all iden-*

*tical*. Hence:

$$\text{(2)} \qquad \text{in } \Pi Y \Pi^{-1}:$$

the diagonal entries in the locations within each segment,
indicated in the RHS of (1) above, *are identical* .

Thus, recalling from Step (1) above that: $c_1 = 1$; $c_j \equiv \sum_{t=1}^{m} b_j$, for $j \in \{2, \ldots, m\}$; (and as in this section $F \subseteq L$), we have at once:

$$\Pi Y \Pi^{-1} \in \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{m} \text{Scalar}(b_i, L).$$

As $Y$ is arbitrary, this gives:

$$\Pi \mathcal{Y} \Pi^{-1} \subseteq \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{m} \text{Scalar}(b_i, L).$$

Hence:

$$\text{(3)} \qquad \mathcal{Y} \subseteq \Pi^{-1} \left[ \mathop{\bigcirc\!\!\!\!\!\triangle}_{i=1}^{m} \text{Scalar}(b_i, L) \right] \Pi.$$

This gives the first desired result of this Corollary.

4) Furthermore, by the definition of the operator $T$, for any two distinct equivalence classes of $T(\mathcal{Y})$, there is some $Y \in \mathcal{Y}$ where: the diagonal entries of $Y$, with locations from these two classes, and with necessarily identical values within each class, have ***distinct values*** for each of the two classes. Thus, the diagonal entries of $\Pi Y \Pi^{-1}$, with locations from the two segments — of the RHS of (1) above that form those two classes, *are distinct*.

This, together with (2), and the definition of the operator $T$, show:

$$(i,j) \in \mathcal{T}\left(\Pi \mathcal{Y} \Pi^{-1}\right)$$

$$\Longleftrightarrow$$

$i$ and $j$ belong to some single equivalence class block,

$\left(i_{c_{t-1}}, \ldots, i_{c_t - 1}\right)$, as in the RHS of (1)

$$\Longleftrightarrow$$

$$(i,j) \in \{i_{c_{t-1}}, \ldots, i_{c_t-1}\}^2, \qquad \text{for some} \quad t \in \{2, \ldots, m\}.$$

Thus, we have at once:

$$\mathcal{T}\left(\Pi \mathcal{Y} \Pi^{-1}\right) = \bigcup_{j=1}^{m} \{i_{c_{j-1}}, \ldots, i_{c_j-1}\}^2 \ ;$$

$$\text{where} \qquad c_1 = 1, \ \text{ and } \ c_{j+1} - c_j = b_j.$$

Thus, at once, by Proposition App. 10a, and clearly simplifying its conclusion, we see at once:

$$\mathcal{C}_L\left(\Pi \mathcal{Y} \Pi^{-1}\right) = \mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{m} M(b_i, L).$$

And so:

$$\mathcal{C}_L(\mathcal{Y}) = \Pi^{-1} \left[\mathop{\bigcirc\kern-0.75em\triangle}_{i=1}^{m} M(b_i, L)\right] \Pi.$$

This gives the second, and last, desired result of this Corollary.

$\square$

iv) **Corollary App. 12**

Let $\mathcal{Y} \subseteq D(n, F)$.

Let $f$ be any *injective* function from $F$ to $L$, that takes 0 to 0.

Without confusion, let $f$ also represent the natural (i.e., element-wise) extension of $f$, from $M(n, F)$ to $M(n, L)$.

**Then:**

$$\mathcal{C}_L\big(f(\mathcal{Y})\big) = \mathcal{C}_L(\mathcal{Y}).$$

**Proof.**

As $\mathcal{Y}$ is a set of diagonal matrices, and $f$ takes 0 to 0, clearly $f(\mathcal{Y})$ is also a set of diagonal matrices — $f(\mathcal{Y}) \subseteq D(n, L)$. As $f$ is injective, it takes distinct diagonal elements to distinct diagonal elements. Then, recalling the earlier definition of the operator $T$, it is immediate, or trivial, to verify directly that: $T\big(f(\mathcal{Y})\big) = T(\mathcal{Y})$. Thus, at once, by Proposition App. 10a: $\mathcal{C}_L\big(f(\mathcal{Y})\big) = \mathcal{C}_L(\mathcal{Y})$.

