Elements with large irreducible submodules contained in maximal subgroups of the general linear group

Dipl.-Math.
Sabina Barbara Pannek

This thesis is presented in partial fulfilment
of the requirements for the degree of
Doctor of Philosophy of
The University of Western Australia
Department of Mathematics.
January 2019

Elements with large irreducible submodules contained in maximal subgroups of the general linear group

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften der RWTH Aachen University zur Erlangung des akademischen Grades einer Doktorin der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Dipl.-Math.
Sabina Barbara Pannek,
geb. Groth

aus

Gdingen, Polen

Berichter: Univ.-Prof. Dr. rer. nat. Gerhard Hiß
Professor Colva M Roney-Dougal

Tag der mündlichen Prüfung: 10. Dezember 2018

To Jürgen, Alina, Laura & Timo

Thesis Declaration

I, Sabina Barbara Pannek certify that:

- This thesis has been substantially accomplished during enrolment in the degree.
- This thesis does not contain material which has been accepted for the award of any other degree or diploma in my name, in any university or other tertiary institution.
- No part of this work will, in the future, be used in a submission in my name, for any other degree or diploma in any university or other tertiary institution without the prior approval of The University of Western Australia and the RWTH Aachen University responsible for the joint-award of this degree.
- This thesis does not contain any material previously published or written by another person, except where due reference has been made in the text.
- The work is not in any way a violation or infringement of any copyright, trademark, patent, or other rights whatsoever of any person.
- This thesis contains published work which has been co-authored.

Authorship Declaration

This thesis contains work that has been published.

Details of the work: [47] A. C. Niemeyer, S. B. Pannek, and C. E. Praeger. Irreducible linear subgroups generated by pairs of matrices with large irreducible submodules, *Arch. Math. (Basel)*, 98(2):105-114. 2012

Location in thesis: Chapter 6 (pp. 93–102), lines 3–7 on p. *xi*, lines 1–5 in the last paragraph on p. 2, lines 4–9 in the second paragraph on p. 5.

Student contribution to work: The author of this thesis was responsible for writing this paper and contributed fully to the mathematical ideas, their exposition and proofs, and handled the submission.

Abstract

This thesis is concerned with a family of so-called *fat elements* in the finite general linear group $\mathrm{GL}(\mathcal{V})$ consisting of all non-singular linear mappings on a finite vector space $\mathcal{V}$. We refer to an element of $\mathrm{GL}(\mathcal{V})$ as being *fat* if it leaves invariant, and acts irreducibly on, a subspace of dimension greater than $\dim(\mathcal{V})/2$. Fatness of an element can be decided efficiently in practice by testing whether its characteristic polynomial f has an irreducible factor of degree greater than $\deg(f)/2$.

Fat elements generalise the concept of ppd-*elements*, which are defined by the property of having orders divisible by certain primes called *p*rimitive *p*rime *d*ivisors. In 1997, Guralnick, Penttila, Praeger and Saxl classified all subgroups of $\mathrm{GL}(\mathcal{V})$ containing ppd-elements. Their work has had a wide variety of applications in computational group theory, number theory, permutation group theory, and geometry.

Our overall goal is to carry out an analogous classification of all subgroups of $\mathrm{GL}(\mathcal{V})$ containing fat elements, and this thesis initiates that project.

We first develop a comprehensive framework necessary for the study of fat elements. This includes new results in elementary number theory (concerning the order of an integer modulo r), theory of finite fields (counting certain irreducible polynomials) and group theory (regarding irreducible semilinear mappings). We then investigate the occurrence of fat elements in various subgroups of the general linear group $\mathrm{GL}(\mathcal{V})$. As in the case of the "ppd-classification", our analysis is patterned by Aschbacher's classification of the maximal subgroups of $\mathrm{GL}(\mathcal{V})$ into nine partly overlapping classes $\mathscr{C}_1, \ldots, \mathscr{C}_8$, and $\mathscr{S}$. We investigate members of the Aschbacher classes $\mathscr{C}_1, \ldots, \mathscr{C}_5, \mathscr{C}_7$ and several representatives of the class $\mathscr{S}$ upon the existence of fat elements. Although a large majority of fat elements in $\mathrm{GL}(\mathcal{V})$ are ppd-elements, we show that members of certain Aschbacher classes with no (or hardly any) ppd-elements do contain fat elements. Therefore, the results we obtain in classes $\mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4, \mathscr{C}_7$ significantly differ from the findings of the "ppd-classification". For groups G contained in the Aschbacher classes $\mathscr{C}_1, \ldots, \mathscr{C}_5$ and (with restrictions in) $\mathscr{C}_7$ we additionally calculate the precise value of, and also determine good lower and upper bounds for, the proportion of all fat elements in G.

Kurzbeschreibung (German abstract)

Die vorliegende Arbeit befasst sich mit einer Familie von Elementen in der allgemeinen linearen Gruppe $\mathrm{GL}(\mathcal{V})$, der Gruppe aller nicht singulären linearen Abbildungen auf einem endlichen Vektorraum $\mathcal{V}$. Diese Familie besteht aus den sogenannten *fetten Elementen*, die wie folgt definiert sind. Ein Element g in $\mathrm{GL}(\mathcal{V})$ heißt *fett*, wenn $\mathcal{V}$ einen $\langle g\rangle$-invarianten Untervektorraum enthält, dessen Dimension größer als $\dim(\mathcal{V})/2$ ist, und auf dem $\langle g\rangle$ irreduzibel operiert. Dies ist gleichbedeutend mit der Eigenschaft, dass das charakteristische Polynom von g einen irreduziblen Faktor besitzt, dessen Grad größer als $\dim(\mathcal{V})/2$ ist. Anhand dieses Kriteriums lassen sich Elemente der $\mathrm{GL}(\mathcal{V})$ in der Praxis effizient auf die Eigenschaft „fett“ untersuchen.

Fette Elemente verallgemeinern ppd-*Elemente*. Darunter verstehen wir Elemente in $\mathrm{GL}(\mathcal{V})$, deren Ordnungen primitive Primteiler (auf Englisch „*p*rimitive *p*rime *d*ivisors“) besitzen. Guralnick, Penttila, Praeger und Saxl klassifizierten im Jahr 1997 alle Untergruppen der $\mathrm{GL}(\mathcal{V})$, die ppd-Elemente enthalten. Ihre Ergebnisse werden seitdem vielfältig angewandt, unter anderem in der algorithmischen Gruppentheorie, der Zahlentheorie, der Theorie der Permutationsgruppen sowie der Geometrie.

Unser langfristiges Ziel ist es, all diejenigen Untergruppen der $\mathrm{GL}(\mathcal{V})$ zu klassifizieren, welche fette Elemente enthalten. Die vorliegende Dissertation kann als Auftakt dieses Projekts betrachtet werden.

Im ersten Teil dieser Arbeit entwickeln wir das mathematische Handwerkszeug, das für das Studium der fetten Elemente notwendig ist. Dabei erhalten wir neue Ergebnisse aus der elementaren Zahlentheorie (über die Ordnung einer Zahl modulo r), der Körpertheorie (über Anzahlen bestimmter irreduzibler Polynome) sowie der Gruppentheorie (über irreduzible semilineare Abbildungen). Der zweite Teil widmet sich der Frage, ob – und gegebenenfalls wie häufig – fette Elemente in verschiedensten Untergruppen der $\mathrm{GL}(\mathcal{V})$ auftreten. Wie auch schon der „ppd-Klassifikation“ liegt unserer Analyse Aschbachers Einteilung der maximalen Untergruppen der $\mathrm{GL}(\mathcal{V})$ in neun sich teilweise überlappende Klassen $\mathscr{C}_1, \ldots, \mathscr{C}_8$ und $\mathscr{S}$ zugrunde. Wir untersuchen die Existenz fetter Ele-

mente in Gruppen, die zu Aschbachers Klassen $\mathscr{C}_1, \ldots, \mathscr{C}_5, \mathscr{C}_7$ gehören, sowie in einigen Repräsentanten der Klasse $\mathscr{S}$. Gleichwohl sich die meisten fetten Elemente in der $\mathrm{GL}(\mathcal{V})$ als ppd-Elemente identifizieren lassen, zeigen wir, dass Vertreter gewisser Aschbacher Klassen, die keinerlei (oder kaum) ppd-Elemente enthalten, sehr wohl fette Elemente aufweisen. Aus diesem Grund unterscheiden sich unsere Resultate in den Klassen $\mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4, \mathscr{C}_7$ wesentlich von den Ergebnissen der „ppd-Klassifikation“. Für Mitglieder G der Klassen $\mathscr{C}_1, \ldots, \mathscr{C}_5$ sowie (mit einigen Einschränkungen) $\mathscr{C}_7$ berechnen wir zudem die genaue Proportion (in G) der in G enthaltenen fetten Elemente. Wir geben für diese Proportion jeweils auch eine gute untere und obere Schranke an.

Acknowledgements

In German, PhD candidates refer to their supervisors as their *Doktormutter* ("doctoral mother") or *Doktorvater* ("doctoral father"). Being a cotutelle student, I feel extremely privileged to have "doctoral parents". I would like to express my sincerest gratitude to my brilliant supervisors Professor Cheryl Praeger and Professor Gerhard Hiß for a multitude of things. I thank them both for sharing their immense knowledge, for their guidance and encouragement, for their advice, for their trust, and for their patience — especially at times when I had to suspend my work. Further, I deeply appreciate all the extra effort and support in regard to the cotutelle agreement, recurring tuition problems, and various other administrative issues. I thank Professor Gerhard Hiß for allowing me to work very independently, while always being available to answer questions in addition to carefully reading my drafts. This has given me the confidence to pursue my own mathematical interests and made me grow as a mathematician. Many thanks to Professor Cheryl Praeger for her ability to "read my mind", that is to understand and structure my thoughts, helping me to solidify my ideas. Special thanks to Cheryl for sharing her enthusiasm for mathematics. Her joyful attitude mixed with tireless work is truly inspiring!

A big — in fact a huge — thank you goes to Professor Alice Niemeyer for sharing her invaluable insights and experiences, for her kindness, and for many stimulating discussions both in Perth and in Aachen.

I would also like to thank Dr. Thomas Stemler who, for most of my candidature, has been the graduate research co-ordinator of the School of Mathematics and Statistics at UWA. His help was always fantastic and very much appreciated.

My research was partly supported by a scholarship awarded by the Studienstiftung des deutschen Volkes (German Academic Scholarship Foundation) and I acknowledge this financial support. Further, I am grateful to the BIBA – Bremer Institut für Produktion und Logistik GmbH at the University of Bremen for providing me with an office during the last two years.

My experience over the past years has been enriched by making many new friends, and it is with their support that I have been able to complete this thesis. On behalf of all of them, I particularly thank Natalie Naehrig and

Katharina Artic (for being the best office colleagues), Gavin Nicklette (for making Perth feel like home) and Lisete Scholz-Sieves (for being the kind soul in Bremen).

Last but foremost, I thank my family. Many thanks to my amazing husband Jürgen. Without his love, understanding and support I would not have made it to the end. Especially during the intense period prior to submission, he has been my super hero taking care of pretty much everything. I also thank our kids Alina, Laura and Timo for their unconditional love and their smiles. Discussions on dragons or horses rather than mathematics were a welcome distraction.

Contents

Chapter 1

Introduction

The central theme of this thesis is a certain family of elements in the finite general linear group $\mathrm{GL}(\mathcal{V})$, the group of all non-singular linear mappings on a finite vector space $\mathcal{V}$. We briefly introduce these elements in Section 1.1 while motivating the work presented in the subsequent chapters. A summary of our main results is given in Section 1.2. Section 1.3 outlines the structure of this thesis.

Notation. Throughout this chapter we assume that $\mathcal{V}$ is a non-trivial, d-dimensional vector space defined over the finite field $\mathbb{F}_q$ of size q.

1.1 Background

The principal motivation for the work reported here stems from a problem in computational group theory. Given a set X of elements from $\mathrm{GL}(\mathcal{V})$, we would like to explore properties of the group G generated by X. Since the order of $\mathrm{GL}(\mathcal{V})$ grows exponentially in d, the group G is potentially huge, limiting the scope of deterministic methods. We therefore often use randomised algorithms in order to answer questions about G. Such algorithms derive information about G by looking at properties of independent, uniformly distributed random elements in G. One property of interest is whether, for some integer e satisfying $d/2 < e \leq d$, the element order is divisible by a *primitive prime divisor* of $q^e - 1$, that is by a prime divisor of $q^e - 1$ which does not divide $q^i - 1$ for any $i < e$. We refer to such elements as *primitive prime divisor elements*, or ppd-*elements* for short. If we wish to specify the values of q, d, and e, we use the term $\mathrm{ppd}(d, q; e)$-*element*. Note that we reserve the names primitive prime divisor element and ppd-element for $\mathrm{ppd}(d, q; e)$-elements with respect to some e strictly larger than $d/2$.

Primitive prime divisor elements have been exploited by Niemeyer and Praeger [48] in order to recognise finite classical groups in their natural representation, that is in order to examine whether a subgroup of $\mathrm{GL}(\mathcal{V})$ contains the group $\Omega(\mathcal{V})$, as defined in [38, p. 14]. (In the linear case, $\Omega(\mathcal{V})$ is the finite special linear group $\mathrm{SL}(\mathcal{V})$, that is the group of all elements in $\mathrm{GL}(\mathcal{V})$ with determinant 1. Otherwise, $\Omega(\mathcal{V})$ is a d-dimensional symplectic, unitary or orthogonal group and the quotient of $\Omega(\mathcal{V})$ by its centre is "generally" simple.) The *Classical Recognition Algorithm* [48] relies, among other things, on the following facts.

(1) We can efficiently identify ppd-elements among elements in $\mathrm{GL}(\mathcal{V})$.

(2) The list of all subgroups of $\mathrm{GL}(\mathcal{V})$ containing ppd-elements is known and reasonably short. (A classification of all such groups is presented in [30].)

(3) Primitive prime divisor elements occur frequently in groups containing $\Omega(\mathcal{V})$, and there are good estimates for the proportions of all ppd-elements in such groups. (Good upper and lower bounds for these proportions are given in [48, Theorem 6.1]. For example, a group G satisfying $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$ contains roughly $\ln(2)|G| \approx 0.69|G|$ ppd-elements.)

Any $\mathrm{ppd}(d, q; e)$-element $g \in \mathrm{GL}(\mathcal{V})$ specifies an e-dimensional and $\langle g \rangle$-invariant subspace $\mathcal{U}$ of $\mathcal{V}$, on which $\langle g \rangle$ acts irreducibly. Since $e > d/2$, the subspace $\mathcal{U}$ is uniquely determined by g. We generalise the concept of ppd-elements by considering elements in $\mathrm{GL}(\mathcal{V})$ which are solely defined by the property of having large, that is at least $(\lfloor d/2 \rfloor + 1)$-dimensional, irreducible subspaces. We call such elements *fat*. More precisely, we refer to $g \in \mathrm{GL}(\mathcal{V})$ as being a $\mathrm{fat}(d, q; e)$-*element* if $\langle g \rangle$ leaves invariant, and acts irreducibly on, a subspace of dimension $e > d/2$. Whether an element $g \in \mathrm{GL}(\mathcal{V})$ is fat can by decided efficiently in practice by testing if its characteristic polynomial has an irreducible factor of degree greater than $d/2$. Checking if the characteristic polynomial has a large irreducible factor is also the first step in the process to determine if $g \in \mathrm{GL}(\mathcal{V})$ is a ppd-element, which is why testing for "fatness" is cheaper than testing for the "ppd-property".

While every ppd-element is fat the converse implication is not true, as the presence of an e-dimensional $\langle g \rangle$-irreducible subspace of $\mathcal{V}$ is not sufficient to guarantee that g is a $\mathrm{ppd}(d, q; e)$-element. For example, for $(d, q) = (3, 3)$, an element of order 8 in $\mathrm{GL}(\mathcal{V})$ is a $\mathrm{fat}(3, 3; 2)$-element but not a $\mathrm{ppd}(3, 3; 2)$-element since $3^2 - 1 = 8$ has no prime divisors which do not divide $3 - 1 = 2$. There are also examples of $\mathrm{fat}(d, q; e)$-elements with orders not divisible by any primitive prime divisor of $q^e - 1$ despite the fact that such divisors exist. The research questions we address in this thesis stem from the observation that, even though fat elements do not necessarily need to be ppd-elements, most fat elements turn out to be ppd-elements. In fact, we show that the upper and lower bounds for the proportion of ppd-elements in $\mathrm{GL}(\mathcal{V})$ given

in [48, Theorem 6.1] also hold for fat elements. Hence, approximately 70% of elements in $\mathrm{GL}(\mathcal{V})$ are fat, of which less than $|\mathrm{GL}(\mathcal{V})|/(d-1)+|\mathrm{GL}(\mathcal{V})|/(d+2)$ are not ppd-elements. The proportion of fat elements which are not ppd-elements is therefore at most c/d for some constant c. The low percentage of fat "non-ppd-elements" suggests that it is feasible to prove a counterpart to the ppd-classification [30] for fat elements. This would open up the possibility to bypass looking for ppd-elements and pave the way for new algorithms based solely on fat elements.

Our long-term goal is hence to carry out a classification of all subgroups of $\mathrm{GL}(\mathcal{V})$ containing fat elements and, moreover, to determine the proportion of fat elements in the relevant groups. The present thesis is a major advance in achieving this goal. A summary of our results is given in the next section. Underlying our analysis is Aschbacher's classification of maximal subgroups of $\mathrm{GL}(\mathcal{V})$ into nine partly overlapping classes $\mathscr{C}_1, \ldots, \mathscr{C}_8$ and $\mathscr{S}$. It turns out that members of certain Aschbacher classes (for example $\mathscr{C}_2, \mathscr{C}_4, \mathscr{C}_7$) contain $\mathrm{fat}(d, q; e)$-elements for some specified values of e, despite having very few or no ppd-elements. Our findings may thus help to recognise members of these classes.

We add that the ppd-classification [30] has been applied widely not only in computational group theory, but also for example in number theory [1], permutation group theory [7, 11, 43], and geometry [4, 37]. We expect a successful completion of our project likewise to find applications outside of computational group theory.

1.2 Summary of main results

Recall that $\mathcal{V}$ is a d-dimensional vector space over $\mathbb{F}_q$. In this thesis we investigate the existence, and determine the proportion, of fat elements in $\mathrm{GL}(\mathcal{V})$ and in members of various Aschbacher classes for $\mathrm{GL}(\mathcal{V})$. A rough description of these classes is given on p. 91. More details on the classes $\mathscr{C}_1, \mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4, \mathscr{C}_5, \mathscr{C}_7$, and $\mathscr{S}$ can be found at the beginning of Chapters 6, 7, 8, 9, 10, 11, and 12.

The presence of fat elements in $\mathrm{GL}(\mathcal{V})$, as well as in many Aschbacher classes, is linked to the existence of certain families of irreducible polynomials defined over the underlying field $\mathbb{F}_q$. In fact, the problem of counting all fat elements in the groups of interest often reduces to counting all polynomials of some specified degrees in the respective family. One such family of polynomials which we consider, and which helps us to determine the proportion (and thus also the existence) of fat elements in members of $\mathscr{C}_2$ and $\mathscr{C}_3$, are *t-hyper-irreducible* polynomials ($t \in \mathbb{N}$). These are polynomials f in the polynomial ring $\mathbb{F}_q[x]$ such that $f(x^t)$ is irreducible. (Hence, 1-*hyper-irreducible* simply means *irreducible*.) As we show in Theorem 3.18, whether or not $\mathbb{F}_q[x]$ contains t-hyper-irreducible polynomials of degree m can be verified by checking if the

order of q modulo $(q^m-1)t$ is equal to mt. We write $\mathrm{ord}(q;(q^m-1)t)=mt$. An equivalent condition is that $\gcd(t,4)\prod_{i=1}^{\ell}t_i$ divides q^m-1, where $t_1,\dots,t_\ell$ are all the distinct odd prime divisors of t.

Definitions 3.5 & 3.22. For $m,t\in\mathbb{N}$ we write $N_q^*(m,t)$ to denote the number of all monic, t-hyper-irreducible polynomials $f\neq x$ of degree m over $\mathbb{F}_q$. Further, we define $N_q^*(m)=N_q^*(m,1)$.

A formula for $N_q^*(m)$ is known and dates back to Gauß [26]. We generalise Gauß' result in Theorem 3.23 by showing that, if $N_q^*(m,t)\neq 0$, then

$$N_q^*(m,t)=\frac{\varphi(t)}{mt}\sum_{j\in J}\mu(j)(q^{m/j}-1),$$

where $\varphi:\mathbb{N}\to\mathbb{N}$ is Euler's totient function, $\mu:\mathbb{N}\to\{-1,0,1\}$ is the Moebius function (see Definition 3.6), and J is the set of all positive divisors j of m such that $(q^m-1)/(q^{m/j}-1)$ and t are coprime. We further present good lower and upper bounds for $N_q^*(m,t)$ in Theorem 3.24. More precisely, assuming that $N_q^*(m,t)\neq 0$, we obtain

$$\frac{\varphi(t)(q^m-1)}{t(m+1)}\leq N_q^*(m,t)\leq\frac{\varphi(t)(q^m-1)}{tm}.$$

The functions $N_q^*(m,t)$ and $N_q^*(m)$ come in handy when calculating proportions of fat elements in the groups considered in this thesis, and we always state these proportions in terms of $N_q^*(m,t)$ and/or $N_q^*(m)$.

Definitions 4.20 & 5.17. (a) Let G be a subgroup of the general semilinear group $\Gamma\mathrm{L}(\mathcal{V})$. We write $\mathrm{irr}(G)$ for the proportion in G of all irreducible elements in G.

(b) Let G be a subset of $\mathrm{GL}(\mathcal{V})$, and let $e\in\mathbb{N}$ be such that $d/2<e\leq d$. We define $\mathrm{fat}(G;e)$ to be the proportion in G of all $\mathrm{fat}(d,q;e)$-elements in G.

We point out that $\mathrm{irr}(G)=\mathrm{fat}(G;d)$ for $G\leq\mathrm{GL}(\mathcal{V})$. Theorem 4.22 shows that a subgroup $G\leq\Gamma\mathrm{L}(\mathcal{V})$ containing $\mathrm{GL}(\mathcal{V})$ satisfies

$$\mathrm{irr}(G)=\sum_{t_0\mid t}\frac{\varphi(t_0)N^*_{q^{1/t_0}}(d)}{\big((q^{1/t_0})^d-1\big)t},\qquad\text{where } t=|G:\mathrm{GL}(\mathcal{V})|,$$

and moreover,

$$\frac{1}{d+1}\leq\mathrm{irr}(G)\leq\frac{1}{d}.$$

Notice that $q=q_0^t$ for some prime power q_0 as $t=|G:\mathrm{GL}(\mathcal{V})|$, and thus q^{1/t_0} is well-defined.

In Theorem 5.18 we calculate the proportion $\mathrm{fat}(G;e)$ for any subgroup G such that $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$. More precisely, we prove that (if $d \geq 2$ and $e > d/2$, then)

$$\mathrm{fat}(G;e) = \frac{N_q^*(e)}{q^e - 1} \tag{1.1}$$

and

$$\frac{1}{e+1} \leq \mathrm{fat}(G;e) < \frac{1}{e}. \tag{1.2}$$

Theorem 6.4 demonstrates that (1.1) and (1.2) remain true if we substitute the group G (with $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$) by the stabiliser in G of some subspace $\mathcal{W} \leq \mathcal{V}$, provided that $\dim(\mathcal{W}) \in [0, d-e] \cup [e, d]$. In Theorem 6.11 we show that for groups G with $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$ most pairs of fat elements from G generate irreducible subgroups, namely we prove that the proportion of pairs of fat elements generating a reducible subgroup, in the set of all pairs in $G \times G$, is less than q^{-d+1}. In Theorem 6.12 we further prove that the conditional probability to obtain a pair (g_1, g_2) in $G \times G$ which generates a reducible subgroup, given that g_1, g_2 are fat elements, is less than $2q^{-d+1}$.

Chapters 7, 8, 9, 10 and 11 are devoted to the study of fat elements in Aschbacher's classes $\mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4, \mathscr{C}_5$ and $\mathscr{C}_7$. Let $G \leq \mathrm{GL}(\mathcal{V})$ be a member of one of these classes, such that

$$G \cong \begin{cases} \mathrm{GL}(m,q) \wr S_t, \text{ where } mt = d, & \text{if } G \in \mathscr{C}_2, \\ \mathrm{GL}(m,q^t).t, \text{ where } t \text{ is prime and } mt = d, & \text{if } G \in \mathscr{C}_3, \\ \mathrm{GL}(m,q) \circ \mathrm{GL}(t,q), \text{ where } mt = d, & \text{if } G \in \mathscr{C}_4, \\ \mathrm{GL}(d, q^{1/t}) \circ \mathbb{F}_q^*, & \text{if } G \in \mathscr{C}_5, \\ \big(\mathrm{GL}(m,q) \circ \mathrm{GL}(m,q)\big).S_2, \text{ where } m^2 = d \geq 4^2, & \text{if } G \in \mathscr{C}_7. \end{cases} \tag{1.3}$$

(Observe that we do not require $m \neq t$ if $G \in \mathscr{C}_4$, or that t is prime if $G \in \mathscr{C}_5$. However, we consider the $\mathscr{C}_7$-class only in the special case where the tensor decomposition of $\mathcal{V}$ has two components and $d \geq 16$.) Then according to Theorems 7.40(*b*), 8.31, 9.25, 10.2(*b*), and 11.3(*a*), the group G contains $\mathrm{fat}(d,q;e)$-elements if and only if

$$\begin{cases} \text{there exist positive integers } m_0 \leq m \text{ and } t_0 \leq t \text{ such} \\ \text{that } \gcd(q,t_0) = 1 \text{ and } \mathrm{ord}(q;(q^{m_0}-1)t_0) = e, & \text{if } G \in \mathscr{C}_2, \\ \text{either } t \mid e, \text{ or } \gcd(q,t) = 1 \text{ and } \mathrm{ord}(q;(q^{m_0}-1)t) = e \\ \text{for some positive integer } m_0 \leq m, & \text{if } G \in \mathscr{C}_3, \\ \text{there exist positive integers } m_0 \leq m \text{ and } t_0 \leq t \\ \text{such that } \gcd(m_0,t_0) = 1 \text{ and } m_0 t_0 = e, & \text{if } G \in \mathscr{C}_4, \\ \text{the integers } e, t \text{ are coprime}, & \text{if } G \in \mathscr{C}_5, \\ \text{there exists positive integers } e_1, e_2 \leq m \text{ such that} \\ \gcd(e_1,e_2) = 1 \text{ and } e_1 e_2 = e, & \text{if } G \in \mathscr{C}_7. \end{cases}$$

An explicit formula for $\mathrm{fat}(G;e)$ is given in Theorems 7.42, 8.33, 9.26, 10.3, and 11.3(b). For simplicity of exposition we only restate our results for $e=d$ here. Recall that $\mathrm{fat}(G;d)=\mathrm{irr}(G)$.[(I)] If G is as in (1.3) above and $\mathrm{irr}(G)\neq 0$, then

$$\mathrm{irr}(G)=\begin{cases}\dfrac{N_q^*(m,t)}{t(q^m-1)}, & \text{if } G\in\mathscr{C}_2,\\[2ex] \dfrac{N_q^*(mt)}{q^{mt}-1}+\dfrac{(t-1)N_q^*(m,t)}{t(q^m-1)}, & \text{if } G\in\mathscr{C}_2 \text{ and } t\mid q^m-1,\\[2ex] \dfrac{N_q^*(mt)}{q^{mt}-1}, & \text{if } g\in\mathscr{C}_3 \text{ and } t\nmid q^m-1,\\[2ex] \dfrac{N_q^*(m)N_q^*(t)}{(q^m-1)(q^t-1)}, & \text{if } G\in\mathscr{C}_4,\\[2ex] \dfrac{N_{q^{1/t}}^*(d)}{(q^{1/t})^d-1}, & \text{if } G\in\mathscr{C}_5,\end{cases}$$

and

$$\begin{cases}\dfrac{\varphi(t)}{t^2(m+1)}\le\mathrm{irr}(G)\le\dfrac{\varphi(t)}{t^2m}, & \text{if } G\in\mathscr{C}_2,\\[2ex] \dfrac{1}{mt+1}+\dfrac{(t-1)^2}{(m+1)t^2}\le\mathrm{irr}(G)\le\dfrac{1}{mt}+\dfrac{(t-1)^2}{mt^2}, & \text{if } G\in\mathscr{C}_3 \text{ and } t\mid q^m-1,\\[2ex] \dfrac{1}{mt+1}\le\mathrm{irr}(G)\le\dfrac{1}{mt}, & \text{if } G\in\mathscr{C}_3 \text{ and } t\nmid q^m-1,\\[2ex] \dfrac{1}{(m+1)(t+1)}\le\mathrm{irr}(G)\le\dfrac{1}{mt}, & \text{if } G\in\mathscr{C}_4,\\[2ex] \dfrac{1}{d+1}\le\mathrm{irr}(G)\le\dfrac{1}{d}, & \text{if } G\in\mathscr{C}_5.\end{cases}$$

If $G\in\mathscr{C}_7$, then G has no irreducible elements but may admit fat elements. We further show in Theorem 11.2 the following. If $G\in\mathscr{C}_7$, as specified in (1.3), and G contains a fat element g, then (somewhat surprisingly) g does not "swap" the two tensor components of the underlying vector space.

Recall that a prime divisor of q^e-1 ($e\in\mathbb{N}$) which does not divide q^i-1 for any $i<e$ is called a primitive prime divisor of q^e-1. Similarly, a prime power divisor of q^e-1 not dividing q^i-1 for any $i<e$ is referred to as a *primitive prime power divisor* of q^e-1. Let $e>d/2$. A $\mathrm{fat}(d,q;e)$-element in $\mathrm{GL}(\mathcal{V})$ is said to be *exceptional* if its order does not admit any primitive prime power divisors of q^e-1. Consider an absolutely irreducible subgroup G of $\mathrm{GL}(\mathcal{V})$ which is not realisable over a proper subfield and which is isomorphic

[(I)] For $G\in\{\mathscr{C}_2,\mathscr{C}_3,\mathscr{C}_4\}$ the value of $\mathrm{irr}(G)=\mathrm{fat}(G;d)$ is also given in Corollary 7.36, Proposition 8.25(b), and Proposition 9.22, respectively.

either to a covering group of a sporadic simple group or to a covering group of a finite simple linear/unitary/symplectic group in characteristic $r \nmid q$. We show in Theorems 12.6 and 12.17 that, with one exception, G does not contain any exceptional fat elements. The exception arises when $G \cong \mathrm{M}_{24}$, $d = 11$ and $q = 2$, in which case the corresponding exceptional fat elements are fat$(11, 2; 6)$-elements of order 21. (Technically, there are two exceptions, as there exist two non-equivalent absolutely irreducible representations of M_{24} of degree 11 over $\mathbb{F}_2$.)

