VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
UNIVERSITY OF SCIENCE

NGUYEN TRUNG NGHIA

SUBPERMUTABLE SUBGROUPS OF SKEW LINEAR GROUPS AND UNIT GROUPS OF REAL GROUP ALGEBRAS

SENIOR THESIS

Ho Chi Minh City - 2021

VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
UNIVERSITY OF SCIENCE

NGUYEN TRUNG NGHIA

SUBPERMUTABLE SUBGROUPS OF SKEW LINEAR GROUPS AND UNIT GROUPS OF REAL GROUP ALGEBRAS

A SENIOR THESIS

ON ALGEBRA AND NUMBER THEORY

ADVISOR
Assoc. Prof. Mai Hoang Bien

Ho Chi Minh City - 2021

Acknowlegements

Foremost, I would like to express my deep and sincere gratitude toward my advisor, Professor Mai Hoang Bien, for giving me an opportunity to do research and providing constructive advice throughout the research. His endless patience, immense enthusiasm, and vast knowledge always have always been inspiring me to pursue a graduate program in mathematics. Besides my advisor, I would like to thank my co-authors of the outcome of the research, Mr. Le Qui Danh and Dr. Nguyen Kim Ngoc, and the remaining members of the general linear group seminar, especially Nguyen Duy Minh Khoi, for their helpful and insightful suggestions during the work.

My sincere thanks also go to Dr. Nguyen Khanh Tung and the best friends of mine, Can Tran Thanh Trung, Tran Hoang Bao Linh and Do Hoang Viet, for their continuous support and encouragement since my first days at the university.

Last but not least, I am deeply thankful to my family, friends, lecturers in the Faculty of Mathematics and Computer Science, especially to Dr. Tran Ngoc Hoi and Dr. Nguyen Van Thin, at VNUHCM-University of Science for what they have been giving to me.

June, 2021

Nguyen Trung Nghia

Contents

Introduction

Permutablity and subpermutablity are very natural generalizations of the well-known notions of normality and subnormality, respectively. The classification of those (sub)permutable groups has been drawing significant attention of group theorists since 1950s. In particular, it is fascinating to ask whether a (sub)permutable subgroup is (sub)normal. There have been many remarkable progress around this topic. For instance, in an article in 1972 (see [Sto72]), Stonehewer listed several groups having subgroup being permutable but subnormal; he also showed that every finite subpermutable subgroup is subnormal. Nonetheless, the most inspiring of his work (in the article [Sto72] as well) was to show that every finitely generated permutable subgroup is subnormal. This dissertation is going to concentrate on the classification of subpermutable subgroups of skew linear groups, and of unit groups of real group algebras. Indeed, we shall prove that every subpermutable subgroup of skew linear groups of degree greater than 1 is subnormal, and is normal in most case except for $\mathrm{GL}_2(\mathbb{F}_3)$, and subsequently that every subpermutable subgroup of unit groups of real group algebras is normal.

Here is a more detailed account of this dissertation.

Chapter 1 introduces basic terminologies of noncommutative ring theory. We aim to concentrate on several classical results in the theory comprising Wedderburn's Theorem, Frobenius's Theorem, Wedderburn-Artin's Theorem, and Maschke's Theorem, which play an important role in the later chapter, and on their detailed proofs. However, most of the prerequisite facts to achieve the goal are elementary and lies outside the scope of this work so that their proofs might be intentionally omitted.

In chapter 2, we will give a brief introduction to skew linear groups and (sub)permutability, paving the way for the aforementioned subject.

Chapter 1

Background

1.1 Noncommutative ring theory

1.1.1 Noncommutative rings

Definition 1.1.1. An *unital associative ring* is an additive group R equipped with a binary operation, namely a *multiplication*, $\cdot : R \times R \to R$ subject to the following axioms:

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$;

(ii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$;

(iii) there is an element $1 \in R$ such that, for every $a \in R$,

$$1 \cdot a = a = a \cdot 1.$$

One can see immediately that the element 1 is unique, and is called the *identity*. Besides, there is nothing to deal with the ring with only one element. Therefore, for the rest of the dissertation, the word "ring" always means an unital associative ring with $1 \neq 0$. For the sake of simplicity, we abbreviate the product $a \cdot b$ to ab for the rest of this dissertation.

Example 1.1.2. (i) Let $(R_i)_{i \in I}$ be a family of rings. The *direct product* of $(R_i)_{i \in I}$ is the cartesian product $\prod_{i \in I} R_i$ equipped with the coordinatewise addition and multiplication, i.e.

$$(r_i)_{i \in I} + (r'_i)_{i \in I} = (r_i + r'_i)_{i \in I} \quad \text{and} \quad (r_i)_{i \in I}(r'_i)_{i \in I} = (r_i r'_i)_{i \in I}.$$

It is in fact a ring with the identity $(1_i)_{i \in I}$.

(ii) The *matrix ring* over a ring R of order n is the ring $\mathcal{M}_n(R)$ of square matrices of order n with entries in R under the matrix addition and multiplication. To be precise, if A and B are matrices of $\mathcal{M}_n(R)$, then its multiplication is a matrix in $\mathcal{M}_n(R)$ determined by

$$[AB]_{ij} = \sum_{k=1}^{n} [A]_{ik}[B]_{kj}.$$

Definition 1.1.3. Regard the additive group R^{op} analogously as R, and define the multiplication $\star : R^{op} \times R^{op} \to R^{op}$ as $a \star b = b \cdot a$. Then, R^{op} is a ring, namely the *opposite ring* of R.

Definition 1.1.4. Two elements a and b of a ring are said to *commute* if $ab = ba$. A ring is said to be *commutative* if all pairs of its elements commute.

Definition 1.1.5. Let $a \neq 0$ be an element of a ring. The element a is said to be *left invertible* if there is an element b such that $ba = 1$. The element is said to be *right invertible* if there is an element c such that $ac = 1$. The element a is said to be *invertible* if a is both left and right invertible.

Suppose that an element a is invertible, i.e. $ba = 1$ and $ac = 1$ for some elements b and c. Then $b = b \cdot 1 = b(ac) = (ba)c = 1 \cdot c = c$. Moreover, one can easily show that the element $b = c$ is uniquely determined by a. Hence, it is now called the *(multiplicative) inverse* of a, and denoted by a^{-1}.

Definition 1.1.6. A *unit* of the ring is an invertible element. The set of all units of a ring R is denoted by R^*.

Proposition 1.1.7. The set of all units of a ring forms a group under the multiplication.

Proof. The proof is omitted on purpose. □

Definition 1.1.8. A *subring* of a ring $(R, +, \cdot, 0, 1)$ is a nonempty subset S preserving the structure of the ring, i.e. a ring $(S, +, \cdot, 0, 1)$ with $S \subseteq R$.

Definition and Proposition 1.1.9. The *center* of a ring R, denoted by $Z(R)$, consists of all elements of R commuting with every element in R, that is,

$$Z(R) = \{z \in R : za = az \text{ for all } a \in R\},$$

and is closed under the addition and multiplication. In other words, the center of a ring is its subring.

Proof. The proof is omitted on purpose. $\square$

Definition 1.1.10. Let R be a ring, and let I be an additive subgroup of R. Then I is a *left ideal* if $rI \subseteq I$ for every $r \in R$, while I is a *right ideal* if $Ir \subseteq I$ for every $r \in R$. Finally, I is said to be a *two-sided ideal* if it is both left and right ideal.

Definition 1.1.11. A ring is said to be *simple* if it has no two-sided ideals besides the zero ideal and itself.

Definition 1.1.12. A *ring homomorphism* between two rings R and R' is an additive group homomorphism $f : R \to R'$ satisfying the following conditions:

(i) $f(rs) = f(r)f(s)$ for all $r, s \in R$;

(ii) $f(1) = 1$.

Definition and Proposition 1.1.13. Let $f : R \to R'$ be a ring homomorphism. The *kernel* of f, denoted by $\mathrm{Ker}f$, defined as

$$\mathrm{Ker}f = \{r \in R : f(r) = 0\},$$

is a two-sided ideal of R. The *image* of f, denoted by $\mathrm{Im}f$, defined as

$$\mathrm{Im}f = f(R),$$

is a subring of R'.

Proof. The proof is omitted on purpose. $\square$

Definition and Proposition 1.1.14. Let I be a two-sided ideal of a ring R. The additive quotient group R/I equipped with the multiplication defined by

$$(r + I)(s + I) = rs + I,$$

for all $r, s \in R$, forms a ring, called the *quotient ring* of R modulo I.

Proof. The proof is omitted on purpose. $\square$

1.1.2 Module theory

For the rest of this section, we assume that R is an arbitrary ring as long as there are no other indications.

Definition 1.1.15. A *(left) module* over R consists of an abelian group $(M, +)$ and a scalar multiplication $\cdot : R \times M \to M$ such that for all $r, s \in R$ and for all $x, y \in M$:

(a) $r \cdot (x + y) = r \cdot x + r \cdot y$;

(b) $(r + s) \cdot x = r \cdot x + s \cdot x$;

(c) $(rs) \cdot x = r \cdot (s \cdot x)$;

(d) $1 \cdot x = x$.

As the preceding subsection, we may write rx instead of $r \cdot x$ if there is no confusion.

Example 1.1.16. (i) The ring R itself has a natural structure of an R-module, namely the *regular module*, denoted by ${}_RR$.

(ii) The additive group R^n has a natural structure of a module over $\mathcal{M}_n(R)$.