□

**Remark**

Recalling from Chapter 5, the definition of the row-functions of a subset $\mathcal{Y} \subseteq D(n, F)$, we easily note the following:

$$R^{(i)}_{\mathcal{Y}} = R^{(j)}_{\mathcal{Y}} \iff (i, j) \in T(\mathcal{Y}).$$

# E. Basic Matrix Varieties

In this section, we let $F$ be any field, and $L$ be any extension field of $F$.

We let $n \in \mathbb{Z}^+$.

## a) Definition

Let $T \subseteq \{1, \ldots, n\}^2$.

Then we let:

$$B(T) \equiv \left\{ M = (m_{ij}) \in M(n,F) \,\middle|\, \forall (i,j) \in T\colon\ m_{ij} = 0 \right\} \subseteq M(n,F).$$

We call a subset of $M(n,F)$ of the form $B(T)$, for some $T$, a *basic matrix variety (over $F$).* When clear, we abbreviate the latter name as: b.m.v. (over $F$).

Clearly, a basic matrix variety can be described as any set of matrices where a specified subset of its entries are forced to be 0, and all the remaining entries are allowed to be arbitrary.

## b) Results

### i) Proposition App. 13

We have the following two results:

1) $\left\{\mathcal{B}_\alpha \subseteq M(n,F) \,\middle|\, \alpha \in \mathcal{A}\right\}$ is a family of b.m.v.'s (over $F$) $\Longrightarrow$ $\bigcap_{\alpha\in\mathcal{A}} \mathcal{B}_\alpha$ is also a b.m.v. (over $F$).

2) $\mathcal{B}$ is a b.m.v. (over $F$) and $\Pi, \Psi \in \mathrm{Perm}(n,F)$ $\Longrightarrow$ $\Pi\,\mathcal{B}\,\Psi$ is also a b.m.v. (over $F$).

**Proof.**

1) $\mathcal{B}_\alpha$ is a b.m.v. (over $F$) $\Longrightarrow$ [ by definition of a b.m.v. ] $\mathcal{B}_\alpha = B\,(T_\alpha)$, for some $T_\alpha \subseteq \{1,\dots,n\}^2$. Thus: $\bigcap_{\alpha\in\mathcal{A}} \mathcal{B}_\alpha = \bigcap_{\alpha\in\mathcal{A}} B\,(T_\alpha)$; but clearly by definition of the operator $B$, the latter is $B\left(\bigcap_{\alpha\in\mathcal{A}} T_\alpha\right)$. As $T_\alpha \subseteq \{1,\dots,n\}^2$, certainly $\bigcap_{\alpha\in\mathcal{A}} T_\alpha \subseteq \{1,\dots,n\}^2$ ; and so by letting $T \equiv \bigcap_{\alpha\in\mathcal{A}} T_\alpha$, we have, with the previous: $T \subseteq \{1,\dots,n\}^2$, and $\bigcap_{\alpha\in\mathcal{A}} \mathcal{B}_\alpha = B(T)$.

This proves (1).

2) As $\mathcal{B}$ is a b.m.v., by definition: $\mathcal{B} = B(T)$, for some $T \subseteq \{1,\dots,n\}^2$. Now $\Pi\,\mathcal{B}$ is $\mathcal{B}$, with the rows of each its elements permuted by $\Pi$; $\Pi\,\mathcal{B}\,\Psi$ is $\Pi\mathcal{B}$, with the columns of each of its elements permuted by $\Psi$. Thus, as $\mathcal{B}$ is the set of matrices where the entries in the positions of $T$ are all 0, and the other entries are arbitrary, so $\Pi\,\mathcal{B}\Psi$ is a set of

matrices where the entries in certain positions are all 0 (even with the same number of positions as in $\mathcal{B}$) and the other entries are arbitrary. Thus, $\Pi \mathcal{B} \Psi$ is a b.m.v.

This proves (2).

□

ii) **Proposition App. 14**

We have the following two results:

1) $Y \in D(n, F) \implies \mathcal{C}_L(Y)$ is a b.m.v. (over $L$).

2) $\mathcal{Y} \subseteq D(n, F)$, and $\Pi$ is any map where $\Pi: \mathcal{Y} \longrightarrow \mathrm{Perm}(n, F)$

$$\implies$$

$$\bigcap\nolimits_{Y \in \mathcal{Y}} \left[\Pi(Y) \cdot \mathcal{C}_L(Y)\right] \quad \text{is a b.m.v. (over } L\text{).}$$

**Proof.**

1) This follows at once from Proposition App. 10a, by letting $T \equiv \{1, \ldots, n\}^2 - T\big(\{Y\}\big) \subseteq \{1, \ldots, n\}^2$ — and then immediately we have: $\mathcal{C}_L(Y) = \mathcal{B}(T)$.