1.3 Layout of thesis

The subsequent 11 chapters are divided into two parts.

Part I is the common mathematical basis for the work reported in Part II. It consists of Chapters 2–5, with Chapters 2, 3, 4 containing stand-alone results which are independent of the fat element context.

Chapter 2 contains results from elementary number theory. Chapter 3 is devoted to counting certain sets of irreducible polynomials over a finite field. Chapter 4 focuses on irreducible non-singular semilinear mappings on a finite vector space. Finally, Chapter 5 serves as an introduction to fat elements.

Part II contains Chapters 6–12 and discusses the occurrence of fat elements in Aschbacher's classes $\mathscr{C}_1, \ldots, \mathscr{C}_5, \mathscr{C}_7$, and $\mathscr{S}$. We reserve one chapter for each of the classes under consideration.

For reasons of clarity and readability we highlight parts of the text in different colours. We use blue for definitions and notation, red for lemmas, propositions and theorems, and highlight remarks and examples in green.

I

DEVELOPING THE THEORY UNDERLYING FAT ELEMENTS

Chapter 2

Some number theoretic results

For a positive integer r, consider the ring $\mathbb{Z}/r\mathbb{Z}$ of integers modulo r and its (multiplicative) group of units $(\mathbb{Z}/r\mathbb{Z})^*$. Elements of $(\mathbb{Z}/r\mathbb{Z})^*$ are of the form $a + r\mathbb{Z}$, where a is a positive integer coprime to r. In particular, $a \neq r$ unless $r = 1$, in which case $\mathbb{Z}/1\mathbb{Z}$ is the zero ring and $(\mathbb{Z}/1\mathbb{Z})^*$ is the trivial group. If a is coprime to r, then we write

$$\operatorname{ord}(a; r) = m$$

to denote that the element $a + r\mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$ has order m. Equivalently, m is the smallest positive integer such that $a^m - 1$ is divisible by r. In this situation we say that m is the *order of a modulo r* and call r a *primitive divisor* of $a^m - 1$. This chapter examines the relation between the integers a, r and m.

We begin in Section 2.1 by considering two number theoretic functions which are closely related to primitive divisors, namely Euler's totient function and the Carmichael function. Section 2.2 is devoted to the order of a modulo r. We are particularly interested in the case where $\operatorname{ord}(a; rt) > \operatorname{ord}(a; r)t/2$ for some positive integer t which is coprime to a. Section 2.3 slightly changes the point of view, focusing on the primitive divisors of $a^m - 1$.

2.1 Euler's totient and Carmichael's functions

Throughout this thesis we write $\mathbb{N}$ for the set of positive integers and use the letter φ to denote *Euler's totient function*, defined by

$$\varphi : \mathbb{N} \to \mathbb{N}, \quad r \mapsto \left|(\mathbb{Z}/r\mathbb{Z})^*\right|.$$

That is, φ assigns to each positive integer r the number of positive integers $a \leq r$ which are coprime to r. We have $\varphi(1) = 1$. For $r \geq 2$, the value of $\varphi(r)$ can be calculated as follows (see for example [49, p. 28]).

Lemma 2.1. *If r is a prime and $k \in \mathbb{N}$, then $\varphi(r^k) = (r-1)r^{k-1}$. If $r, s \in \mathbb{N}$ are coprime, then $\varphi(rs) = \varphi(r)\varphi(s)$.*

Observe that $\varphi(r)$ is even for all integers $r \geq 3$.

Given a positive integer a we use the summation symbol $\sum_{d|a}$ to denote that the sum runs through all positive divisors d of a (including the trivial divisor $d = 1$ and the non-proper divisor $d = a$).

Lemma 2.2. *Let $a, b \in \mathbb{N}$. Then the following hold.*

(a) We have $\sum_{d|a} \varphi(d) = a$.

(b) The set $\{1, \ldots, ab\}$ contains $a\varphi(b)$ elements which are coprime to b.

Proof. (a) Holds by [41, Theorem 3 − 9]

(b) Observe that the assertion holds for $b = 1$. We thus assume that $b \geq 2$. An element $\ell \in \{1, \ldots, ab\}$ is coprime to b if and only if $\ell = sb + r$ where s, r are integers satisfying $0 \leq s < a$, $1 \leq r < b$, and $\gcd(r, b) = 1$. Hence, there are precisely $a\varphi(b)$ choices for ℓ. □

Lemma 2.3. *Let $r \in \mathbb{N}$ be divisible by at least two distinct primes, and let ℓ be one of these primes. Then $\varphi(r) \leq (\ell - 1)(r - \ell)/\ell < (\sqrt{r} - 1)^2$.*

Proof. Let $r = \ell_1^{a_1}\ell_2^{a_2}\cdots\ell_k^{a_k}$, where $\ell_1, \ell_2, \ldots, \ell_k$ are pairwise distinct primes and $a_1, a_2, \ldots, a_k \in \mathbb{N}$. Using Lemma 2.1, we obtain

$$\varphi(r) = r\prod_{i=1}^{k}\left(1 - \frac{1}{\ell_i}\right) \leq r\left(1 - \frac{1}{\ell_1}\right)\left(1 - \frac{1}{\ell_2}\right).$$

Since $\ell_1/r \leq 1/\ell_2$ we get $(1 - 1/\ell_2) \leq (1 - \ell_1/r)$, and then

$$\varphi(r) \leq r\left(1 - \frac{1}{\ell_1}\right)\left(1 - \frac{\ell_1}{r}\right) = \frac{(\ell_1 - 1)(r - \ell_1)}{\ell_1}.$$

In order to complete the proof it remains to show that $(\ell_1 - 1)(r - \ell_1)/\ell_1 < r - 2\sqrt{r} + 1$. (We remark that the the inequality $\varphi(r) < r - 2\sqrt{r} + 1$ is proved in [28, Corollary 1].) Observe that

$$\begin{aligned} r - 2\sqrt{r} + 1 - \frac{(\ell_1 - 1)(r - \ell_1)}{\ell_1} &= r - 2\sqrt{r} + 1 - r + \ell_1 + \frac{r}{\ell_1} - 1 \\ &= \frac{r}{\ell_1} - 2\sqrt{r} + \ell_1 \\ &= \left(\sqrt{\frac{r}{\ell_1}} - \sqrt{\ell_1}\right)^2. \end{aligned}$$

Certainly, $(\sqrt{r/\ell_1} - \sqrt{\ell_1})^2 \geq 0$. If $(\sqrt{r/\ell_1} - \sqrt{\ell_1})^2 = 0$, then $\sqrt{r/\ell_1} = \sqrt{\ell_1}$, and hence $r = \ell_1^2$, which contradicts r being divisible by at least two distinct primes. This proves the assertion. □

We shall also consider another number theoretic function which is closely related to Euler's totient function: We write λ for the *Carmichael function*

$$\lambda : \mathbb{N} \to \mathbb{N}, \quad r \mapsto \exp\big((\mathbb{Z}/r\mathbb{Z})^*\big),$$

assigning to each positive integer r the exponent of the group $(\mathbb{Z}/r\mathbb{Z})^*$, that is the least common multiple of the orders of all elements in $(\mathbb{Z}/r\mathbb{Z})^*$. This function was first introduced by Carmichael [16] in 1910 and is therefore named after him. We have $\lambda(1) = 1$. For $r \geq 2$ the value of $\lambda(r)$ can be calculated as follows (see [16, p. 232] or [49, p. 29]).

Lemma 2.4. *Let $k \in \mathbb{N}$. We have $\lambda(2^k) = 2^{k-1}$ if $k \in \{1, 2\}$, and $\lambda(2^k) = 2^{k-2}$ if $k \geq 3$. If r is an odd prime, then $\lambda(r^k) = r^{k-1}(r-1) = \varphi(r^k)$.*
If $r, s \in \mathbb{N}$ are coprime, then $\lambda(rs) = \operatorname{lcm}\{\lambda(r), \lambda(s)\}$.

Note that $\lambda(r)$ divides $\varphi(r)$ for all positive integers r. Moreover, if $r \geq 3$, then $\lambda(r)$ is even. Observe further that $\lambda(r') \mid \lambda(r)$ if $r' \mid r$.

Remark 2.5. The Carmichael function is implemented in GAP [24]. For $r \in \mathbb{N}$, the value of $\lambda(r)$ can be accessed by calling

```
gap> Lambda(r);
```

Lemma 2.6. *Let $s, m, m' \in \mathbb{N}$ be such that $s \geq 3$ is odd and $m \geq 2m'$. Then $\lambda(s^m + s^{m'}) \leq (s^m - 1)/4$.*

Proof. Let $c, k \in \mathbb{N}$ be such that c is odd and $s^{m-m'} + 1 = 2^k c$. Note that s and c are coprime. Since $s^m + s^{m'} = s^{m'} 2^k c$, by Lemma 2.4 we have

$$\lambda(s^m + s^{m'}) = \operatorname{lcm}\big\{\lambda(s^{m'}), \lambda(2^k), \lambda(c)\big\}.$$

Now, since $s^{m'} \geq s \geq 3$, the integer $\lambda(s^{m'})$ is even. Moreover, either $\lambda(2^k)$ or $\lambda(c)$ is also even. (To see that this is true, we apply Lemma 2.4. If $k \geq 3$, then $\lambda(2^k) = 2^{k-2}$ and thus $\lambda(2^k)$ is even. If $k = 2$, then $\lambda(2^k) = 2$ is even. If $k = 1$, then by assumption $c \neq 1$ and thus, recalling that c is an odd positive integer, we have $c \geq 3$, whence $\lambda(c)$ is even.) It follows that $\lambda(s^m + s^{m'})$ divides, and hence is less or equal to, $\lambda(s^{m'})\lambda(2^k)\lambda(c)/2$. Then by Lemma 2.4 we obtain

$$\lambda(s^m + s^{m'}) \leq \frac{\lambda(s^{m'}) 2^k c}{4}.$$

Using $\lambda(s^{m'}) \leq s^{m'} - 1$ and recalling that $2^k c = s^{m-m'} + 1$, we conclude that

$$\lambda(s^m + s^{m'}) \leq \frac{(s^{m'} - 1)(s^{m-m'} + 1)}{4} = \frac{s^m - s^{m-m'} + s^{m'} - 1}{4} \leq \frac{s^m - 1}{4}. \quad \square$$

2.2 The order of an integer modulo r

Recall that elements in $(\mathbb{Z}/r\mathbb{Z})^*$ are of the form $a + r\mathbb{Z}$ where a is a positive integer coprime to r.

Definition 2.7. Let $a, r \in \mathbb{N}$ be coprime. We call the (multiplicative) order of $a + r\mathbb{Z} \in (\mathbb{Z}/r\mathbb{Z})^*$ the *order of a modulo r* and denote it by $\operatorname{ord}(a; r)$.

Remark 2.8. For coprime, positive integers a, r, we can access the value of $\operatorname{ord}(a; r)$ in GAP [24] by calling

```
gap> OrderMod(a,r);
```

2.2.1 Basic properties

Lemma 2.9. *Let $a, r, k \in \mathbb{N}$ be such that $\gcd(a, r) = 1$.*

(a) *We have $r \mid a^k - 1$ if and only if $\operatorname{ord}(a; r) \mid k$.*

(b) *If $r' \in \mathbb{N}$ is such that $r' \mid r$, then $\operatorname{ord}(a; r') \mid \operatorname{ord}(a; r)$.*

(c) *We have $\operatorname{ord}\big(a^k; r\big) = \operatorname{ord}(a; r)/\gcd(\operatorname{ord}(a; r), k)$.*

Proof. Let $m = \operatorname{ord}(a; r)$.

(a) Let ℓ, s be non-negative integers such that $s < m$ and

$$k = \ell m + s. \tag{2.1}$$

Since $a^m \equiv 1 \pmod{r}$ we have $a^{\ell m} \equiv 1 \pmod{r}$. Then (2.1) yields $a^k \equiv a^s \pmod{r}$. Thus, $r \mid a^k - 1$ if and only if $a^s \equiv 1 \pmod{r}$, which (recalling that $s < m$) is the case if and only if $s = 0$, that is by (2.1) if and only if $m \mid k$.

(b) Since $r \mid a^m - 1$, any divisor r' of r also divides $a^m - 1$. Then part (a) of the current lemma (applied to $k = m$ and $r = r'$) yields $\operatorname{ord}(a; r') \mid m$.

(c) Set $m' = \operatorname{ord}\big(a^k; r\big)$. Then m' is the smallest positive integer such that $r \mid a^{km'} - 1$. Hence, using part (a), we see that m' is the smallest positive integer such that $m \mid km'$. Thus, $m' = m/\gcd(m, k)$. □

Lemma 2.10. *Let $a, m, n \in \mathbb{N}$. Then $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.*

Proof. Set $\ell = \gcd(a^m - 1, a^n - 1)$ and $k = \gcd(m, n)$. Let $i \in \{m, n\}$.

We have $a^i - 1 = (a^k - 1)(a^{i-k} + a^{i-2k} + \cdots + a^k + 1)$ and, in particular, $a^k - 1 \mid a^i - 1$. Thus, $a^k - 1 \mid \ell$.

Conversely, since $\ell \mid a^i - 1$, by Lemma 2.9(a) we have $\operatorname{ord}(a; \ell) \mid i$. Thus, $\operatorname{ord}(a; \ell) \mid k$, and then, applying Lemma 2.9(a) one more time, we conclude that $\ell \mid a^k - 1$. □

Lemma 2.11. *Let $a, r, m \in \mathbb{N}$ be such that $\gcd(a, r) = 1$. The following are equivalent.*

(a) *We have $\operatorname{ord}(a; r) = m$.*

(b) *The integer r divides $a^m - 1$ but does not divide $a^i - 1$ for any positive integer $i < m$.*

(c) *The integer r divides $a^m - 1$ but does not divide $a^i - 1$ for any proper divisors i of m.*

Proof. By definition, the order of a modulo r is the smallest positive integer m such that $a^m + r\mathbb{Z} = 1 + r\mathbb{Z}$ (that is such that $a^m - 1$ is divisible by r). This shows the equivalence of (a) and (b).

Clearly, (b) implies (c). We complete the proof by showing that (c) entails (b). So, assume that (c) holds. Seeking a contradiction, suppose that r divides $a^i - 1$ for some positive integer $i < m$. Then r divides $\gcd(a^m - 1, a^i - 1)$ which, by Lemma 2.10, is equal to $a^{\gcd(m,i)} - 1$. This contradicts our assumption, for $\gcd(m, i)$ is a proper divisor of m. □

Lemma 2.12. *Let $a, r, \ell, k \in \mathbb{N}$ be such that $1 \le \ell < k$, and r is a prime not dividing a. Then $\operatorname{ord}\big(a; r^k\big) = \operatorname{ord}\big(a; r^{k-\ell}\big) r^{\ell'}$ for some non-negative integer $\ell' \le \ell$. In particular, $\operatorname{ord}\big(a; r^k\big)$ divides $\operatorname{ord}\big(a; r^{k-\ell}\big) r^{\ell}$.*

Proof. We only prove the case $\ell = 1$, that is we verify that

$$\operatorname{ord}\big(a; r^k\big) = \operatorname{ord}\big(a; r^{k-1}\big) r^j, \quad \text{for some } j \in \{0, 1\},$$

as the assertion then follows by repeatedly applying this special case. Let $m = \operatorname{ord}\big(a; r^{k-1}\big)$. By Lemma 2.9($b$) we have $m \mid \operatorname{ord}\big(a; r^k\big)$. Hence, it suffices to show that $\operatorname{ord}\big(a; r^k\big) \mid mr$. By the definition of m we have $r^{k-1} \mid a^m - 1$, and in particular, $a^m \equiv 1 \pmod{r}$. Then

$$\underbrace{a^{m(r-1)} + a^{m(r-2)} + \cdots + a^m + 1}_{r \text{ summands}} \equiv 0 \pmod{r}.$$

That is, r divides $a^{m(r-1)}+\cdots+a^m+1=(a^{mr}-1)/(a^m-1)$. Thus, $r(a^m-1)\mid a^{mr}-1$. Then, recalling that $r^{k-1}\mid a^m-1$, we see that $r^k\mid a^{mr}-1$. Using Lemma 2.9(a) we conclude that $\operatorname{ord}\bigl(a;r^k\bigr)\mid mr$. □

Lemma 2.13. *Let $a,r,k\in\mathbb{N}$ be such that $\gcd(a,r)=1$. Then*

$$\operatorname{ord}\bigl(a^k;r\bigr)\;\Bigm|\;\frac{\lambda(r)}{\gcd\bigl(\lambda(r),k\bigr)}\;\Bigm|\;\frac{\varphi(r)}{\gcd\bigl(\varphi(r),k\bigr)}.$$

In particular, $\operatorname{ord}(a;r)\mid\lambda(r)\mid\varphi(r)$.

Proof. By Lemma 2.9(c) we have $\operatorname{ord}\bigl(a^k;r\bigr)=\operatorname{ord}(a;r)/\gcd(\operatorname{ord}(a;r),k)$, that is

$$\operatorname{ord}\bigl(a^k;r\bigr)=\frac{\operatorname{lcm}\bigl\{\operatorname{ord}(a;r),k\bigr\}}{k}.$$

Since (by definition) $\operatorname{ord}(a;r)$ divides $\lambda(r)$, recalling from Section 2.1 that $\lambda(r)$ is a divisor of $\varphi(r)$, it follows that

$$\operatorname{ord}\bigl(a^k;r\bigr)\;\Bigm|\;\frac{\operatorname{lcm}\bigl\{\lambda(r),k\bigr\}}{k}\;\Bigm|\;\frac{\operatorname{lcm}\bigl\{\varphi(r),k\bigr\}}{k},$$

that is $\operatorname{ord}\bigl(a^k;r\bigr)\mid\lambda(r)/\gcd(\lambda(r),k)\mid\varphi(r)/\gcd(\varphi(r),k)$, as asserted. □

Lemma 2.14. *Let $a,r,k\in\mathbb{N}$ be such that r is a prime not dividing a.*

(a) *If $r=2$, then $\operatorname{ord}(a;r)=1$, $\operatorname{ord}(a;r^2)\mid 2$, and $\operatorname{ord}\bigl(a;r^k\bigr)\mid r^{k-2}$ for $k\geq 3$.*

(b) *If r is odd, then $\operatorname{ord}\bigl(a;r^k\bigr)\mid(r-1)r^{k-1}$.*

Proof. The assertion holds by Lemma 2.4 and (the "in particular" part of) Lemma 2.13. □

Lemma 2.15. *Let $a,r,s\in\mathbb{N}$ be such that $\gcd(a,rs)=\gcd(r,s)=1$. Then $\operatorname{ord}(a;rs)=\operatorname{lcm}\{\operatorname{ord}(a;r),\operatorname{ord}(a;s)\}$.*

Proof. By the Chinese Remainder Theorem, $\mathbb{Z}/rs\mathbb{Z}$ and $\mathbb{Z}/r\mathbb{Z}\times\mathbb{Z}/s\mathbb{Z}$ are isomorphic via the ring isomorphism $b+rs\mathbb{Z}\mapsto(b+r\mathbb{Z},b+s\mathbb{Z})$. Then

$$(\mathbb{Z}/rs\mathbb{Z})^*\cong(\mathbb{Z}/r\mathbb{Z})^*\times(\mathbb{Z}/s\mathbb{Z})^*.$$

Being an element of a direct product, $(a+r\mathbb{Z},a+s\mathbb{Z})$ has order equal to the least common multiple of the orders of $a+r\mathbb{Z}\in(\mathbb{Z}/r\mathbb{Z})^*$ and $a+s\mathbb{Z}\in(\mathbb{Z}/s\mathbb{Z})^*$. This proves the assertion. □

Definition 2.16. Let $r \in \mathbb{N}$, let s be a prime, and let k be the non-negative integer such that $s^k \mid r$ and $s^{k+1} \nmid r$. We write $(r)_s = s^k$ and $(r)_{s'} = r/s^k$, and refer to $(r)_s$ and $(r)_{s'}$ as the *s-part* of r and, respectively, the *s'-part* of r.

Note that, if a prime s does not divide a positive integer r, then $(r)_s = 1$.

Lemma 2.17. *Let a, r, t be positive integers such that $\gcd(a, rt) = 1$. Then $\operatorname{ord}(a; rt) \leq \operatorname{ord}(a; r)t$.*

Proof. Let t' be the largest divisor of t which is coprime to r. We then have $\gcd(rt/t', t') = 1$. Thus, by Lemma 2.15, $\operatorname{ord}(a; rt)$ equals the least common multiple of, and thus divides the product of, $\operatorname{ord}(a; rt/t')$ and $\operatorname{ord}(a; t')$. Using $\operatorname{ord}(a; t') \leq t'$ we obtain

$$\operatorname{ord}(a; rt) \leq \operatorname{ord}\left(a; \frac{rt}{t'}\right) t'.$$

We prove the assertion by showing that $\operatorname{ord}(a; rt/t') \leq \operatorname{ord}(a; r)t/t'$. To this end, let $s_1, \ldots, s_\ell$ be the distinct prime divisors of r. Recall (from the definition of t') that each prime factor of t/t' divides r. Hence, $s_1, \ldots, s_\ell$ are also (all of) the distinct prime divisors of rt/t'. Applying Lemma 2.15 we obtain

$$\operatorname{ord}\left(a; \frac{rt}{t'}\right) = \operatorname{lcm}\left\{\operatorname{ord}\left(a; \left(\frac{rt}{t'}\right)_{s_1}\right), \ldots, \operatorname{ord}\left(a; \left(\frac{rt}{t'}\right)_{s_\ell}\right)\right\}. \tag{2.2}$$

By (the "in particular" part of) Lemma 2.12 we see that for $i \in \{1, \ldots, \ell\}$,

$$\operatorname{ord}\left(a; \left(\frac{rt}{t'}\right)_{s_i}\right) \quad \text{divides} \quad \operatorname{ord}(a; (r)_{s_i})\left(\frac{t}{t'}\right)_{s_i}.$$

Thus, by (2.2), $\operatorname{ord}(a; rt/t')$ is a divisor of the least common multiple of the $\operatorname{ord}(a; (r)_{s_i})(t/t')_{s_i}$, $i \in \{1, \ldots, \ell\}$. Hence,

$$\operatorname{ord}\left(a; \frac{rt}{t'}\right) \mid \underbrace{\operatorname{lcm}\{\operatorname{ord}(a; (r)_{s_1}), \ldots, \operatorname{ord}(a; (r)_{s_\ell})\}}_{=\operatorname{ord}(a;r)} \frac{t}{t'}.$$

Recalling from Lemma 2.15 that $\operatorname{lcm}\{\operatorname{ord}(a; (r)_{s_1}), \ldots, \operatorname{ord}(a; (r)_{s_\ell})\} = \operatorname{ord}(q; r)$, it follows that $\operatorname{ord}(a; rt/t')$ divides, and thus is less than or equal to, $\operatorname{ord}(a; r)t/t'$. □

2.2.2 The case $\operatorname{ord}(a; rt) > \operatorname{ord}(a; r)t/2$

If a, r, t are positive integers such that a and rt are coprime then, as we may recall from Lemma 2.17, $\operatorname{ord}(a; rt)$ is less than or equal to $\operatorname{ord}(a; r)t$. We are particularly interested in the situation where $\operatorname{ord}(a; rt) > \operatorname{ord}(a; r)t/2$. Observe that, if $a = 1$, then $\operatorname{ord}(1; rt) > \operatorname{ord}(1; r)t/2$ precisely when $t = 1$.

Lemma 2.18. *Let $a, r, t \in \mathbb{N}$ be such that $a \geq 2$ and $\gcd(a, rt) = 1$. Let $m = \operatorname{ord}(a; r)$, and let $\operatorname{ord}(a; rt) > mt/2$. Then the following hold.*

(*a*) *We have $\gcd(t, (a^m - 1)/r) = 1$.*

(*b*) *We have $\gcd(4, t) \mid r$.*

(*c*) *If t contains a prime divisor s which does not divide r, then s is uniquely determined, s is odd, and $\operatorname{ord}(a; s) = s - 1$.*

Proof. For a prime s, recall (from Definition 2.16) the notions of the s-part and s'-part of a positive integer.

(*a*) Suppose that there exists a prime divisor s of t which divides $(a^m - 1)/r$. Then $rs \mid a^m - 1$. Hence, by Lemma 2.9(*a*) we get $\operatorname{ord}(a; rs) \mid m$. Recalling that $\operatorname{ord}(a; r) = m$, Lemma 2.9(*b*) reveals that $m \mid \operatorname{ord}(a; rs)$. Thus,

$$\operatorname{ord}(a; rs) = m.$$

Then Lemma 2.17 yields the contradiction $\operatorname{ord}(a; rt) \leq \operatorname{ord}(a; rs)t/s \leq mt/2$.

(*b*) Seeking a contradiction, suppose that $\gcd(4, t) \nmid r$. By Lemma 2.17 we have

$$\operatorname{ord}(a; rt) \leq \operatorname{ord}(a; r(t)_2)\,(t)_{2'},$$

which applying Lemma 2.15 (and using the fact that $r/\gcd(2, r)$ is odd) is equivalent to

$$\operatorname{ord}(a; rt) \leq \operatorname{lcm}\left\{\underbrace{\operatorname{ord}\left(a; \frac{r}{\gcd(2, r)}\right)}_{=:x}, \underbrace{\operatorname{ord}(a; \gcd(2, r)(t)_2)}_{=:y}\right\}(t)_{2'}. \tag{2.3}$$

Because $\gcd(4, t)$ does not divide r, we get $2 \mid \gcd(2, r)(t)_2$ if $\gcd(2, r) = 1$, and $8 \mid \gcd(2, r)(t)_2$ if $\gcd(2, r) = 2$. Using Lemma 2.14(*a*), it follows that

$$y \mid \frac{(t)_2}{2}. \tag{2.4}$$

Now, by Lemma 2.9(*b*), x is a divisor of $m = \operatorname{ord}(a; r)$. Combining this fact with (2.3) and (2.4) yields

$$\operatorname{ord}(a; rt) \leq \operatorname{lcm}\left\{m, \frac{(t)_2}{2}\right\}(t)_{2'}.$$

Thus, $\operatorname{ord}(a; rt) \leq mt/2$, which is not true.

(c) Suppose that t contains two prime divisors s, ℓ which do not divide r. By part (b) of the current lemma we have

$$2 \nmid s\ell.$$

Seeking a contradiction, assume that $s \neq \ell$. Then by Lemma 2.17 we get

$$\operatorname{ord}(a; rt) \leq \operatorname{ord}(a; r(t)_s(t)_\ell)\frac{t}{(t)_s(t)_\ell},$$

which according to Lemma 2.15 is equivalent to writing

$$\operatorname{ord}(a; rt) \leq \operatorname{lcm}\Big\{\underbrace{\operatorname{ord}(a; r)}_{=m}, \operatorname{ord}(a; (t)_s), \operatorname{ord}(a; (t)_\ell)\Big\}\frac{t}{(t)_s(t)_\ell}. \tag{2.5}$$

Now, by Lemma 2.14(b), $\operatorname{ord}(a; (t)_s)$ divides $(s-1)(t)_s/s$ and $\operatorname{ord}(a; (t)_\ell)$ is a divisor of $(\ell-1)(t)_\ell/\ell$. Hence, (2.5) yields

$$\operatorname{ord}(a; rt) \leq \operatorname{lcm}\left\{m, (s-1)\frac{(t)_s}{s}, (\ell-1)\frac{(t)_\ell}{\ell}\right\}\frac{t}{(t)_s(t)_\ell},$$

and thus

$$\operatorname{ord}(a; rt) \leq \operatorname{lcm}\{s-1, \ell-1\}\frac{mt}{s\ell}. \tag{2.6}$$

Recalling that $s-1$ and $\ell-1$ are even, we have $\operatorname{lcm}\{s-1, \ell-1\} < s\ell/2$. Then $\operatorname{ord}(a; rt) < mt/2$ by (2.6). As this is not true, we conclude that $s = \ell$.

It remains to show that $\operatorname{ord}(a; s) = s-1$. By (the "in particular" part of) Lemma 2.13, $\operatorname{ord}(a; s)$ divides $\varphi(s) = s-1$. Seeking a contradiction suppose that $\operatorname{ord}(a; s) \neq s-1$. Then

$$\operatorname{ord}(a; s) \leq \frac{s-1}{2}.$$

Since by Lemma 2.17 we have $\operatorname{ord}(a; (t)_s) \leq \operatorname{ord}(a; s)(t)_s/s$, it follows that $\operatorname{ord}(a; (t)_s) \leq (s-1)(t)_s/(2s)$, whence

$$\operatorname{ord}(a; (t)_s) < \frac{(t)_s}{2}. \tag{2.7}$$

Now, by Lemma 2.15, $\operatorname{ord}(a; rt)$ is equal to the least common multiple of, and thus is less or equal to the product of, $\operatorname{ord}(a; r(t)_{s'})$ and $\operatorname{ord}(a; (t)_s)$. Thus, using Lemma 2.17 (by which $\operatorname{ord}(a; r(t)_{s'}) \leq m(t)_{s'}$), we get

$$\operatorname{ord}(a; rt) \leq m(t)_{s'}\operatorname{ord}(a; (t)_s),$$

which combined with (2.7) yields $\operatorname{ord}(a; rt) < m(t)_{s'}(t)_s/2 = mt/2$. Contradiction. □

We next classify all triples $(a, r, t) \in \mathbb{N}^3$ satisfying $a \geq 2$, $\gcd(a, rt) = 1$ and $\operatorname{ord}(a; rt) = \operatorname{ord}(a; r)t$. The implication "$(b) \Rightarrow (a)$" is essentially proved in [42, Theorem 3.34].

Proposition 2.19. *Let $a, r, t \in \mathbb{N}$ be such that $a \geq 2$ and $\gcd(a, r) = 1$. Let $m = \operatorname{ord}(a; r)$. The following are equivalent.*

(a) We have $\gcd(a, rt) = 1$ and $\operatorname{ord}(a; rt) = mt$.

(b) Every prime divisor of t divides r but not $(a^m - 1)/r$, and $\gcd(4, t) \mid r$.