(iii) Let R_η be some ring in a family of rings $(R_i)_{i\in I}$, and M an R_η-module. Then, M can be regarded as a module over $\prod_{i\in I} R_i$, that is,

$$(r_i)_{i\in I} m := r_\eta m.$$

Definition 1.1.17. Let M be an R-module, and N an additive subgroup of M. Then N is said to be a *submodule* of M, denoted by $N \leq M$, if it is closed under the scalar multiplication.

Notation 1.1.18. Let M be an R-module, and let X be a subset of M. An *R-linear combination* of X is a finite sum of products of an element of R and of X. We denote by RX the set of all R-linear combination of X, that is,

$$RX = \left\{ \sum_{\text{finite}} r_i x_i : r_i \in R, x_i \in X \right\}.$$

Proposition 1.1.19. The intersection of a family of submodules is a submodule as well.

Proof. The proof is omitted on purpose. □

Proposition 1.1.20. Let X be a nonempty subset of an R-module M. Then, there is a smallest submodule of M containing X, which is precisely RX.

Proof. The statement is a consequence of Proposition 1.1.19 and the definition of R-linear combination. □

Notation 1.1.21. Let $(M_i)_{i\in I}$ be a family of submodules of an R-module M. Denote by $\sum_{i\in I} M_i$ the *sum* of $(M_i)_{i\in I}$ defined by

$$\sum_{i\in I} M_i = \left\{ \sum_{\text{finite sum}} m_i : m_i \in M_i \right\}.$$

Proposition 1.1.22. Let $(M_i)_{i\in I}$ be a family of submodules of an R-module M. Then its sum is the smallest submodule containing all the M_i's.

Proof. The proof is omitted on purpose. □

Definition and Proposition 1.1.23. Let N be a submodule of an R-module M. Then the additive quotient group M/N is an R-module, called the *quotient module* of M modulo N, where the scalar multiplication is defined as

$$r(m+N) = rm + N,$$

for all $r \in R$ and $m \in M$.

Proof. The proof is omitted on purpose. □

Definition 1.1.24. An *R-homomorphism* between two R-modules M and M' is an additive map $f : M \to M'$ satisfying $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$. The set of all R-homomorphisms from M to M' is denoted by $\mathrm{Hom}_R(M, M')$.

Definition and Proposition 1.1.25. Let $f : M \to M'$ be an R-homomorphism. The *kernel* of f, denoted by $\mathrm{Ker} f$, defined as

$$\mathrm{Ker} f = \{r \in M : f(r) = 0\},$$

and the *image* of f defined as

$$\mathrm{Im} f = f(M),$$

are submodules of M and M', respectively.

Proof. The proof is omitted on purpose. □

Definition 1.1.26. Let $(M_i)_{i\in I}$ be a family of R-modules. Firstly, their *direct product*, denoted by $\prod_{i\in I} M_i$, is the cartesian product of their underlying set together with the componentwise addition and the scalar multiplication distributing all over the components. Secondly, their *external direct sum*, denoted by $\bigoplus_{i\in I} M_i$, is a proper submodule of $\prod_{i\in I} M_i$ consisting of all elements of the form $(m_i)_{i\in I}$ where all but finitely many m_i's are equal to zero.

Remark that when index set I has finitely many elements, then the external direct product coincides with the direct product.

Definition 1.1.27. Let M be an R-module, and $(M_i)_{i\in I}$ a family of its submodule. Then, M is said to be the *internal direct sum* of $(M_i)_{i\in I}$ if $M = \sum_{i\in I} M_i$ and $M_j \cap \sum_{i\neq j} M_i = 0$.

A distinction between external and internal direct sum has been made, although they are isomorphic. Where ambiguity comes up, the readers should be able to make their own distinction depend on the context. For example, if the formula $V \oplus V$ appears, it always means the external direct sum.

Definition 1.1.28. A submodule N is a *direct summand* of an R-module M if there is a submodule N' of M such that

$$M = N \oplus N'.$$

Definition 1.1.29. An R-module homomorphism $f : M \to M$ of module M is called an *R-endomorphism* of M. We write $\mathrm{End}_R(M)$ instead of $\mathrm{Hom}_R(M, M)$ and call it the *endomorphism ring* of M.

The term "ring" in Definition 1.1.29 comes from the natural structure of the ring on the set $\mathrm{End}_R(M)$, where the multiplication is the function composition.

Proposition 1.1.30. The endomorphism ring of the regular module ${}_RR$ is isomorphic as rings to the opposite ring of R, that is,

$$\mathrm{End}_R({}_RR) \simeq R^{op}.$$

Proof. See [Rot02, Proposition 8.12]. □

Proposition 1.1.31. Let n be a positive integer. Then we have a ring isomorphism

$$\mathcal{M}_n(R)^{op} \simeq \mathcal{M}_n(R^{op}).$$

Proof. See [Rot02, Proposition 8.13]. □

Definition 1.1.32. An R-module M is *simple* if $M \neq 0$ and M has no proper submodules.

Definition 1.1.33. Let M be an R-module. A *composition series* of M is a finite chain of submodules of M for which

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_n = 0$$

such that all the *factor modules* $M_0/M_1, \ldots, M_{n-1}/M_n$ are simple. The number n is called the *length* of the composition series.

Two composition series are said to be *equivalent* if there is a one-to-one correspondence between their sets of all factor modules so that corresponding factor modules are isomorphic.

Theorem 1.1.34 (Jordan-Hölder Theorem)**.** *If there is a composition series of a fixed module, then the length is invariant of the module. Furthermore, every other composition series is equivalent to it.*

Proof. See [Rot02, Theorem 8.18]. □

1.1.3 Division rings, Fields and Algebras

The notion of division rings is the core of this dissertation, spanning predominantly over the work. The aims of this subsection is introducing one of the main division rings, that is, the real quaternion as well as the proofs of two renowned results on division rings.

Definition 1.1.35. A *division ring* is a ring in which every nonzero element is a unit.

When division rings are equipped with the commutative property, one gains the most complete rings, which are called fields.

Definition 1.1.36. A *field* is a commutative division ring.

The proper noncommutative ring was first described by the Irish mathematician William Rowan Hamilton, which is called the quaternion. The quaternion can be regarded as a extension of the field of complex numbers. It is denoted by $\mathbb{H}$, which stands for Hamilton.

Example 1.1.37. Let $\mathbb{H}$ be a four-dimensional vector space over $\mathbb{R}$. Pick a basis of $\mathbb{H}$ and denote by $\{1, i, j, k\}$. Define a multiplication on the basis of $\mathbb{H}$ as follows:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Subsequently, we expand the multiplication on arbitrary elements of $\mathbb{H}$ by extending $\mathbb{R}$-linearity which naturally forms a ring, called the *real quaternion* with the identity 1. Moreover, $\mathbb{H}$ is a division ring. To see this, for any element $\alpha = a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$, define its *conjugate* by

$$\overline{\alpha} = a - bi - cj - dk.$$

An easy computation shows that

$$\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2 = \overline{\alpha}\alpha$$

whose square root is called the *norm* of α, and denoted by $|\alpha|$. Hence, if α is nonzero then so is its norm, which leads to that α is invertible, and its inverse is

$$\alpha^{-1} = \frac{\overline{\alpha}}{|\alpha|^2}.$$

Definition 1.1.38. We define the *characteristic* of a division ring D, denoted by $\mathrm{char}(D)$, as the smallest positive integer n satisfying $1 + \cdots + 1 = 0$, where the amount of 1's in the left-hand side is n. If there is no such a number, we say that its characteristic is 0.

Proposition 1.1.39. The characteristic of a division ring is either 0 or a prime number. In other words, either $\mathbb{Q}$ or the field of p elements, where p is a prime number, can be embedded into a division ring, and is called *the prime subfield*.

Proof. The proof is omitted on purpose. $\square$

Definition 1.1.40. An *algebra* over a field $\mathbb{F}$ is a ring R which is also an $\mathbb{F}$-vector space with the same addition operation, and the scalar multiplication satisfying

$$r \cdot (xy) = (r \cdot x)y = x(r \cdot y),$$

for all $r \in \mathbb{F}$ and $x, y \in R$.

Definition 1.1.41. A *subalgebra* of an algebra over a field is a vector subspace which is closed under the multiplication.

Definition and Proposition 1.1.42. Let R be an algebra over a field $\mathbb{F}$, and X a subset of R. The *centralizer* of X, denoted by $C_R(X)$, defined by

$$C_R(X) = \{r \in R : rx = xr \, \text{for all} \, x \in X\},$$

is a subalgebra of R.

Proof. The proof is omitted on purpose. $\square$

Definition 1.1.43. An *algebra homomorphism* between two algebras R and S over a field $\mathbb{F}$ is a ring homomorphism $f : R \to S$ satisfying

$$f(r \cdot x) = r \cdot f(x),$$

for all $r \in \mathbb{F}$ and $x \in R$.

Remark 1.1.44. If R is an algebra over a field $\mathbb{F}$, it is straightforward that $\mathbb{F}$ and the center $Z(R)$ are algebras over $\mathbb{F}$. A map $f : \mathbb{F} \to Z(R)$ defined by

$$f(r) = r \cdot 1,$$

for all $r \in \mathbb{F}$, is an algebra homomorphism. Furthermore, it is an injection since $\mathbb{F}$ is a field, which means that $\mathbb{F}$ can be regarded to be embedded into R.

Definition 1.1.45. A *division algebra* over a field is an algebra over the field whose underlying ring is a division ring.