2) This now follows immediately from Step (1) above, then using Proposition App. 13, Part (2), and then finally using Proposition App. 13, Part (1).

□

iii) **Proposition App. 15** (A Key Argument)

Let $\mathcal{B}$ be a basic matrix variety (over $F$).

**Then:**

$$G\ell(n,F)\cap\mathcal{B}\neq\emptyset \quad\Longrightarrow\quad \mathrm{Perm}(n,F)\cap\mathcal{B}\neq\emptyset.$$

**Proof.**

1) As $\mathcal{B}$ is a b.m.v., we may let: $\mathcal{B}=B(T)$, for some $T\subseteq\{1,\ldots,n\}^2$.

2) As given $G\ell(n,F)\cap\mathcal{B}\neq\emptyset$, then $\mathcal{B}$ contains an invertible element $P$ ( of $M(n,F)$ ).

3) As $P$ is invertible, at least one of the entries in its first column is not 0. Consider the set of *all* entries in its first column that are not 0. For each such entry, consider the $(n-1)\times(n-1)$ submatrix obtained from $P$ by crossing out the row and column of that entry. At least one of these $(n-1)\times(n-1)$ submatrices so obtained, must have determinant not 0; otherwise, by expanding $P$ about its first column, $P$ would have determinant 0 [ recall, by construction, these particular $(n-1)\times(n-1)$ submatrices "run over" precisely the entries of column 1 of $P$, that are not 0 ]. Let $Q$ be one of these $(n-1)\times(n-1)$ submatrices, and let $(i,1)$ be the entry from which it was "obtained".

4) As $P$ belongs to $\mathcal{B}$, and by Step (1): $\mathcal{B}=B(T)$; then by definition of $T$, we thus must have: $(i,1)\notin T$. Thus, by definition of a b.m.v.,

the $(i,1)$–entries of $\mathcal{B}$ must be arbitrary. So $\mathcal{B}$ certainly contains a matrix with a 1 in the $(i,1)$–entry. As the rest of the entries in that column are either 0, or arbitrary, $\mathcal{B}$ certainly contains a matrix with first column all 0's and a 1 in position $(i,1)$. Similarly, as the rest of the entries in that row [ row $i$ ] are either 0, or arbitrary, $\mathcal{B}$ certainly contains a matrix with first column all 0's, a 1 in position $(i,1)$, and all other entries in row $i$ are 0's.

5) Now let $\overline{\mathcal{B}} \equiv$ the subset of $\mathcal{B}$, where each matrix has column 1 all 0's, with a 1 in position $(i,1)$, and all other entries in row $i$ are 0's. By Step (4), $\overline{\mathcal{B}}$ is a non-empty subset of $\mathcal{B}$: $\emptyset \neq \overline{\mathcal{B}} \subseteq \mathcal{B}$.

6) Now let $\overline{\mathcal{B}}' \equiv$ the set of $(n-1)\times(n-1)$ matrices, obtained from $\overline{\mathcal{B}}$, by taking each element of $\overline{\mathcal{B}}$, and crossing out column 1 and row $i$. By construction of both $\overline{\mathcal{B}}'$, and $Q$ above, clearly: $Q \in \overline{\mathcal{B}}'$.

7) Furthermore, as $\mathcal{B}$ is a b.m.v., certain of its entries are forced to be 0, and all the remaining entries are allowed to be arbitrary. Thus, in Step (5), following the construction of $\overline{\mathcal{B}}$ from $\mathcal{B}$, clearly the $(i,1)$–entry of $\overline{\mathcal{B}}$ is forced to be 1, certain other entries are forced to be 0, and all the remaining entries are allowed to be arbitrary. Thus now, in Step (6), following the construction of $\overline{\mathcal{B}}'$ from $\overline{\mathcal{B}}$, clearly we have only that certain entries of $\overline{\mathcal{B}}'$ are forced to be 0, and all the remaining entries are allowed to be arbitrary. Thus, $\overline{\mathcal{B}}'$ is a b.m.v.