Proof. If $t = 1$, then there is nothing to show. (In this case condition (a) simplifies to $\gcd(a, r) = 1$, $\operatorname{ord}(a; r) = m$, and both equations hold by assumption, while condition (b) is trivially true.) If $r = 1$, then $m = 1$ and condition (a) simplifies to $\gcd(a, t) = 1$, $\operatorname{ord}(a; t) = t$, which is true if and only if $t = 1$, as asserted. We may thus assume that

$$r, t \geq 2.$$

First, suppose that condition (b) holds. Because each prime divisor of t divides r, recalling that $\gcd(a, r) = 1$, we see that $\gcd(a, rt) = 1$. Further, by [42, Theorem 3.34] we have $\operatorname{ord}(a; rt) = mt$. (In order to see that we may indeed apply [42, Theorem 3.34], observe that $4 \mid t$ implies $4 \mid r \mid a^m - 1$. Hence, $t \equiv 0 \pmod 4$ implies that $a^m \equiv 1 \pmod 4$.)

Conversely, suppose that condition (a) holds. From Lemma 2.18$(a)(b)$ we know that

$$\gcd\left(t, \frac{a^m - 1}{r}\right) = 1 \quad \text{and} \quad \gcd(4, t) \mid r.$$

It remains to show that every prime divisor of t divides r. Seeking a contradiction, assume that a prime s divides t and $s \nmid r$. (By Lemma 2.18(c) the prime s is uniquely determined, but we do not use this fact here.) By Lemma 2.15 we have $\operatorname{ord}(a; rt) = \operatorname{lcm}\big\{\operatorname{ord}(a; r(t)_{s'}), \operatorname{ord}(a; (t)_s)\big\}$, whence

$$\operatorname{ord}(a; rt) \leq \operatorname{ord}(a; r(t)_{s'}) \operatorname{ord}(a; (t)_s). \tag{2.8}$$

Note that by Lemma 2.17 we have

$$\operatorname{ord}(a; r(t)_{s'}) \leq \operatorname{ord}(a; r)\,(t)_{s'}. \tag{2.9}$$

Since $(t)_s > 1$, according to Lemma 2.14(b) the order of a modulo $(t)_s$ divides $(s - 1)(t)_s/s$, and thus $\operatorname{ord}(a; (t)_s) < (t)_s$. Combining the latter with (2.8) and (2.9) yields the contradiction $\operatorname{ord}(a; rt) < \operatorname{ord}(a; r)t$. □

Example 2.20. We calculate examples of triples $(a, m, t) \in \mathbb{N}^3$ satisfying the following condition.

$$\gcd(a, t) = 1, \quad \operatorname{ord}(a; (a^m - 1)t) = mt \tag{2.10}$$

(a) Suppose that $m = 10$, $t = 100$, and $a \geq 2$. By Proposition 2.19 (applied to $r = a^{10} - 1$), condition (2.10) holds if and only if $a^{10} - 1$ is divisible by 2, 5, and $\gcd(4, 100) = 4$. That is,

$$(2.10) \text{ holds} \quad \Leftrightarrow \quad 20 \mid a^{10} - 1.$$

By Euler's totient theorem we have $20 \mid a^{\varphi(20)} - 1 = a^8 - 1$. Hence, by Lemma 2.10, $20 \mid a^{10}-1$ if and only if 20 divides $a^{\gcd(8,10)}-1 = (a+1)(a-1)$. We conclude that

$$(2.10) \text{ holds} \quad \Leftrightarrow \quad a \equiv \pm 1 \pmod{10}.$$

(b) Suppose that $t = 2$ and $a \geq 2$. By Proposition 2.19 (applied to $r = a^m - 1$), condition (2.10) is satisfied if and only if $2 \mid a^m - 1$, that is if and only if a is odd.

Lemma 2.21. *Let $a, m, t \in \mathbb{N}$ be such that $a \geq 2$, t is a prime not dividing a, and $mt/2 \leq \operatorname{ord}(a; (a^m - 1)t) \leq mt$. Then $\operatorname{ord}(a; (a^m - 1)t) \in \{mt, m(t-1)\}$.*

Proof. If $t \mid a^m - 1$, then by Proposition 2.19 (applied to $r = a^m - 1$) we get $\operatorname{ord}(a; (a^m - 1)t) = mt$. So, suppose that $t \nmid a^m - 1$. Then Lemma 2.15 yields

$$\operatorname{ord}(a; (a^m - 1)t) = \operatorname{lcm}\big\{\operatorname{ord}(a; a^m - 1), \operatorname{ord}(a; t)\big\}.$$

Since $\operatorname{ord}(a; a^m - 1) = m$, since by (the "in particular" part of) Lemma 2.13 we get $\operatorname{ord}(a; t) \mid \varphi(t) = t-1$, and since (according to our assumption) we have $\operatorname{ord}(a; (a^m - 1)t) \geq mt/2$, we conclude that $\operatorname{ord}(a; (a^m - 1)t) = m(t-1)$. □

For a prime s, recall (from Definition 2.16) the notions of the s-part and the s'-part of a positive integer. Recall further from Lemma 2.9(b) that, given $a, r, t \in \mathbb{N}$ such that a and rt are coprime, we have $\operatorname{ord}(a; r) \mid \operatorname{ord}(a; rt)$.

Lemma 2.22. *Let $a, r, t \in \mathbb{N}$ be such that $a \geq 2$ and $\gcd(a, rt) = 1$. Let $m = \operatorname{ord}(a; r)$ and suppose that $mt/2 < \operatorname{ord}(a; rt) < mt$. Let*

$$s = \frac{t}{\gcd\big(\frac{\operatorname{ord}(a;rt)}{m}, t\big)}.$$

Then s is an odd prime divisor of t, $s \nmid a^m - 1$, and $\operatorname{ord}(a; r(t)_{s'}) = m(t)_{s'}$.

Proof. Let $e = \mathrm{ord}(a; rt)$. Since $e > mt/2$, from Lemma 2.18$(a)(b)$ we know that

$$\gcd\Big(t, \frac{a^m - 1}{r}\Big) = 1, \quad \gcd(4, t) \mid r.$$

If all prime divisors of t divide r, then Proposition 2.19 yields the contradiction $e = mt$. Hence, there exists a prime divisor ℓ of t not dividing r. By Lemma 2.18(c), ℓ is the unique prime divisor of t which does not divide r. Recalling that $\gcd\big(t, (a^m - 1)/r\big) = 1$, it follows that

$$\ell \nmid a^m - 1 \tag{2.11}$$

and that

$$\text{every prime divisor of } (t)_{\ell'} \text{ divides } r \text{ but not } \frac{a^m - 1}{r}. \tag{2.12}$$

Further, by Lemma 2.18(c),

$$\ell \neq 2. \tag{2.13}$$

Now, since $\gcd(4, t)$ is a divisor of r (whence $\gcd(4, (t)_{\ell'})$ divides r), recalling that (2.12) holds, Proposition 2.19 yields

$$\mathrm{ord}(a; r(t)_{\ell'}) = m(t)_{\ell'}. \tag{2.14}$$

By Lemma 2.14(b) we have

$$\mathrm{ord}(a; (t)_\ell) \mid \frac{(\ell - 1)(t)_\ell}{\ell}. \tag{2.15}$$

Combining (2.14), (2.15) with Lemma 2.15 (according to which e is equal to the least common multiple, and thus divides the product, of $\mathrm{ord}(a; r(t)_{\ell'})$ and $\mathrm{ord}(a; (t)_\ell)$), reveals that $e \mid mt(\ell - 1)/\ell$. Since (by assumption) the integer e is strictly bigger than $mt/2$, it follows that $e = mt(\ell - 1)/\ell$. Then

$$s = \frac{t}{\gcd\big(\frac{t(\ell-1)}{\ell}, t\big)} = \frac{t}{\frac{t}{\ell}\underbrace{\gcd(\ell - 1, \ell)}_{=1}} = \ell,$$

and the assertion holds by (2.11), (2.13), and (2.14). □

2.3 Primitive divisors of $a^m - 1$

Consider positive integers a, r, m, where a and r are coprime. Recall from Lemma 2.11 that $\mathrm{ord}(a; r)$ is equal to m if and only if r divides $a^m - 1$ and r does not divide $a^i - 1$ for any positive integer $i < m$. This equivalence motivates the following name for r.

Definition 2.23. Let $a, r, m \in \mathbb{N}$. We call r a *primitive divisor* of $a^m - 1$ if $\gcd(a, r) = 1$ and $m = \operatorname{ord}(a; r)$.

If, in addition, r is a prime, then r is called a *primitive prime divisor* of $a^m - 1$. And if r is a (not necessarily proper) power of a prime, then r is referred to as a *primitive prime power divisor* of $a^m - 1$.

A word of caution needs to be added to the definition above. In the literature, the term *primitive divisor of* $a^m - 1$ has different meanings. Some authors (see for example [5, 8]) define a primitive divisor of $a^m - 1$ to be a divisor of $a^m - 1$ which is coprime to $a^i - 1$ for all $i < m$. Others (see [15]) reserve this term for primes only (that is define primitive divisors to be "our" primitive prime divisors). Still others (see [27]) distinguish between *strong primitive divisors* of $a^m - 1$ (these are the divisors of $a^m - 1$ which are coprime to each $a^i - 1$, $i < m$) and *weak primitive divisors* (these are "our" primitive divisors).

We next specify conditions on positive integers a, m under which primitive divisors, primitive prime divisors, and respectively, primitive prime power divisors of $a^m - 1$ exist. If $a = 1$, then primitive divisors of $a^m - 1 = 0$ exist if and only if $m = 1$. In such a case any positive integer r is a primitive divisor of $a^m - 1$. If $(a, m) = (2, 1)$, then there are no primitive prime power divisors of $a^m - 1 = 1$ (as there are no prime powers dividing 1). However, in this case, 1 is a primitive divisor of $a^m - 1$. Next, suppose that $a, m \geq 2$. According to [49, p. 34], in 1886, Bang [6] proved that there exists a primitive prime divisor of $a^m - 1$ unless $(a, m) = (2, 6)$ or $m = 2$ and $a + 1$ is a power of 2.[(I)] In order to demonstrate that (for $a, m \geq 2$) there always exist primitive prime power divisors of $a^m - 1$, we verify the existence of such divisors in cases where $a^m - 1$ has no primitive prime divisors. That is, we check that, if $(a, m) = (2, 6)$ or if $m = 2$ and a is of the form $2^k - 1$ for some $k \geq 2$, then there exists a prime power r satisfying $m = \operatorname{ord}(a; r)$. Indeed, $6 = \operatorname{ord}(2; 9)$ and $2 = \operatorname{ord}\big(2^k - 1; 2^{k+1}\big)$. In summary we obtain the following.

Lemma 2.24. *Let a, m be positive integers.*

(a) *Primitive divisors of $a^m - 1$ exist unless $a = 1$ and $m \neq 1$.*

(b) *Primitive prime power divisors of $a^m - 1$ exist unless $a = 1$ and $m \neq 1$, or $(a, m) = (2, 1)$.*

(c) (Bang [6]) *Primitive prime divisors of $a^m - 1$ exist unless $a = 1$ and $m \neq 1$, or $(a, m) \in \{(2, 1), (2, 6), (2^k - 1, 2)\}$, $k \geq 2$.*

[(I)] In the literature the existence of primitive prime divisors of $a^m - 1$ is usually traced back to Zsigmondy [55, p. 283] who, in 1892, proved a generalised version of Bang's theorem. Often, primitive prime divisors are misleadingly referred to as *Zsigmondy primes* (see for example [23, 50]).

Primitive divisors of a^m-1 might or might not have a proper divisor which itself is a primitive divisor of a^m-1. In order to distinguish between these two types we introduce the term *minimal primitive divisor*.

Definition 2.25. Let $a, m \in \mathbb{N}$. We call a primitive divisor r of a^m-1 *minimal*, if for all proper divisors r' of r, r' is not a primitive divisor of a^m-1.

By Definition 2.23 and Lemma 2.9(b), r is a minimal primitive divisor of a^m-1 if and only if $\mathrm{ord}(a;r)=m$ and, for all proper divisors r' of r, $\mathrm{ord}(a;r')$ properly divides $\mathrm{ord}(a;r)$. Let us consider some examples of minimal and non-minimal primitive divisors.

Example 2.26. Recall from Lemma 2.15 that, for positive integers a, r, s satisfying $\gcd(a, rs)=\gcd(r,s)=1$, we get $\mathrm{ord}(a;rs)=\mathrm{lcm}\{\mathrm{ord}(a;r),\mathrm{ord}(a;s)\}$.

(a) Now, $\mathrm{ord}(2;3)=2$ and $\mathrm{ord}(2;7)=3$, whence $\mathrm{ord}(2;21)=\mathrm{lcm}\{2,3\}=6$. Since 3 and 7 are the only proper and non-trivial divisors of 21, it follows that 21 is a minimal primitive divisor of 2^6-1.

Similarly, since $\mathrm{ord}(2;9)=6$, and since 3 is the only proper and non-trivial divisor of 9, (recalling that $\mathrm{ord}(2;3)=2$) we see that 9 is a minimal primitive divisor of 2^6-1.

(b) Consider the integer $116=4\times 29$. We have $\mathrm{ord}(23;4)=2$ and $\mathrm{ord}(23;29)=7$, whence $\mathrm{ord}(23;116)=\mathrm{lcm}\{2,7\}=14$. Besides 4 and 29 the integer 116 has two other proper, non-trivial divisors, namely 2 and 58. Since $\mathrm{ord}(23;2)=1$ and $\mathrm{ord}(23;58)=7$ it follows that 116 is a minimal primitive divisor of $23^{14}-1$.

We have $\mathrm{ord}(5;4)=1$ and $\mathrm{ord}(5;29)=14$. Hence, $\mathrm{ord}(5;116)=\mathrm{lcm}\{1,14\}=14$, and 116 is a primitive divisor of $5^{14}-1$ but as such it is not minimal.

Note that minimal primitive divisors are not uniquely determined as, by Example 2.26(a) both 21 and 9 are minimal primitive divisors of 2^6-1.

Lemma 2.27. *Let $a, m, r, r' \in \mathbb{N}$ be such that $m\geq 2$, r is a minimal primitive divisor of a^m-1, $r'\geq 2$, $r' \mid r$, and $\gcd(r', r/r')=1$. Then*

$$\mathrm{ord}(a;r') \nmid \mathrm{ord}\Big(a;\frac{r}{r'}\Big).$$

Proof. If $\mathrm{ord}(a;r')$ divides $\mathrm{ord}(a;r/r')$, then according to Lemma 2.15 we obtain $\mathrm{ord}(a;r)=\mathrm{lcm}\{\mathrm{ord}(a;r'),\mathrm{ord}(a;r/r')\}=\mathrm{ord}(a;r/r')$, which contradicts the minimality of r as a primitive divisor of a^m-1. □

Lemma 2.28. *Let $a, m, r \in \mathbb{N}$ be such that $m \geq 2$ and r is a minimal primitive divisor of $a^m - 1$. Then the following hold.*

(*a*) *If r is even, then $4 \mid r$.*

(*b*) *We have $r \notin \{12, 15, 20, 24, 40, 48, 51, 60, 68, 80, 85, 96\}$.*

(*c*) *If a is a square, then $\gcd(r, 16) \in \{1, 16\}$ and $\gcd(r, 9) \in \{1, 9\}$.*

Proof. (*a*) Suppose that r is even (whence a is odd). Seeking a contradiction assume that $4 \nmid r$. Let $r' = 2$. (Then $r' \geq 2$, $r' \mid r$ and $\gcd(r', r/r') = 1$.) Now, $\operatorname{ord}(a; r')$ is equal to 1, and hence $\operatorname{ord}(a; r')$ divides $\operatorname{ord}(a; r/r')$. Using Lemma 2.27 it follows that r is not a minimal primitive divisor of $a^m - 1$, which is not true.

(*b*) Seeking a contradiction, suppose that $r \in \{12, 15, 20, 24, 40, 48, 51, 60, 68, 80, 85, 96\}$. Observe that we can write r as a product $r = r_1 r_2$ where r_1, r_2 are coprime integers contained in the set $\{3, 4, 5, 8, 16, 17, 20, 32\}$. Using Lemma 2.4, we see that $\lambda(r_1)$ and $\lambda(r_2)$ are powers of 2. More precisely, we have

$$\lambda(r_i) = \begin{cases} 2, & \text{if } r_i \in \{3, 4, 8\}, \\ 4, & \text{if } r_i \in \{5, 16, 20\}, \\ 8, & \text{if } r_i = 32, \\ 16, & \text{if } r_i = 17. \end{cases}$$

Then according to (the "in particular" part of) Lemma 2.13, $\operatorname{ord}(a; r_1)$ and $\operatorname{ord}(a; r_2)$ are also powers of 2. In particular, either $\operatorname{ord}(a; r_1)$ divides $\operatorname{ord}(a; r_2)$ or vice versa. Then Lemma 2.27 (applied to $r' = r_1$ if $\operatorname{ord}(a; r_1) \mid \operatorname{ord}(a; r_2)$, and to r_2 else) implies that r is not a minimal primitive divisor of $a^m - 1$.

(*c*) Assume that a is a square, say $a = a_0^2$. Recall from Definition 2.16 the meaning of $(r)_2$ and $(r)_3$. Seeking a contradiction, we assume that $\gcd(r, 16) \notin \{1, 16\}$ or $\gcd(r, 9) \notin \{1, 9\}$. Then, using part (*a*) of the current lemma, we get

$$(r)_2 \in \{4, 8\} \quad \text{or} \quad (r)_3 = 3.$$

Let $r' = (r)_2$ if $(r)_2 \in \{4, 8\}$, and $r' = (r)_3$ else. According to Lemma 2.4 we have $\lambda(r') = 2$. Hence, by Lemma 2.13 we get $1 = \operatorname{ord}(a_0^2; r') = \operatorname{ord}(a; r')$. Then $\operatorname{ord}(a; r')$ divides $\operatorname{ord}(a; r/r')$ whence by Lemma 2.27, r is not a minimal primitive divisor. This proves the assertion. □

Chapter 3

Number of irreducible polynomials with certain properties

In this chapter we consider certain sets of irreducible polynomials defined over a finite field $\mathbb{F}$ and determine their quantities.

In Section 3.1 we collect some basic properties of irreducible polynomials over $\mathbb{F}$. Section 3.2 deals with monic, irreducible polynomials over $\mathbb{F}$ which have the same non-zero constant term. In Section 3.3, we count all monic irreducible polynomials $f \neq x$ of some specified degree $m \in \mathbb{N}$ over $\mathbb{F}$ such that, given $t \in \mathbb{N}$ and an integer e satisfying $e > mt/2$, the polynomial $f(x^t)$ contains an irreducible factor of degree e. (Section 3.3 contains Theorems 3.18, 3.23, and 3.24.) Section 3.4 is concerned with irreducible tensor products of monic polynomials. Finally, in Section 3.5 we consider the number of all monic irreducible polynomials $f \neq x$ defined over a finite extension field $\mathbb{E}$ of $\mathbb{F}$ such that, writing f^σ for the polynomial obtained from f by applying a field automorphism $\sigma \in \mathrm{Gal}(\mathbb{E} : \mathbb{F})$ to every coefficient of f, the polynomial $\prod_{\sigma \in \mathrm{Gal}(\mathbb{E}:\mathbb{F})} f^\sigma$ is irreducible over $\mathbb{F}$.

Notation. Throughout this chapter let q be a power of a prime p.

3.1 Irreducible polynomials

The ring $\mathbb{Z}/p\mathbb{Z}$ forms a field with p elements, which we also denote by $\mathbb{F}_p$. Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. (The field $\overline{\mathbb{F}_p}$ is unique up to isomorphism.) Then, by writing $\mathbb{F}_q$, we mean the unique subfield of $\overline{\mathbb{F}_q}$ containing q elements. The set of all non-zero elements in $\mathbb{F}_q$ forms a cyclic group under multiplication,

and we denote this group by $\mathbb{F}_q^*$. The ring of all polynomials with coefficients in $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[x]$. We assume that the zero polynomial has degree $-\infty$.

Definition 3.1. A polynomial $f \in \mathbb{F}_q[x]$ is called *irreducible* if f has positive degree and any decomposition $f = f_1 f_2$ with $f_1, f_2 \in \mathbb{F}_q[x]$ implies that either f_1 or f_2 has degree 0. Otherwise, f is said to be *reducible*.

Consider a polynomial $f \in \mathbb{F}_q[x]$ of positive degree. Given an extension field $\mathbb{E}$ of $\mathbb{F}_q$, we may naturally view f as a polynomial over $\mathbb{E}$. By saying that f is irreducible/reducible *over* $\mathbb{E}$ we mean that f has this property as an element of $\mathbb{E}[x]$. The *order* of a non-zero element $\omega \in \mathbb{E}$ (written as $|\omega|$) refers to the order of ω in the cyclic group $\mathbb{E}^*$. A *root* of f is an element ω in some (possibly non-proper) extension field of $\mathbb{F}_q$ satisfying $f(\omega) = 0$. The *splitting field* of f is the smallest (with respect to inclusion) extension field of $\mathbb{F}_q$ which contains all roots of f.

Our first lemma summarises some (well-known) properties of roots of an irreducible polynomial.

Lemma 3.2. *Let $m \in \mathbb{N}$, and let $f \in \mathbb{F}_q[x]$ be irreducible of degree m.*

(a) *The polynomial f has m distinct roots.*

(b) *If ω is a root of f, then $\omega, \omega^q, \omega^{q^2}, \ldots, \omega^{q^{m-1}}$ are all the roots of f.*

(c) *The splitting field of f over $\mathbb{F}_q$ is given by $\mathbb{F}_{q^m}$.*

(d) *If $f \neq x$, then all roots of f lie in $\mathbb{F}_{q^m}^*$ and have the same order.*

(e) *If $e \in \mathbb{F}_q[x]$ is irreducible and some root of e is a root of f, then $e = \alpha f$ for some $\alpha \in \mathbb{F}_q^*$.*

Proof. Parts (a) and (b) hold by [42, Theorem 2.14]. Part (c) restates [42, Corollary 2.15].

In order to verify part (d), assume that $f \neq x$. Then f contains a non-zero root ω, which by part (c) lies in $\mathbb{F}_{q^m}^*$. By part (b), the roots of f are given by $\omega, \omega^q, \omega^{q^2}, \ldots, \omega^{q^{m-1}}$. Hence, all roots are elements of $\mathbb{F}_{q^m}^*$. Recall that $|\omega^{q^i}|$ denotes the multiplicative order of ω^{q^i} in $\mathbb{F}_{q^m}^*$. Since $|\omega|$ and q are coprime, we get $|\omega^{q^i}| = |\omega| \gcd(|\omega|, q^i)^{-1} = |\omega|$ for all $i \in \{1, \ldots, m-1\}$.

Finally, let $e \in \mathbb{F}_q[x]$ be irreducible such that e and f have a common root, say ω. Let g be the minimal polynomial of ω over $\mathbb{F}_q$. By [42, Theorem 3.33(ii)], g divides f and e, which (recalling that f, e are irreducible) reveals that $g = \alpha f = \beta e$ for some $\alpha, \beta \in \mathbb{F}_q^*$. Then $e = \alpha\beta^{-1} f$. □

Recall from Definition 2.7 the notion of $\mathrm{ord}(a; r)$, where $a, r \in \mathbb{N}$ are coprime.

Lemma 3.3. *Let $m \in \mathbb{N}$. An element $\omega \in \mathbb{F}_{q^m}^*$ does not lie in any proper subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$ if and only if* $\operatorname{ord}(q; |\omega|) = m$.

Proof. Let $\omega \in \mathbb{F}_{q^m}^*$. Then $|\omega|$ divides $|\mathbb{F}_{q^m}^*| = q^m - 1$. The subfields of $\mathbb{F}_{q^m}$ which contain $\mathbb{F}_q$ are precisely the fields $\mathbb{F}_{q^n}$ for all divisors n of m (see [42, Theorem 2.6]). Hence, ω does not lie in any proper subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$ if and only if $\omega \notin \mathbb{F}_{q^n}^*$ for all proper divisors n of m, which (recalling that $\mathbb{F}_{q^m}^*$ is cyclic) is equivalent to saying that $|\omega|$ does not divide $q^n - 1$ for any proper divisor n of m. The assertion then holds by Lemma 2.11. □

Whether or not a polynomial is irreducible can be read off the order of any of its non-zero roots. (If $f \in \mathbb{F}_q[x]$ does not contain any non-zero roots in $\mathbb{F}_q$, then f is reducible unless $f = x$.)

Lemma 3.4. *Let $f \in \mathbb{F}_q[x]$ contain a non-zero root ω. Then f is irreducible if and only if* $\operatorname{ord}(q; |\omega|) = \deg(f)$.

Proof. Assume that f is irreducible. Let $m = \deg(f)$. By Lemma 3.2(c), $\omega \in \mathbb{F}_{q^m}$. If ω lies in a proper subfield $\mathbb{K}$ of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$, then by Lemma 3.2(b) all roots of f lie in $\mathbb{K}$, in which case f splits over $\mathbb{K}$. As this contradicts Lemma 3.2(c), by Lemma 3.3 we get $\operatorname{ord}(q; |\omega|) = m$.

Conversely, suppose that $\operatorname{ord}(q; |\omega|) = \deg(f)$. Let $f_0 \in \mathbb{F}_q[x]$ be an irreducible factor of f such that $f_0(\omega) = 0$. By the first part of this proof we obtain $\deg(f_0) = \operatorname{ord}(q; |\omega|)$. Hence, $\deg(f_0) = \deg(f)$ and f is irreducible. □

Definition 3.5. Given a positive integer m we let $N_q^*(m)$ be the number of all monic, irreducible polynomials $f \neq x$ of degree m in $\mathbb{F}_q[x]$.

For $m \in \mathbb{N}$ the value of $N_q^*(m)$ can be determined using a formula (presented in Lemma 3.7 below) which involves the following arithmetic function originally introduced by Moebius in 1832.

Definition 3.6. The *Moebius function* $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes}, \\ 0, & \text{if } n \text{ is divisible by the square of a prime.} \end{cases}$$

Our next lemma dates back to Gauß, who proved it for q prime (see [26, p. 611]) even though his arguments also hold for q being a prime power.

Lemma 3.7 (Gauß [26]). *For $m \in \mathbb{N}$, $N_q^*(m) = m^{-1} \sum_{n|m} \mu(n)(q^{m/n} - 1)$.*

Proof. If $m = 1$, then the monic, irreducible polynomials $f \neq x$ of degree 1 over $\mathbb{F}_q$ have the form $x - \alpha$, $\alpha \in \mathbb{F}_q^*$. Hence, $N_q^*(1) = q - 1$, which matches the assertion.

If $m \geq 2$, then $N_q^*(m)$ is the number of all monic, irreducible polynomials of degree m in $\mathbb{F}_q[x]$ and the assertion holds by [42, Lemma 3.23 and Theorem 3.25]. □

For a rational number r, let $\lceil r \rceil$ denote the smallest integer which is at least r, and let $\lfloor r \rfloor$ be the largest integer not greater than r.

Lemma 3.8. *Let $a, m \in \mathbb{N}$ be such that $a, m \geq 2$ and $(m, a) \notin \{(2, 2), (4, 2), (6, 2)\}$. Then $\sum_{n|m, n<m}(a^n - 1) < (a^m - 1)/(m + 1)$.*

Proof. Suppose that $2 \leq m \leq 8$. Then the inequality $\sum_{n|m,n<m}(a^n - 1) < (a^m - 1)/(m + 1)$ is equivalent to

$$\begin{cases} a^2 - 3a + 2 > 0, & \text{if } m = 2, \\ a^3 - 4a + 3 > 0, & \text{if } m = 3, \\ a^4 - 5a^2 - 5a + 9 > 0, & \text{if } m = 4, \\ a^5 - 6a + 5 > 0, & \text{if } m = 5, \\ a^6 - 7a^3 - 7a^2 - 7a + 20 > 0, & \text{if } m = 6, \\ a^7 - 8a + 7 > 0, & \text{if } m = 7, \\ a^8 - 9a^4 - 9a^2 - 9a + 26 > 0, & \text{if } m = 8. \end{cases}$$

Recalling that $a \geq 3$ if $m \in \{2, 4, 6\}$, one can easily verify that the assertion is true. So suppose that $m \geq 9$. Then $a^{\lceil m/2 \rceil - 1} > m + 1$, and hence

$$a^{\lfloor m/2 \rfloor + 1} - 1 < \underbrace{\frac{a^{\lceil m/2 \rceil - 1}}{m + 1}}_{>1} a^{\lfloor m/2 \rfloor + 1} - 1 = \frac{a^m}{m + 1} - 1 < \frac{a^m - 1}{m + 1}.$$

Then (using $a - 1 \geq 1$) we have $(a^{\lfloor m/2 \rfloor + 1} - 1)/(a - 1) < (a^m - 1)/(m + 1)$, which is the same as saying that

$$\sum_{i=0}^{\lfloor m/2 \rfloor} a^i < \frac{a^m - 1}{m + 1}. \tag{3.1}$$

Now, a proper divisor of m is at most equal to $\lfloor m/2 \rfloor$. It follows that, $\sum_{n|m,n<m}(a^n - 1) \leq \sum_{i=1}^{\lfloor m/2 \rfloor}(a^i - 1) < \sum_{i=0}^{\lfloor m/2 \rfloor} a^i$, which combined with (3.1) yields $\sum_{n|m,n<m}(a^n - 1) < (a^m - 1)(m + 1)$, as needed. □

Lemma 3.9. *Let $m \in \mathbb{N}$. Then the following hold.*

(*a*) *The value of $mN_q^*(m)$ is the number of all elements in $\mathbb{F}_{q^m}^*$ which do not lie in any proper subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$.*

(*b*) *Let $\ell \in \mathbb{N}$. Then $\ell\, N_q^*(m\ell) \leq N_{q^\ell}^*(m)$.*

(*c*) *We have $N_q^*(1) = q - 1$. If $m \geq 2$, then*

$$\frac{q^m - 1}{m+1} \leq N_q^*(m) < \frac{q^m - 1}{m}.$$

Proof. (*a*) Let $\widehat{f} \in \mathbb{F}_q[x]$ be the product of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$, and let R be the set of all roots of $\widehat{f}$. By Lemma 3.2(*a*)(*e*) each irreducible factor of $\widehat{f}$ has m distinct roots, and no two distinct irreducible factors of $\widehat{f}$ have a root in common. Hence,

$$|R| = mN_q^*(m).$$

By Lemma 3.2(*d*), R is a subset of $\mathbb{F}_{q^m}^*$. If an irreducible factor f of $\widehat{f}$ has a root in a proper subfield $\mathbb{F}_{q^n}$ of $\mathbb{F}_{q^m}$, then Lemma 3.2(*b*) implies that all roots of f lie in $\mathbb{F}_{q^n}$, which contradicts $\mathbb{F}_{q^m}$ being the splitting field of f over $\mathbb{F}_q$ (see Lemma 3.2(*c*)). Hence,

$$R \subseteq \{\alpha \in \mathbb{F}_{q^m}^* \mid \alpha \notin \mathbb{F}_{q^n} \text{ for all proper divisors } n \text{ of } m\}.$$

Consider an element $\omega \in \mathbb{F}_{q^m}^*$ which does not lie in any proper subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$. By Lemma 3.3 we have $\operatorname{ord}(q; |\omega|) = m$. Let $f \in \mathbb{F}_q[x]$ be the minimal polynomial of ω over $\mathbb{F}_q$. Since f is irreducible and $f(\omega) = 0$, Lemma 3.4 yields $\deg(f) = m$. It follows that $\omega \in R$, whence

$$R \supseteq \{\alpha \in \mathbb{F}_{q^m}^* \mid \alpha \notin \mathbb{F}_{q^n} \text{ for all proper divisors } n \text{ of } m\},$$

which proves the assertion.