Note that our definition of division algebra does not require its center to be equal to the given field, which is slightly different from the notions having been used in [Rot02, Chapter 9].

Example 1.1.46. The field of real numbers $\mathbb{R}$, field of complex numbers $\mathbb{C}$, and quaternion $\mathbb{H}$ are both division algebras over $\mathbb{R}$.

Definition 1.1.47. An algebra over a field is called *simple* if it is simple regarded as the ring.

Definition 1.1.48. An algebra R over a field $\mathbb{F}$ is *central simple* if it is finite-dimensional (regarded as the vector space), simple, and its center is equal to $\mathbb{F}$, i.e. $Z(R) = \mathbb{F}$.

Remark 1.1.49. It is obvious that the center of a division ring is a field. Every finite-dimensional division algebra over its center is a central simple algebra (over its center). In particular, the field of real numbers $\mathbb{R}$ and the quaternion $\mathbb{H}$ are central simple algebras over $\mathbb{R}$.

Theorem 1.1.50. *Then the dimension of a central simple algebra over its field is a perfect square of an integer. In particular, the dimension of a finite-dimensional division algebra over its center is a perfect square of a nonzero integer.*

Proof. See [Rot02, Theorem 9.114-(ii)]. $\square$

Proposition 1.1.51. Let D be a division algebra over an arbitrary field. Then a subfield E of D is a maximal subfield if and only if $C_D(E) = E$.

Proof. See [Rot02, Lemma 9.117]. $\square$

Corollary 1.1.52. *If E is a maximal subfield of a division algebra D over a field $\mathbb{F}$, then E contains the center of D. In particular, E contains $\mathbb{F}$.*

Proof. The proof is direct from Proposition 1.1.51. $\square$

Proposition 1.1.53. Let D be a finite-dimensional division algebra over its center $Z(D)$, and let E be a maximal subfield of D. Then the dimension of D over E is equal to the dimension of E over $Z(D)$. In particular, all maximal subfields of D have the same degree over $Z(D)$, which is equal to the square root of the dimension of D over $Z(D)$.

Proof. See [Rot02, Theorem 9.118 and Corollary 9.119]. $\square$

Theorem 1.1.54 (Skolem-Noether Theorem)**.** *Let R be a central simple algebra over a field $\mathbb{F}$, and let S and T be isomorphic simple subalgebras of R. If $\varphi : S \to T$ is an isomorphism, then there is a unit a of A such that $\varphi(s) = a^{-1}sa$ for all $s \in S$.*

Proof. See [Rot02, Corollary 9.121]. $\square$

Before proceeding to two main results of this subsection, let us recall the notion of *normalizer*:

$$N_G(H) = \{a \in G : a^{-1}Ha = H\},$$

where H is a subgroup of a group G. Secondly, a *conjugate* of H is a set of the form $x^{-1}Hx$ for some element x of G. One sees immediately that two conjugates $x^{-1}Hx$ and $y^{-1}Hy$ coincide if and only if $xy^{-1} \in N_G(H)$. Therefore, the number of conjugates of H in G is equal to $[G : H]$.

Theorem 1.1.55 (Wedderburn's Theorem)**.** *Every finite division ring is a field.*

Proof. Suppose that D is a properly noncommutative finite division ring, so that it is a division algebra over its center $Z(D) := \mathbb{F}$. Choose an arbitrary maximal subfield F of D. For each element d of D, the simple extension field $\mathbb{F}(d) \ni d$ of $\mathbb{F}$ is a proper subfield of D for D is noncommutative, and hence there is a maximal subfield F_d (by the usual argument using Zorn's Lemma) containing $\mathbb{F}(d)$. According to Proposition 1.1.53, every F_d has the same degree over $\mathbb{F}$, and hence has the same order (as of F). Since they are finite fields and of the same order, they are all isomorphic (to F). Applying Skolem-Noether Theorem, we gain that $F_d = x_d^{-1}Fx_d$ for some nonzero element x_d of D corresponding to each element d of D. As a result, we have that $D = \bigcup_{d \in D} F_d = \bigcup_{d \in D} x_d^{-1}Fx_d = \bigcup_{x \in D^*} x^{-1}Fx$, and so

$$D^* = \bigcup_{x \in D^*} x^{-1}F^*x.$$

On the other side, note that F^* is a proper subgroup of D^*, which means that $[D^* : F^*] > 1$. Using the remark above, the number of conjugates of F^* is equal to $[D^* : N_G(F^*)] \leq [D^* : F^*]$. Since the identity is in all the conjugates, the union of all conjugates of F^* has at most

$$[D^* : F^*](|F^*| - 1) + 1 = |D^*| - ([D^* : F^*] - 1)$$

elements, which strictly less than number of elements of D^*, a contradiction. In conclusion, D must be commutative. $\square$

Theorem 1.1.56 (Frobenius's Theorem)**.** *Let D be a finite-dimensional division algebra over the field of real numbers $\mathbb{R}$. Then D is isomorphic to either the field of real numbers $\mathbb{R}$, the field of complex numbers $\mathbb{C}$ or the quaternion $\mathbb{H}$.*

Proof. Without loss of generality, we may assume that $\mathbb{R}$ is a subfield of D. Since D is a finite-dimensional vector space over $\mathbb{R}$, so is $Z(D)$. It is familiar in the Fields Theory that there are only two finite field extensions (up to isomorphism) of $\mathbb{R}$: they are either $\mathbb{R}$ or $\mathbb{C}$. Therefore, either $Z(D) = \mathbb{R}$ or $Z(D) = \mathbb{C}$.

In the former case, if D is commutative possessing $\mathbb{R}$ as the center, then D must be equal to $\mathbb{R}$. If otherwise, pick a maximal subfield E of D. As stated in Proposition 1.1.53, we obtain that

$$\dim_E(D) = \dim_{\mathbb{R}}(E),$$

where $2 \leq \dim_E(D)$ since D is not commutative and $\dim_{\mathbb{R}}(E) \leq 2$. As a result, we have $\dim_E(D) = \dim_{\mathbb{R}}(E) = 2$, which leads to $\dim_{\mathbb{R}}(D) = 4$ and $\dim_{\mathbb{R}}(E) = 2$. We may then identify E with $\mathbb{C}$. Recall that the complex conjugation is an automorphism of E. The Skolem-Noether Theorem tells us that there is a nonzero element λ of D such that $\overline{z} = \lambda^{-1} z \lambda$ for every $z \in \mathbb{C}$. Specifically, we have $-\lambda i = i\lambda$, which implies that $\lambda^2 i = i\lambda^2$, or equivalently that $\lambda^2 \in C_D(\mathbb{C}) = \mathbb{C}$ according to Proposition 1.1.51. Again, we have $\overline{\lambda^2} = \lambda^{-1}\lambda^2\lambda = \lambda^2$, so that $\lambda^2 \in \mathbb{R}$. If $\lambda^2 > 0$, there is some $x \in \mathbb{R}$ such that $\lambda^2 = x^2$. Then, λ is a real number, contradicting to the fact that $-\lambda i = i\lambda$. Hence, $\lambda^2 = -x^2$ for some nonzero real number x. Set $j := \lambda/x$. It is now routine to verify that $1, i, j, ij$ act as $1, i, j, k$, respectively, in the quaternion. In conclusion, D is isomorphic to $\mathbb{H}$.

In the latter case, if D is not commutative, pick a maximal subfield E of D. Note that the only finite field extension of $\mathbb{C}$ is itself. By Proposition 1.1.53, we have that

$$\dim_E(D) = \dim_{\mathbb{C}}(E) = 1,$$

which results that $D = E$, or that D is commutative, which contradicts to our assumption. Therefore, D must be commutative, and it follows that $D = \mathbb{C}$. $\square$

1.1.4 Semisimple rings

Definition 1.1.57. A module is *semisimple* if it is a direct sum of simple submodules. A ring is *left semisimple* if the regular module is semisimple.

Proposition 1.1.58. A module is semisimple if and only if every its submodule is a direct summand.

Proof. See [Rot02, Proposition 8.42]. □

Proposition 1.1.59. If R is a left semisimple ring, then every R-module is semisimple.

Proof. See [Rot02, Proposition 8.43-(ii)]. □

Proposition 1.1.60.

(i) A left semisimple ring is a direct sum of a finite number of minimal left ideals.

(ii) The direct product of a finite number of left semisimple rings is a left semisimple ring.

Proof. The former statement can be rephrased into the regular module of a left semisimple ring is a direct sum of a finite number of simple submodules. The details of both assertions are given in [Rot02, Corollary 8.44]. □

The next discussion will be used in the proof of the Wedderburn-Artin Theorem.

Proposition 1.1.61. Let M and L be R-modules. Suppose that there are some submodules $V_1, \dots V_n$ of M such that they are all isomorphic to L. Then, there is a ring isomorphism

$$\mathrm{End}_R\left(\sum_{i=1}^{n} V_i\right) \simeq \mathcal{M}_n\left(\mathrm{End}_R(L)\right).$$

Proof. See [Rot02, Proposition 8.24]. □

Proposition 1.1.62. Let M be an R-module which can be written as direct sum of submodules $W_1, \dots, W_m$, that is,

$$M = W_1 \oplus \cdots \oplus W_m.$$

Assume that $\mathrm{Hom}_R(W_i, W_j) = 0$ for all $i \neq j$. Then, there is a ring ismorphism

$$\mathrm{End}_R(M) \simeq \mathrm{End}_R(W_1) \times \cdots \times \mathrm{End}_R(W_m).$$

Proof. See [Rot02, Corollary 8.26]. □

Lemma 1.1.63 (Schur's Lemma)**.** *Let V, W be simple R-modules.*

(i) If $V \not\simeq W$, then $Hom_R(V, W) = 0$.