8) Now as $Q$ is invertible and belongs to $\overline{\mathcal{B}}'$, and $\overline{\mathcal{B}}'$ consists of $(n-1)\times(n-1)$ matrices and [ by Step (7) ] *is a b.m.v.*, inductively we may assume that $\overline{\mathcal{B}}'$ contains an $(n-1)\times(n-1)$ permutation matrix, say $\Psi$. Thus, by the construction now of $\overline{\mathcal{B}}$, this set itself contains an $n \times n$ matrix where $\Psi$ is in "$Q$'s" position, and column 1 is all 0's, with a 1 in position $(i,1)$, and all other entries in row $i$ are 0's. This resulting matrix, by its elementary construction, is clearly a permutation matrix, and is contained in $\overline{\mathcal{B}}$. By Step (5), the latter is a subset of $\mathcal{B}$; and hence, $\mathcal{B}$ contains a permutation matrix.

By induction, this completes the proof. □

iv) **Proposition App. 16** (A Key Result)

Let $\mathcal{Y} \subseteq D(n,F)$.

Let $M \in G\ell(n,L)$.

Suppose $M$ normalizes $\mathcal{Y}$: $M^{-1}\mathcal{Y}M = \mathcal{Y}$.

**Then:**

$\exists \Pi \in \mathrm{Perm}(n, F)$:

i) $M\Pi^{-1} \in C_L^{\times}(\mathcal{Y})$.

ii) $\forall Y \in \mathcal{Y}$: $\Pi^{-1} Y \Pi = M^{-1} Y M$.

I.e., the conjugation action of $M$ on $\mathcal{Y}$, "can be replaced", *element-wise*, by the conjugation action of a single permutation matrix on $\mathcal{Y}$.

iii) $\Pi^{-1} \mathcal{Y} \Pi = M^{-1} \mathcal{Y} M$.

**Proof.**

1) As given that $M$ normalizes $\mathcal{Y}$:

$$(1) \qquad \forall Y \in \mathcal{Y}: \exists Z \in \mathcal{Y}: \qquad M Y M^{-1} = Z.$$

2) As $Y$ and $Z$ in the above equation are diagonal matrices, the diagonal entries of $Z$ must be a permutation of the diagonal entries of $Y$ [ e.g., take the characteristic polynomial of both sides of the above equation ]. Thus, by basic properties of permutation matrices:

$$\exists \Pi(Y) \in \mathrm{Perm}(n, F): \qquad Z = \Pi(Y)\, Y\, \Pi(Y)^{-1}.$$

Substituting this in (1), we have:

$$(2) \quad \forall Y \in \mathcal{Y}: \exists \Pi(Y) \in \mathrm{Perm}(n, F): \qquad M Y M^{-1} = \Pi(Y)\, Y\, \Pi(Y)^{-1}.$$

Hence:

$$\forall Y \in \mathcal{Y}\colon \exists\, \Pi(Y) \in \mathrm{Perm}(n, F)\colon \qquad M\,\Pi(Y)^{-1} \in \mathcal{C}_L(Y)\,.$$

So:

$$\forall Y \in \mathcal{Y}\colon \exists\, \Pi(Y) \in \mathrm{Perm}(n, F)\colon \qquad M \in \Pi(Y) \cdot \mathcal{C}_L(Y)\,.$$

Thus:

(3)
$$M \in \bigcap_{Y \in \mathcal{Y}} \left[\Pi(Y) \cdot \mathcal{C}_L(Y)\right].$$

3) Now by Proposition App. 14, Part (2), the RHS of (3) above is a basic matrix variety. As $M$ is given invertible, this b.m.v. contains an invertible matrix. Thus, by Proposition App. 15, this b.m.v. contains a permutation matrix, say $\Pi$. Thus: $\Pi \in \left[\text{ the RHS of (3) }\right]$. Thus, at once:

$$\forall Y \in \mathcal{Y}\colon \qquad \Pi \in \Pi(Y) \cdot \mathcal{C}_L(Y).$$

Hence [ recall $\mathcal{C}_L(Y)$ is the centralizer of $Y$ (over $L$) ]:

$$\forall Y \in \mathcal{Y}\colon \qquad \Pi\, Y\, \Pi^{-1} = \Pi(Y)\, Y\, \Pi(Y)^{-1}.$$