(*b*) By part (*a*) of the current lemma $m\ell\, N_q^*(m\ell)$ and $mN_{q^\ell}^*(m)$ are the numbers of all elements in $\mathbb{F}_{q^{m\ell}}^*$ which do not lie in any proper subfield of $\mathbb{F}_{q^{m\ell}}$ containing $\mathbb{F}_q$, and respectively, containing $\mathbb{F}_{q^\ell}$. Since $\mathbb{F}_q \subseteq \mathbb{F}_{q^\ell}$ it follows that $m\ell\, N_q^*(m\ell) \leq mN_{q^\ell}^*(m)$, whence $\ell\, N_q^*(m\ell) \leq N_{q^\ell}^*(m)$.

(*c*) By Lemma 3.7, $N_q^*(1) = q - 1$. Let $m \geq 2$. As we may deduce from part (*a*) of the current lemma we have $|\mathbb{F}_{q^m}^*| = \sum_{n|m} nN_q^*(n)$, whence $q^m - 1 \geq N_q^*(1) + mN_q^*(m)$. Recalling that $N_q^*(1) = q - 1 \geq 1$, we get $q^m - 1 \geq 1 + mN_q^*(m)$, which proves the upper bound for $N_q^*(m)$.

In order to verify the lower bound for $N_q^*(m)$, observe that by Lemma 3.7, $(m+1)N_q^*(m)$ is equal to

$$\begin{cases} 3\big((2^2-1)-(2-1)\big)/2 = 2^2-1, & \text{if } (m,q)=(2,2),\\ 5\big((2^4-1)-(2^2-1)+0(2^1-1)\big)/4 = 2^4-1, & \text{if } (m,q)=(4,2),\\ 7\big((2^6-1)-(2^3-1)-(2^2-1)+(2-1)\big)/6 = 2^6-1, & \text{if } (m,q)=(6,2), \end{cases}$$

and hence

$$N_q^*(m) = \frac{q^m-1}{m+1} \quad \text{if } (m,q) \in \big\{(2,2),(4,2),(6,2)\big\}. \tag{3.2}$$

Now, assume that $(m,q) \notin \{(2,2),(4,2),(6,2)\}$. From part (a) of the current lemma we deduce that $mN_q^*(m) \geq |\mathbb{F}_{q^m}^*| - \sum |\mathbb{F}_{q^n}^*|$, where the sum is over all proper divisors n of m. Then

$$mN_q^*(m) \geq (q^m-1) - \sum_{\substack{n|m,\\ n<m}} (q^n-1),$$

which, using the inequality $\sum_{n|m,n<m}(q^n-1) < (q^m-1)/(m+1)$ given in Lemma 3.8, reveals that $mN_q^*(m) > (q^m-1)m/(m+1)$. Then $N_q^*(m) > (q^m-1)/(m+1)$, and this completes the proof. □

3.2 Prescribed constant term

The *constant term* of $f \in \mathbb{F}_q[x]$ is given by $f(0) \in \mathbb{F}_q$. Here we determine the number of all monic, irreducible polynomials over $\mathbb{F}_q$ which share their degree and which have the same non-zero constant term (see Proposition 3.12).

Let $m \in \mathbb{N}$. The *norm* of an element $\omega \in \mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$ is given by

$$\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = \prod_{i=0}^{m-1} \omega^{q^i} \in \mathbb{F}_q,$$

that is $\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = \omega^{(q^m-1)/(q-1)}$. Observe that $\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(0) = 0$. Further (according to [42, Theorem 2.28$(i)(ii)$]) the mapping

$$\mathbb{F}_{q^m}^* \to \mathbb{F}_q^*, \quad \alpha \mapsto \mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\alpha)$$

is a surjective group homomorphism.

Lemma 3.10. *Let $m \in \mathbb{N}$. Let $f \in \mathbb{F}[x]$ be a monic, irreducible polynomial of degree m, and let ω be a root of f. Then $\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = (-1)^m f(0)$.*

Proof. As we may deduce from Lemma 3.2(*b*), $f(x) = \prod_{i=0}^{m-1}(x - \omega^{q^i})$. Hence, $f(0) = (-1)^m \prod_{i=0}^{m-1} \omega^{q^i} = (-1)^m \mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega)$. □

Recall the Definition 3.6 of the Moebius function. The following result is known as the *additive Moebius inversion formula*, see [42, Theorem 3.24(*i*)].

Lemma 3.11. *Let h and H be two functions from $\mathbb{N}$ into an additively written abelian group G. Then*

$$H(m) = \sum_{n|m} h(n) \quad \text{for all } m \in \mathbb{N}$$

if and only if

$$h(m) = \sum_{n|m} \mu(n) H\left(\frac{m}{n}\right) \quad \text{for all } m \in \mathbb{N}.$$

Unless $f = x$, the constant term of a monic, irreducible polynomial $f \in \mathbb{F}[x]$ is non-zero. The following result specifies the number of all monic, irreducible polynomials of a given degree over $\mathbb{F}_q$ which have a prescribed non-zero constant term.

Proposition 3.12. *Let $m \in \mathbb{N}$, $\alpha \in \mathbb{F}_q^*$. The number of all monic, irreducible polynomials $f \in \mathbb{F}_q[x]$ with $\deg(f) = m$ and $f(0) = \alpha$ equals $N_q^*(m)/(q-1)$.*

Proof. For $n \in \mathbb{N}$, let $h(n)$ be the number of all elements in $\mathbb{F}_{q^m}^*$ satisfying $\mathrm{ord}(q; |\omega|) = n$ and $\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = (-1)^m \alpha$. Since all elements of $\mathbb{F}_{q^m}^*$ have order dividing $q^m - 1$ and since $\mathrm{ord}(q; q^m - 1) = m$, by Lemma 2.9(*b*) we get $\mathrm{ord}(q; |\omega|) \mid m$ for all $\omega \in \mathbb{F}_{q^m}^*$. Then

$$\sum_{n|m} h(n) = \left|\left\{\omega \in \mathbb{F}_{q^m}^* \middle| \mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = (-1)^m \alpha\right\}\right|.$$

The set $\{\omega \in \mathbb{F}_{q^m}^* | \mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = (-1)^m \alpha\}$ is a coset of the kernel of the surjective group homomorphism $\mathbb{F}_{q^m}^* \to \mathbb{F}_q^*, \omega \mapsto \mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega)$, and thus contains $(q^m - 1)/(q - 1)$ elements. Hence,

$$\sum_{n|m} h(n) = \frac{q^m - 1}{q - 1}.$$

We next apply Lemma 3.11 to $G = \mathbb{Z}$, h, and $H : \mathbb{N} \to \mathbb{Z}, x \mapsto (q^x - 1)/(q - 1)$ obtaining

$$h(m) = \sum_{n|m} \mu(n) \frac{q^{m/n} - 1}{q - 1}.$$

By Lemma 3.7, the latter simplifies to

$$h(m) = \frac{mN_q^*(m)}{q-1}.$$

It remains to show that $h(m)/m$ is the number of all monic, irreducible polynomials f over $\mathbb{F}_q$ satisfying $\deg(f) = m$ and $f(0) = \alpha$. To this end, let $\widehat{f} \in \mathbb{F}_q[x]$ be the product of all such polynomials, and let R be the set of all roots of $\widehat{f}$. By Lemma 3.2$(a)(e)$ each irreducible factor of $\widehat{f}$ contains m distinct roots, and no two distinct factors of $\widehat{f}$ share the same root. Hence,

$$\left|\left\{f \in \mathbb{F}_q[x] \mid f \text{ monic, irreducible}, \deg(f) = m, f(0) = \alpha\right\}\right| = \frac{|R|}{m}. \tag{3.3}$$

By Lemma 3.2(d), R is a subset of $\mathbb{F}_{q^m}^*$. Further, due to Lemmas 3.4, 3.10, each root ω of $\widehat{f}$ satisfies $\mathrm{ord}(q; |\omega|) = m$ and $\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = (-1)^m\alpha$. Hence,

$$|R| \leq h(m).$$

Consider an element $\omega \in \mathbb{F}_{q^m}^*$ with $\mathrm{ord}(q; |\omega|) = m$ and $\mathrm{N}_{\mathbb{F}_{q^m}:\mathbb{F}_q}(\omega) = (-1)^m\alpha$. Let $f \in \mathbb{F}_q[x]$ be the minimal polynomial of ω over $\mathbb{F}_q$. Then $f(\omega) = 0$ and f is monic and irreducible. By Lemma 3.4 we have $\deg(f) = m$. Further, by Lemma 3.10 we get $f(0) = \alpha$. Thus, $\omega \in R$, whence

$$|R| \geq h(m).$$

It follows that $|R| = h(m)$, which combined with Equation (3.3) completes the proof. □

3.3 Compositions with monic monomials

Given a polynomial $f \in \mathbb{F}_q[x]$ and a positive integer t, we consider the composition $f(x^t)$ of f and the monic monomial x^t. If $f(x^t)$ is irreducible (over $\mathbb{F}_q$), then we refer to f as *t-hyper-irreducible* (see Definition 3.13 below). Such polynomials are irreducible over $\mathbb{F}_q$. We

(1) present necessary and sufficient conditions under which $f \in \mathbb{F}_q[x]$ is t-hyper-irreducible (see Proposition 3.16);

(2) characterise all pairs $(m, t) \in \mathbb{N}^2$ such that the polynomial ring $\mathbb{F}_q[x]$ contains t-hyper-irreducible polynomials of degree m (see Theorem 3.18);

(3) derive a formula for the precise value of, and also give a good upper and lower bound for, the number of all monic, t-hyper-irreducible polynomials of some given degree (if any exist, see Theorems 3.23 and 3.24).

The second part of this section is devoted to polynomials $f \in \mathbb{F}_q[x]$ which are *almost t-hyper-irreducible* in the sense that f is irreducible and $f(x^t)$ contains an irreducible factor of degree strictly bigger than $\deg(f)t/2$. We

(1) give necessary and sufficient conditions under which an irreducible polynomial $f \in \mathbb{F}_q[x]$ is "almost t-hyper-irreducible" (see Lemma 3.26);

(2) characterise all triples $(m, t, e) \in \mathbb{N}^3$ with $e > mt/2$, for which $\mathbb{F}_q[x]$ contains an irreducible polynomial f such that $\deg(f) = m$ and $f(x^t)$ has an irreducible (over $\mathbb{F}_q$) factor of degree e (see Proposition 3.28);

(3) determine the number of all monic, "almost t-hyper-irreducible" polynomials of some given degree in $\mathbb{F}_q[x]$ (if any exist) and give a good upper and lower bound on that quantity (see Propositions 3.29, 3.31).

3.3.1 Hyper-irreducible polynomials

Definition 3.13. Let $f \in \mathbb{F}_q[x]$ and $t \in \mathbb{N}$. We refer to f as *t-hyper-irreducible* if $f(x^t)$ is irreducible (over $\mathbb{F}_q$).

Thus, 1-*hyper-irreducible* simply means *irreducible*. Observe that, if $f \in \mathbb{F}_q[x]$ is reducible, then $f(x^t)$ is reducible over $\mathbb{F}_q$ for all $t \in \mathbb{N}$. This shows that any t-hyper-irreducible polynomial is irreducible. More generally, any t-hyper-irreducible polynomial is t_0-hyper-irreducible for all divisors t_0 of t.

Lemma 3.14. *Let f be an irreducible polynomial over $\mathbb{F}_q$, and let $t \in \mathbb{N}$. Suppose that $f(x^t)$ contains an irreducible factor of degree strictly greater than* $\deg(f)t/2$. *Then* $\gcd(q, t) = 1$.

In particular, the existence of t-hyper-irreducible polynomials in $\mathbb{F}_q[x]$ implies that $\gcd(q, t) = 1$.

Proof. Let $f_0 \in \mathbb{F}_q[x]$ be the irreducible factor of $f(x^t)$ such that $\deg(f_0) > \deg(f)t/2$. If $\gcd(t, q) \neq 1$, then the characteristic p of $\mathbb{F}_q$ divides t. In this case, writing $f(x) = \sum_{i=0}^{m} \alpha_i x^i$, we get

$$f(x^t) = \sum_{i=0}^{m} \alpha_i x^{ti} = \left(\sum_{i=0}^{m} \alpha_i^{q/p} x^{ti/p} \right)^p,$$

which yields the contradiction $\deg(f_0) \leq mt/p \leq mt/2$. □

As preparation to characterise t-hyper-irreducible polynomials via the order of their roots (in Proposition 3.16 below) we require the following result.

Lemma 3.15. *Let $f \in \mathbb{F}_q[x]$ contain a non-zero root ω, and let $t \in \mathbb{N}$ be coprime to q. Then $f(x^t)$ has a root of order $|\omega|t$.*

Proof. Since $x - \omega$ divides f, the polynomial $x^t - \omega$ is a factor of $f(x^t)$. We prove the assertion by showing that $x^t - \omega$ has a root of order $|\omega|t$.

(*i*) We begin with the special case where t is prime. Let α be a root of $x^t - \omega$. (Hence, $\alpha^t = \omega$.) If $|\alpha|$ is divisible by t, then $|\omega|t = |\alpha^t| \gcd(|\alpha|, t) = |\alpha|$, as needed. So, suppose that t does not divide $|\alpha|$. By [42, Theorem 2.42(*i*)] there exists a t-th root of unity over $\mathbb{F}_q$ of order t, say β. Then $(\alpha\beta)^t = \omega$, that is $\alpha\beta$ is a root of $x^t - \omega$. Moreover, since $|\alpha|$ and t are coprime and since $t = |\beta|$, the order of $\alpha\beta$ is divisible by t. By what we have already proved, $|\omega|t = |\alpha\beta|$, as asserted.

(*ii*) Let $t_1, \ldots, t_\ell$ be (not necessarily distinct) primes such that $t = \prod_{i=1}^{\ell} t_i$. By part (*i*) of the current proof, the polynomial $x^{t_1} - \omega$ contains a root of order $|\omega|t_1$, say ω_1. Applying (*i*) to the polynomial $x^{t_2} - \omega_1$ we see that $x^{t_2} - \omega_1$ contains a root of order $|\omega_1|t_2 = |\omega|t_1t_2$. Since $x - \omega_1 \mid x^{t_1} - \omega$ we have $x^{t_2} - \omega_1 \mid x^{t_1t_2} - \omega$. It follows that $x^{t_1t_2} - \omega$ has a root of order $|\omega|t_1t_2$. Repeatedly applying this procedure, we conclude that $x^t - \omega = x^{t_1 \cdots t_\ell} - \omega$ contains a root of order $|\omega|t_1 \cdots t_\ell = |\omega|t$. □

The following characterisation of t-hyper-irreducible polynomials is a generalisation of Lemma 3.4. (We can retrieve the statement of Lemma 3.4 from Proposition 3.16 by setting $t = 1$.) It also generalises [42, Theorem 3.75] which covers the case $m = 1$.

Proposition 3.16. *Let $f \in \mathbb{F}_q[x]$ contain a non-zero root ω, and let $t \in \mathbb{N}$. Let $m = \deg(f)$. The following are equivalent.*

(*a*) *The polynomial f is t-hyper-irreducible.*

(*b*) *The integers t, q are coprime and $\operatorname{ord}(q; |\omega|t) = mt$.*

(*c*) *We have $\operatorname{ord}(q; |\omega|) = m$, the integer $\gcd(4, t)$ divides $|\omega|$, and each prime divisor of t divides $|\omega|$ but not $(q^m - 1)/|\omega|$.*

Proof. First, suppose that condition (*a*) holds. Then by (the "in particular" part of) Lemma 3.14, t and q are coprime. By Lemma 3.15 the polynomial $f(x^t)$ contains a root of order $|\omega|t$. Since (by assumption) $f(x^t)$ is irreducible over $\mathbb{F}_q$, Lemma 3.4 yields $\operatorname{ord}(q; |\omega|t) = \deg\big(f(x^t)\big) = mt$.

Next, assume that condition (*b*) is satisfied. From Lemma 2.17 we deduce that $\operatorname{ord}(q; |\omega|) = m$. The rest of (*c*) follows from Proposition 2.19 (applied to $a = q$ and $r = |\omega|$).

Finally, suppose that condition (c) holds. By Proposition 2.19 we obtain $\gcd(q,t) = 1$ and $\operatorname{ord}(q;|\omega|t) = mt = \deg\big(f(x^t)\big)$. Since by Lemma 3.15 the polynomial $f(x^t)$ contains a root of order $|\omega|t$, Lemma 3.4 reveals that $f(x^t)$ is irreducible (over $\mathbb{F}_q$), that is (a) holds. □

Example 3.17. Let ω be a primitive element of $\mathbb{F}_9$ (that is, ω is a generator of $\mathbb{F}_9^*$). Since $|\omega| = 8$, $|\omega^2| = 4$, and since the integers 8 and 4 divide 3^2-1 but not 3^1-1, we have $2 = \operatorname{ord}(3;|\omega|) = \operatorname{ord}(3;|\omega^2|)$. For $i \in \{1,2\}$, let f_i be the minimal polynomial of ω^i over $\mathbb{F}_3$. (Then $f_1, f_2 \in \mathbb{F}_3[x]$ are irreducible, and by Lemma 3.4 both polynomials have degree 2.) Let $t \geq 2$ be an integer.

(a) By Proposition 3.16 the polynomial f_1 is t-hyper-irreducible if and only if each prime divisor of t divides $|\omega| = 8$ (but not $8/8 = 1$) and $\gcd(4,t) \mid 8$. Hence, f_1 is t-hyper-irreducible if and only if t is a power of 2.

(b) If f_2 is t-hyper-irreducible, then by Proposition 3.16 all prime divisors of t divide $|\omega^2| = 4$ but not $(3^2-1)/4 = 2$, which is not possible. Hence, $f_2(x^t)$ is reducible for all $t \geq 2$.

For every positive integer m there exists an irreducible polynomial of degree m in $\mathbb{F}_q[x]$. This is not true for t-hyper-irreducible polynomials. Our next result sheds light on when $\mathbb{F}_q[x]$ contains t-hyper-irreducible polynomials of a given degree.

Theorem 3.18. *Let $m, t \in \mathbb{N}$. The following are equivalent.*

(a) *There exists a t-hyper-irreducible polynomial of degree m in $\mathbb{F}_q[x]$.*

(b) *The integers t, q are coprime and $\operatorname{ord}(q;(q^m-1)t) = mt$.*

(c) *Writing $t_1, \ldots, t_\ell$ for (all) the distinct odd prime divisors of t, we have $\gcd(t,4)\prod_{i=1}^{\ell} t_i \mid q^m - 1$.*

Proof. The implication "$(b) \Rightarrow (c)$" holds by Proposition 2.19.

Assume that condition (c) holds. Let ω be a primitive element of $\mathbb{F}_{q^m}$ (whence $|\omega| = q^m - 1$) and let f be the minimal polynomial of ω over $\mathbb{F}_q$. Then $\deg(f) = m$. By Proposition 3.16 the polynomial f is t-hyper-irreducible.

It remains to show that (a) implies (b). The assertion holds trivially for $t = 1$. So we assume that $t \geq 2$. Let $f \in \mathbb{F}_q[x]$ be a t-hyper-irreducible polynomial of degree m. Then f is irreducible. Note that all roots of f are non-zero. (If 0 is a root of f, then $f(x) = x$. But in such a case f is t-hyper-irreducible if and only if $t = 1$, which contradicts our assumption $t \geq 2$.) Let ω be a root of f. By Proposition 3.16 we get

$$\gcd(q,t) = 1, \quad mt = \operatorname{ord}(q;|\omega|t).$$

Now, since $\omega \neq 0$ and f is irreducible, by Lemma 3.2(c) the element ω lies in $\mathbb{F}_{q^m}^*$. Then $|\omega|t$ divides $(q^m-1)t$. Hence, by Lemma 2.9(b) we have $\operatorname{ord}(q;|\omega|t) \mid \operatorname{ord}(q;(q^m-1)t)$, that is (recalling that $mt = \operatorname{ord}(q;|\omega|t)$),

$$mt \mid \operatorname{ord}(q;(q^m-1)t).$$

Using Lemma 2.17 (by which $\operatorname{ord}(q;(q^m-1)t) \leq \operatorname{ord}(q;q^m-1)t = mt$) it follows that $\operatorname{ord}(q;(q^m-1)t) = mt$, and the proof is complete. □

The following example is obtained by combining Example 2.20 and Theorem 3.18.

Example 3.19. (a) The polynomial ring $\mathbb{F}_q[x]$ contains 100-hyper-irreducible polynomials of degree 10 if and only if $q \equiv \pm 1 \pmod{10}$.

(b) For $m \in \mathbb{N}$, the polynomial ring $\mathbb{F}_q[x]$ contains 2-hyper-irreducible polynomials of degree m if and only if q is odd.

In order to determine (in Theorem 3.23 below) the number of all t-hyper-irreducible polynomials of some given degree in $\mathbb{F}_q[x]$ we need two preliminary lemmas. Recall that $\varphi : \mathbb{N} \to \mathbb{N}$ denotes Euler's totient function.

Lemma 3.20. *Let G be a cyclic group and let t be a divisor of $|G|$. Then G contains $|G|\varphi(t)/t$ elements g such that $|G|/|g|$ and t are coprime.*

Proof. Let h be a generator of G, whence the elements of G are given by h^ℓ, $\ell \in \{1,\dots,|G|\}$. Since $|G|/|h^\ell| = \gcd(|G|,\ell)$, we see that $|G|/|h^\ell|$ is coprime to t if and only if $\gcd(|G|,\ell)$ is coprime to t, which (recalling that t is a divisor of $|G|$) is the case if and only if $\gcd(\ell,t) = 1$.

Thus, the number of elements g in G satisfying $\gcd\big(|G|/|g|,t\big) = 1$ equals the number of integers $\ell \in \{1,\dots,|G|\}$ such that $\gcd(\ell,t) = 1$. Then the assertion holds by Lemma 2.2(b) (applied to $a = |G|/t$ and $b = t$). □

A positive integer n is said to be *square-free* if for all prime divisors s of n, s^2 does not divide n. Observe that 1 is square-free.

Lemma 3.21. *Let $m,t \in \mathbb{N}$. Let*

$$J = \left\{ n \in \mathbb{N} \mid n \text{ divides } m,\ \gcd\left(\frac{q^m-1}{q^{m/n}-1}, t\right) = 1 \right\}.$$

Then the following hold.

(a) *If $j \in J$ and $j_0 \mid j$, then $j_0 \in J$.*

(b) *Let r be the product of all distinct primes in J if any exist, and let $r = 1$ else. Then $\{n \in \mathbb{N} \mid n \text{ divides } r\} = \{j \in J \mid j \text{ square-free}\}$.*

Proof. (*a*) Let $j \in J$ and let j_0 be a divisor of j. Seeking a contradiction, assume that $j_0 \notin J$. Then

$$\gcd\left(\frac{q^m-1}{q^{m/j_0}-1}, t\right) \neq 1.$$

Since m/j divides m/j_0, by Lemma 2.10 we have $q^{m/j}-1 \mid q^{m/j_0}-1$. Then $\gcd\big((q^m-1)(q^{m/j_0}-1)^{-1}, t\big) \mid \gcd\big((q^m-1)(q^{m/j}-1)^{-1}, t\big)$. In particular, $\gcd\big((q^m-1)(q^{m/j}-1)^{-1}, t\big) \neq 1$. This is not true since $j \in J$.

(*b*) The assertion trivially holds for $J = \{1\}$. So suppose that $J \neq \{1\}$. Then by part (*a*) of the current lemma, J contains primes. Let $r_1, \ldots, r_\ell$ be (all) the distinct primes in J, whence $r = \prod_{i=1}^{\ell} r_i$. Since $1 \in J$, in order to prove the assertion it suffices to show that

$$\{n \in \mathbb{N} \mid n \geq 2, n \text{ divides } r\} = \{j \in J \mid j \geq 2, j \text{ square-free}\}.$$

Consider a divisor $n \geq 2$ of r. We may assume that $n = \prod_{i=1}^{k} r_i$ for some positive integer $k \leq \ell$. Since $r_1, \ldots, r_k$ are pairwise distinct prime divisors of m, their product n is a square-free divisor of m. Let $(q^m-1)_t$ be the product of the s-parts of q^m-1 for all prime divisors s of t. Observe that, for all $i \in \{1, \ldots, k\}$, the condition $\gcd\big((q^m-1)(q^{m/r_i}-1)^{-1}, t\big) = 1$ implies that $(q^m-1)_t \mid q^{m/r_i}-1$. Thus, $(q^m-1)_t$ divides $\gcd\big(q^{m/r_1}-1, \ldots, q^{m/r_k}-1\big)$, which according to Lemma 2.10 is equal to $q^{\gcd(m/r_1,\ldots,m/r_k)}-1 = q^{m/n}-1$. Then $\gcd\big((q^m-1)(q^{m/n}-1)^{-1}, t\big) = 1$, whence $n \in J$.

Conversely, consider a square-free element $j \geq 2$ of J. By part (*a*) of the current lemma, each prime divisor of j lies in J. Hence, $j \mid r$. □

Definition 3.22. For $m, t \in \mathbb{N}$ we write $N_q^*(m,t)$ to denote the number of all monic, t-hyper-irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$.

Recall (from Definition 3.5) that $N_q^*(m)$ is the number of all monic, irreducible polynomials $f \neq x$ of degree m in $\mathbb{F}_q[x]$, whence

$$N_q^*(m) = N_q^*(m,1).$$

Recall further the Definition 3.6 of the Moebius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$.

Theorem 3.23. *Let $m, t \in \mathbb{N}$. If $N_q^*(m,t) \neq 0$, then*

$$N_q^*(m,t) = \frac{\varphi(t)}{mt} \sum_{j \in J} \mu(j)(q^{m/j}-1),$$

where $J = \left\{j \in \mathbb{N} \mid j \text{ divides } m, \gcd\left(\frac{q^m-1}{q^{m/j}-1}, t\right) = 1\right\}$.

Proof. The proof follows the approach taken in [17] to derive a formula for the number of all monic, irreducible polynomials of a given degree over $\mathbb{F}_q$.

Suppose that $N_q^*(m,t) \neq 0$. Let $\widehat{f} \in \mathbb{F}_q[x]$ be the product of all monic, t-hyper-irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$, and let R be the set of all roots of $\widehat{f}$. (Recall that t-hyper-irreducible polynomials are irreducible.) By Lemma 3.2$(a)(e)$ each irreducible factor of $\widehat{f}$ has m distinct roots, and no two distinct irreducible factors of $\widehat{f}$ share a root. Hence,

$$N_q^*(m,t) = \frac{|R|}{m}. \tag{3.4}$$

Let t_0 be the product of $\gcd(4,t)$ and all distinct odd prime divisors of t. As we may deduce from Lemma 2.1 we have

$$\frac{\varphi(t_0)}{t_0} = \frac{\varphi(t)}{t}. \tag{3.5}$$

By Lemma 3.2(d), $R \subseteq \mathbb{F}_{q^m}^*$. Then Proposition 3.16 yields

$$R = \left\{ \omega \in \mathbb{F}_{q^m}^* \mid \operatorname{ord}(q;|\omega|) = m,\ t_0 \text{ divides } |\omega|,\ \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1 \right\}.$$

Since $N_q^*(m,t) \neq 0$, by Theorem 3.18 the integer t_0 divides $q^m - 1$. This shows that any element $\omega \in \mathbb{F}_{q^m}^*$ satisfying $\gcd\big((q^m-1)|\omega|^{-1}, t_0\big) = 1$ has order divisible by t_0. Hence,

$$R = \left\{ \omega \in \mathbb{F}_{q^m}^* \mid \operatorname{ord}(q;|\omega|) = m,\ \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1 \right\}.$$

By Lemma 3.3, for $\omega \in \mathbb{F}_{q^m}^*$ the condition $\operatorname{ord}(q;|\omega|) = m$ is equivalent to saying that ω does not lie in any maximal subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$. Such maximal subfields have order $q^{m/j}$ where j is a prime divisor of m. Thus,

$$R = \left\{ \omega \in \mathbb{F}_{q^m}^* \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1 \right\} \setminus A, \tag{3.6}$$

where

$$A = \bigcup_{\substack{j \mid m,\\ j \text{ prime}}} \left\{ \omega \in \mathbb{F}_{q^{m/j}}^* \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1 \right\}.$$

If j is a prime divisor of m which is not an element of J (as defined in the assumption), then $\gcd\big((q^m-1)|\omega|^{-1}, t_0\big) \neq 1$ for all $\omega \in \mathbb{F}_{q^{m/j}}^*$, in which case the set $\big\{\omega \in \mathbb{F}_{q^{m/j}}^* \mid \gcd\big((q^m-1)|\omega|^{-1}, t_0\big) = 1\big\}$ is empty. This shows that

$$A = \bigcup_{\substack{j \in J,\\ j \text{ prime}}} \left\{ \omega \in \mathbb{F}_{q^{m/j}}^* \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1 \right\}.$$

If $j_1, \dots, j_\ell \in J$ are distinct primes and $s = \prod_{i=1}^{\ell} j_i$, then the intersection $\bigcap_{i=1}^{\ell} \mathbb{F}^*_{q^{m/j_i}}$ is equal to $\mathbb{F}^*_{q^{m/s}}$. Using the inclusion-exclusion principle, it follows that

$$\begin{aligned}|A| = &\sum_{\substack{j\in J,\\ j \text{ prime}}} \left|\left\{\omega \in \mathbb{F}^*_{q^{m/j}} \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1\right\}\right| \\ &- \sum_{\substack{j_1,j_2\in J,\\ j_1,j_2 \text{ distinct primes}}} \left|\left\{\omega \in \mathbb{F}^*_{q^{m/(j_1j_2)}} \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1\right\}\right| \\ &+ \sum_{\substack{j_1,j_2,j_3\in J,\\ j_1,j_2,j_3 \text{ distinct primes}}} \left|\left\{\omega \in \mathbb{F}^*_{q^{m/(j_1j_2j_3)}} \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1\right\}\right| \\ &- \dots\end{aligned}$$

As we may deduce from Lemma 3.21(b), a product of distinct primes from J is a square-free element of J; and moreover, each non-trivial, square-free element of J is a product of distinct primes from J. Thus,

$$|A| = -\sum_{\substack{j\in J,\\ j\neq 1}} \mu(j) \left|\left\{\omega \in \mathbb{F}^*_{q^{m/j}} \mid \gcd\left(\frac{q^m-1}{|\omega|}, t_0\right) = 1\right\}\right|.$$

Now, consider an element $j \in J$. Then (by definition) we have

$$\gcd\left(\frac{q^m-1}{q^{m/j}-1}, t_0\right) = 1. \tag{3.7}$$

Recalling that $t_0 \mid q^m - 1$, (3.7) implies that $t_0 \mid q^{m/j} - 1$. The condition (3.7) also implies that an element $\omega \in \mathbb{F}^*_{q^{m/j}}$ satisfies $\gcd\big((q^m-1)|\omega|^{-1}, t_0\big) = 1$ if and only if $\gcd\big((q^{m/j}-1)|\omega|^{-1}, t_0\big) = 1$. Hence,

$$|A| = -\sum_{\substack{j\in J,\\ j\neq 1}} \mu(j) \left|\left\{\omega \in \mathbb{F}^*_{q^{m/j}} \mid \gcd\left(\frac{q^{m/j}-1}{|\omega|}, t_0\right) = 1\right\}\right|,$$

and thus by (3.6),

$$|R| = \sum_{j\in J} \mu(j) \left|\left\{\omega \in \mathbb{F}^*_{q^{m/j}} \mid \gcd\left(\frac{q^{m/j}-1}{|\omega|}, t_0\right) = 1\right\}\right|.$$

Then Lemma 3.20 (applied to $G = \mathbb{F}^*_{q^{m/j}}$ and $t = t_0$) yields

$$|R| = \frac{\varphi(t_0)}{t_0} \sum_{j\in J} \mu(j)(q^{m/j}-1),$$

which combined with Equations (3.4), (3.5) finalises the proof. □

Theorem 3.24. *Let $m, t \in \mathbb{N}$ be such $N_q^*(m,t) \neq 0$. Then*

$$\frac{\varphi(t)(q^m-1)}{t(m+1)} \leq N_q^*(m,t) \leq \frac{\varphi(t)(q^m-1)}{tm}.$$

Whether or not the upper bound is strict is discussed in Remark 3.25 below.