(ii) If $V \simeq W$, then every nonzero element of $Hom_R(V, W)$ is an isomorphism. In particular, $End_R(V)$ is a division ring.

Proof. (i) Let f be an element of $\mathrm{Hom}_R(V, W)$. If $f \neq 0$, then $\mathrm{Ker} f \neq V$ and $\mathrm{Im} f \neq 0$. Since V and W are both simple, we have $\mathrm{Ker} f = 0$ and $\mathrm{Im} f = W$. In other words, f is an isomorphism conflicting with the presumption. Thus, f must be zero.

(ii) Suppose that f is a nonzero element of $\mathrm{Hom}_R(V, W)$. It follows that $\mathrm{Im} f \neq 0$ and $\mathrm{Ker} f \neq V$. Since V and W are simple, we deduce that $\mathrm{Im} f = W$ and $\mathrm{Ker} f = 0$. Equivalently, f is an isomorphism.

□

The following proposition illustrates the first examples of left semisimple rings.

Proposition 1.1.64.

(i) The matrix ring over a division ring is a left semisimple ring.

(ii) Let $D_1, \ldots, D_m$ be division rings and $n_1, \ldots, n_m$ positive integers. Then,

$$\mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_m}(D_m)$$

is a left semisimple ring.

Proof. (i) Let D be a division ring and $n \geq 1$ an integer. First, we claim that D^n is a simple $\mathcal{M}_n(D)$-module. Indeed, it is obvious to observe that $\mathcal{M}_n(D)v = D^n$ for every nonzero element of D^n.

Now, we have a direct sum composition (as modules)

$$\mathcal{M}_n(D) = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_n,$$

where $\mathcal{C}_i$ is a left ideal of $\mathcal{M}_n(D)$ comprising all the matrices whose columns other than ith column are equal to zero. Immediately, one sees that $\mathcal{C}_i \simeq D^n$ as $\mathcal{M}_n(D)$-modules. Henceforth, we get ${}_{\mathcal{M}_n(D)}\mathcal{M}_n(D) \simeq n \cdot D^n$, which leads to the fact that $\mathcal{M}_n(D)$ is a left semisimple ring.

(ii) This is a subsequence of part (i) and Proposition 1.1.60-(ii).

$\square$

Remark 1.1.65. As we have seen in the proof of Proposition 1.1.64-(i), we see that D^n is a simple $\mathcal{M}_n(D)$-module. We claim that it is unique (up to isomorphism). In fact, assume that W is another simple $\mathcal{M}_n(D)$-module, and w is its arbitrary nonzero element. Consider the following $\mathcal{M}_n(D)$-homomorphism:

$$\begin{array}{rcl} f :_{\mathcal{M}_n(D)} \mathcal{M}_n(D) & \to & W, \\ x & \mapsto & x \cdot w. \end{array}$$

Since W is simple and $f(1) = w \neq 0$, we have that f is surjective. By Isomorphism Theorem of modules, we obtain that $W \simeq_{\mathcal{M}_n(D)} \mathcal{M}_n(D)/\mathrm{Ker} f$, where $\mathrm{Ker} f$ is a maximal $\mathcal{M}_n(D)$-module. Applying Jordan-Hölder Theorem for the decomposition of ${}_{\mathcal{M}_n(D)}\mathcal{M}_n(D)$ in the proof of Proposition 1.1.64-(i), it follows that ${}_{\mathcal{M}_n(D)}\mathcal{M}_n(D)/\mathrm{Ker} f \simeq D^n$. Thus, $W \simeq D^n$ as $\mathcal{M}_n(D)$-modules.

Interestingly, it turns out that these cover all of the examples (up to isomorphism). This is shown in the following extraordinary result.

Theorem 1.1.66 (Wedderburn–Artin I Theorem)**.** *Let R be a left semisimple ring. Then $R \simeq \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_r}(D_r)$ for some division rings $D_1, \ldots, D_r$ and positive integers $n_1, \ldots, n_r$. The number r is uniquely determined, as are the pairs $(n_1, D_1), \ldots, (n_r, D_r)$ (up to permutation).*

Proof. According to Proposition 1.1.60-(i), ${}_R R$ can be decomposed into a finite direct sum of minimal left ideals. By grouping these left ideals into same isomorphic classes, we can write

$$_R R \simeq \bigoplus_{i=1}^{r} n_i V_i, \tag{1.1.66.1}$$

where $\{V_1, \ldots, V_r\}$ is a set of representatives of the isomorphism classes of simple R-modules. Firstly, as Proposition 1.1.30, we have an isomorphism of rings

$$R \simeq \mathrm{End}_R({}_R R)^{\mathrm{op}}.$$

Secondly, by Schur's Lemma, $\mathrm{Hom}_R(n_i V_i, n_j V_j) \simeq \prod_{k=1}^{n_i n_j} \mathrm{Hom}_R(V_i, V_j) = 0$ for all $i \neq j$, so that Proposition 1.1.62 applies to give a ring isomorphism

$$\mathrm{End}_R({}_R R)^{\mathrm{op}} \simeq \left(\prod_{i=1}^{r} \mathrm{End}_R(n_i V_i) \right)^{\mathrm{op}} \simeq \prod_{i=1}^{r} \mathrm{End}_R(n_i V_i)^{\mathrm{op}}.$$

Lastly, by Proposition 1.1.61 and Proposition 1.1.31, there is a ring isomorphism

$$\prod_{i=1}^{r} \mathrm{End}_R(n_i V_i)^{\mathrm{op}} \simeq \prod_{i=1}^{r} \mathcal{M}_{n_i} \left(\mathrm{End}_R(V_i)\right)^{\mathrm{op}} \simeq \prod_{i=1}^{r} \mathcal{M}_{n_i} \left(\mathrm{End}_R(V_i)^{\mathrm{op}}\right),$$

where $D_i := \mathrm{End}_R(V_i)^{\mathrm{op}}$'s are division rings as stated in Schur's Lemma.

For the uniqueness, suppose that we have another ring isomorphism

$$R \simeq \prod_{i=1}^{s} \mathcal{M}_{m_i}(\Delta_i),$$

where Δ_i's are division rings. As mentioned in the Remark 1.1.65, $\Delta_i^{m_i}$'s are the unique simple $\mathcal{M}_{m_i}(\Delta_i)$-modules (up to isomorphism), respectively. Each $\Delta_i^{m_i}$ can be regarded as module over R in a natural manner. Observe that $\Delta_i^{m_i} \not\simeq \Delta_j^{m_j}$ for all $i \neq j$ as R-modules, and that $\Delta_i^{m_i}$ is simple as R-module (since R is considered containing each $\mathcal{M}_{m_i}(\Delta_i)$). Henceforth, we have an R-isomorphism $\mathcal{M}_{m_i}(\Delta_i) \simeq m_i \cdot \Delta_i^{m_i}$ for all i. Thus, we obtain an isomorphism of R-modules

$$_R R = \bigoplus_{i=1}^{s} m_i \cdot \Delta_i^{m_i}. \tag{1.1.66.2}$$

According to Jordan-Hölder Theorem for two decompositions (1.1.66.1) and (1.1.66.2), we conclude that $r = s$, $m_i = n_{\sigma(i)}$ and $\Delta_i^{m_i} \simeq V_{\sigma(i)}$ as R-modules for some permutation $\sigma \in S_r$. Finally, we show that $\Delta_i \simeq \mathrm{End}_{\mathcal{M}_{m_i}(\Delta_i)}(\Delta_i^{m_i})^{\mathrm{op}}$. In fact, consider the following map:

$$\begin{array}{rcl} f : \Delta_i & \to & \mathrm{End}_{\mathcal{M}_{m_i}(\Delta_i)}(\Delta_i^{m_i})^{\mathrm{op}}, \\ \delta & \mapsto & f_\delta, \end{array}$$

where $f_\delta : \Delta_i^{m_i} \to \Delta_i^{m_i}$ determined by $f_\delta(v) = v\delta$. It is routine to check that f is an injective homomorphism. To prove the surjection of f, we pick $\lambda \in \mathrm{End}_{\mathcal{M}_{m_i}(\Delta_i)}(\Delta_i^{m_i})^{\mathrm{op}}$ and write $\lambda(e_1) = e_1 d + \sum_{i=2}^{m_i} e_i d_i$. It follows that

$$\lambda(v) = \lambda([v, 0, \ldots, 0]e_1) = [v, 0, \ldots, 0]\lambda(e_1) = vd,$$

for all $v \in \Lambda_i^{m_i}$. As a result, we get $\lambda = f_d$, or that f is a surjective. Therefore, we conclude that

$$D_{\sigma(i)} = \mathrm{End}_R\left(V_{\sigma(i)}\right)^{\mathrm{op}} \simeq \mathrm{End}_R(\Delta_i^{m_i})^{\mathrm{op}} \simeq \mathrm{End}_{\mathcal{M}_{m_i}(\Delta_i)}(\Delta_i^{m_i})^{\mathrm{op}} \simeq \Delta_i.$$

□

Symmetrically, a ring is said to be *right semisimple* if its right regular module is semisimple, i.e. a direct sum of it simple submodules. It is not difficult to realize that R is right semisimple if and only if R^{op} is left semisimple. In the preceding theorem, we are able to establish an isomorphism

$$R^{\text{op}} \simeq \prod_{i=1}^{r} \mathcal{M}_{n_i}\left(\text{End}_R(V_i)\right),$$

which deduces that R^{op} is left semisimple.