Thus, by (2), we have:

$$\forall Y \in \mathcal{Y}\colon \qquad \Pi\, Y\, \Pi^{-1} = M\, Y\, M^{-1}.$$

Thus:

$$\forall Y \in \mathcal{Y}\colon \qquad M\,\Pi^{-1} \in \mathcal{C}_L\big(\{Y\}\big).$$

Hence:

$$M\,\Pi^{-1} \in \bigcap_{Y \in \mathcal{Y}} \mathcal{C}_L\big(\{\mathcal{Y}\}\big).$$

So, clearly, at once:

$$M\,\Pi^{-1} \in \mathcal{C}_L(\mathcal{Y}).$$

Since both $M$ and $\Pi$ are invertible, we now have:

$$(4) \qquad M\,\Pi^{-1} \in \mathcal{C}_L^{\times}(\mathcal{Y}).$$

This proves (i).

4) By (4), we have:

$$M = \Pi\, C, \qquad \text{for some} \quad C \in \mathcal{C}_L(\mathcal{Y}).$$

As $\mathcal{C}_L(\mathcal{Y})$ is the centralizer of $\mathcal{Y}$, the previous gives (ii) immediately [ by direct substitution of $M$ ].

The result in (iii) follows immediately, and a fortiori, from the result in (ii).

□

### v) **Corollary App. 17**

Let $\mathcal{A}, \mathcal{B} \subseteq D(n, F)$.

Let $P \in G\ell(n, L)$.

Suppose: $P^{-1} \mathcal{A} P \subseteq \mathcal{B}$.

**Then:**

$$\exists\,\Pi \in \mathrm{Perm}(n,F)\colon \qquad \Pi^{-1}\mathcal{A}\,\Pi = P^{-1}\mathcal{A}P \subseteq \mathcal{B}.$$

**Proof.**

1) As given $P^{-1}\mathcal{A}P \subseteq \mathcal{B}$, we have:

$$(1) \qquad \forall A \in \mathcal{A}\colon \exists B \in \mathcal{B}\colon \qquad P^{-1}AP = B.$$

2) Equation (1) is very similar to equation (1) in the Proof of the previous result — Proposition App. 16. As $A$ and $B$ here are both diagonal matrices, Steps (2)–(4) of that same Proof follow identically, with:

$$\text{“}M\text{”} \equiv P, \qquad \text{“}Y\text{”} \equiv A, \qquad \text{“}Z\text{”} \equiv B.$$

3) This gives, in particular, the result (iii) of that Proposition — which here, in the above notation, gives:

$$\exists\,\Pi \in \mathrm{Perm}(n,F)\colon \qquad \Pi^{-1}A\,\Pi = P^{-1}AP.$$

Together with the last line of the given, the previous gives the conclusion of this Corollary.

□

# F. Centralizers of Algebras and Matrices

**Proposition App. 18**

Let $A$ be any $k$–algebra.

For all $S \subseteq A$, let $\mathcal{C}_A(S)$ be the centralizer of $S$ in $A$:

$$\mathcal{C}_A(S) \equiv \{a \in A \,|\, \forall s \in S\colon\ as = sa\} \subseteq A.$$

**Then:**

$\forall S \subseteq A$:

1) $S \subseteq T \subseteq A \implies \mathcal{C}_A(S) \supseteq \mathcal{C}_A(T)$.

2) $S \subseteq \mathcal{C}_A^2(S)$.

3) $\mathcal{C}_A^3(S) = \mathcal{C}_A(S)$.

4) $S$ is itself the centralizer of some subset of $A \iff \mathcal{C}_A^2(S) = S$.

**Proof.**

1) As the centralizer operator is (trivially) inclusion-reversing, this is immediate.

2) Let $s \in S$. So, by definition: $\forall c \in \mathcal{C}_A(S)$: $sc = cs$. Thus: $\forall c \in \mathcal{C}_A(S)$: $cs = sc$. Thus, by definition: $s \in \mathcal{C}_A\big(\mathcal{C}_A(S)\big) = \mathcal{C}_A^2(S)$. As $s$ is arbitrary, we have: $S \subseteq \mathcal{C}_A^2(S)$.