Proof. Let r be as defined in Lemma 3.21(b). (Recall that $\mu(n) = 0$ if $n \in \mathbb{N}$ is not square-free.) Then according to Lemma 3.21(b) and Theorem 3.23 we obtain

$$N_q^*(m,t) = \frac{\varphi(t)}{mt} \sum_{n|r} \mu(n)(q^{m/n}-1),$$

and thus by Lemma 3.7,

$$N_q^*(m,t) = \frac{\varphi(t)}{mt} r N_{q^{m/r}}^*(r). \tag{3.8}$$

From Lemma 3.9(c) we get $rN_{q^{m/r}}^*(r) \leq (q^{m/r})^r - 1 = q^m - 1$, which (together with (3.8)) proves the upper bound for $N_q^*(m,t)$. Further, according to Lemma 3.9(b) (applied to $\ell = m/r$) we have $rN_{q^{m/r}}^*(r) \geq mN_q^*(m)$. By Lemma 3.9($c$) we then obtain $rN_{q^{m/r}}^*(r) \geq m(q^m-1)/(m+1)$, which (combined with (3.8)) verifies the lower bound for $N_q^*(m,t)$. □

Comparing Lemma 3.9(c) with Theorem 3.24 we see the following. If $\mathbb{F}_q[x]$ contains monic, t-hyper-irreducible polynomials of degree m (for some $m, t \in \mathbb{N}$), then the number of all such polynomials is roughly equal to $\varphi(t)/t$ times the number of all monic irreducible polynomials of degree m over $\mathbb{F}_q$.

Remark 3.25. Suppose that we are in the situation of Theorem 3.23, that is suppose that $m, t \in \mathbb{N}$ is such that $N_q^*(m,t) \neq 0$, and let

$$J = \left\{ j \in \mathbb{N} \mid j \text{ divides } m,\ \gcd\left(\frac{q^m-1}{q^{m/j}-1}, t\right) = 1 \right\}.$$

(a) If $J = \{1\}$ then by Theorem 3.23 we have

$$N_q^*(m,t) = \frac{\varphi(t)(q^m-1)}{tm}.$$

(b) If $J \neq \{1\}$ (that is, if $J \supsetneq \{1\}$), then using the same arguments as in lines 1-7 in the proof of Theorem 3.24 we obtain

$$N_q^*(m,t) < \frac{\varphi(t)(q^m-1)}{tm}.$$

3.3.2 Almost hyper-irreducible polynomials

Lemma 3.26. *Let $m, t, e \in \mathbb{N}$ be such that $e > mt/2$. Let $f \in \mathbb{F}_q[x]$ be irreducible such that $\deg(f) = m$ and $f(0) \neq 0$. Let ω be a root of f. Then $f(x^t)$ contains an irreducible (over $\mathbb{F}_q$) factor of degree e if and only if $\gcd(q, t) = 1$ and $\operatorname{ord}(q; |\omega| t) = e$.*

Proof. First, assume that $f(x^t)$ has an irreducible factor $f_0 \in \mathbb{F}_q[x]$ with $\deg(f_0) = e$. By Lemma 3.14, t and q are coprime. Let ξ be a root of f_0. Note that $\xi \neq 0$. By Lemma 3.4 we have

$$\operatorname{ord}(q; |\xi|) = e. \tag{3.9}$$

Recalling that $f_0 \mid f(x^t)$ we see that ξ^t is a root of f. Then Lemma 3.2(d) yields $|\xi^t| = |\omega|$. Thus,

$$|\xi| = |\omega| \gcd(t, |\xi|). \tag{3.10}$$

By Lemma 2.17 we have

$$\operatorname{ord}(q; |\omega| \gcd(t, |\xi|)) \leq \operatorname{ord}(q; |\omega|) \gcd(t, |\xi|). \tag{3.11}$$

Now, by (3.9) and (3.10) the left hand-side of (3.11) is equal to $e > mt/2$. Further, by Lemma 3.4 the right hand-side of (3.11) equals $m \gcd(t, |\xi|)$. Hence, $\gcd(t, |\xi|) = t$. Then by (3.9), (3.10) we get $\operatorname{ord}(q; |\omega| t) = e$.

Conversely, assume that $\gcd(q, t) = 1$ and $\operatorname{ord}(q; |\omega| t) = e$. According to Lemma 3.15 the polynomial $f(x^t)$ contains a root ξ of order $|\omega| t$. Let f_0 be an irreducible (over $\mathbb{F}_q$) factor of $f(x^t)$ which contains ξ as a root. Then by Lemma 3.4 we have $\deg(f_0) = \operatorname{ord}(q; |\xi|) = \operatorname{ord}(q; |\omega| t) = e$. □

Example 3.27. Let ω be a primitive element of $\mathbb{F}_8$, and let f be the minimal polynomial of ω over $\mathbb{F}_2$. (Then $|\omega| = 7$ and $f \in \mathbb{F}_2[x]$ is irreducible of degree 3.) Let $t = 5$. According to Lemma 2.15 we have

$$\operatorname{ord}(2; |\omega| t) = \operatorname{lcm}\{\operatorname{ord}(2; 7), \operatorname{ord}(2; 5)\} = \operatorname{lcm}\{3, 4\} = 12 > \deg(f) t/2.$$

Thus, by Lemma 3.26 the polynomial $f(x^5)$ has an irreducible (over $\mathbb{F}_2$) factor of degree 12.

Proposition 3.28. *Let $m, t, e \in \mathbb{N}$ satisfy $e > mt/2$. Then $\mathbb{F}_q[x]$ contains an irreducible polynomial f of degree m such that $f(x^t) \in \mathbb{F}_q[x]$ has an irreducible (over $\mathbb{F}_q$) factor of degree e if and only if $\gcd(t, q) = 1$, $\operatorname{ord}(q; (q^m - 1)t) = e$.*

Proof. Let $f \in \mathbb{F}_q[x]$ be irreducible such that $\deg(f) = m$ and $f(x^t) \in \mathbb{F}_q[x]$ has an irreducible factor of degree e. If $t = 1$, then $\gcd(t, q) = 1$ and $e = m = \operatorname{ord}(q; (q^m - 1)t)$. So suppose that $t \geq 2$ and let ω be a root of f. Note that $f(0) \neq 0$. (If 0 is a root of f then, recalling that f is irreducible, we have $f(x) = x$. But, since $t \geq 2$, the irreducible factors of x^t have degree $1 \leq \deg(f)t/2$). Then Lemma 3.26 reveals that

$$\gcd(q, t) = 1, \quad e = \operatorname{ord}(q; |\omega|t).$$

Lemma 3.2(d) states that $\omega \in \mathbb{F}_{q^m}^*$. Hence, $|\omega|t$ divides $(q^m - 1)t$, which is why by Lemma 2.9(b) we have $\operatorname{ord}(q; |\omega|t) \mid \operatorname{ord}(q; (q^m - 1)t)$, that is (recalling that $e = \operatorname{ord}(q; |\omega|t)$),

$$e \mid \operatorname{ord}(q; (q^m - 1)t).$$

Using Lemma 2.17 (by which $\operatorname{ord}(q; (q^m - 1)t) \leq \operatorname{ord}(q; q^m - 1)t = mt$) and $e > mt/2$, it follows that $\operatorname{ord}(q; (q^m - 1)t) = e$.

Conversely, suppose that q, t are coprime and $\operatorname{ord}(q; (q^m - 1)t) = e$. Let ω be a primitive element of $\mathbb{F}_{q^m}^*$ (whence $|\omega| = q^m - 1$) and let f be the minimal polynomial of ω over $\mathbb{F}_q$ (whence $f \in \mathbb{F}_q[x]$ is irreducible with $\deg(f) = m$). By Lemma 3.26 the polynomial $f(x^t)$ contains an irreducible (over $\mathbb{F}_q$) factor of degree e. □

For $m, t \in \mathbb{N}$, recall the Definition 3.22 of $N_q^*(m, t)$. A formula for $N_q^*(m, t)$ is given in Theorem 3.23. Further, for a positive integer r and a prime s, recall from Definition 2.16 the meaning of $(r)_s$ and $(r)_{s'}$.

Proposition 3.29. *Let $m, t, e \in \mathbb{N}$ satisfy $e > mt/2$. Let T be the number of all monic, irreducible polynomials $f \neq x$ over $\mathbb{F}_q$ such that $\deg(f) = m$ and $f(x^t)$ contains an irreducible (over $\mathbb{F}_q$) factor of degree e. Suppose that $T \neq 0$.*

(a) *If $e = mt$, then $T = N_q^*(m, t)$.*

(b) *If $e < mt$, then $m \mid e$, the integer $s = t/\gcd(e/m, t)$ is an odd prime, and $T = N_q^*\big(m, (t)_{s'}\big)$.*

Proof. Part (a) holds by Definition 3.13. So suppose that $e < mt$. Then $t \geq 2$ (because $t = 1$ implies that $e = m = mt$). Since $T \neq 0$, Proposition 3.28 yields

$$\gcd(t, q) = 1 \quad \text{and} \quad \operatorname{ord}(q; (q^m - 1)t) = e.$$

By Lemma 2.9(b), $\operatorname{ord}(q; q^m - 1)$ divides $\operatorname{ord}(q; (q^m - 1)t)$, that is $m \mid e$. Further, by Lemma 2.22 (applied to $a = q$, $r = q^m - 1$),

$$s \text{ is an odd prime}, \quad s \nmid q^m - 1.$$

Let $\mathfrak{T}$ be the set of all monic, irreducible polynomials $f \in \mathbb{F}_q[x]$ such that $\deg(f) = m$ and $f(x^t)$ contains an irreducible factor of degree e. Observe that

$x \notin \mathfrak{T}$ (because, for $t \geq 2$, the irreducible factors of x^t have degree $1 \leq mt/2$.) By definition,

$$T = |\mathfrak{T}|.$$

We prove the assertion by showing that $\mathfrak{T}$ is the set of all monic, $(t)_{s'}$-hyper-irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$.

To this end, consider a polynomial $f \in \mathfrak{T}$ and let ω be a root of f. By Lemma 3.2(d) the order of ω divides $q^m - 1$. In particular, $\gcd(q, |\omega|) = 1$, whence (recalling that t and q are coprime) we get $\gcd(q, |\omega|t) = 1$. Further by Lemma 3.4 and Lemma 3.26 we have $\operatorname{ord}(q; |\omega|) = m$ and $\operatorname{ord}(q; |\omega|t) = e$. Then according to Lemma 2.22 (applied to $a = q$ and $r = |\omega|$) we obtain $\operatorname{ord}(q; |\omega|(t)_{s'}) = m(t)_{s'}$. By Proposition 3.16 this means that f is $(t)_{s'}$-hyper-irreducible.

Conversely, let $f \neq x$ be a monic, $(t)_{s'}$-hyper-irreducible polynomial of degree m over $\mathbb{F}_q$. Let ω be a root of f. Again, by Lemma 3.2(d) the order of ω divides $q^m - 1$. Recalling that $s \nmid q^m - 1$, it follows that $s \nmid |\omega|$, and thus by Lemma 2.15,

$$\operatorname{ord}(q; |\omega|t) = \operatorname{lcm}\big\{\operatorname{ord}(q; |\omega|(t)_{s'}), \operatorname{ord}(q; (t)_s)\big\}.$$

As we may deduce from Propositions 3.16 and Theorem 3.18, $\operatorname{ord}(q; |\omega|(t)_{s'})$ is equal to $\operatorname{ord}(q; (q^m - 1)(t)_{s'})$. Hence,

$$\operatorname{ord}(q; |\omega|t) = \operatorname{lcm}\big\{\operatorname{ord}(q; (q^m - 1)(t)_{s'}), \operatorname{ord}(q; (t)_s)\big\},$$

which (recalling that $s \nmid q^m - 1$) by Lemma 2.15 simplifies to

$$\operatorname{ord}(q; |\omega|t) = \operatorname{ord}(q; (q^m - 1)t).$$

Thus, $\operatorname{ord}(q; |\omega|t) = e$, and then $f \in \mathfrak{T}$ by Lemma 3.26. □

Example 3.30. Let $q = 5$, $m = 5$, and $t = 99$. Then $\gcd(t, q) = 1$ and (as we may calculate by hand or in GAP [24], see Remark 2.8) we have

$$\operatorname{ord}(q; (q^m - 1)t) = 330 > mt/2.$$

By Proposition 3.28 there exist monic, irreducible polynomials $f \in \mathbb{F}_5[x]$ of degree 5 such that $f(x^{99})$ has an irreducible (over $\mathbb{F}_5$) factor of degree 330. Since $99/\gcd(330/5, 99) = 3$, by Proposition 3.29 the number of all such polynomials is equal to $N_5^*(5, (99)_{3'}) = N_5^*(5, 11)$. By Theorem 3.23 we obtain

$$N_q^*(5, 11) = \varphi(11)(5^5 - 1)/55 = 568.$$

(For comparison: By Lemma 3.7 the number of all monic, irreducible polynomials of degree 5 in $\mathbb{F}_5[x]$ equals $N_5^*(5) = (5^5 - 5^1)/5 = 624$.)

We next present a good upper and lower bound for the value of T as specified in Proposition 3.29. The case $e = mt$ is covered in Theorem 3.24 above, which is why we assume that $mt/2 < e < mt$.

Proposition 3.31. *Let $m, t, e \in \mathbb{N}$ satisfy $mt/2 < e < mt$. Let T be the number of all monic, irreducible polynomials $f \in \mathbb{F}_q[x]$ such that $\deg(f) = m$ and $f(x^t)$ contains an irreducible (over $\mathbb{F}_q$) factor of degree e. Suppose that $T \neq 0$. Then $m \mid e$, the integer $s = t/\gcd(e/m, t)$ is an odd prime and*

$$\frac{\varphi\big((t)_{s'}\big)(q^m-1)}{(t)_{s'}(m+1)} \leq T \leq \frac{\varphi\big((t)_{s'}\big)(q^m-1)}{(t)_{s'}m}.$$

Proof. By Proposition 3.29(*b*), m divides e, s is an odd prime, and $T = N_q^*(m,(t)_{s'})$. The rest of the assertion follows from Theorem 3.24. □

Suppose that we are in the situation of Proposition 3.31. Recalling (from the proof of Proposition 3.31) that $T = N_q^*(m,(t)_{s'})$ and using Remark 3.25 we obtain the following. If there exists a divisor $j \neq 1$ of m such that $(t)_{s'}$ is coprime to $(q^m-1)/(q^{m/j}-1)$, then the upper bound given in Proposition 3.31 is not strict, that is

$$T < \frac{\varphi\big((t)_{s'}\big)(q^m-1)}{(t)_{s'}m}.$$

Otherwise, we have

$$T = \frac{\varphi\big((t)_{s'}\big)(q^m-1)}{(t)_{s'}m}.$$

3.4 Tensor products of polynomials

Definition 3.32. Let $m, t \in \mathbb{N}$. Let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_t$ be elements in some extension field of $\mathbb{F}_q$ such that

$$f(x) = \prod_{i=1}^{m}(x-\alpha_i) \quad \text{and} \quad g(x) = \prod_{i=1}^{t}(x-\beta_i)$$

are (monic) polynomials over $\mathbb{F}_q$. The *tensor product* of f and g is given by

$$(f \otimes g)(x) = \prod_{i=1}^{m}\prod_{j=1}^{t}(x-\alpha_i\beta_j).$$

The tensor product of monic polynomials is a special case of the *composed product* introduced in [9]. If f, g are as in Definition 3.32, then by [9, line 3 on p. 119] the coefficients of $f \otimes g$ lie in $\mathbb{F}_q$.

Our motivation to consider tensor products of monic polynomials arises from the following fact. If (for $m, t \in \mathbb{N}$) the matrix $A = (a_{ij})_{1 \le i,j \le m}$ is an element of $\mathrm{GL}(m, q)$ and if $B \in \mathrm{GL}(t, q)$, then the characteristic polynomial of the *Kronecker product*

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in \mathrm{GL}(mt, q)$$

is given by $f \otimes g$, where f is the characteristic polynomial of A and g is the characteristic polynomial of B.

Lemma 3.33. *Let f_1, f_2, g_2, g_2 be monic polynomials over $\mathbb{F}_q$. Then*

$$(f_1 f_2) \otimes (g_1 g_2) = (f_1 \otimes g_1)(f_1 \otimes g_2)(f_2 \otimes g_1)(f_2 \otimes g_2).$$

Proof. Let $\deg(f_1) = m_0$, $\deg(f_1 f_2) = m$, $\deg(g_1) = t_0$, and $\deg(g_1 g_2) = t$. Let $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_t$ be elements in some extension field of $\mathbb{F}_q$ such that

$$f_1(x) = \prod_{i=1}^{m_0}(x - \alpha_i), \qquad f_2(x) = \prod_{i=m_0+1}^{m}(x - \alpha_i),$$
$$g_1(x) = \prod_{i=1}^{t_0}(x - \beta_i), \qquad g_2(x) = \prod_{i=t_0+1}^{t}(x - \beta_i).$$

By definition we have $((f_1 f_2) \otimes (g_1 g_2))(x) = \prod_{i=1}^{m}\prod_{j=1}^{t}(x - \alpha_i\beta_j)$, which is equal to

$$\overbrace{\left(\prod_{i=1}^{m_0}\prod_{j=1}^{t_0}(x - \alpha_i\beta_j)\right)}^{=(f_1 \otimes g_1)(x)} \times \overbrace{\left(\prod_{i=1}^{m_0}\prod_{j=t_0+1}^{t}(x - \alpha_i\beta_j)\right)}^{=(f_1 \otimes g_2)(x)} \times$$
$$\underbrace{\left(\prod_{i=m_0+1}^{m}\prod_{j=1}^{t_0}(x - \alpha_i\beta_j)\right)}_{=(f_2 \otimes g_1)(x)} \times \underbrace{\left(\prod_{i=m_0+1}^{m}\prod_{j=t_0+1}^{t}(x - \alpha_i\beta_j)\right)}_{=(f_2 \otimes g_2)(x)}.$$

Hence, $(f_1 f_2) \otimes (g_1 g_2) = (f_1 \otimes g_1)(f_1 \otimes g_2)(f_2 \otimes g_1)(f_2 \otimes g_2)$, as asserted. □

Lemma 3.34. *Let $f \neq x$ and $g \neq x$ be monic irreducible polynomials over $\mathbb{F}_q$. If $h \in \mathbb{F}_q[x]$ is an irreducible factor of $f \otimes g$, then* $\deg(h) \mid \operatorname{lcm}\{\deg(f), \deg(g)\}$.

Proof. Let $h \in \mathbb{F}_q[x]$ be an irreducible factor of $f \otimes g$, and let γ be a root of h. Since h divides $f \otimes g$, there exist roots α, β of f and g, respectively, such that $\gamma = \alpha\beta$. In particular, (since $g(0) \neq 0$ and $h(0) \neq 0$) we have $\gamma \neq 0$. Then by Lemma 3.4, $\deg(h) = \operatorname{ord}(q; |\gamma|)$.

Let $m = \deg(f)$, $t = \deg(g)$, and $\ell = \operatorname{lcm}\{m, t\}$. Since f, g are irreducible, Lemma 3.2(d) yields $\alpha \in \mathbb{F}_{q^m}^*, \beta \in \mathbb{F}_{q^t}^*$. Then $\gamma \in \mathbb{F}_{q^\ell}^*$, whence $|\gamma|$ divides $q^\ell - 1$. Using Lemma 2.9(a) we conclude that $\operatorname{ord}(q; |\gamma|) \mid \ell$, which (recalling that $\deg(h) = \operatorname{ord}(q; |\gamma|)$) proves the assertion. □

Lemma 3.35 (Brawley & Carlitz [9])**.** *Let f, g be monic polynomials of positive degree over $\mathbb{F}_q$ such that $f(0), g(0) \neq 0$. Then $f \otimes g \in \mathbb{F}_q[x]$ is irreducible if and only if the polynomials f and g are irreducible and have coprime degrees.*

Proof. Let $\mathbb{E}$ be the splitting field of the product $fg \in \mathbb{F}_q[x]$. For $\alpha, \beta \in \mathbb{F}_q^*$ let $\alpha \otimes \beta = \alpha\beta$. The assertion holds by [9, Theorem 2] applied to $(G, \diamond) = (\mathbb{E}^*, \otimes)$ and $f \diamond g = f \otimes g$. (In [9] the set $M_G(q, x)$ is the set of all monic polynomials of positive degree in $\mathbb{F}_q$ which have all roots in G.) □

Recall from Definition 3.5 that $N_q^*(m)$ is the number of all monic, irreducible polynomials $f \neq x$ of degree m in $\mathbb{F}_q[x]$.

Proposition 3.36. *Let $m, t \in \mathbb{N}$ be coprime. The number of polynomials $f \otimes g \in \mathbb{F}_q[x]$, where $f \neq x$ and $g \neq x$ are monic, irreducible polynomials over $\mathbb{F}_q$ with $\deg(f) = m$, $\deg(g) = t$, is equal to $N_q^*(m)N_q^*(t)/(q-1)$.*

Proof. Let S be the set of all tensor products $f \otimes g \in \mathbb{F}_q[x]$, where $f \neq x$ and $g \neq x$ are monic, irreducible polynomials over $\mathbb{F}_q$ with $\deg(f) = m$, $\deg(g) = t$. Each $h \in S$ has degree mt and, moreover, is irreducible by Lemma 3.35. Thus, by Lemma 3.2(a), each $h \in S$ has mt distinct roots. Since by Lemma 3.2(e) no two distinct polynomials in S have a root in common, writing R for the set of all roots of $\prod_{h \in S} h$, we have

$$|S| = \frac{|R|}{mt}.$$

Let $P = \{(\alpha, \beta) \in \mathbb{F}_{q^m}^* \times \mathbb{F}_{q^t}^* \mid \operatorname{ord}(q; |\alpha|) = m, \operatorname{ord}(q; |\beta|) = t\}$. By Lemma 3.3 and Lemma 3.9(a) we have

$$|P| = mtN_q^*(m)N_q^*(t).$$

In order to prove the lemma it remains to show that $|R| = |P|/(q-1)$. To this end, recall from Definition 3.32 that each $\gamma \in R$ can be written as

a product $\gamma = \alpha\beta$ for some root α of an irreducible polynomial of degree m over $\mathbb{F}_q$ and some root β of an irreducible polynomial of degree t over $\mathbb{F}_q$. In such a case Lemma 3.4 yields $(\alpha, \beta) \in P$. Conversely, given $(\alpha, \beta) \in P$, the product $\alpha\beta$ is a root of the tensor product $f \otimes g$, where f and g are the minimal polynomials over $\mathbb{F}_q$ of α and β, respectively. In such a case, (since $f, g \in \mathbb{F}_q[x]$ are monic and irreducible and) since by Lemma 3.4 we have $\deg(f) = m, \deg(g) = t$, it follows that $f \otimes g \in S$, and thus $\alpha\beta \in R$. Hence,

$$R = \big\{\alpha\beta \mid (\alpha, \beta) \in P\big\}.$$

Consider $(\alpha_1, \beta_1), (\alpha_2, \beta_2) \in P$. We have $\alpha_1\beta_1 = \alpha_2\beta_2$ if and only if $\alpha_1/\alpha_2 = \beta_2/\beta_1 \in \mathbb{F}_{q^m}^* \cap \mathbb{F}_{q^t}^*$. Since m and t are coprime, Lemma 2.10 implies that $\mathbb{F}_{q^m}^* \cap \mathbb{F}_{q^t}^* = \mathbb{F}_q^*$. We conclude that $\alpha_1\beta_1 = \alpha_2\beta_2$ if and only if there exists $\varepsilon \in \mathbb{F}_q^*$ such that $(\alpha_1, \beta_1) = (\alpha_2\varepsilon, \beta_2\varepsilon^{-1})$. This shows that $|R| = |P|/(q-1)$, as needed. □

3.5 Galois twisted polynomials

Let t be a positive integer. We write $\mathrm{Aut}(\mathbb{F}_{q^t})$ for the group of all field automorphisms on $\mathbb{F}_{q^t}$. For $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^t})$ and $\omega \in \mathbb{F}_{q^t}$, the image of ω under σ is denoted by ω^σ. Given a polynomial $f \in \mathbb{F}_{q^t}[x]$, we write f^σ for the polynomial obtained from f by applying σ to every coefficient of f. The *Galois group* $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$ of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$ consists of all automorphisms $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^t})$ satisfying $\alpha^\sigma = \alpha$ for all $\alpha \in \mathbb{F}_q$. By [42, Theorem 2.21] the group $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$ is cyclic of order t and

$$\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q) = \big\{\mathbb{F}_{q^t} \to \mathbb{F}_{q^t}, \alpha \mapsto \alpha^{q^i} \mid 0 \le i \le t-1\big\}.$$

Definition 3.37. Let $t \in \mathbb{N}$ and let $f \in \mathbb{F}_{q^t}[x]$. We call the polynomial $\prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\sigma$ the *Galois-twist* of f over $\mathbb{F}_q$.

Observe that the Galois-twist over $\mathbb{F}_q$ of a polynomial $f \in \mathbb{F}_{q^t}[x]$ is invariant under $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$, and thus lies in $\mathbb{F}_q[x]$.

Lemma 3.38. *Let $t \in \mathbb{N}$, and let $f \in \mathbb{F}_{q^t}[x]$ be irreducible. The polynomial $\prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\sigma$ splits over $\mathbb{F}_q$ into irreducible factors of the same degree.*

Proof. Let ω be a root of f, and let $m = \deg(f)$. Since f is irreducible (over $\mathbb{F}_{q^t}$), by Lemma 3.2(*b*) the roots of f are given by $\omega, \omega^{q^t}, \ldots, \omega^{q^{t(m-1)}}$. Thus, the roots of $\prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\sigma$ consist of the elements $\omega, \omega^q, \ldots, \omega^{q^{mt-1}}$. In particular, every root of $\prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\sigma$ has the same order, and the assertion follows from Lemma 3.4. □

Proposition 3.39. *Let $m, t, e \in \mathbb{N}$ be such that $e > mt/2$. The number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_{q^t}$ such that the Galois-twist of f over $\mathbb{F}_q$ has an irreducible (over $\mathbb{F}_q$) factor of degree e is equal to*

$$\begin{cases} N_q^*(mt)t \neq 0, & \text{if } e = mt, \\ 0, & \text{else.} \end{cases}$$

Proof. Let S be the set of all monic, irreducible polynomials $f \neq x$ over $\mathbb{F}_{q^t}$ such that the Galois-twist of f over $\mathbb{F}_q$ contains an irreducible (over $\mathbb{F}_q$) factor of degree e. Since $e > mt/2$, Lemma 3.38 implies that

$$S \neq \emptyset \quad \Longleftrightarrow \quad e = mt.$$

So, suppose that $e = mt$. Let $\widehat{f} \in \mathbb{F}_{q^t}[x]$ be the product of all polynomials in S and let R be the set of all roots of $\widehat{f}$. From Lemma 3.2$(a)(e)$ we obtain

$$|S| = \frac{|R|}{m}.$$

In order to complete the proof, we show that $|R| = mtN_q^*(mt)$.