Corollary 1.1.67. *A ring is left semisimple if and only if it is right semisimple.*

Henceforth, we are able to say that a ring is *semisimple* without emphasizing the side of semisimplicity.

Definition 1.1.68. An algebra over a field is *semisimple* if it is finite-dimensional over the field and it is a semisimple ring.

Theorem 1.1.69 (Wedderburn–Artin II Theorem)**.** *Let R be semisimple algebra over a field $\mathbb{F}$. Then $R \simeq \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_r}(D_r)$ for some finite-dimensional division algebras $D_1, \ldots, D_r$ over $\mathbb{F}$ and positive integers $n_1, \ldots, n_r$. The number r is uniquely determined, as are the pairs $(n_1, D_1), \ldots, (n_r, D_r)$ (up to permutation).*

Proof. From what we have been deduced in Wedderburn–Artin I Theorem, it remains to show that all D_i's are finite-dimensional division algebras over $\mathbb{F}$. Write

$${}_RR \simeq \bigoplus_{i=1}^{r} n_i V_i,$$

where $\{V_1, \ldots, V_r\}$ is a set of representatives of the isomorphism classes of simple R-modules. Since R is finite-dimensional over $\mathbb{F}$, so are V_i's and $\text{End}_R(V_i)$'s as well. Besides, each $\text{End}_R(V_i)$ possesses a natural structure of $\mathbb{F}$-algebra. Thus, the proof is completed. □

Using the same argument in the proof of Frobenius Theorem on the algebraically closed field $\mathbb{C}$, we deduce that every finite-dimensional division algebra over an algebraically closed field is precisely the field, and hence the following result.

Corollary 1.1.70. *Let R be semisimple algebra over an algebraically closed field $\mathbb{F}$. Then $R \simeq \mathcal{M}_{n_1}(\mathbb{F}) \times \cdots \times \mathcal{M}_{n_r}(\mathbb{F})$ for some positive integers $n_1, \ldots, n_r$. The number r is uniquely determined as well as the tuple $(n_1, \ldots, n_r)$ (up to a permutation).*

1.1.5 Group algebras and Maschke's Theorem

In this subsection, we devote ourselves entirely to establishing the prominent Maschke's Theorem on the so-called group algebras, that is, it concerns the semisimplicity of certain group algebras. The most importance of Maschke's Theorem is that it tells of the decomposition of representations of finite groups into irreducible pieces. More precisely, in group representation theory, there is an one-to-one correspondence between a representation of a finite group and a module over the corresponding group algebra. On the other hand, as stated in Proposition 1.1.59, the semisimplicity of the group algebra implies the semisimplicity of all the modules over it, and hence our concern.

Definition 1.1.71. Let G be a finite group, and let $\mathbb{F}$ be a field. The *group algebra* $\mathbb{F}G$ is an algebra over $\mathbb{F}$ whose vector space possesses a basis labelled by all the elements of G, and the multiplication is defined by

$$\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{h\in G}\beta_h h\right)=\sum_{\zeta\in G}\left(\sum_{gh=\zeta}\alpha_g\beta_h\right)\zeta,$$

for all tuples $(\alpha_g)_{g\in G}$ and $(\beta_h)_{h\in G}$.

Remark 1.1.72. The identity in the group algebra $\mathbb{F}G$ is $1\cdot 1$. Moreover, G can be embedded inherently into the group algebra $\mathbb{F}G$.

Theorem 1.1.73 (Maschke's Theorem)**.** *Let $\mathbb{F}$ be a field whose characteristic does not divide the order of a finite group G. Then, the group algebra $\mathbb{F}G$ is semisimple.*

Proof. According to Proposition 1.1.58, it is equivalent to prove that every submodule of the regular module ${}_{\mathbb{F}G}\mathbb{F}G$ is a direct summand. Recall that the projection characterizes the direct summand (over an arbitrary ring) in the sense that each decomposition $V=U\oplus W$ corresponds to the projection $\pi:V\to U$, and vice versa. Suppose that U is a submodule of ${}_{\mathbb{F}G}\mathbb{F}G$. As vector spaces, there is another $\mathbb{F}$-space V such that ${}_{\mathbb{F}G}\mathbb{F}G=U\oplus V$. It gives rise to the $\mathbb{F}$-linear projection $\pi:{}_{\mathbb{F}G}\mathbb{F}G\to U$ on U. We would like to alter the above map to obtain an $\mathbb{F}G$-linear map by the so-called "average" process. Consider the following map

$$\begin{array}{rcl}\psi:\mathbb{F}G & \to & U,\\ x & \mapsto & \frac{1}{|G|}\sum_{g\in G}g\cdot\pi(g^{-1}\cdot x),\end{array}$$

for all $x \in \mathbb{F}G$. The assumption that the characteristic of $\mathbb{F}$ does not divide the order of G gives the well-definedness of ψ. It remains to verify that the map above is an $\mathbb{F}G$-linear projection on U. It is straightforward that ψ is $\mathbb{F}$-linear, and induces the identity on U. Finally, for every $h \in G$, we have

$$\begin{aligned}
\psi(h \cdot x) &= \frac{1}{|G|}\sum_{g\in G} g \cdot \pi\left(g^{-1} \cdot (h \cdot x)\right) \\
&= \frac{1}{|G|}\sum_{g\in G} g \cdot \pi\left((h^{-1}g)^{-1} \cdot x\right) \\
&= \frac{1}{|G|}\sum_{g\in G} (hg) \cdot \pi\left(g^{-1} \cdot x\right) \\
&= h\left(\frac{1}{|G|}\sum_{g\in G} g \cdot \pi\left(g^{-1} \cdot x\right)\right) \\
&= h \cdot \psi(x),
\end{aligned}$$

for all $x \in \mathbb{F}G$. Therefore, there is an $\mathbb{F}G$-module W such that ${}_{\mathbb{F}G}\mathbb{F}G = U \oplus W$ as $\mathbb{F}G$-modules as desired. $\square$

Chapter 2

Subpermutable subgroups of skew linear groups and unit groups of real group algebras

2.1 Preliminaries

2.1.1 General linear groups over division rings

In the previous chapter, we have encountered the matrix rings over divsions rings as well as its semisimplicity. Now we take a closer look at its so-called general linear group, which is the set of all units of the matrix ring.

To begin with, we will recall that many concepts of linear algebra over fields remaining applicable to the case of division rings. For instance, the Gaussian elimination is appropriate as well. We only need to pay attention at the side of the multiplication of elements in division rings since they are not commutative in general.

Definition 2.1.1. The *general linear group* of degree n over a division ring D, denoted by $\mathrm{GL}_n(D)$, is the set of all invertible matrices of degree n with entries in D, together with the usual matrix multiplication.

Denote by $\mathbb{F}_q$, where q is a positive integer, the field of q elements.

Proposition 2.1.2. The general linear group of degree 2 over the field of two elements is isomorphic to the symmetric group of degree 3, that is,

$$\mathrm{GL}_2(\mathbb{F}_2) \simeq S_3.$$

Proof. Note that $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$ and $\mathrm{GL}_2(\mathbb{F}_2)$ is nonabelian. It is well-known that every nonabelian of order 6 is isomorphic to S_3. The proof is completed. $\square$

Proposition 2.1.3. There is a unique subgroup of the general linear group of degree 2 over the field of three elements isomorphic to the quaternion group.

Proof. The group homomorphism $f : Q_8 \to \mathrm{GL}_2(\mathbb{F}_3)$ given by

$$1 \mapsto I_2, \qquad i \mapsto \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad k \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

is both well-defined and injective since $\mathrm{char}(\mathbb{F}_3) \neq 2$. Moreover, $f(Q_8)$ is the only subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ having the structure of the quaternion. $\square$

Recall that the Dieudonné determinant (cf. [LY21, Theorem 2.6-(i)]), which applies to matrices with entries in division rings, generalizes the notion of accustomed determinant applying to matrices with entries in fields. To be precise, if D is a division ring, then the Dieudonné determinant is a group homomorphism $\det : \mathrm{GL}_n(D) \to D^*/[D^*, D^*]$, where $D^*/[D^*, D^*]$ is the abelianization of D^*. As mentioned above, many facts in linear algebra is applicable in the case of division rings:

(i) The determinant of the identity is 1;

(ii) if two rows are exchanged, then the determinant is multiplied by -1;

(iii) if a row is left multiplied by an element $\alpha \in D^*$, then so is the determinant;

(iv) if a row is replaced by the sum of that row and a multiple of another row, then the determinant is invariant;

(v) the determinant is multiplicative, that is, $\det(AB) = \det(A)\det(B)$ for all invertible matrices A and B.

Definition 2.1.4. The *special linear group* of degree n over a division ring D, denoted by $\mathrm{SL}_n(D)$, is the kernel of the Dieudonné determinant $\det : \mathrm{GL}_n(D) \to D^*/[D^*, D^*]$.

Example 2.1.5. For a given positive integer $n \geq 2$ and a division ring D, we denote by $e_{ij} \in \mathcal{M}_n(D)$ the matrix whose (i, j)-th entry is 1 and all other entries are zeros. For $i \neq j$ and $\alpha \in D$, we set $T_{ij}(\alpha) = I_n + \alpha e_{ij}$, named a *transvection*. By the above facts, one sees that $T_{ij}(\alpha) \in \mathrm{SL}_n(D)$ for all $i \neq j$ and $\alpha \in D$.