3) By the previous: $S \subseteq \mathcal{C}_A^2(S)$. Thus, by Step (1): $\mathcal{C}_A(S) \supseteq \mathcal{C}_A^3(S)$. But $\mathcal{C}_A^3(S) = \mathcal{C}_A^2\big(\mathcal{C}_A(S)\big)$; and using the previous again: $\mathcal{C}_A^2\big(\mathcal{C}_A(S)\big) \supseteq \mathcal{C}_A(S)$. So now we have: $\mathcal{C}_A^3(S) \supseteq \mathcal{C}_A(S)$. The conclusions of the last, and the second, sentences here give: $\mathcal{C}_A(S) \supseteq \mathcal{C}_A^3(S) \supseteq \mathcal{C}_A(S)$. Thus: $\mathcal{C}_A^3(S) = \mathcal{C}_A(S)$.

4) $(\Longleftarrow)$:

$\mathcal{C}_A^2(S) = S \implies S = \mathcal{C}_A\big(\mathcal{C}_A(S)\big)$. Thus, $S$ is the centralizer of $\mathcal{C}_A(S) \subseteq A$.

$(\Longrightarrow)$:

Suppose: $S = \mathcal{C}_A(T)$, for some $T \subseteq A$. Thus: $\mathcal{C}_A^2(S) = \mathcal{C}_A^3(T)$. So, by Step (3) above: $\mathcal{C}_A^2(S) = \mathcal{C}_A(T)$. Thus, by the supposition here on $S$: $\mathcal{C}_A^2(S) = S$.

□

**Proposition App. 19**

Let $n \in \mathbb{Z}^+$.

Let $L/F$ be any extension of fields.

Let $\mathcal{A}, \mathcal{B} \subseteq M(n, F)$.

**Then:**

$$\mathcal{C}_F(\mathcal{A}) = \mathcal{C}_F(\mathcal{B}) \quad \Longleftrightarrow \quad \mathcal{C}_L(\mathcal{A}) = \mathcal{C}_L(\mathcal{B}).$$

**Proof.**

($\Longleftarrow$) This follows immediately, by intersecting both sides of the RHS of the desired conclusion, with $M(n, F)$.

($\Longrightarrow$) 1) In this step, we will use the Hilbert Basis Theorem at one point. (It might be possible that the original desired conclusion can be obtained without the use of this.)

Let $E$ be any extension field of $F$, and $\mathcal{D} \subseteq M(n, E)$. We show that with $\mathcal{C}_E(\mathcal{D})$, its argument, $\mathcal{D}$, can be "replaced" with a finite subset of itself.

a) Now by definition:

$$(1) \qquad \mathcal{C}_E(\mathcal{D}) \; = \left\{ C \in M(n, E) \,\middle|\, \forall\, D \in \mathcal{D}\colon \quad C\,D - D\,C = O_n \right\}$$

[ recall, $\mathrm{O}_n$ is the $n \times n$ zero matrix ].

When written out entry-wise, the matrix equation: $C\,D - D\,C = O_n$ is a system of $n^2$ (potentially infinite) homogeneous linear equations for the finitely–many $\left[ = n^2 \right]$ entries of $C$. The coefficients in each such equation are from the matrix $D$ alone — *and so, also, are coefficients from $k$ alone.*

Let $\mathcal{S}(\mathcal{D})$ be the set of homogeneous linear equations just described. Thus, $\mathcal{S}(\mathcal{D})$ is a set of (potentially infinite) homogeneous linear equations in $n^2$ unknowns (the entries of $C$), *with coefficients from* $k$. Thus, we may say:

$$(2) \qquad \mathcal{C}_E(\mathcal{D}) = \left\{ C \in M(n,E) \,\middle|\, \text{the entries of } C \text{ satisfy all equations of } \mathcal{S}(\mathcal{D}) \right\}.$$

b) Now using the Hilbert Basis Theorem, the solution set of the equations in $\mathcal{S}(\mathcal{D})$ [being linear, and hence polynomial], belonging to any particular extension field of $k$, is the same as the solution set of some finite subset of $\mathcal{S}(\mathcal{D})$.

Let $\mathcal{F}(\mathcal{D})$ be any of the finite subsets of $\mathcal{S}(\mathcal{D})$ just described. Thus, $\mathcal{F}(\mathcal{D})$ is a finite set of homogeneous linear equations in $n^2$ unknowns (the entries of $C$), *with coefficients from* $k$, and whose solutions, over any particular extension field of $k$, are the same as the solutions of $\mathcal{S}(\mathcal{D})$.