First, consider an element $\omega \in R$. Then ω is a root of (some polynomial in S, that is of) some monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_{q^t}$. By Lemma 3.2(d) we get $\omega \in \mathbb{F}_{q^{mt}}^*$. Since ω is also a root of the Galois-twist $\prod_{\xi \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\xi$ of f over $\mathbb{F}_q$, which has degree mt and which (by assumption) is irreducible over $\mathbb{F}_q$, Lemmas 3.3, 3.4 imply that ω does not lie in any proper subfield of $\mathbb{F}_{q^{mt}}$ containing $\mathbb{F}_q$. Thus, by Lemma 3.9(a) we have

$$|R| \leq mtN_q^*(mt).$$

Conversely, let ω be an element of $\mathbb{F}_{q^{mt}}^*$ which does not lie in any proper subfield of $\mathbb{F}_{q^{mt}}$ containing $\mathbb{F}_q$. Then by Lemma 3.3 we have

$$\mathrm{ord}(q; |\omega|) = mt. \tag{3.12}$$

Let f be the minimal polynomial of ω over $\mathbb{F}_{q^t}$. Using Lemma 2.9(c) and Equation (3.12) we see that $\mathrm{ord}(q^t; |\omega|) = m$. Hence, by Lemma 3.4 the polynomial f has degree m. Now, ω is also a root of the Galois-twist, say g, of f over $\mathbb{F}_q$. Since $\deg(g) = mt$ and since (3.12) holds, Lemma 3.4 reveals that g is irreducible (over $\mathbb{F}_q$). It follows that $f \in S$ and thus $\omega \in R$. Hence, any element in $\mathbb{F}_{q^{mt}}^*$ which does not lie in a proper subfield of $\mathbb{F}_{q^{mt}}$ containing $\mathbb{F}_q$ is an element of R. Then Lemma 3.9(a) yields

$$mtN_q^*(mt) \leq |R|.$$

(Note that by Lemma 3.9(c), $tN_q^*(mt) \geq t(q^{mt} - 1)/(mt + 1) > 0$.) □

Chapter 4

Irreducible semilinear mappings

This chapter is devoted to irreducible, non-singular, semilinear mappings on finite vector spaces. Some of the results in this chapter may apply to (finite and infinite) fields. Nevertheless, we assume the following.

Notation. Throughout this chapter let $\mathbb{F}$ be a finite field and let $\mathcal{V}, \mathcal{W}$ be non-trivial finite dimensional vector spaces defined over $\mathbb{F}$.

We begin in Section 4.1 with a few basic definitions and properties concerning semilinear mappings between finite vector spaces. In Section 4.2 we turn our attention to the case where a non-singular semilinear mapping g on $\mathcal{V}$, is *irreducible*, that is where g does not leave invariant any non-trivial and proper subspaces of $\mathcal{V}$. In Section 4.3 we count all irreducible non-singular semilinear mappings on $\mathcal{V}$. This number is specified in Theorem 4.22. Section 4.4 investigates the characteristic polynomial of g, viewed as a linear mapping over the fixed field of its associated field automorphism.

4.1 Semilinear mappings

Recall that we write $\mathrm{Aut}(\mathbb{F})$ for the group of all field automorphisms on $\mathbb{F}$. If $\mathbb{K}$ is a subfield of $\mathbb{F}$ and $\sigma \in \mathrm{Aut}(\mathbb{F})$, then the restriction $\sigma|_{\mathbb{K}}$ is an element of $\mathrm{Aut}(\mathbb{K})$. The image of $\alpha \in \mathbb{F}$ under $\sigma \in \mathrm{Aut}(\mathbb{F})$ is denoted by α^σ. For a polynomial $f \in \mathbb{F}[x]$ we write f^σ to denote the polynomial obtained by applying σ to every coefficient of f. Similarly, given a matrix A over $\mathbb{F}$ we write A^σ to denote the matrix obtained by applying σ to every entry of A.

Our convention is to denote mappings between vector spaces on the right.

A mapping $g : \mathcal{V} \to \mathcal{W}$ is said to be $\mathbb{F}$-*semilinear*, or simply *semilinear*, if there exists an element $\sigma \in \mathrm{Aut}(\mathbb{F})$ such that for all $v_1, v_2 \in \mathcal{V}$ and all $\alpha \in \mathbb{F}$

we have

$$(v_1 + \alpha v_2)g = v_1 g + \alpha^\sigma v_2 g. \tag{4.1}$$

If $g : \mathcal{V} \to \mathcal{W}$ is semilinear and $g \neq 0$, then the automorphism σ satisfying (4.1) is uniquely determined. In this context, g is also called *σ-semilinear*, and σ is referred to as the field automorphism *associated* with g. Note that linear mappings $\mathcal{V} \to \mathcal{W}$ are precisely the $\mathrm{id}_{\mathbb{F}}$-semilinear mappings from $\mathcal{V}$ to $\mathcal{W}$.

The *kernel* and *image* of a semilinear mapping $g : \mathcal{V} \to \mathcal{W}$ are given by $\ker(g) = \{v \in \mathcal{V} \mid vg = 0\}$ and $\mathrm{im}(g) = \{vg \mid v \in \mathcal{V}\} = \mathcal{V}g$, respectively. Observe that $\ker(g) \leq \mathcal{V}$, $\mathrm{im}(g) \leq \mathcal{W}$, and that g maps subspaces of $\mathcal{V}$ onto subspaces of $\mathcal{W}$. (To verify the latter, let $\mathcal{X} \leq \mathcal{V}$. Then $\mathcal{X}g$ is the image of the semilinear mapping $\mathcal{X} \to \mathcal{W}, x \mapsto xg$, whence $\mathcal{X}g$ is a subspace of $\mathcal{W}$.) The mapping g is called *non-singular* if $\ker(g) = \{0\}$.

The set of all non-singular semilinear mappings on $\mathcal{V}$ forms a group under composition, the *general semilinear group* $\Gamma\mathrm{L}(\mathcal{V})$. If the context is clear, we may also denote this group by $\Gamma\mathrm{L}(\dim(\mathcal{V}), |\mathbb{F}|)$. The set of all non-singular linear mappings on $\mathcal{V}$ is also a group under composition, the *general linear group* $\mathrm{GL}(\mathcal{V})$. The mapping $\Gamma\mathrm{L}(\mathcal{V}) \to \mathrm{Aut}(\mathbb{F})$ assigning to each non-singular, semilinear mapping on $\mathcal{V}$ its associated field automorphism, is a group homomorphism with kernel $\mathrm{GL}(\mathcal{V})$. Thus, $\mathrm{GL}(\mathcal{V})$ is a normal subgroup of $\Gamma\mathrm{L}(\mathcal{V})$. In fact, $\Gamma\mathrm{L}(\mathcal{V})$ is the semi-direct product

$$\Gamma\mathrm{L}(\mathcal{V}) \cong \mathrm{Aut}(\mathbb{F}) \ltimes \mathrm{GL}(\mathcal{V}).$$

In order to construct an explicit isomorphism $\mathrm{Aut}(\mathbb{F}) \ltimes \mathrm{GL}(\mathcal{V}) \to \Gamma\mathrm{L}(\mathcal{V})$, we suppose that $m = \dim(\mathcal{V})$ and fix a basis $\mathfrak{B} = \{v_1, \ldots, v_m\}$ of $\mathcal{V}$. Then mapping $(\sigma, h) \in \mathrm{Aut}(\mathbb{F}) \ltimes \mathrm{GL}(\mathcal{V})$ onto

$$g : \mathcal{V} \to \mathcal{V}, \quad \sum_{i=1}^{m} \alpha_i v_i \mapsto \sum_{i=1}^{m} \alpha_i^\sigma v_i h, \quad (\alpha_1, \ldots, \alpha_m \in \mathbb{F})$$

yields a group isomorphism $\mathrm{Aut}(\mathbb{F}) \ltimes \mathrm{GL}(\mathcal{V}) \to \Gamma\mathrm{L}(\mathcal{V})$.

If, as above, $m = \dim(\mathcal{V})$ and $\mathfrak{B} = \{v_1, \ldots, v_m\}$ is a basis of $\mathcal{V}$ then, given an element $h \in \mathrm{GL}(\mathcal{V})$, we write $h_{\mathfrak{B}}$ for the $(m \times m)$-matrix satisfying $v_i h = \sum_{j=1}^{m} (h_{\mathfrak{B}})_{i,j} v_j$ for all $i, j \in \{1, \ldots, m\}$. We call $h_{\mathfrak{B}}$ the *matrix of h with respect to $\mathfrak{B}$*. By mapping each element $g \in \mathrm{GL}(\mathcal{V})$ onto $g_{\mathfrak{B}}$ we obtain the group isomorphism

$$\mathrm{GL}(\mathcal{V}) \to \mathrm{GL}(m, |\mathbb{F}|), \quad g \mapsto g_{\mathfrak{B}} \tag{4.2}$$

between $\mathrm{GL}(\mathcal{V})$ and the group $\mathrm{GL}(m, |\mathbb{F}|)$ of all invertible $(m \times m)$-matrices over $\mathbb{F}$.

We may naturally view $\mathcal{V}$ as a vector space defined over a subfield of its underlying field $\mathbb{F}$.

Definition 4.1. Let $\mathbb{K}$ be a subfield of $\mathbb{F}$.

(*a*) We write $\mathcal{V}_{\mathbb{K}}$ for the $\mathbb{K}$-vector space obtained from $\mathcal{V}$ by restricting scalar multiplication on $\mathcal{V}$ to $\mathbb{K}$.

(*b*) If $g \in \Gamma\mathrm{L}(\mathcal{V}_{\mathbb{F}})$, then $g_{\mathbb{K}}$ denotes g viewed as a mapping on $\mathcal{V}_{\mathbb{K}}$.

In order to emphasise that $\mathcal{V}$ is an $\mathbb{F}$-vector space (and to avoid confusion) we may sometimes add the subscript $\mathbb{F}$ to $\mathcal{V}$ (that is, write $\mathcal{V}_{\mathbb{F}}$ instead of $\mathcal{V}$). Observe that, given a subfield $\mathbb{K}$ of $\mathbb{F}$, we have $\dim(\mathcal{V}_{\mathbb{K}}) = \dim(\mathcal{V}_{\mathbb{F}})|\mathbb{F} : \mathbb{K}|$ and

$$\Gamma\mathrm{L}(\mathcal{V}_{\mathbb{F}}) \cong \{g_{\mathbb{K}} \mid g \in \Gamma\mathrm{L}(\mathcal{V})\} \leq \Gamma\mathrm{L}(\mathcal{V}_{\mathbb{K}}),$$
$$\mathrm{GL}(\mathcal{V}_{\mathbb{F}}) \cong \{g_{\mathbb{K}} \mid g \in \mathrm{GL}(\mathcal{V})\} \leq \mathrm{GL}(\mathcal{V}_{\mathbb{K}}).$$

An element $g \in \Gamma\mathrm{L}(\mathcal{V})$ is said to be $\mathbb{K}$-*linear* if for all $\alpha \in \mathbb{K}$ and all $v \in \mathcal{V}$ we have $(\alpha v)g = \alpha vg$, that is if $g_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$. In such a case we sometimes refer to the minimal/characteristic polynomial of $g_{\mathbb{K}}$ as the minimal/characteristic polynomial of g *on* $\mathcal{V}_{\mathbb{K}}$. If $g \in \Gamma\mathrm{L}(\mathcal{V})$ is σ-semilinear, then $g^{|\sigma|}$ is $\mathbb{F}$-linear. In fact, $|\sigma|$ is the smallest positive integer t such that g^t is $\mathbb{F}$-linear.

Definition 4.2. Let $g \in \Gamma\mathrm{L}(\mathcal{V})$ and let t be the order of its associated field automorphism. We refer to $g^t \in \mathrm{GL}(\mathcal{V})$ as the *linear part* of g.

Consider $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $h \in \mathrm{GL}(\mathcal{V})$, and fix an isomorphism $\iota : \mathrm{Aut}(\mathbb{F}) \ltimes \mathrm{GL}(\mathcal{V}) \to \Gamma\mathrm{L}(\mathcal{V})$. Then $g = \iota(\sigma, h)$ is a σ-semilinear element of $\Gamma\mathrm{L}(\mathcal{V})$ with linear part $\ell = g^{|\sigma|}$. We need to be careful not to confuse ℓ with $\iota(\mathrm{id}_{\mathbb{F}}, h)$.

If A is a subgroup of $\mathrm{Aut}(\mathbb{F})$, then $\{\alpha \in \mathbb{F} \mid \alpha^\sigma = \alpha \text{ for all } \sigma \in A\}$ is a subfield of $\mathbb{F}$, the *fixed field* of A. The *fixed field* of an element $\sigma \in \mathrm{Aut}(\mathbb{F})$ is the fixed field of $\langle\sigma\rangle$. As presented below, the characteristic polynomial of the linear part of an element in $\Gamma\mathrm{L}(\mathcal{V})$ is defined over the fixed field of its associated field automorphism.

Lemma 4.3. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$, let $\ell \in \mathrm{GL}(\mathcal{V})$ be the linear part of g, let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of the field automorphism associated with g, and let $\xi \in \mathbb{F}[x]$ be the characteristic polynomial of ℓ (on $\mathcal{V}_{\mathbb{F}}$). Then the following hold.*

(*a*) *We have $\xi \in \mathbb{K}[x]$.*

(*b*) *The minimal polynomial of $\ell_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$ divides ξ.*

Proof. (*a*) Let σ be the field automorphism associated with g, let $m = \dim(\mathcal{V})$, and let $\mathfrak{B} = \{v_1, \ldots, v_m\}$ be a basis of $\mathcal{V}$. Define $h \in \mathrm{GL}(\mathcal{V})$ by

$$v_i h = v_i g, \quad \text{for all } i \in \{1, \ldots, m\},$$

and let $s \in \Gamma\mathrm{L}(\mathcal{V})$ denote the σ-semilinear mapping on $\mathcal{V}$ given by

$$\left(\sum_{i=1}^{d} \alpha_i v_i\right) s = \alpha^\sigma v_i, \quad \text{for all } \alpha_1, \ldots, \alpha_m \in \mathbb{F}.$$

Then $g = sh$. Since ℓ is a power of g we have $\ell = g^{-1}\ell g$, that is $\ell = h^{-1}s^{-1}\ell sh$, and thus

$$h\ell h^{-1} = s^{-1}\ell s \in \mathrm{GL}(\mathcal{V}). \tag{4.3}$$

According to the definition of s and ℓ we have $v_i s^{-1}\ell s = v_i \ell s$ for all $i \in \{1, \ldots, m\}$. Thus,

$$(s^{-1}\ell s)_{\mathfrak{B}} = (\ell_{\mathfrak{B}})^\sigma, \tag{4.4}$$

where $(s^{-1}\ell s)_{\mathfrak{B}}$ and $\ell_{\mathfrak{B}}$ are the matrices of $s^{-1}\ell s$ and ℓ, respectively, with respect to the basis $\mathfrak{B}$.

Recall that ξ is the characteristic polynomial of ℓ. Being a conjugate of ℓ in $\mathrm{GL}(\mathcal{V})$ the element $h\ell h^{-1}$ has ξ as its characteristic polynomial. Equations (4.3) and (4.4) then reveal that ξ is also the characteristic polynomial of $(\ell_{\mathfrak{B}})^\sigma$. Writing $\mathbf{1}$ for the $(m \times m)$-identity matrix over $\mathbb{F}$, we thus have $\xi = \det(x\mathbf{1} - (\ell_{\mathfrak{B}})^\sigma)$. Since $\det(x\mathbf{1} - (\ell_{\mathfrak{B}})^\sigma) = (\det(x\mathbf{1} - \ell_{\mathfrak{B}}))^\sigma = \xi^\sigma$, we conclude that $\xi = \xi^\sigma$, and hence $\xi \in \mathbb{K}[x]$.

(*b*) The minimal polynomial of $\ell_{\mathbb{K}}$ divides any polynomial over $\mathbb{K}$ which annihilates ℓ. This proves the assertion, for $\xi \in \mathbb{K}[x]$ by part (*a*), and $\xi(\ell) = 0$ (by the Cayley-Hamilton Theorem). □

4.2 Irreducible semilinear mappings

Recall that $\mathcal{V} \neq \{0\}$ is a finite vector space over $\mathbb{F}$.

Definition 4.4. Let $G \leq \Gamma\mathrm{L}(\mathcal{V})$, and let $\mathcal{U} \leq \mathcal{V}$.

(*a*) We say that $\mathcal{U}$ is *G-invariant* and that G *leaves* $\mathcal{U}$ *invariant* if $\mathcal{U}g = \mathcal{U}$ for all $g \in G$. If $\mathcal{U}$ is G-invariant and there exists a non-trivial, proper, G-invariant subspace of $\mathcal{U}$, then $\mathcal{U}$ is called *G-reducible* and G is said to *act reducibly* on $\mathcal{U}$. If $\mathcal{U} \neq \{0\}$ and $\mathcal{U}$ is G-invariant but not G-reducible, then $\mathcal{U}$ is said to be *G-irreducible* and G is said to *act irreducibly* on $\mathcal{U}$.

(*b*) We say that G is *irreducible*, or *reducible*, according as $\mathcal{V}$ is G-irreducible, or G-reducible. An element $g \in \Gamma\mathrm{L}(\mathcal{V})$ is *irreducible/reducible* if the group $\langle g \rangle$ has this property.

(*c*) We write $G_{\mathcal{U}} = \{g \in G \mid \mathcal{U}g = \mathcal{U}\}$ for the maximal (with respect to inclusion) subgroup of G which leaves $\mathcal{U}$ invariant.

Given an element $g \in \Gamma\mathrm{L}(\mathcal{V})$ and a $\langle g \rangle$-invariant subspace $\mathcal{U} \leq \mathcal{V}$, we let $g|_{\mathcal{U}}$ denote the restriction of g to $\mathcal{U}$. If $\mathcal{U} \neq \{0\}$, then $g|_{\mathcal{U}} \in \Gamma\mathrm{L}(\mathcal{U})$, and g and $g|_{\mathcal{U}}$ have the same associated field automorphism.

4.2.1 Basic properties

Lemma 4.5. *Let $g, h \in \Gamma\mathrm{L}(\mathcal{V})$. Then g is irreducible if and only if $h^{-1}gh$ is irreducible.*

Proof. Suppose that g is irreducible. Seeking a contradiction, assume that $\mathcal{W}$ is a non-trivial and proper subspace of $\mathcal{V}$ and that $\mathcal{W}h^{-1}gh = \mathcal{W}$. Then $(\mathcal{W}h^{-1})g = \mathcal{W}h^{-1}$, which means that $\mathcal{W}h^{-1}$ is $\langle g \rangle$-invariant. Since $\mathcal{W}h^{-1}$ is a non-trivial and proper subspace of $\mathcal{V}$, we conclude that g is reducible, which is not true.

Conversely, if $h^{-1}gh$ is irreducible, then (using the same arguments as above) we see that $h(h^{-1}hg)h^{-1} = g$ is irreducible. □

The question whether or not an element $g \in \Gamma\mathrm{L}(\mathcal{V})$ is irreducible can be answered by looking at the characteristic polynomial of its linear part (as introduced in Definition 4.2). Recall from Lemma 4.3(a) that all coefficients of that polynomial lie in the fixed field of the field automorphism associated with g.

Proposition 4.6. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$, let $\ell \in \mathrm{GL}(\mathcal{V})$ be the linear part of g, and let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of the field automorphism associated with g. Let $\xi \in \mathbb{K}[x]$ be the characteristic polynomial of ℓ (on $\mathcal{V}_{\mathbb{F}}$), and let $\eta \in \mathbb{K}[x]$ be the minimal polynomial of $\ell_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$.*

(a) *If g is irreducible, then $\xi = \eta$.*

(b) *The following are equivalent.*

- (i) *The element g is irreducible.*
- (ii) *The polynomial η is irreducible over $\mathbb{K}$ and $\deg(\eta) = \dim(\mathcal{V}_{\mathbb{F}})$.*
- (iii) *The polynomial ξ is irreducible over $\mathbb{K}$.*

Proof. Let $t = |\mathbb{F} : \mathbb{K}|$, whence t is the order of the field automorphism of $\mathbb{F}$ associated with g. We prove the assertion using several results from [20]. As a first step, we explain the relevant notation used in that paper: Our element g corresponds to T or T', our t corresponds to n (whence ℓ corresponds to T^n or $(T')^n$); our fields $\mathbb{F}$ and $\mathbb{K}$ correspond to K and K_0, respectively; $\mathbb{K}[\ell]$ corresponds to F, and $\mathcal{V}$ is denoted by V.

If η is irreducible over $\mathbb{K}$, then $\mathbb{K}[\ell]$ is an extension field of $\mathbb{K}$ of degree $|\mathbb{K}[\ell] : \mathbb{K}| = \deg(\eta)$. In this case, we can impose on $\mathcal{V}$ the structure of a $\mathbb{K}[\ell]$-vector space by defining the scalar multiplication as $\alpha v = v\alpha$ for all $\alpha \in \mathbb{K}[\ell]$. We denote that $\mathbb{K}[\ell]$-vector space by $\mathcal{V}_{\mathbb{K}[\ell]}$. Hence, if η is irreducible over $\mathbb{K}$, then

$$\dim\big(\mathcal{V}_{\mathbb{K}[\ell]}\big) = \frac{\dim(\mathcal{V}_{\mathbb{K}})}{|\mathbb{K}[\ell] : \mathbb{K}|} = \frac{\dim(\mathcal{V}_{\mathbb{F}})|\mathbb{F} : \mathbb{K}|}{|\mathbb{K}[\ell] : \mathbb{K}|},$$

which (using $\dim(\mathcal{V}_{\mathbb{F}}) = \deg(\xi)$, $|\mathbb{F} : \mathbb{K}| = t$, and $|\mathbb{K}[\ell] : \mathbb{K}| = \deg(\eta)$) yields

$$\dim\big(\mathcal{V}_{\mathbb{K}[\ell]}\big) = \frac{\deg(\xi)t}{\deg(\eta)}. \tag{4.5}$$

(a) Suppose that g is irreducible. Then by [20, Lemma 2.2] the polynomial η is irreducible over $\mathbb{K}$. Thus, Equation (4.5) holds. Combining (4.5) with [20, Proposition 3.1 and Theorem 2.4], by which $\dim(\mathcal{V}_{\mathbb{K}[\ell]}) = t$, we obtain $\deg(\eta) = \deg(\xi)$. Since, according to Lemma 4.3(b), the polynomial η divides ξ, we conclude that $\xi = \eta$.

(b) Suppose that condition (i) holds. Then, as shown in the proof of part (a) (of the current lemma), η is irreducible over $\mathbb{K}$ and $\deg(\eta) = \deg(\xi) = \dim(\mathcal{V}_{\mathbb{F}})$. Thus, condition ($ii$) is satisfied.

Assume that (ii) holds. Since $\eta \mid \xi$ by Lemma 4.3(b), and since $\deg(\xi) = \dim(\mathcal{V}_{\mathbb{F}})$, it follows that $\xi = \eta$, whence condition (iii) holds.

Finally, in order to verify the implication "(iii) $\Rightarrow$ (i)", (recall from Lemma 4.3(a) that $\xi \in \mathbb{K}[x]$ and) suppose that ξ is irreducible over $\mathbb{K}$. Since $\eta \mid \xi$ by Lemma 4.3(b), we get $\eta = \xi$, and in particular, η is irreducible over $\mathbb{K}$. Then (4.5) holds. Since $\deg(\eta) = \deg(\xi)$, Equation (4.5) yields $\dim(\mathcal{V}_{\mathbb{K}[\ell]}) = t$. By [20, Corollary 2.5]) this proves that g is irreducible. □

Lemma 4.7. *Let $\sigma \in \mathrm{Aut}(\mathbb{F})$ and let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of σ. For $i \in \{1, 2\}$ let g_i be an irreducible, σ-semilinear element of $\Gamma\mathrm{L}(\mathcal{V})$, and let $\ell_i \in \mathrm{GL}(\mathcal{V})$ be the linear part of g_i. The following are equivalent.*

(a) *There exists an element $h \in \mathrm{GL}(\mathcal{V}_{\mathbb{F}})$ such that $h^{-1}g_1h = g_2$.*

(b) *The elements ℓ_1, ℓ_2 are conjugate in $\mathrm{GL}(\mathcal{V}_{\mathbb{F}})$.*

(c) *The elements $(\ell_1)_{\mathbb{K}}, (\ell_2)_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$ have the same minimal polynomial.*

(d) *The elements $\ell_1, \ell_2 \in \mathrm{GL}(\mathcal{V}_{\mathbb{F}})$ have the same characteristic polynomial.*

Proof. By [20, Theorem 2.10(a) and Proposition 3.1][(I)] conditions (a), (b), (c)

[(I)] The notation used in [20] is explained in (the first paragraph of) the proof of Proposition 4.6.

are equivalent. Let $i \in \{1, 2\}$. Since g_i is irreducible, by Proposition 4.6(a) the characteristic polynomial of ℓ_i is equal to the minimal polynomial of $(\ell_i)_{\mathbb{K}}$. This shows the equivalence of (c) and (d). □

Suppose that we are in the situation of Lemma 4.7. In Corollary 4.27(a) below, we give another equivalent condition to g_1, g_2 being conjugate in $\mathrm{GL}(\mathcal{V}_{\mathbb{F}})$. More precisely, we prove that g_1, g_2 are conjugate in $\mathrm{GL}(\mathcal{V}_{\mathbb{F}})$ if and only if g_1, g_2 have the same characteristic polynomial on $\mathcal{V}_{\mathbb{K}}$.

Elements in $\mathrm{GL}(\mathcal{V})$ are associated with the trivial field automorphism on $\mathbb{F}$. Thus, if $g \in \mathrm{GL}(\mathcal{V})$, then the fixed field of its associated field automorphism is $\mathbb{F}$ and the linear part of g is g itself. Using Proposition 4.6 and Lemma 4.7 we obtain the following well-known results on irreducible elements in $\mathrm{GL}(\mathcal{V})$.

Lemma 4.8. (a) *An element of* $\mathrm{GL}(\mathcal{V})$ *is irreducible if and only if its characteristic polynomial is irreducible over* $\mathbb{F}$.

(b) *Two irreducible elements in* $\mathrm{GL}(\mathcal{V})$ *are conjugate in* $\mathrm{GL}(\mathcal{V})$ *if and only if they have the same characteristic polynomial.*

4.2.2 Construction

A finite field can be naturally considered as a vector space over any of its subfields. Suppose that $\mathbb{V}$ is an extension field of $\mathbb{F}$. We write $\mathbb{V}_{\mathbb{F}}$ to denote $\mathbb{V}$ viewed as a vector space over $\mathbb{F}$. Observe that $\dim(\mathbb{V}_{\mathbb{F}}) = |\mathbb{V} : \mathbb{F}|$.

It is well known (see [33, Satz 3.10, p. 165]) that an irreducible element $g \in \mathrm{GL}(\mathbb{V}_{\mathbb{F}})$ is conjugate in $\mathrm{GL}(\mathbb{V}_{\mathbb{F}})$ to a mapping

$$\mathbb{V}_{\mathbb{F}} \to \mathbb{V}_{\mathbb{F}}, \quad v \mapsto v\omega,$$

where ω is an element of $\mathbb{V}^*$ which does not lie in any proper subfield of $\mathbb{V}$ containing $\mathbb{F}$. (We can choose ω to be any root of the characteristic polynomial of g, which, as we may recall from Lemma 4.8(a), is irreducible over $\mathbb{F}$). Dempwolff [20] generalises this result and presents a construction of irreducible elements in $\Gamma\mathrm{L}(\mathbb{V}_{\mathbb{F}})$. He shows that, if $\dim(\mathbb{V}_{\mathbb{F}})$ is coprime to the order of $\sigma \in \mathrm{Aut}(\mathbb{F})$, then an irreducible, non-singular, σ-semilinear mapping on $\mathbb{V}_{\mathbb{F}}$ is conjugate in $\mathrm{GL}(\mathbb{V}_{\mathbb{F}})$ to

$$\mathbb{V}_{\mathbb{F}} \to \mathbb{V}_{\mathbb{F}}, \quad v \mapsto v^{\gamma}\omega, \tag{4.6}$$

for some $\gamma \in \mathrm{Aut}(\mathbb{V})$ and $\omega \in \mathbb{V}^*$ (such that $|\gamma| = |\sigma|$ and the norm of ω over the fixed field of γ is a root of the characteristic polynomial of the linear part of g.) If $d = \gcd(\dim(\mathbb{V}_{\mathbb{F}}), |\sigma|) \neq 1$, then an irreducible, σ-semilinear element $g \in \Gamma\mathrm{L}(\mathbb{V}_{\mathbb{F}})$ transitively permutes the summands of a direct sum decomposition of $\mathbb{V}_{\mathbb{F}}$, which consists of d equal dimensional subspaces, and

moreover, the restriction of g^d to any of those subspaces has the form (4.6). We restate Dempwolff's construction [20, 3.3] in Lemma 4.9.

Consider a prime power q and $t \in \mathbb{N}$. Recall (from Section 3.5) that the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$ of $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$ consists of all automorphisms $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^t})$ satisfying $\alpha^\sigma = \alpha$ for all $\alpha \in \mathbb{F}_q$. The group $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$ is cyclic of order t and we have

$$\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q) = \left\{ \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}, \alpha \mapsto \alpha^{q^i} \mid 0 \leq i \leq t-1 \right\}. \tag{4.7}$$

The generators of $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$ are precisely the automorphisms of $\mathbb{F}_{q^t}$ with fixed field $\mathbb{F}_q$. They have the form $\mathbb{F}_{q^t} \to \mathbb{F}_{q^t}$, $\alpha \mapsto \alpha^{q^r}$ for some $r \in \mathbb{N}$ coprime to t. Let $\omega \in \mathbb{F}_{q^t}$. Recall that the norm $\mathrm{N}_{\mathbb{F}_{q^t}:\mathbb{F}_q}(\omega)$ of ω over $\mathbb{F}_q$ is given by $\mathrm{N}_{\mathbb{F}_{q^t}:\mathbb{F}_q}(\omega) = \prod_{i=0}^{t-1} \omega^{q^i} \in \mathbb{F}_q$. Equivalently, by (4.7) we get

$$\mathrm{N}_{\mathbb{F}_{q^t}:\mathbb{F}_q}(\omega) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} \omega^\sigma.$$

The mapping assigning to each element of $\mathbb{F}_{q^t}$ its norm over $\mathbb{F}_q$ is surjective (see [42, Theorem 2.28$(i)(ii)$]).