In case of fields, it is known that all the transvections generate the special linear group. In fact, it holds for division rings as well.

Theorem 2.1.6. *The special linear group of degree $n \geq 2$ over a division ring D is generated by all the transvections.*

Proof. It was proved in [LY21, Theorem 1.1-(a)]. □

Theorem 2.1.7. *Let D be a division ring and $n \geq 2$ an integer.*

(i) The center $Z(\mathrm{GL}_n(D)) = Z(D)^* \cdot I_n$.

(ii) The center $Z(\mathrm{SL}_n(D)) = (Z(D)^* \cdot I_n) \cap \mathrm{SL}_n(D)$.

Proof. See [LY21, Theorem 1.2-(a)] for *(ii)*. □

Definition 2.1.8. The *projective special linear group* of degree n over a division ring D, denoted by $\mathrm{PSL}_n(D)$, is the quotient group of the special linear group over its center.

The following result asserts the simplicity of the projective special linear group of degree $n \geq 2$ as long as D has at least 4 elements when $n = 2$.

Proposition 2.1.9. Let D be a division ring and $n \geq 2$ an integer such that $|D| \geq 4$ when $n = 2$. Then the projective special linear group of degree n over D is simple.

Proof. The detail is referred to [LY21, Theorem 1.2-(b)]. □

To conclude this subsection, we state the following remarkable result:

Lemma 2.1.10. *Let D be a division ring and $n \geq 2$ an integer such that $|D| \geq 4$ when $n = 2$. Assume that N is a non-central subgroup of $\mathrm{GL}_n(D)$. The following statements are equivalent:*

(1) N contains $\mathrm{SL}_n(D)$;

(2) N is normal in $\mathrm{GL}_n(D)$;

(3) N is subnormal in $\mathrm{GL}_n(D)$.

Proof. The implication *(2)* $\Rightarrow$ *(3)* is trivial, and *(3)* $\Rightarrow$ *(1)* is a consequence of [MA98, Theorem 4]. Lastly, we note that $\mathrm{SL}_n(D) = [\mathrm{GL}_n(D), \mathrm{GL}_n(D)]$ in our situation (cf. [LY21, Theorem 1.1-(b)]), so if $\mathrm{SL}_n(D)$ is contained in N, then so is $[\mathrm{GL}_n(D), \mathrm{GL}_n(D)]$. Thus, $N \trianglelefteq \mathrm{GL}_n(D)$. □

2.1.2 Permutable and Subpermutable subgroups

Definition 2.1.11. A subgroup H of a group G is *permutable* in G, denoted by $H \leq_p G$, if $HK = KH$ for every subgroup K of G.

Some authors use the term "quasinormal" instead of "permutable". However, for consistence, we would stick to the notion "quasinormal" in the entire dissertation.

Definition 2.1.12. A subgroup H of a group G is *subpermutable* in G if there is a finite chain of subgroups of G

$$H = H_n \leq \cdots \leq H_1 \leq H_0 = G,$$

such that H_{i+1} is permutable in H_i for all indices i.

Lemma 2.1.13. *Let G be a group.*

(i) For any subgroup K of G, if H is a permutable subgroup of G, then so is $H \cap K$ of K;

(ii) if H and K are both permutable in G, then so is HK;

(iii) for a normal subgroup N of G, if H is a permutable subgroup of G containing N, then so is H/N of G/N;

(iv) for a homomorphism ϕ from G, if H is permutable in G, then so is $\phi(H)$ in $\phi(G)$.

Proof. (i) For every subgroup L of K, we have

$$(H \cap K)L = HL \cap KL = LH \cap LK = L(H \cap K).$$

(ii) Note that $HK = KH$ which implies that HK is a group. Then, for every subgroup L of G, we have

$$(HK)L = H(KL) = H(LK) = (HL)K = (LH)K = L(HK).$$

(iii) For every subgroup L/N of G/N, we have

$$(H/N)(L/N) = (HL)/N = (LH)/N = (L/N)(H/N).$$

(iv) Note that every subgroup T of $\phi(G)$ has the form $\phi(L)$, where $L = \phi^{-1}(T)$. Then we have

$$T\phi(H) = \phi(L)\phi(H) = \phi(LH) = \phi(HL) = \phi(H)\phi(L) = \phi(H)T.$$

□

To close the subsection, we shall introduce two remarkable results on the permutability, including a classical one on the permutability of simple groups and a sequel to a recent paper linking the permutability and subnormality.

Theorem 2.1.14. *A simple group only has itself and the trivial subgroup as its permutable subgroups.*

Proof. See [Sto72, Corollary C2]. □

Proposition 2.1.15. Let H be a permutable subgroup of a group G. Then, either

- H is subnormal in G; or
- G is radical over H, that is, for every element $x \in G$, there is some positive integer n_x such that $x^{n_x} \in H$.

Proof. See [DBH21, Lemma 2.4]. □

2.2 Subpermutable subgroups of skew linear groups

Our goal in this section is to establish an equivalence between subpermutability and other properties in skew linear groups of degree greater than 1 apart from $\mathrm{GL}_2(\mathbb{F}_3)$ (up to isomorphism). Furthermore, we will indicate a counterexample for $\mathrm{GL}_2(\mathbb{F}_3)$ for the sake of completion.

Lemma 2.2.1. *Let D be a division ring and $n \geq 2$ an integer such that $|D| \geq 4$ when $n = 2$. Then, every proper permutable subgroup of $\mathrm{SL}_n(D)$ is central.*

Proof. Assume by contradiction that there is a proper non-central permutable subgroup Q of $\mathrm{SL}_n(D)$. Denote by Z the center of $\mathrm{SL}_n(D)$. By putting $H = QZ$, we see that H is permutable in $\mathrm{SL}_n(D)$, and hence so is H/Z in $\mathrm{SL}_n(D)/Z = \mathrm{PSL}_n(D)$ (cf. Lemma 2.1.13-*(iii)*). As the simplicity of $\mathrm{PSL}_n(D)$ as stated in Proposition 2.1.9, we deduce that H/Z is either trivial or equal to $\mathrm{PSL}_n(D)$ (see Theorem 2.1.14). Nonetheless, neither case holds. Indeed, the former situation occurs if and only if Q is central in $\mathrm{SL}_n(D)$, contradicting to the presumption. On the other hand, the latter situation results in $H = \mathrm{SL}_n(D)$. Besides, Q is normal in H because for all $q \in Q$ and $pz = x \in H$, where $p \in Q$ and $z \in Z$,

$$x^{-1}qx = z^{-1}p^{-1}qpz = p^{-1}qp \in Q.$$

To sum up, we then obtain a chain of normal subgroups $Q \trianglelefteq H = \mathrm{SL}_n(D) \trianglelefteq \mathrm{GL}_n(D)$, which means that Q is subnormal in $\mathrm{GL}_n(D)$. Thus, by Lemma 2.1.10, Q contains $\mathrm{SL}_n(D)$, a contradiction. $\square$

By means of the previous lemma, we are able to come up with the main result of this section.

Theorem 2.2.2. *Let D be a division ring and $n \geq 2$ an integer such that $D \not\cong \mathbb{F}_3$ when $n = 2$. Suppose that Q is a non-central subgroup of $\mathrm{GL}_n(D)$. The following statements are equivalent:*

(1) Q contains $\mathrm{SL}_n(D)$;

(2) Q is normal in $\mathrm{GL}_n(D)$;

(3) Q is subnormal in $\mathrm{GL}_n(D)$;

(4) Q is permutable in $\mathrm{GL}_n(D)$*;*

(5) Q is subpermutable in $\mathrm{GL}_n(D)$*.*

Proof. When $n = 2$ and $D \simeq \mathbb{F}_2$, it follows that $\mathrm{GL}_n(D) \simeq S_3$ (cf. Proposition 2.1.2), and so $\mathrm{SL}_n(D) \simeq A_3$. Moreover, the non-central subgroups of S_3 comprise $A_3, \langle(1\,2)\rangle, \langle(2\,3)\rangle$, and $\langle(3\,1)\rangle$, where A_3 satisfies all five conditions above, and others satisfy none.