Thus, we may now say:

$$(3) \qquad \mathcal{C}_E(\mathcal{D}) = \left\{ C \in M(n,E) \,\middle|\, \text{the entries of } C \text{ satisfy the finitely-many equations of } \mathcal{F}(\mathcal{D}) \right\}.$$

2) Now let $\mathcal{F}(\mathcal{D})$ be as in Part (1,b) above. By using the reduced-row echelon form for $\mathcal{F}(\mathcal{D})$ [as it is finite], its $n^2$-variable solution set over the

extension field $E$ of $k$, is generated by some basis of (the $k$–vector space) $M(n,k)$. Let $\mathcal{G}(\mathcal{D}) \subseteq M(n,k)$ be any such basis. [ Thus note: $\mathcal{G}(\mathcal{D})$ is necessarily finite; and, in fact, $\left|\mathcal{G}(\mathcal{D})\right| \leq n^2$. ]

Thus, by (3), we may now say:

$$\mathcal{C}_E(\mathcal{D}) = \mathrm{Span}_E\big(\mathcal{G}(\mathcal{D})\big) \quad \text{and} \quad \dim_E\big(\mathcal{C}_E(\mathcal{D})\big) = \left|\mathcal{G}(\mathcal{D})\right|.$$

Summarizing, starting from Step (1) above, we may now say:

(4) $\qquad \forall\, E$ an extension field of $k: \forall \mathcal{D} \subseteq M(n,E):$

$\exists\, \mathcal{G}(\mathcal{D})$ a $k$–basis of $M(n,k)$

[ necessarily finite, and of cardinality $\leq n^2$ ]:

$$\mathcal{C}_E(\mathcal{D}) = \mathrm{Span}_E\big(\mathcal{G}(\mathcal{D})\big) \quad \text{and} \quad \dim_E\big(\mathcal{C}_E(\mathcal{D})\big) = \left|\mathcal{G}(\mathcal{D})\right|.$$

3) Now we apply (4) to our given situation here.

So, we suppose:

(5) $$\mathcal{C}_k(\mathcal{A}) = \mathcal{C}_k(\mathcal{B}).$$

Additionally, we may let:

(6) $\quad \mathcal{G}(\mathcal{A}) \subseteq M(n,k) \quad$ be as in (4); and then also, in particular:

$\mathcal{G}(\mathcal{A})$ is a finite set of $k$–linearly independent elements of $M(n,k)$, and

$$\left|\mathcal{G}(\mathcal{A})\right| \leq n^2.$$

a) Now by (4), first with $E \equiv k$, and then with $E \equiv L$; and then by (6) — letting $\left|\mathcal{G}(\mathcal{A})\right| = s$, we have at once:

$$(7)\qquad \begin{aligned} \mathcal{C}_k(\mathcal{A}) &= \operatorname{Span}_k\big(\mathcal{G}(\mathcal{A})\big); &\quad \dim_k\big(\mathcal{C}_k(\mathcal{A})\big) &= s. \\ \mathcal{C}_L(\mathcal{A}) &= \operatorname{Span}_L\big(\mathcal{G}(\mathcal{A})\big); &\quad \dim_L\big(\mathcal{C}_L(\mathcal{A})\big) &= s. \end{aligned}$$

b) By (7) and (3), we have: $\mathcal{C}_k(\mathcal{B}) = \operatorname{Span}_k\big(\mathcal{G}(\mathcal{A})\big)$. So, in particular: $\mathcal{C}_k(\mathcal{B}) \supseteq \mathcal{G}(\mathcal{A})$. As (trivially) $\mathcal{C}_L(\mathcal{B}) \supseteq \mathcal{C}_k(\mathcal{B})$, we have now: $\mathcal{C}_L(\mathcal{B}) \supseteq \mathcal{G}(\mathcal{A})$. As $\mathcal{C}_L(\mathcal{B})$ is clearly as subspace of $M(n,L)$, we have: $\mathcal{C}_L(\mathcal{B}) \supseteq \operatorname{Span}_L\big(\mathcal{G}(\mathcal{A})\big)$. Thus, by (3), we now have:

$$(8)\qquad \mathcal{C}_L(\mathcal{B}) \supseteq \mathcal{C}_L(\mathcal{A}).$$

c) Now using (4), with "$\mathcal{D}$" $\equiv \mathcal{B}$, we have:

$$\begin{aligned} \dim_L\big(\mathcal{C}_L(\mathcal{B})\big) &= \left|\mathcal{G}(\mathcal{B})\right| && [\text{“}E\text{”} \equiv L,\ \text{“}\mathcal{D}\text{”} \equiv \mathcal{B}, \text{ in (4)}] \\ &= \dim_k\Big(\operatorname{Span}_k\big(\mathcal{G}(\mathcal{B})\big)\Big) && [\text{“}E\text{”} \equiv k,\ \text{“}\mathcal{D}\text{”} \equiv \mathcal{B}, \text{ in (4)}] \\ &= \dim_k\big(\mathcal{C}_k(\mathcal{B})\big) && [\text{“}E\text{”} \equiv k,\ \text{“}\mathcal{D}\text{”} \equiv \mathcal{B}, \text{ in (4)}] \\ &= \dim_k\big(\mathcal{C}_k(\mathcal{A})\big) && [\text{ by (3) }] \\ &= \dim_L\big(\mathcal{C}_L(\mathcal{A})\big) && [\text{ by (7) }]. \end{aligned}$$

Thus, summarizing:

$$(9)\qquad \dim_L\big(\mathcal{C}_L(\mathcal{B})\big) = \dim_L\big(\mathcal{C}_L(\mathcal{A})\big).$$

d) Thus, by (8), and (9), we have at once:

$$\mathcal{C}_L(\mathcal{B}) = \mathcal{C}_L(\mathcal{A}).$$

This completes $(\Longrightarrow)$, and so completes the proof.

$\square$

# Bibliography

1. Artin, Emil; *Galois Theory*; Notre Dame Mathematical Lectures, Number 2, Second Edition; University of Notre Dame Press; 1944.

2. Lang, Serge; *Linear Algebra*, Second Edition; Addison–Wesley Publishing Company; 1972.

3. Marcus, Daniel; *Number Fields*; Springer–Verlag, New York; 1977.

4. Weyl, Hermann; *Algebraic Theory Of Numbers*; Annals Of Mathematics Studies, Number 1; Princeton University Press, Princeton; 1940.

# Autobiographical Statement

**Born and Raised:** New Rochelle, NY

**High School:** New Rochelle High School; Graduated 1972

- Primary Interests: Mathematics, Sciences, Spanish.
- Received a number of mathematics and science awards upon graduation.
- Received a small prize from the Tomorrow's Scientists and Engineers Contest for a mathematics paper:

  "Gaussian Integers and the Representability of an Integer as the Sum of Two Squares".
- Attended several NSF programs, including:
  - A summer program in the biology and chemistry of plants, at The Boyce Thompson Institute for Plant Research; Yonkers, NY.
  - Three summers at the Mathematics Program, at the Ohio State University; Columbus, Ohio; taught by the late Dr. Arnold E. Ross. Number Theory, Introductory Abstract Algebra, and Combinatorics were studied.

**College:** MIT; S.B., 1976 — Mathematics; Phi Beta Kappa, Sigma Xi

- Undergraduate Thesis (voluntary):

  "A Generalization Of Euler's $\varphi$-Function And Applications".

- Primary Interests: Algebra, Number Theory.
- Additional Interests: Physics — Classical Mechanics, Classical E&M.

**Graduate School:** MIT; S.M., 1985 — Electrical Eng. & Computer Sci.;

Hertz Foundation Fellow

- Master's Thesis:

  "Algebraic And Graph-Theoretic Aspects Of Resistive Networks".

- Primary Interests:
  - Electrical Engineering: Network Theory, Switching Circuit Theory, Signal Processing.
  - Computer Science: Programming Languages, Formal Language Theory And Automata.

**Graduate School:** The Graduate Center of CUNY;

M. Phil., 1991 — Mathematics;

Mathematics Graduate Fellowship (3-year)

- Primary Interests: Algebra, Number Theory.

**Papers:** On The Power Sums Of The Roots Of A Polynomial;

Mathematics Magazine, Vol. 59, No. 4, Oct. 1986.

**Industry Experience:**

- IBM Corporation; 360 Hamilton Avenue; White Plains, NY
  - Field Engineering Division — Headquarters;

    Information Systems Department.
  - Senior Programming Technician: 1977-1979.
- IBM Corporation; Yorktown Heights, NY
  - Research Division — Watson Research Center;

    Computer Algebra Group.
  - Visiting Pre-Doctoral Scientist: 1985-1986.