If m, t are positive integers with $\gcd(m,t) = d$, then (by Bezout's identity) there exists an integer c satisfying $cm \equiv d \pmod{t}$. The integer c is not uniquely determined. In fact, $c'm \equiv d \pmod{t}$ if and only if $c' = c + kt/d$ for some $k \in \mathbb{Z}$ (see [41, Theorem $2-6$]). In Lemma 4.9 below we shall consider the cm-th power of an element $\widehat{\sigma} \in \mathrm{Gal}(\mathbb{F}_{q^{mt/d}} : \mathbb{F}_q)$. Since $\widehat{\sigma}^{ktm/d}$ is the identity on $\mathbb{F}_{q^{mt/d}}$, we get

$$\alpha^{\widehat{\sigma}^{(c+kt/d)m}} = \left(\alpha^{\widehat{\sigma}^{cm}}\right)^{\widehat{\sigma}^{ktm/d}} = \alpha^{\widehat{\sigma}^{cm}}$$

for all $\alpha \in \mathbb{F}_{q^{mt/d}}$ and all $k \in \mathbb{Z}$. This shows that the automorphism $\widehat{\sigma}^{cm}$ does not depend on the choice of c.

We are now ready to state Lemma 4.9 which is based on [20, 3.3].

Lemma 4.9. *Assume the following.*

- *Let q be a prime power, let $m, t \in \mathbb{N}$, and let $d = \gcd(m,t)$.*
- *Let $\omega \in \mathbb{F}^*_{q^{mt/d}}$ be such that the norm $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ of ω over $\mathbb{F}_{q^m}$ does not lie in any proper subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$.*
- *Let σ be a generator of the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$.*
- *Let $r \in \mathbb{N}$ be such that $\alpha^\sigma = \alpha^{q^r}$ for all $\alpha \in \mathbb{F}_{q^t}$, and let $\widehat{\sigma} \in \mathrm{Aut}(\mathbb{F}_{q^{mt/d}})$ be (an extension of σ) given by $\alpha^{\widehat{\sigma}} = \alpha^{q^r}$ $(\alpha \in \mathbb{F}_{q^{mt/d}})$.*
- *Let $c \in \mathbb{N}$ satisfy $cm \equiv d \pmod{t}$, and let $\gamma = \widehat{\sigma}^{cm} \in \mathrm{Aut}(\mathbb{F}_{q^{mt/d}})$.*

- *Let* $\rho = \gamma\widehat{\sigma}^{-d+1} \in \mathrm{Aut}(\mathbb{F}_{q^{mt/d}})$.
- *Let* $\mathbb{V} = \mathbb{F}_{q^{mt}}$, *and let* $\{b_1, \ldots, b_d\}$ *be an* $\mathbb{F}_{q^{mt/d}}$*-basis of* $\mathbb{V}$.

Consider the mapping $r_{\sigma,\omega} : \mathbb{V}_{\mathbb{F}_{q^t}} \to \mathbb{V}_{\mathbb{F}_{q^t}}$ *given by*

$$\alpha_1 b_1 + \alpha_2 b_2 + \cdots + \alpha_d b_d \;\mapsto\; \alpha_d^{\rho}\omega b_1 + \alpha_1^{\widehat{\sigma}} b_2 + \cdots + \alpha_{d-1}^{\widehat{\sigma}} b_d$$

(for all $\alpha_1, \ldots, \alpha_d \in \mathbb{F}_{q^{mt/d}}$*). Let* $\eta \in \mathbb{F}_q[x]$ *be the minimal polynomial of* $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ *over* $\mathbb{F}_q$*. Then the following hold.*

(*a*) *The mapping* $r_{\sigma,\omega}^t$ *is* $\mathbb{F}_{q^t}$*-linear. Its minimal polynomial on* $\mathbb{V}_{\mathbb{F}_q}$ *equals* η*. In particular, the minimal polynomial of* $r_{\sigma,\omega}^t$ *on* $\mathbb{V}_{\mathbb{F}_q}$ *is irreducible of degree* m*.*

(*b*) *The mapping* $r_{\sigma,\omega}$ *is* σ*-semilinear, non-singular, and irreducible.*

(*c*) *Let* $g \in \Gamma\mathrm{L}(\mathbb{V}_{\mathbb{F}_{q^t}})$ *be irreducible with associated field automorphism* σ*. The following are equivalent.*

  (*i*) *The elements* g *and* $r_{\sigma,\omega}$ *are conjugate in* $\mathrm{GL}(\mathcal{V}_{\mathbb{F}_{q^t}})$.

  (*ii*) $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ *is a root of the minimal polynomial of* g^t *on* $\mathbb{V}_{\mathbb{F}_q}$.

  (*iii*) $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ *is a root of the characteristic polynomial of* g^t *on* $\mathbb{V}_{\mathbb{F}_{q^t}}$.

Proof. Let $\beta = \mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$. By definition, η is irreducible. Since, by assumption, β does not lie in any subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$, by Lemmas 3.3, 3.4 we have $\deg(\eta) = m$. Note that $|\sigma| = t$.

(*a*) As we may read off the definition of $r_{\sigma,\omega}$ (or look it up in [20, 3.3]), we have

$$r_{\sigma,\omega}^t : \mathbb{V}_{\mathbb{F}_{q^t}} \to \mathbb{V}_{\mathbb{F}_{q^t}}, \quad \left(\sum_{i=1}^{d} \alpha_i b_i\right) \;\mapsto\; \sum_{i=1}^{d} \alpha_i \beta^{\widehat{\sigma}^{i-1}} b_i. \tag{4.8}$$

Hence, $r_{\sigma,\omega}^t$ is $\mathbb{F}_{q^t}$-linear. Since $\eta \in \mathbb{F}_q[x]$ is the minimal polynomial of β over $\mathbb{F}_q$, the polynomial $\eta^{\widehat{\sigma}^i}$ (by which we mean the polynomial obtained by applying $\widehat{\sigma}^i$ to every coefficient of η) is the minimal polynomial of $\beta^{\widehat{\sigma}^i}$ over $\mathbb{F}_q$. By definition, $\widehat{\sigma}$ fixes each element of $\mathbb{F}_q$. Since $\eta \in \mathbb{F}_q[x]$ we see that $\eta = \eta^{\widehat{\sigma}^i}$ for all $i \in \{1, \ldots, d-1\}$. Hence, η is the minimal polynomial over $\mathbb{F}_q$ of $\beta^{\widehat{\sigma}^i}$ for all $i \in \{0, \ldots, d-1\}$. Then, using (4.8), we obtain

$$\eta\big(r_{\sigma,\omega}^t\big) : \mathbb{V}_{\mathbb{F}_{q^t}} \to \mathbb{V}_{\mathbb{F}_{q^t}}, \quad \left(\sum_{i=1}^{d} \alpha_i b_i\right) \;\mapsto\; \sum_{i=1}^{d} \alpha_i \underbrace{\eta\big(\beta^{\widehat{\sigma}^{i-1}}\big)}_{=0} b_i = 0,$$

that is

$$\eta(r_{\sigma,\omega}^t) = 0.$$

Since the minimal polynomial of $r_{\sigma,\omega}^t$ on $\mathbb{F}_q$, say η', divides any polynomial over $\mathbb{F}_q$ which annihilates $r_{\sigma,\omega}^t$, we get $\eta' \mid \eta$. This proves the assertion because ($\deg(\eta') \neq 0$ and) η is irreducible over $\mathbb{F}_q$.

(*b*) Note that $(\gamma\widehat{\sigma}^{-d+1})|_{\mathbb{F}_{q^t}} = \widehat{\sigma}|_{\mathbb{F}_{q^t}} = \sigma$. Hence, for all $\alpha \in \mathbb{F}_{q^t}$ and all $v \in \mathbb{V}_{\mathbb{F}_{q^t}}$, we have $(\alpha v)r_{\sigma,\omega} = \alpha^\sigma v r_{\sigma,\omega}$. Further, $(v_1 + v_2)r_{\sigma,\omega} = v_1 r_{\sigma,\omega} + v_2 r_{\sigma,\omega}$ for all $v_1, v_2 \in \mathbb{V}_{\mathbb{F}_{q^t}}$. This shows that $r_{\omega,\sigma}$ is σ-semilinear. Since $\ker(r_{\sigma,\omega}) = \{0\}$, the mapping $r_{\sigma,\omega}$ is non-singular.

From part (*a*) of the current lemma we know that the minimal polynomial of $r_{\sigma,\omega}^t$ on $\mathbb{V}_{\mathbb{F}_q}$ is irreducible (over $\mathbb{F}_q$) of degree $m = \dim(\mathbb{V}_{\mathbb{F}_{q^t}})$. Then by Proposition 4.6(*b*), $r_{\sigma,\omega}$ is irreducible.

(*c*) Since $|\sigma| = t$, the linear part of g is given by g^t. Since g is irreducible, by Proposition 4.6(*a*) the minimal polynomial of g^t on $\mathbb{V}_{\mathbb{F}_q}$ equals the characteristic polynomial of g^t on $\mathbb{V}_{\mathbb{F}_{q^t}}$. In order to show the assertion it thus suffices to verify the equivalence of conditions (*i*) and (*ii*).

Let η' be the minimal polynomial of g^t on $\mathbb{V}_{\mathbb{F}_q}$. Recall that η denotes the minimal polynomial of $\beta = \mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ over $\mathbb{F}_q$. Since g is irreducible, by Proposition 4.6(*b*) the polynomial η' is irreducible over $\mathbb{F}_q$. Thus, condition (*ii*) holds if and only if $\eta' = \eta$, that is (by part (*a*) of the current lemma) if and only if η' equals the minimal polynomial of $r_{\sigma,\omega}^t$ on $\mathbb{V}_{\mathbb{F}_q}$. By Lemma 4.7, the latter is equivalent to condition (*i*). □

The order of an element $g \in \Gamma\mathrm{L}(\mathcal{V})$ is the product of the orders of its linear part and its associated field automorphism. If g is irreducible, then the order of its linear part satisfies the following.

Lemma 4.10. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$ be irreducible, and let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of its associated field automorphism. Let $\ell \in \mathrm{GL}(\mathcal{V})$ be the linear part of g, and let $\eta \in \mathbb{K}[x]$ be the minimal polynomial of $\ell_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$. Let β be a root of η. Then the following hold.*

(*a*) *The order of ℓ equals $|\beta|$.*

(*b*) *We have $\mathrm{ord}(|\mathbb{K}|; |\ell|) = \dim(\mathcal{V})$. In particular, $|\ell|$ divides $|\mathbb{K}|^{\dim(\mathcal{V})} - 1$.*

Proof. Let $m = \dim(\mathcal{V}_{\mathbb{F}})$, let $t = |\mathbb{F} : \mathbb{K}|$, and let $q = |\mathbb{K}|$ (whence $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_{q^t}$.) We identify $\mathcal{V}$ with the finite field $\mathbb{F}_{q^{mt}}$ viewed as a vector space over $\mathbb{F}_{q^t}$. Let $d = \gcd(m, t)$, let σ be the field automorphism associated with g, and let $\omega \in \mathbb{F}_{q^{mt/d}}^*$ be such that $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega) = \beta$. (Recall that the norm map is surjective, which is why ω exists.) Define $r_{\sigma,\omega}$ as in Lemma 4.9.

Then by Lemma 4.9(c) the elements g and $r_{\sigma,\omega}$ are conjugate in $\mathrm{GL}(\mathcal{V})$, and in particular $|g| = |r_{\sigma,\omega}|$. Since $\ell = g^{|\sigma|} = g^t$, it follows that

$$|\ell| = |r_{\sigma,\omega}^t|.$$

(a) The mapping $r_{\sigma,\omega}^t$ is given in (4.8). Thus,

$$|r_{\sigma,\omega}^t| = \gcd\big(|\beta|, |\beta^{\widehat{\sigma}}|, \ldots, |\beta^{\widehat{\sigma}^{d-1}}|\big),$$

where $\widehat{\sigma}$ is as defined in Lemma 4.9. Since $|\beta| = |\beta^{\widehat{\sigma}^{i-1}}|$ for all $i \in \{1, \ldots, d\}$, recalling that $|\ell| = |r_{\sigma,\omega}^t|$, we obtain $|\ell| = |\beta|$.

(b) By Proposition 4.6(b) the polynomial η is irreducible of degree m. Then $\beta \neq 0$ and Lemma 3.4 yields $\mathrm{ord}(q; |\beta|) = m$. In particular, $|\beta|$ is a divisor of $q^m - 1$ (by Lemma 2.11). Then the assertion follows by part (a) of the current lemma. □

For convenience, we restate the linear case of Lemma 4.10.

Lemma 4.11. *Let $g \in \mathrm{GL}(\mathcal{V})$ be irreducible, and let β be a root of the characteristic/minimal polynomial of g. Then the following hold.*

(a) *We have $|g| = |\beta|$.*

(b) *Let $q = |\mathbb{F}|$ and $m = \dim(\mathcal{V})$. Then $\mathrm{ord}(q; |g|) = m$. In particular, $|g|$ divides $q^m - 1$.*

Proof. Consider g as an element of $\Gamma\mathrm{L}(\mathcal{V})$. Then g is associated with the trivial field automorphism on $\mathbb{F}$. Hence, the fixed field of that field automorphism is $\mathbb{F}$, and the linear part of g is g itself. By Proposition 4.6(a) the minimal polynomial of g coincides with the characteristic polynomial of g. The assertion then holds by Lemma 4.10. □

While according to Lemma 4.11(b) an irreducible element $g \in \mathrm{GL}(\mathcal{V})$ satisfies $\mathrm{ord}(|\mathbb{F}|; |g|) = \dim(\mathcal{V})$, we emphasise that the inverse implication is not true. (A counterexample is given in Example 5.5.) However, if we assume that g lies in an irreducible cyclic subgroup of $\mathrm{GL}(\mathcal{V})$, then the fact that $\mathrm{ord}(|\mathbb{F}|; |g|) = \dim(\mathcal{V})$ does imply that g is irreducible.

Lemma 4.12. *Let $g \in \mathrm{GL}(\mathcal{V})$ be irreducible, let $q = |\mathbb{F}|$, and let $m = \dim(\mathcal{V})$. An element $h \in \langle g \rangle$ is irreducible if and only if $\mathrm{ord}(q; |h|) = m$.*

Proof. If h is irreducible, then by Lemma 4.11(b) we have $\mathrm{ord}(q; |h|) = m$.

So suppose that $\mathrm{ord}(q; |h|) = m$. Let $\ell \in \mathbb{N}$ be such that $h = g^\ell$ and let β be a root of the characteristic polynomial of g. By Lemma 4.11(a) we have

$|g| = |\beta|$. Hence, $|h| = |\beta^\ell|$, and thus (by assumption) $\operatorname{ord}\big(q; |\beta^\ell|\big) = m$. Since β^ℓ is a root of the characteristic polynomial of h, the assertion follows from Lemmas 3.4, 4.8(a). □

The following is well-known and can be found for example in [33, p. 588, Hilfssatz 19.6].

Lemma 4.13. *Let G be a finite group, let $g \in G$, and let p be a prime. Then there exist uniquely determined elements $g_1, g_2 \in \langle g\rangle$ such that $|g_1|$ is a power of p, $|g_2|$ is coprime to p, and $g = g_1 g_2 = g_2 g_1$.*

Definition 4.14. In the situation of Lemma 4.13 the element g_1 is called the *p-part* of g, and the element g_2 is referred to as the *p'-part* of g. We write g_p and $g_{p'}$ to denote the p-part, and respectively, the p'-part, of g.

Lemma 4.15. *Let p be the characteristic of $\mathbb{F}$ and let $g \in \mathrm{GL}(\mathcal{V})$. Suppose that $\langle g\rangle$ acts irreducibly on a non-trivial subspace $\mathcal{U} \leq \mathcal{V}$. Then $(g_{p'})|_{\mathcal{U}} = g|_{\mathcal{U}}$.*

In particular, $\mathcal{U}$ is $\langle g_{p'}\rangle$-irreducible.

Proof. Since the elements g_p and $g_{p'}$ are powers of g, $\mathcal{U}$ is $\langle g_{p'}\rangle$-invariant and $\langle g_p\rangle$-invariant. Recalling that $g = g_p g_{p'} = g_{p'} g_p$, it follows that

$$g|_{\mathcal{U}} = (g_{p'})|_{\mathcal{U}}\,(g_p)|_{\mathcal{U}} = (g_p)|_{\mathcal{U}}\,(g_{p'})|_{\mathcal{U}}. \tag{4.9}$$

Moreover, we have

$$g|_{\mathcal{U}} = (g|_{\mathcal{U}})_{p'}\,(g|_{\mathcal{U}})_p = (g|_{\mathcal{U}})_p\,(g|_{\mathcal{U}})_{p'}.$$

Since p does not divide the orders of $(g_{p'})|_{\mathcal{U}}$ and $(g|_{\mathcal{U}})_{p'}$, and because the orders of $(g_p)|_{\mathcal{U}}$ and $(g|_{\mathcal{U}})_p$ are powers of p, using Lemma 4.13 we conclude that

$$\begin{aligned} (g|_{\mathcal{U}})_{p'} &= (g_{p'})|_{\mathcal{U}}, \\ (g|_{\mathcal{U}})_p &= (g_p)|_{\mathcal{U}}. \end{aligned} \tag{4.10}$$

Now, since $\mathcal{U}$ is $\langle g\rangle$-irreducible, by Lemma 4.11(b) the order of $g|_{\mathcal{U}}$ is coprime to p. Thus $(g|_{\mathcal{U}})_p = \mathrm{id}_{\mathcal{U}}$, that is by (4.10) we have $(g_p)|_{\mathcal{U}} = \mathrm{id}_{\mathcal{U}}$. Then (4.9) yields $(g_{p'})|_{\mathcal{U}} = g|_{\mathcal{U}}$. In particular, $\mathcal{U}$ is $\langle g_{p'}\rangle$-irreducible. □

We conclude this section considering the characteristic polynomial of an irreducible element in $\mathrm{GL}(\mathcal{V})$ viewed as a linear mapping over some subfield $\mathbb{K}$ of $\mathbb{F}$. Recall from Definition 3.37 that the Galois-twist over $\mathbb{K}$ of a polynomial $f \in \mathbb{F}[x]$ is given by $\prod_{\sigma\in\mathrm{Gal}(\mathbb{F}:\mathbb{K})} f^\sigma$ (where f^σ denotes the polynomial in $\mathbb{F}[x]$ obtain by applying σ to each coefficient of f). Recall further that $\prod_{\sigma\in\mathrm{Gal}(\mathbb{F}:\mathbb{K})} f^\sigma \in \mathbb{K}[x]$.

Lemma 4.16. *Let $g \in \mathrm{GL}(\mathcal{V})$ be irreducible and let $\mathbb{K}$ be a subfield of $\mathbb{F}$. The characteristic polynomial of $g_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$ is the Galois-twist over $\mathbb{K}$ of the characteristic/minimal polynomial of g.*

Proof. Let $m = \dim(\mathcal{V}_{\mathbb{F}})$. Assume that $\mathbb{F} = \mathbb{F}_{q^t}$ and $\mathbb{K} = \mathbb{F}_q$. We identify $\mathcal{V}$ with the field $\mathbb{F}_{q^{mt}}$ viewed as vector space over $\mathbb{F}_{q^t}$.

Let $f \in \mathbb{F}_{q^t}[x]$ be the characteristic polynomial of g and let ω be a root of f. By Lemma 4.8(a), the polynomial f is irreducible. (Hence, f is also the minimal polynomial of g). By Lemmas 3.3, 3.4, the element ω lies in $\mathbb{F}^*_{q^{mt}}$ but in no proper subfield of $\mathbb{F}_{q^{mt}}$ containing $\mathbb{F}_{q^t}$. Then by Lemma 4.9(c), applied to $(q^t, m, 1)$ instead of (q, m, t), g is conjugate in $\mathrm{GL}(\mathcal{V})$ to

$$r_\omega : \mathbb{F}_{q^{mt}} \to \mathbb{F}_{q^{mt}}, \quad v \mapsto v\omega.$$

Let $\eta \in \mathbb{F}_q[x]$ be the minimal polynomial of ω over $\mathbb{F}_q$. Then η is the monic, irreducible polynomial of minimal degree over $\mathbb{F}_q$ to annihilate (ω and thus also) r_ω. Thus, η is the minimal polynomial of $(r_\omega)_{\mathbb{F}_q}$, and hence also the minimal polynomial of $g_{\mathbb{F}_q}$. Let $d = \mathrm{ord}(q; |\omega|)$. By Lemma 3.2($b$) we get

$$\eta = \prod_{i=0}^{d-1} (x - \omega^{q^i}).$$

Let $\widehat{f}$ be the characteristic polynomial of $g_{\mathbb{F}_q}$. Then $\widehat{f}$ is a power of η, whence

$$\begin{aligned} \widehat{f} = \left(\prod_{i=0}^{d-1} (x - \omega^{q^i}) \right)^{mt/d} &= \prod_{i=0}^{mt-1} (x - \omega^{q^i}) \\ &= \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)} \prod_{i=0}^{m-1} (x - \omega^{q^{ti}})^\sigma. \end{aligned}$$

This proves the assertion, because (recalling that $f \in \mathbb{F}_{q^t}[x]$ is irreducible) by Lemma 3.2(b) we have $f = \prod_{i=0}^{m-1} (x - \omega^{q^{ti}})$. □

4.3 Counting irreducible semilinear mappings

Consider an element $g \in \Gamma\mathrm{L}(\mathcal{V})$ and let σ be the field automorphism associated with g. The coset $g\mathrm{GL}(\mathcal{V})$ consists of all elements in $\Gamma\mathrm{L}(\mathcal{V})$ which are σ-semilinear. Since $h^{-1}gh$ is again σ-semilinear for all $h \in \mathrm{GL}(\mathcal{V})$, and because by Lemma 4.5 conjugation (with elements from $\mathrm{GL}(\mathcal{V})$) does not change whether or not an element in $g\mathrm{GL}(\mathcal{V})$ is irreducible, it follows that $\mathrm{GL}(\mathcal{V})$ acts via conjugation on the set of all irreducible elements in $g\mathrm{GL}(\mathcal{V})$.

Lemma 4.17. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$ and let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of the automorphism associated with g. Let $\mathfrak{I}$ be the set of all orbits of irreducible elements in $g\mathrm{GL}(\mathcal{V})$ under conjugation by $\mathrm{GL}(\mathcal{V})$. By mapping a representative r of each orbit in $\mathfrak{I}$ onto the minimal polynomial on $\mathcal{V}_{\mathbb{K}}$ of the linear part of r, we obtain a bijection*

$$\mathfrak{I} \to \big\{ f \in \mathbb{K}[x] \mid f \neq x, f \text{ monic, irreducible}, \deg(f) = \dim(\mathcal{V}) \big\}.$$

Proof. Let σ be the field automorphism associated with g.

Let $h \in g\mathrm{GL}(\mathcal{V})$ be irreducible. Then h is σ-semilinear. Let f be the minimal polynomial on $\mathcal{V}_{\mathbb{K}}$ of the linear part of h. Then $f \neq x$ and f is monic. Further, according to Proposition 4.6(b) the polynomial f is irreducible and $\deg(f) = \dim(\mathcal{V})$. Hence, by mapping a representative r of each orbit in $\mathfrak{I}$ onto the minimal polynomial on $\mathcal{V}_{\mathbb{K}}$ of the linear part of r, we obtain a mapping

$$\iota : \mathfrak{I} \to \big\{ f \in \mathbb{K}[x] \mid f \neq x, f \text{ monic, irreducible}, \deg(f) = \dim(\mathcal{V}) \big\}.$$

Observe that ι does not depend on the choice of the respective representative r.

By Lemma 4.7, ι is injective. In order to verify that ι is surjective, let $f \neq x$ be a monic and irreducible polynomial of degree $\dim(\mathcal{V})$ over $\mathbb{K}$. Let $m = \dim(\mathcal{V})$, $t = |\sigma|$, $d = \gcd(m, t)$, and $q = |\mathbb{K}|$. (Then $\mathbb{K} = \mathbb{F}_q$ and $\mathbb{F} = \mathbb{F}_{q^t}$.) We identify $\mathcal{V}$ with the finite field $\mathbb{F}_{q^{mt}}$ viewed as a vector space over $\mathbb{F}_{q^t}$. By Lemma 3.2(d), all roots of f lie in $\mathbb{F}_{q^m}^*$. Choose $\omega \in \mathbb{F}_{q^{mt/d}}^*$ such that $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ is a root of f. (The element ω exists because the norm map is surjective.) Then f is the minimal polynomial of $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ over $\mathbb{F}_q$. Since f is irreducible over $\mathbb{F}_q$ with $\deg(f) = m$, by Lemmas 3.3, 3.4 the element $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ lies in $\mathbb{F}_{q^m}$, but does not lie in any proper subfield of $\mathbb{F}_{q^m}$ containing $\mathbb{F}_q$. Further, (recalling that $|\sigma| = t$) we have $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$. Let $r_{\sigma,\omega}$ be as defined in Lemma 4.9. Then $r_{\sigma,\omega}^t$ is the linear part of $r_{\sigma,\omega}$. By Lemma 4.9(a) the minimal polynomial of $r_{\sigma,\omega}^t$ on $\mathcal{V}_{\mathbb{K}}$ is equal to f. Moreover, by Lemma 4.9(b), $r_{\sigma,\omega}$ is an irreducible, σ-semilinear element of $\Gamma\mathrm{L}(\mathcal{V})$. □

For a group G, a subgroup $H \leq G$, and a subset $\mathcal{X} \subseteq G$, the *centraliser* of $\mathcal{X}$ in H is given by $C_H(X) = \{h \in H \mid xh = hx \text{ for all } x \in X\}$. In order to simplify notation, we write $C_H(g)$ instead of $C_H(\langle g\rangle)$.

Proposition 4.18. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$ be irreducible and let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of its associated field automorphism. The centraliser $C_{\mathrm{GL}(\mathcal{V})}(g)$ of $\langle g\rangle$ in $\mathrm{GL}(\mathcal{V})$ is cyclic of order $|\mathbb{K}|^{\dim(\mathcal{V}_{\mathbb{F}})} - 1$.*

Proof. For $\omega \in \mathbb{F}^*$, let r_ω denote the element of $\mathrm{GL}(\mathcal{V}_{\mathbb{K}})$ given by $v \mapsto v\omega$. Let $R = \{r_\omega \mid \omega \in \mathbb{F}^*\} \leq \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$. Let $m = \dim(\mathcal{V}_{\mathbb{F}})$, let $\{v_1, \ldots, v_m\}$ be a

basis of $\mathcal{V}_{\mathbb{F}}$, and let $\mathcal{V}_i \leq \mathcal{V}_{\mathbb{F}}$ denote the $\mathbb{F}$-span of v_i ($i \in \{1, \ldots, m\}$). Then R acts irreducibly on each subspace $(\mathcal{V}_i)_{\mathbb{K}} \leq \mathcal{V}_{\mathbb{K}}$, and $\mathcal{V}_{\mathbb{K}} = (\mathcal{V}_1)_{\mathbb{K}} \oplus \cdots \oplus (\mathcal{V}_m)_{\mathbb{K}}$. By [33, Hilfssatz 3.11, p. 166], applied to $\mathfrak{G} = N_{\mathrm{GL}(\mathcal{V}_{\mathbb{K}})}(R) \leq \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$, $\mathfrak{A} = R$, and $V = \mathcal{V}_{\mathbb{K}} = (\mathcal{V}_1)_{\mathbb{K}} \oplus \cdots \oplus (\mathcal{V}_m)_{\mathbb{K}}$, the group $\mathrm{GL}(\mathcal{V}_{\mathbb{F}})$ is equal to the centraliser of R in $N_{\mathrm{GL}(\mathcal{V}_{\mathbb{K}})}(R)$, which in turn is equal to $C_{\mathrm{GL}(\mathcal{V}_{\mathbb{K}})}(R)$. Thus,

$$C_{\mathrm{GL}(\mathcal{V}_{\mathbb{F}})}(g) = C_{\mathrm{GL}(\mathcal{V}_{\mathbb{K}})}\big(\langle R, g\rangle\big).$$

By [20, Lemma 2.1(b)] the group $\langle R, g\rangle$ acts irreducibly on $\mathcal{V}_{\mathbb{K}}$, which is why (using Schur's Lemma) we get

$$C_{\mathrm{GL}(\mathcal{V}_{\mathbb{K}})}\big(\langle R, g\rangle\big) = C_{\mathrm{End}(\mathcal{V}_{\mathbb{K}})}\big(\langle R, g\rangle\big) \setminus \{\mathbf{0}\},$$

where $\mathbf{0}$ denotes the zero element in $\mathrm{End}(\mathcal{V}_{\mathbb{K}})$. Further, writing ℓ for the linear part of g, [20, Theorem 2.4] yields

$$C_{\mathrm{End}(\mathcal{V}_{\mathbb{K}})}\big(\langle R, g\rangle\big) = \mathbb{K}[\ell].$$

The combination of the three equations above reveals that

$$C_{\mathrm{GL}(\mathcal{V}_{\mathbb{F}})}(g) = \mathbb{K}[\ell] \setminus \{\mathbf{0}\}.$$

Now, by Proposition 4.6(b) the minimal polynomial of ℓ on $\mathcal{V}_{\mathbb{K}}$ is irreducible of degree m. Thus, $\mathbb{K}[\ell]$ is an extension field of $\mathbb{K}$ with $|\mathbb{K}[\ell] : \mathbb{K}| = m$. Hence, $C_{\mathrm{GL}(\mathcal{V}_{\mathbb{F}})}(g) = \mathbb{K}[\ell]^*$ is cyclic of order $|\mathbb{K}|^m - 1$. □

We note that centralisers in $\mathrm{GL}(\mathcal{V})$ of irreducible elements from $\mathrm{GL}(\mathcal{V})$ are often referred to as *Singer cycles* in $\mathrm{GL}(\mathcal{V})$; see [33, p. 187, Satz 7.3(a)]. They are self-centralising and conjugate in $\mathrm{GL}(\mathcal{V})$.

For a prime power q and a positive integer m, recall from Definition 3.5 the notion of $N_q^*(m)$.

Lemma 4.19. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$, let $\mathbb{F}_q \subseteq \mathbb{F}$ be the fixed field of the automorphism associated with g, and let $m = \dim(\mathcal{V})$. The number of all irreducible elements in $g\mathrm{GL}(\mathcal{V})$ is equal to $N_q^*(m)|\mathrm{GL}(\mathcal{V})|/(q^m - 1)$.*

Proof. The group $\mathrm{GL}(\mathcal{V})$ acts via conjugation on the set of all irreducible elements in $g\mathrm{GL}(\mathcal{V})$. According to Lemma 4.17 this action has $N_q^*(m)$ orbits. By (the orbit-stabiliser-theorem and) Proposition 4.18 each orbit has length $|\mathrm{GL}(\mathcal{V})|/(q^m - 1)$. This yields a total of $N_q^*(m)|\mathrm{GL}(\mathcal{V})|/(q^m - 1)$ irreducible elements in $g\mathrm{GL}(\mathcal{V})$. □

Definition 4.20. Let A be a subset of $\Gamma\mathrm{L}(\mathcal{V})$. We write $\mathrm{irr}(A)$ for the proportion in A of all irreducible elements in A.