Now, consider either $n \geq 3$ or $n = 2$ and $|D| \geq 4$. As stated in Lemma 2.1.10, we obtain an equivalence between *(1)*, *(2)*, and *(3)*. Secondly, the implications *(2)* $\Rightarrow$ *(4)* $\Rightarrow$ *(5)* is trivial. Thus, it remains to show that *(5)* $\Rightarrow$ *(1)*. In fact, by the definition of subpermutability, there is a finite chain of subgroups of $\mathrm{GL}_n(D)$

$$Q = Q_r \leq \cdots \leq Q_1 \leq Q_0 = \mathrm{GL}_n(D)$$

such that Q_{i+1} is permutable in Q_i for all indices i. We shall prove by induction on i that Q_i contains $\mathrm{SL}_n(D)$. For $i = 0$, it is straightforward that $\mathrm{SL}_n(D) \subseteq \mathrm{GL}_n(D) = Q_0$. Assume that the statement holds for $i = m \geq 0$, that is, $\mathrm{SL}_n(D) \subseteq Q_m$. It remains to show that $\mathrm{SL}_n(D) \subseteq Q_{m+1}$. The inductive hypothesis is equivalent to that Q_m is normal in $\mathrm{GL}_n(D)$ according to Lemma 2.1.10. The fact that Q_{m+1} is permutable in Q_m deduces that either Q_{m+1} is subnormal in Q_m or Q_m is radical over Q_{m+1} (see Proposition 2.1.15). If Q_{m+1} is subnormal in Q_m, then Q_{m+1} is subnormal in $\mathrm{GL}_n(D)$ as well since $Q_m \trianglelefteq \mathrm{GL}_n(D)$. By Lemma 2.1.10, we imply that $\mathrm{SL}_n(D) \subseteq Q_{m+1}$ as desired. If Q_m is radical over Q_{m+1}, that is, for every $x \in Q_m$, there exists some $n_x \in \mathbb{N}_{\geq 1}$ such that $x^{n_x} \in Q_{m+1}$, we claim that $Q_{m+1} \cap \mathrm{SL}_n(D)$ is non-central. Indeed, we denote by P the prime subfield of D:

(i) If $P \simeq \mathbb{Q}$, by setting $x = T_{1n}(1) = I_n + e_{1n} \in \mathrm{SL}_n(D) \subseteq Q_m$, we have that $Q_{m+1} \ni x^{n_x} = I_n + n_x e_{1n}$ for some $n_x \in \mathbb{N}_{\geq 1}$. Thus, $I_n + n_x e_{1n} \in Q_{m+1} \cap \mathrm{SL}_n(D)$ is a non-central element, which follows that $Q_{m+1} \cap \mathrm{SL}_n(D)$ is non-central;

(ii) if $P \simeq \mathbb{F}_p$ for some prime number p, for each $\alpha \in D^*$ and each pair of indices $1 \leq i \neq j \leq n$, we let $s_{\alpha ij}$ be the smallest positive integer such that $T_{ij}(\alpha)^{s_{\alpha ij}} \in Q_{m+1}$. If there is a triple (α, i, j) such that $\gcd(s_{\alpha ij}, p) = 1$, that is, there are some integers k, ℓ such that $k s_{\alpha ij} + \ell p = 1.$, then

$$T_{ij}(\alpha) = T_{ij}((k s_{\alpha ij} + \ell p)\alpha) = T_{ij}(k s_{\alpha ij} \alpha) = (T_{ij}(\alpha)^{s_{\alpha ij}})^k \in Q_{m+1} \cap \mathrm{SL}_n(D),$$

which leads to $Q_{m+1} \cap \mathrm{SL}_n(D)$ is non-central. On the other side, if $\gcd(s_{\alpha ij}, p) = p$ for all triples (α, i, j), then $s_{\alpha ij} = p$ due to the fact that $T_{ij}(\alpha)^p = T_{ij}(p\alpha) = I_n$, and the minimality of $s_{\alpha ij}$. In other words, $T_{ij}(\alpha)$ is of order p for all triples (α, i, j). We assert that $T_{ij}(\alpha)^{-1} Q_{m+1} T_{ij}(\alpha) = Q_{m+1}$ for all triples (α, i, j). In fact, if $T_{ij}(\alpha) \in Q_{m+1}$, it is clearly true; otherwise, because Q_{m+1} is permutable in Q_m, so $Q_{m+1}\langle T_{ij}(\alpha)\rangle = \langle T_{ij}(\alpha)\rangle Q_{m+1}$ - it is hence a group - by the definition of permutability. Furthermore,

$$[Q_{m+1}\langle T_{ij}(\alpha)\rangle : Q_{m+1}] = p.$$

By [HS99, Theorem 1], it follows that $Q_{m+1} \trianglelefteq Q_{m+1}\langle T_{ij}(\alpha)\rangle$, or equivalently that $T_{ij}(\alpha)^{-1} Q_{m+1} T_{ij}(\alpha) = Q_{m+1}$. Thus, our assertion has been proved. Now, according to Theorem 2.1.6, we have $\mathrm{SL}_n(D) = \langle T_{ij}(\alpha) : \alpha \in D^* \rangle$, which results in $S^{-1} Q_{m+1} S = Q_{m+1}$ for all $S \in \mathrm{SL}_n(D)$. Applying [NBH17, Theorem 3.1], we get that $\mathrm{SL}_n(D) \subseteq Q_{m+1}$, which is equivalent to $Q_{m+1} \cap \mathrm{SL}_n(D) = \mathrm{SL}_n(D)$, a non-central group.

Thus, the claim has been shown. Recall that Q_{m+1} is permutable in Q_m, which deduces that $Q_{m+1} \cap \mathrm{SL}_n(D)$ is permutable in $Q_m \cap \mathrm{SL}_n(D) = \mathrm{SL}_n(D)$ (see Lemma 2.1.13-*(i)*). Therefore, as a consequence of Lemma 2.2.1, it follows that $Q_{m+1} \cap \mathrm{SL}_n(D) = \mathrm{SL}_n(D)$, or equivalently, $\mathrm{SL}_n(D) \subseteq Q_{m+1}$ as desired. In conclusion, $Q_r = Q$ contains $\mathrm{SL}_n(D)$. □

Corollary 2.2.3. *Let D be an arbitrary division ring and $n \geq 2$ an integer. Then, every subpermutable subgroup of $\mathrm{GL}_n(D)$ is subnormal.*

Proof. It is directly implied from [Sto72, Theorem 4.2] for $\mathrm{GL}_2(\mathbb{F}_3)$ and Theorem 2.2.2. □

Proposition 2.2.4. There exists a subpermutable subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ which is not normal.

Proof. As stated in Proposition 2.1.3, we are able to regard Q_8 as a subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$, where

$$1 = I_2, \qquad i = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad j = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad k = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Furthermore, since there are no other subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$ isomorphic to Q_8, the quaternion Q_8 is normal in $\mathrm{GL}_2(\mathbb{F}_3)$. Besides, the subgroup $\langle i\rangle$ of Q_8 is of index 2, and hence is normal. To sum up, $\langle i\rangle$ is a subnormal, and hence subpermutable, subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$ through the normal series

$$\langle i\rangle \triangleleft Q_8 \triangleleft \mathrm{GL}_2(\mathbb{F}_3),$$

but it is not normal in $\mathrm{GL}_2(\mathbb{F}_3)$ since

$$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \notin \langle i\rangle.$$

$\square$

2.3 Subpermutable subgroups of unit groups of real group algebras

In this section, we aim to establish an analogue of Theorem 2.2.2 but for $D = \mathbb{H}$ and $n = 1$, and subsequently show that every subpermutable subgroup of the unit group of a real group algebra is normal. Before doing so, we recall some basic facts about the real quaternion.

Recall that the norm of an element $\alpha = a + bi + cj + dk \in \mathbb{H}$ is defined by

$$|\alpha| = \sqrt{\alpha \cdot \overline{\alpha}} = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

An element $\alpha \in \mathbb{H}$ is nonzero if and only if $|\alpha|$ is nonzero; if so, then its inverse is simplified as

$$\alpha^{-1} = \frac{\overline{\alpha}}{|\alpha|^2}.$$

Furthermore, the norm is mulplicative, that is, $|\alpha\beta| = |\alpha||\beta|$ for all $\alpha, \beta \in \mathbb{H}$, and so it commutes with the inverse operator, that is, $|\alpha^{-1}| = |\alpha|^{-1}$ for all $\alpha \in \mathbb{H}$. Now, we define $\mathbb{H}_1$ to be the subset of $\mathbb{H}$ whose norm is 1, that is,

$$\mathbb{H}_1 = \{a + bi + cj + dk \in \mathbb{H} : a^2 + b^2 + c^2 + d^2 = 1\},$$

with the multiplication as in $\mathbb{H}$. It turns out to be a normal subgroup of $\mathbb{H}^*$, and moreover, it takes a role as $\mathrm{SL}_n(D)$ in the previous section. Notice also that $\mathbb{H}_1$ is non-central as it contains i, and $Z(\mathbb{H}_1) = \pm 1$.

Theorem 2.3.1. *Let Q be a non-central subgroup of the unit $\mathbb{H}^*$ of the real quaternion. The following assertions are equivalent:*

(1) Q contains $\mathbb{H}_1$;

(2) Q is normal in $\mathbb{H}^*$;

(3) Q is subnormal in $\mathbb{H}^*$;

(4) Q is permutable in $\mathbb{H}^*$;

(5) Q is subpermutable in $\mathbb{H}^*$.

Proof. The technique we have used in Theorem 2.2.2 is reused but with a slight modification. The implications *(2)* $\Rightarrow$ *(3)* and *(2)* $\Rightarrow$ *(4)* $\Rightarrow$ *(5)* clearly follow due to the definitions of the concepts while *(2)* $\Rightarrow$ *(1)* and *(3)* $\Rightarrow$ *(2)*, respectively, hold because of [Gre78, Claim, Page 163] and [Gre78, Example, Page 162], respectively. Thus, it remains to show the implications *(1)* $\Rightarrow$ *(2)* and *(5)* $\Rightarrow$ *(2)*.

(1) $\Rightarrow$ *(2)*: Remark that for every $\alpha, \beta \in \mathbb{H}^*$, we have

$$|[\alpha, \beta]| = |\alpha^{-1}\beta^{-1}\alpha\beta| = |\alpha^{-1}||\beta^{-1}||\alpha||\beta| = 1,$$

which means that every commutator element of $\mathbb{H}^*$ is contained in $\mathbb{H}_1$. Therefore, if $\mathbb{H}_1$ is contained in Q, then so is $[\mathbb{H}^*, \mathbb{H}^*]$. Consequently, Q is normal in $\mathbb{H}^*$.

(5) $\Rightarrow$ *(2)*: Assume that Q is subpermutable in $\mathbb{H}^*$ and

$$Q = Q_r \leq_p \cdots \leq_p Q_1 \leq_p Q_0 = \mathbb{H}^*$$

is a permutable series of Q in $\mathbb{H}^*$. Note that every Q_i is non-central as it contains Q. We shall induct on i that Q_i is normal in $\mathbb{H}^*$. For $i = 0$, it is trivial that $Q_0 = \mathbb{H}^* \trianglelefteq \mathbb{H}^*$. Suppose that the statement holds for some $i = m \geq 0$, that is, Q_m is normal in $\mathbb{H}^*$. We need to show that Q_{m+1} is normal in $\mathbb{H}^*$ as well. According to Proposition 2.1.15, it follows that either Q_{m+1} is subnormal in Q_m or Q_m is radical over Q_{m+1}. If Q_{m+1} is subnormal in Q_m, then Q_{m+1} is subnormal in $\mathbb{H}^*$ for $Q_m \trianglelefteq \mathbb{H}^*$, which deduces that $Q_{m+1} \trianglelefteq \mathbb{H}^*$ by [Gre78, Example, Page 162]. If Q_m is radical over Q_{m+1}, it means that, for every element $x \in Q_m$, there exists some positive integer n_x such that $x^{n_x} \in Q_{m+1}$. For the sake of simplicity, we set $N = Q_{m+1} \cap \mathbb{H}_1$ and $M = NZ(\mathbb{H}_1)$. Observe that we have already shown that *(1)* $\Leftrightarrow$ *(2)*. In particular, $\mathbb{H}_1 \subseteq Q_m$ by the assumption. From the observation above, it is sufficient to show that $\mathbb{H}_1 \subseteq Q_{m+1}$, or equivalently, $N = \mathbb{H}_1$. Therefore, by applying Lemma 2.1.13 repeatedly, $N = Q_{m+1} \cap \mathbb{H}_1$ is permutable in $Q_m \cap \mathbb{H}_1 = \mathbb{H}_1$, and hence $M/Z(\mathbb{H}_1) = NZ(\mathbb{H}_1)/Z(\mathbb{H}_1)$ is permutable in $\mathbb{H}_1/Z(\mathbb{H}_1)$. On the other hand, according to [Lam03, (5.8)], we have $\mathbb{H}_1/Z(\mathbb{H}_1) \simeq \mathrm{SO}(3)$ - a simple group (see [Sti08, Subsection 2.3, Page 33] for details). Combining the two assertions above together with Lemma 2.1.14, it follows that either $M = Z(\mathbb{H}_1)$ or $M = \mathbb{H}_1$. If the former situation holds, then $N \subseteq Z(\mathbb{H}_1) = \{\pm 1\}$. Besides, for every element $x \in \mathbb{H}_1 \subseteq Q_m$, there exists some positive integer n_x such that $x^{n_x} \in Q_{m+1} \cap \mathbb{H}_1 = N$, so $x^{2n_x} = 1$ for every $x \in \mathbb{H}_1$. In other words, $\mathbb{H}_1$ is a torsion group, which concludes that $\mathbb{H}_1$ is central (cf. [Her78, Theorem 8]), contradicting to our remark above. Thus, it must satisfy that $M = \mathbb{H}_1$, and so $[\mathbb{H}_1 : N] = [M : N] = [NZ(\mathbb{H}_1) : N] \leq 2$. Subsequently, we obtain that N is a normal subgroup of $\mathbb{H}_1$, and hence N is a subnormal subgroup of $\mathbb{H}^*$. Applying [Gre78, Example, Page 162] and [Gre78, Claim, Page 163] respectively, we get that N is normal in $\mathbb{H}^*$ and then $N = \mathbb{H}_1$, as desired. To sum up, Q_i is normal in $\mathbb{H}^*$ for all $i \geq 0$, and thus specifically that Q is normal in $\mathbb{H}^*$. The proof is complete. □

Corollary 2.3.2. *If D is either a field or the real quaternion and $n \geq 1$ is an integer, then every subpermutable subgroup of $\mathrm{GL}_n(D)$ except for $\mathrm{GL}_2(\mathbb{F}_3)$ (up to isomorphism) is normal.*

Proof. Let N be a subpermutable subgroup of $\mathrm{GL}_n(D)$. If N is central, it is obviously normal in $\mathrm{GL}_n(D)$. Otherwise, the statement is deduced from Theorem 2.2.2 for $n > 1$ and Theorem 2.3.1 for $n = 1$. □

Theorem 2.3.3. *Every subpermutable subgroup of the unit group of the real group algebra of a finite group is normal.*

Proof. Let G be a finite group and Q a subpermutable subgroup of the unit group $(\mathbb{R}G)^*$ of the real group algebra of G over $\mathbb{R}$. Assume furthermore that Q is non-central since there is nothing to do with the centrality. Let

$$Q = Q_r \leq_p \cdots \leq_p Q_1 \leq_p Q_0 = (\mathbb{R}G)^*$$

be a permutable series of Q in $(\mathbb{R}G)^*$. According to Theorem 1.1.73 or known as Maschke's Theorem, the group algebra $\mathbb{R}G$ is a semisimple algebra over $\mathbb{R}$. Then, by Theorem 1.1.69 or known as Wedderburn-Artin II Theorem, we have an algebra isomorphism

$$\mathbb{R}G \simeq \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_s}(D_s),$$

where D_k's are finite-dimensional division algebras over $\mathbb{R}$ and n_k's are positive integers. Furthermore, the number s and the pairs (n_k, D_k)'s are uniquely determined. Consequently, we obtain a group isomorphism

$$(\mathbb{R}G)^* \simeq \mathrm{GL}_{n_1}(D_1) \times \cdots \times \mathrm{GL}_{n_s}(D_s).$$

Then, for every subgroup Q_k of $(\mathbb{R}G)^*$ in the permutable series, there are subgroups $Q_{k,\ell}$'s of $\mathrm{GL}_{n_\ell}(D_\ell)$'s respectively such that

$$Q_k \simeq Q_{k,1} \times \cdots \times Q_{k,s}.$$

By Lemma 2.1.13, we obtain s permutable series

$$Q_{r,\ell} \leq_p \cdots \leq_p Q_{1,\ell} \leq_p Q_{0,\ell} = \mathrm{GL}_{n_\ell}(D_\ell),$$

where $1 \leq \ell \leq s$. In other words, $Q_{r,\ell}$ is subpermutable in $\mathrm{GL}_{n_\ell}(D_\ell)$ for every $1 \leq \ell \leq s$. On the other hand, since every D_k is a finite-dimensional division algebras over $\mathbb{R}$, it is isomorphic to either $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$ (see Theorem 1.1.56). Therefore, by applying Corollary 2.3.2, $Q_{r,\ell}$ is normal in $\mathrm{GL}_{n_\ell}(D_\ell)$, and so $Q_{r,1} \times \cdots \times Q_{r,s}$ is normal in $\mathrm{GL}_{n_1}(D_1) \times \cdots \times \mathrm{GL}_{n_s}(D_s)$, or equivalently, Q is normal in $(\mathbb{R}G)^*$. The proof is complete. $\square$

References

[DBH21] L. Q. Danh, M. H. Bien, and B. X. Hai. "Permutable Subgroups in $GL_n(D)$ and Applications to Locally Finite Group Algebras". In: *Vietnam Journal of Mathematics* (2021). DOI: 10.1007/s10013-021-00513-8.

[Gre78] G. R. Greenfield. "A note on subnormal subgroups of division algebras". In: *Canadian Journal of Mathematics* 30.1 (1978), pp. 161–163.

[Her78] I. N. Herstein. "Multiplicative commutators in division rings". In: *Israel Journal of Mathematics* 31 (1978), pp. 180–188.

[HS99] A. Hassani and S. Sedghi. "On the Quasi-Normality and Subnormality of Subgroups of Finite Groups". In: *Vietnam Journal of Mathematics* 27.3 (1999), pp. 253–258.

[Lam03] T. Y. Lam. "Hamilton's quaternions". In: *Handbook of Algebra* 3 (2003), pp. 429–454.

[LY21] Chun-Yi Lin and Chia-Fu Yu. "Dieudonné's determinants and structure of general linear groups over division rings revisited". In: *Bulletin of the Institute of Mathematics Academia Sinica (New Series)* 16.1 (2021), pp. 21–47. DOI: 10.21915/BIMAS.2021102.

[MA98] M. Mahdavi-Hezavehi and S. Akbari. "Some special subgroups of $GL_n(D)$". In: *Algebra Colloquium* 5 (1998), pp. 361–370.

[NBH17] N. K. Ngoc, M. H. Bien, and B. X. Hai. "Free subgroups in almost subnormal subgroups of general skew linear groups". In: *St. Petersburg Mathematical Journal* 28.5 (2017), pp. 707–717.

[Rot02] J. J. Rotman. *Advanced Modern Algebra*. Prentice Hall, Upper Saddle River, NJ, 2002. ISBN: 0-13-087868-5.

[Sti08] J. Stillwell. *Naive Lie Theory*. Undergraduate Texts in Mathematics. Springer-Verlag New York, 2008. ISBN: 978-0-387-78214-0. DOI: 10.1007/978-0-387-78214-0.

[Sto72] S. W. Stonehewer. "Permutable subgroups of infinite groups". In: *Mathematische Zeitschrift* 125 (1972), pp. 1–16. DOI: 10.1007/BF01111111.

Index