Corollary 4.21. *Let $q = |\mathbb{F}|$, $m = \dim(\mathcal{V})$, and $G = \mathrm{GL}(\mathcal{V})$. Then*

$$\mathrm{irr}(G) = \frac{N_q^*(m)}{q^m - 1}.$$

Moreover,

$$\frac{1}{m+1} \le \mathrm{irr}(G) \le \frac{1}{m}.$$

If $m \ge 2$, then the upper bound is not strict, that is $\mathrm{irr}(G) < 1/m$. If $m = 1$, then $\mathrm{irr}(G) = 1$.

Proof. By Lemma 4.19 (applied to $g = \mathrm{id}_{\mathcal{V}}$), $\mathrm{irr}(G)|G| = N_q^*(m)|G|/(q^m - 1)$, as asserted. The "moreover" part follows from Lemma 3.9(*c*). □

We next generalise Corollary 4.21 to subgroups of $\Gamma\mathrm{L}(\mathcal{V})$ containing $\mathrm{GL}(\mathcal{V})$. Let G be such a group and let

$$\nu : G \to \mathrm{Aut}(\mathbb{F}) \tag{4.11}$$

be the group homomorphism assigning to each $g \in G$ the field automorphism associated with g. Then (since $\mathrm{GL}(\mathcal{V})$ is the kernel of ν)

$$|G : \mathrm{GL}(\mathcal{V})| = |\mathrm{im}(\nu)|.$$

Hence, writing $\mathbb{K}$ for the fixed field of $\mathrm{im}(\nu)$, we have $|G : \mathrm{GL}(\mathcal{V})| = |\mathbb{F} : \mathbb{K}|$.

Theorem 4.22. *Let G be a group satisfying $\mathrm{GL}(\mathcal{V}) \le G \le \Gamma\mathrm{L}(\mathcal{V})$. Let $m = \dim(\mathcal{V})$, let $t = |G : \mathrm{GL}(\mathcal{V})|$, and let q be such that $\mathbb{F} = \mathbb{F}_{q^t}$. Then*

$$\mathrm{irr}(G) = \sum_{t_0 \mid t} \frac{\varphi(t_0) N_{q^{t/t_0}}^*(m)}{\big((q^{t/t_0})^m - 1\big)t}.$$

Moreover,

$$\frac{1}{m+1} \le \mathrm{irr}(G) \le \frac{1}{m}.$$

If $m \ge 2$, then the upper bound is not strict, that is $\mathrm{irr}(G) < 1/m$. If $m = 1$, then $\mathrm{irr}(G) = 1$.

Proof. Let ν be as defined in (4.11) above. Then

$$|\mathrm{im}(\nu)| = t$$

(and $\mathbb{F}_q$ is the fixed field of $\mathrm{im}(\nu)$). Moreover,

$$G = \{g \in \Gamma\mathrm{L}(\mathcal{V}) \mid g \text{ is } \sigma\text{-semilinear for some } \sigma \in \mathrm{im}(\nu)\}.$$

Observe that the fixed field of $\sigma \in \mathrm{im}(\nu)$ is given by $\mathbb{F}_{q^{t/|\sigma|}}$. Observe further that the group $\mathrm{im}(\nu)$ is cyclic. (Hence, for each divisor t_0 of t, there are precisely $\varphi(t_0)$ elements of order t_0 in $\mathrm{im}(\nu)$.) Recall that each coset of $\mathrm{GL}(\mathcal{V})$ in G consist of all elements in G which have the same associated field automorphism. Using Lemma 4.19 we conclude that there is a total of

$$\mathrm{irr}(G)|G| = \sum_{t_0|t} \frac{\varphi(t_0) N^*_{q^{t/t_0}}(m) |\mathrm{GL}(\mathcal{V})|}{(q^{t/t_0})^m - 1}$$

irreducible elements in G. Hence,

$$\mathrm{irr}(G) = \sum_{t_0|t} \frac{\varphi(t_0) N^*_{q^{t/t_0}}(m)}{\big((q^{t/t_0})^m - 1\big)t}, \tag{4.12}$$

as asserted. It remains to prove the "moreover" part. By Lemma 3.9(c) equation (4.12) yields

$$\begin{cases} \mathrm{irr}(G) = \displaystyle\sum_{t_0|t} \frac{\varphi(t_0)}{t}, & \text{if } m = 1, \\ \displaystyle\sum_{t_0|t} \frac{\varphi(t_0)}{t(m+1)} \le \mathrm{irr}(G) < \sum_{t_0|t} \frac{\varphi(t_0)}{tm}, & \text{if } m \ge 2. \end{cases}$$

Then the assertion holds by Lemma 2.2(a). □

4.4 Characteristic polynomial over the fixed field of the associated field automorphism

We use the construction in Lemma 4.9 to describe (in Proposition 4.26 below) the characteristic polynomial of an irreducible element $g \in \Gamma\mathrm{L}(\mathcal{V})$ on $\mathcal{V}_{\mathbb{K}}$, where $\mathbb{K}$ is the fixed field of the field automorphism associated with g. To this end, we need a few more results.

Proposition 4.23. *Suppose that $\mathcal{V} = \bigoplus_{i=1}^{d} \mathcal{V}_i$, where d is a divisor of $\dim(\mathcal{V})$ and $\mathcal{V}_1, \dots, \mathcal{V}_d \le \mathcal{V}$ are $\dim(\mathcal{V})/d$-dimensional subspaces of $\mathcal{V}$. Let $g \in \mathrm{GL}(\mathcal{V})$ satisfy $\mathcal{V}_i g = \mathcal{V}_{i+1}$ for $i \in \{1, \dots, d-1\}$ and $\mathcal{V}_d g = \mathcal{V}_1$. Let $f \in \mathbb{F}[x]$ be the characteristic polynomial of the restriction $g^d|_{\mathcal{V}_1}$. Then the characteristic polynomial of g is given by $f(x^d)$.*

Proof. Let $m = \dim(\mathcal{V})/d$, whence $\dim(\mathcal{V}_i) = m$ for all $i \in \{1, \dots, d\}$. Let $\mathbf{0}$ and $\mathbf{1}$ denote the $(m \times m)$-zero matrix, and respectively the $(m \times m)$-identity matrix, over $\mathbb{F}$. Let $\mathfrak{B} = \{v_1, \dots, v_{md}\}$ be a basis of $\mathcal{V}$ such that for $i \in$

$\{0,\dots,d-1\}$ we have $\mathcal{V}_1 g^i = \langle v_{im+1},\dots,v_{(i+1)m}\rangle$. Then the matrix $g_{\mathfrak{B}}$ with respect to $\mathfrak{B}$ equals

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & g_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & g_2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & g_{d-1} \\ g_d & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix},$$

for some $g_1,\dots,g_d \in \mathrm{GL}(m,|\mathbb{F}|)$. Let $h = g_1\cdots g_d \in \mathrm{GL}(m,|\mathbb{F}|)$. Observe that the matrix of $g^d|_{\mathcal{V}_1}$ with respect to $\{v_1,\dots,v_m\}$ is equal to h. Hence, f is the characteristic polynomial of h.

Let $\xi \in \mathbb{F}[x]$ be the characteristic polynomial of g. Observe that $g_{\mathfrak{B}}^d$ is a block diagonal matrix with diagonal blocks h, $g_1^{-1}hg_1$, $(g_1g_2)^{-1}h(g_1g_2)$, $\dots$, $(g_1\cdots g_{d-1})^{-1}h(g_1\cdots g_{d-1})$. Let b denote the block diagonal matrix with diagonal blocks $\mathbf{1}$, g_1, g_1g_2, $\dots$, $g_1\cdots g_{d-1}$. Then

$$bgb^{-1} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & \mathbf{1} \\ h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix},$$

whence $\xi(x) = \det(A)$, where

$$A = \begin{pmatrix} x\mathbf{1} & -\mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & x\mathbf{1} & -\mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & -\mathbf{1} \\ -h & \mathbf{0} & \cdots & \cdots & x\mathbf{1} \end{pmatrix}.$$

We next use elementary transformations of rows and columns, in order to transform A into a matrix A_d whose determinant is equal to $\det(A)$, and hence equal to $\xi(x)$. Set $A_0 = A$. For $i \in \{1,\dots,d-1\}$ we transform A_{i-1} into the matrix A_i by multiplying the i-th row of blocks of A_{i-1} by x and adding it to the $(i+1)$-th row of blocks of A_{i-1}. Then

$$A_{d-1} = \begin{pmatrix} x\mathbf{1} & -\mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ x^2\mathbf{1} & \mathbf{0} & -\mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ x^{d-1}\mathbf{1} & \vdots & & \ddots & -\mathbf{1} \\ x^d\mathbf{1} - h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix}.$$

Finally, let A_d be the matrix obtained from A_{d-1} by multiplying the $(i+1)$-th column of blocks (of A_{d-1}) by x^i and adding it to the first column of blocks (of A_{d-1}), for $i \in \{1, \dots, d-1\}$. Then

$$A_d = \begin{pmatrix} \mathbf{0} & -\mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & -\mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & -\mathbf{1} \\ x^d\mathbf{1} - h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix}.$$

After repeatedly applying Laplace expansion along the (respective) first line (for $m(d-1)$ times), we obtain

$$\begin{aligned} \det(A_d) &= \left((-1)(-1)^{(m+1)+1}\right)^{m(d-1)} \det(x^d\mathbf{1} - h) \\ &= (-1)^{(m+3)m(d-1)} \det(x^d\mathbf{1} - h) \\ &= \det(x^d\mathbf{1} - h) \\ &= f(x^d), \end{aligned}$$

which proves the assertion. □

Lemma 4.24. *Let $\mathbb{V}$ be an extension field of $\mathbb{F}$, let γ be a generator of $\mathrm{Gal}(\mathbb{V}:\mathbb{F})$, let $\omega \in \mathbb{V}^*$, and let $g \in \mathrm{GL}(\mathbb{V}_\mathbb{F})$ be given by $\alpha \mapsto \alpha^\gamma\omega$. Then there exists an element $\alpha_0 \in \mathbb{V}^*$ such that $\{\alpha_0, \alpha_0 g, \alpha_0 g^2, \dots, \alpha_0 g^{\dim(\mathbb{V}_\mathbb{F})-1}\}$ is a basis of $\mathbb{V}_\mathbb{F}$.*

Proof. Let $q = |\mathbb{F}|$ and $t = \dim(\mathbb{V}_\mathbb{F})$, whence $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{V} = \mathbb{F}_{q^t}$. Then the automorphism γ is given by $\alpha^\gamma = \alpha^{q^r}$ $(\alpha \in \mathbb{V})$ for some integer r coprime to t.

(*i*) As a first step, we assume that $r = 1$. Let $\eta \in \mathbb{F}[x]$ be the minimal polynomial of g. According to [46, Theorem 2.1] the assertion (for $r = 1$) is satisfied if and only if η is equal to the characteristic polynomial of g, that is if and only if $\deg(\eta) = t$. Seeking a contradiction, assume that $\deg(\eta) < t$. Say, $\eta(x) = \sum_{i=0}^{d} \beta_i x^i$ for some $d < t$ and $\beta_0, \dots, \beta_d \in \mathbb{F}$, $\beta_d \neq 0$. Then, for all $\alpha \in \mathbb{V}$, we get

$$0 = \alpha\left(\sum_{i=0}^{d} \beta_i g^i\right) = \sum_{i=0}^{d} \beta_i \alpha g^i = \beta_0\alpha + \sum_{i=1}^{d} \beta_i \alpha^{q^i} \omega^{(q^i-1)/(q-1)}.$$

Thus every $\alpha \in \mathbb{V}$ is a root of the polynomial

$$M(x) = \beta_0 x + \sum_{i=1}^{d} \beta_i \omega^{(q^i-1)/(q-1)} x^{q^i}.$$

But since M has degree q^d, it has at most $q^d < q^t = |\mathbb{V}|$ roots, which yields a contradiction.

(*ii*) Now, we (turn to the general case and) assume that r is a positive integer coprime to t. Let $c \in \mathbb{N}$ be such that $cr \equiv 1 \,(\mathrm{mod}\, t)$. Then

$$g^c : \mathbb{V}_{\mathbb{F}} \to \mathbb{V}_{\mathbb{F}}, \quad \alpha \mapsto \alpha^q \omega^{(q^{rc}-1)/(q^r-1)}.$$

By part (*i*) there exists $\alpha_0 \in \mathbb{V}^*$ such that the $\mathbb{F}$-span of the elements $\alpha_0, \alpha_0 g^c, \alpha_0 g^{2c}, \ldots \alpha_0 g^{(t-1)c}$ equals $\mathbb{V}_{\mathbb{F}}$. Let t_0 be the smallest positive integer such that $\alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t_0-1}$ are $\mathbb{F}$-linearly independent. Then $\langle \alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t_0-1} \rangle$ is $\langle g \rangle$-invariant. Since, for all $n \in \mathbb{N}$,

$$\alpha_0 g^n \in \langle \alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t_0-1} \rangle g^n = \langle \alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t_0-1} \rangle,$$

it follows that

$$\underbrace{\langle \alpha_0, \alpha_0 g^c, \alpha_0 g^{2c}, \ldots, \alpha_0 g^{(t-1)c} \rangle}_{=\mathbb{V}_{\mathbb{F}}} \leq \langle \alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t_0-1} \rangle.$$

Then $\langle \alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t_0-1} \rangle = \mathbb{V}_{\mathbb{F}}$, whence $t_0 = \dim(\mathbb{V}_{\mathbb{F}}) = t$ and the elements $\alpha_0, \alpha_0 g, \alpha_0 g^2, \ldots, \alpha_0 g^{t-1}$ form a basis of $\mathbb{V}_{\mathbb{F}}$. □

Lemma 4.25. *Suppose that we are in the situation of Lemma 4.9. The characteristic polynomial of $r_{\sigma,\omega}$ on $\mathbb{V}_{\mathbb{F}_q}$ is given by $\eta(x^t)$.*

Proof. Let $\mathbb{E} = \mathbb{F}_{q^{mt/d}}$. We may assume that $b_1 = 1$. (This is because, while $r_{\sigma,\omega}$ depends on the choice of the basis $\{b_1, \ldots, b_d\}$ as specified in Lemma 4.9, choosing a different basis results in an element conjugate to $r_{\sigma,\omega}$.) Then

$$\mathbb{V}_{\mathbb{F}_q} = \mathbb{E}_{\mathbb{F}_q} \oplus (\mathbb{E}_{\mathbb{F}_q}) r_{\sigma,\omega} \oplus \cdots \oplus (\mathbb{E}_{\mathbb{F}_q}) r_{\sigma,\omega}^{d-1}$$

and $(\mathbb{E}_{\mathbb{F}_q}) r_{\sigma,\omega}^d = \mathbb{E}_{\mathbb{F}_q}$. Thus, in order to prove the assertion, by Proposition 4.23 it suffices to show that the characteristic polynomial of the restriction $r_{\sigma,\omega}^d$ to $\mathbb{E}_{\mathbb{F}_q}$ is given by $\eta(x^{t/d})$.

To this end, recall (from Lemma 4.9) the definition of $\gamma \in \mathrm{Aut}(\mathbb{E})$. Being the m-th power of an automorphism which fixes (every element of) $\mathbb{F}_q$, γ acts trivially on $\mathbb{F}_{q^m}$. As shown in [20, p. 1203], we have $|\gamma| = t/d$, and thus

$$\langle \gamma \rangle = \mathrm{Gal}(\mathbb{E} : \mathbb{F}_{q^m}).$$

Let $h = r_{\sigma,\omega}^d|_{\mathbb{E}}$. According to the definition of $r_{\sigma,\omega}$, the mapping h is $\mathbb{F}_{q^m}$-linear. More precisely, for all $\alpha \in \mathbb{E}$ we have

$$\alpha h = \alpha^\gamma \omega.$$

Then, for all $\alpha \in \mathbb{E}$, we get $\alpha h^{t/d} = \alpha^{\gamma^{t/d}} \omega^{\gamma^{t/d-1}} \omega^{\gamma^{t/d-2}} \cdots \omega^\gamma \omega$, whence

$$\alpha h^{t/d} = \alpha \mathrm{N}_{\mathbb{E}:\mathbb{F}_{q^m}}(\omega).$$

Now, by Lemma 4.24 (applied to $\mathbb{F} = \mathbb{F}_{q^m}$ and $\mathbb{V} = \mathbb{E}$) there exists $\alpha_0 \in \mathbb{E}^*$ such that $\{\alpha_0 h^i \mid 0 \leq i \leq t/d - 1\}$ is an $\mathbb{F}_{q^m}$-basis of $\mathbb{E}$. Let $\mathcal{X}$ denote the $\mathbb{F}_{q^m}$-span of α_0, viewed as an $\mathbb{F}_q$-vector space. Then

$$\mathbb{E}_{\mathbb{F}_q} = \mathcal{X} \oplus \mathcal{X}h \oplus \cdots \oplus \mathcal{X}h^{t/d-1}.$$

Since $\alpha_0 h^{t/d} = \alpha_0 \mathrm{N}_{\mathbb{E}:\mathbb{F}_{q^m}}(\omega)$ (and since $\mathrm{N}_{\mathbb{E}:\mathbb{F}_{q^m}}(\omega) \in \mathbb{F}_{q^m}$) we further see that

$$\mathcal{X}h^{t/d} = \mathcal{X}.$$

We may thus (again) apply Proposition 4.23 and see that the characteristic polynomial of h on $\mathbb{E}_{\mathbb{F}_q}$ is equal to $\eta_0(x^{t/d})$ where η_0 is the characteristic polynomial of $h^{t/d}|_{\mathcal{X}}$. (It remains to show that $\eta_0 = \eta$.) Recall that $h^{t/d}|_{\mathcal{X}}$ is given by $\alpha \mapsto \alpha \mathrm{N}_{\mathbb{E}:\mathbb{F}_{q^m}}(\omega)$. Recall further (from the assumption) that η is the minimal polynomial of $\mathrm{N}_{\mathbb{E}:\mathbb{F}_{q^m}}(\omega)$ over $\mathbb{F}_q$. Since η is the (unique) monic polynomial of minimal degree over $\mathbb{F}_q$ which annihilates $\mathrm{N}_{\mathbb{E}:\mathbb{F}_{q^m}}(\omega)$, it is also the (unique) monic polynomial of minimal degree over $\mathbb{F}_q$ which annihilates $h^{t/d}|_{\mathcal{X}}$. Thus, η is the minimal polynomial of $h^{t/d}|_{\mathcal{X}}$. Since (as noted in the first paragraph of the proof of Lemma 4.9) $\deg(\eta) = m$, it follows that $\eta = \eta_0$, and the proof is complete. □

Recall that $\mathcal{V} \neq \{0\}$ is a finite vector space over $\mathbb{F}$.

Proposition 4.26. *Let $g \in \Gamma\mathrm{L}(\mathcal{V})$ be irreducible with associated field automorphism $\sigma \in \mathrm{Aut}(\mathbb{F})$. Let $\mathbb{K} \subseteq \mathbb{F}$ be the fixed field of σ and $t = |\sigma|$. Let $f \in \mathbb{K}[x]$ be the minimal polynomial on $\mathcal{V}_{\mathbb{K}}$ of the linear part of g. Then $f(x^t)$ is the characteristic polynomial of $g_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$.*

Proof. Let $m = \dim(\mathcal{V})$ and $q = |\mathbb{K}|$ (whence $\mathbb{K} = \mathbb{F}_q$, $\mathbb{F} = \mathbb{F}_{q^t}$). We identify $\mathcal{V}$ with the finite field $\mathbb{F}_{q^{mt}}$ viewed as a vector space over $\mathbb{F}_{q^t}$. Let $d = \gcd(m, t)$.

By Proposition 4.6(b) the polynomial f is irreducible of degree $\dim(\mathcal{V}) = m$. Thus, by Lemma 3.2(d), all roots of f lie in $\mathbb{F}_{q^m}^*$. Let $\omega \in \mathbb{F}_{q^{mt/d}}^*$ be such that the norm $\mathrm{N}_{\mathbb{F}_{q^{mt/d}}:\mathbb{F}_{q^m}}(\omega)$ of ω over $\mathbb{F}_{q^m}$ is a root of f. (Recall that the norm map is surjective, which is why ω exists.) Since σ has order t, the linear part of g is given by g^t. Hence, by Lemma 4.9(c), g is conjugate to, and thus has the same characteristic polynomial as, the element $r_{\sigma,\omega}$ specified in Lemma 4.9. Then the assertion follows from Lemmas 4.9(a), 4.25. □

Corollary 4.27. *Let $\sigma \in \mathrm{Aut}(\mathbb{F})$ with fixed field $\mathbb{K}$.*

(a) *Let g_1, g_2 be irreducible, σ-semilinear elements of $\Gamma\mathrm{L}(\mathcal{V}_{\mathbb{F}})$. Then g_1, g_2 are conjugate in $\mathrm{GL}(\mathcal{V}_{\mathbb{F}})$ if and only if $(g_1)_{\mathbb{K}}, (g_2)_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$ have the same characteristic polynomial.*

(b) *Let $f \in \mathbb{K}[x]$ be a monic, irreducible polynomial of degree $\dim(\mathcal{V})$. Then there exists an irreducible, σ-semilinear element $g \in \Gamma\mathrm{L}(\mathcal{V})$ such that the characteristic polynomial of $g_{\mathbb{K}} \in \mathrm{GL}(\mathcal{V}_{\mathbb{K}})$ is equal to $f(x^{|\sigma|})$.*

Proof. Part (a) holds by Lemma 4.7 and Proposition 4.26, while part (b) follows from Lemma 4.17 and Proposition 4.26. □

Chapter 5

Fat elements in the finite general linear group

Notation. Throughout this chapter let d, p, q be positive integers such that $d \geq 2$, p is a prime, and q is a power of p. Further, suppose that $\mathcal{V}$ is a d-dimensional vector space defined over the finite field $\mathbb{F}_q$ of order q.

The leading part of this thesis is played by certain elements in the finite general linear group $\mathrm{GL}(\mathcal{V})$, which we refer to as being *fat*. In this chapter we introduce, and investigate some properties of, fat elements and two other related families of elements, namely ppd-*elements* and pppd-*elements*.

The concept of ppd-elements, which is an abbreviation for *p*rimitive *p*rime *d*ivisor elements, was introduced by Niemeyer and Praeger [48] in order to design an algorithm to examine whether, in its natural representation, a subgroup G of $\mathrm{GL}(\mathcal{V})$ contains a classical group in the sense of [38, (2.1.16)]. Primitive prime power divisor elements, or pppd-elements for short, generalise the idea of ppd-elements and made their debut in DiMuro's PhD thesis [21]; see also DiMuro's subsequent article [22]. The name *primitive prime (power) divisor element* arises from the condition that, for any such element g in $\mathrm{GL}(\mathcal{V})$, there exists an integer $e > d/2$ such that g has order divisible by a *primitive prime (power) divisor* of $q^e - 1$, as introduced in Definition 2.23. Without giving more details at the moment, we note that our definition of pppd-elements slightly differs from the original definition given in [21, 22]. We discuss this difference in Remark 5.9. An element g in $\mathrm{GL}(\mathcal{V})$ is called *fat* if $\langle g \rangle$ acts irreducibly on a subspace of $\mathcal{V}$ of dimension strictly bigger than $d/2$. Such elements were defined by Niemeyer, Praeger and the author in [47]. As presented in Lemma 5.8, fat elements generalise the concept of pppd-elements, as each pppd-element determines a "large" (by which we mean at least $(\lfloor d/2 \rfloor + 1)$-dimensional) subspace

of $\mathcal{V}$ on which it acts irreducibly. We shall refer to fat elements which are not pppd-elements as being *exceptional*. This term is justified by Lemma 5.12 and Corollary 5.19, according to which a large majority of fat elements in $\mathrm{GL}(\mathcal{V})$ turns out to consist of ppd-elements. A fortiori most fat elements in $\mathrm{GL}(\mathcal{V})$ are pppd-elements.

We begin in Section 5.1 by defining the families of fat elements, ppd-elements and pppd-elements in $\mathrm{GL}(\mathcal{V})$ and discussing their existence in $\mathrm{GL}(\mathcal{V})$ and their relationship to one another. In Section 5.2 we determine the precise number of all fat elements in subgroups of $\mathrm{GL}(\mathcal{V})$ containing the special linear group $\mathrm{SL}(\mathcal{V})$. The result is presented in terms of proportions; see Theorem 5.18. Section 5.3 introduces exceptional fat elements and specifies some necessary conditions in order that such elements exist.

5.1 Introducing fat elements

Recall Definition 4.4(a). Recall further from Definition 2.23 the notion of primitive prime (power) divisors.

Definition 5.1. Let $g \in \mathrm{GL}(\mathcal{V})$ and let $e \in \mathbb{N}$ satisfy $d/2 < e \leq d$.

(a) We say that g is *fat*, or more precisely a $\mathrm{fat}(d, q; e)$-*element*, if $\langle g \rangle$ acts irreducibly on an e-dimensional subspace of $\mathcal{V}$.

(b) We call g a pppd-*element*, or more precisely a $\mathrm{pppd}(d, q; e)$-*element*, if its order is divisible by a primitive prime power divisor of $q^e - 1$.

(c) We call g a ppd-*element*, or more precisely a $\mathrm{ppd}(d, q; e)$-*element*, if its order is divisible by a primitive prime divisor of $q^e - 1$.

Observe that $\mathrm{fat}(d, q; d)$-elements in $\mathrm{GL}(\mathcal{V})$ are precisely the irreducible elements in $\mathrm{GL}(\mathcal{V})$. We use both terms interchangeably. Throughout this thesis, we reserve the terms *fat element*, pppd-*element*, and ppd-*element* for a $\mathrm{fat}(d, q; e)$-element, $\mathrm{pppd}(d, q; e)$-element and a $\mathrm{ppd}(d, q; e)$-element, respectively, relative to an integer e strictly bigger than $d/2$.

In the situation of Definition 5.1(a), the e-dimensional and $\langle g \rangle$-irreducible subspace of $\mathcal{V}$ is uniquely determined. To see that this is true, assume that there exist two $\langle g \rangle$-irreducible subspaces $\mathcal{U}_1, \mathcal{U}_2 \leq \mathcal{V}$ of dimension e. Then the intersection $\mathcal{U}_1 \cap \mathcal{U}_2$ is $\langle g \rangle$-invariant and (since $\dim(\mathcal{U}_i) > \dim(\mathcal{V})/2$, $i \in \{1, 2\}$) we have $\mathcal{U}_1 \cap \mathcal{U}_2 \neq \{0\}$. For $i \in \{1, 2\}$, the irreducibility of $\mathcal{U}_i$ implies that $\mathcal{U}_1 \cap \mathcal{U}_2 = \mathcal{U}_i$. It follows that $\mathcal{U}_1 = \mathcal{U}_2$.

As shown below, whether or not an element $g \in \mathrm{GL}(\mathcal{V})$ is fat, can be detected by factorising its characteristic polynomial.

Lemma 5.2. *Let $g \in \mathrm{GL}(\mathcal{V})$ and let $e \in \mathbb{N}$ satisfy $d/2 < e \leq d$. Then g is a $\mathrm{fat}(d, q; e)$-element if and only if its characteristic polynomial has an irreducible (over $\mathbb{F}_q$) factor of degree e.*

Proof. First, suppose that g is a $\mathrm{fat}(d, q; e)$-element. Let $\mathcal{U}$ be the (uniquely determined) e-dimensional subspace of $\mathcal{V}$ on which $\langle g \rangle$ acts irreducibly. Then the restriction $g|_{\mathcal{U}}$ of g to $\mathcal{U}$ is an irreducible element of $\mathrm{GL}(\mathcal{U})$. Let $f \in \mathbb{F}_q[x]$ be the characteristic polynomial of $g|_{\mathcal{U}}$. Then $\deg(f) = e$ and f is a divisor of the characteristic polynomial of g. By Lemma 4.8(a), f is irreducible.

Conversely, assume that the characteristic polynomial of g has an irreducible factor $f \in \mathbb{F}_q[x]$ of degree e. Let $\mathcal{U}$ be the kernel of $f(g)$, that is let $\mathcal{U} = \{v \in \mathcal{V} \mid vf(g) = 0\}$. Since $(ug)f(g) = uf(g)g = 0g = 0$ for all $u \in \mathcal{U}$, we see that $\mathcal{U}$ is $\langle g \rangle$-invariant. Now, the polynomial f annihilates the restriction $g|_{\mathcal{U}}$. Thus, the minimal polynomial of $g|_{\mathcal{U}}$ divides f. Since f is irreducible, this means that f is the minimal polynomial of $g|_{\mathcal{U}}$. Because $\deg(f) = e > d/2$ (and since each irreducible factor of the characteristic polynomial of $g|_{\mathcal{U}}$ has to divide f) it follows that f is also the characteristic polynomial of $g|_{\mathcal{U}}$. Thus, $\dim(\mathcal{U}) = \deg(f) = e$. Moreover, by Lemma 4.8(a) the element $g|_{\mathcal{U}}$ is irreducible, which is the same as saying that $\langle g \rangle$ acts irreducibly on $\mathcal{U}$. Thus, g is a $\mathrm{fat}(d, q; e)$-element. □

The characterisation of fat elements presented in Lemma 5.2 above implies that $\mathrm{fat}(d, q; e)$-elements exist in $\mathrm{GL}(\mathcal{V})$ for all e with $d/2 < e \leq d$. In order to check whether this also holds true for ppd- and pppd-elements, fix an integer e satisfying $d/2 < e \leq d$ and recall Definitions 2.23, 5.1. As we may deduce from [33, p. 187, Satz 7.3(a)] the group $\mathrm{GL}(\mathcal{V})$ contains a cyclic subgroup of order $q^e - 1$. Hence, if r is a primitive prime (power) divisor of $q^e - 1$, then $\mathrm{GL}(\mathcal{V})$ contains an element of order r. (Alternatively, this can be also deduced from Sylow's first theorem and the fact that $|\mathrm{GL}(\mathcal{V})| = q^{d(d-1)/2} \prod_{i=1}^{d} (q^i - 1)$.) It follows that the existence of pp(p)d-elements in $\mathrm{GL}(\mathcal{V})$ is equivalent to the existence of primitive prime (power) divisors of $q^e - 1$, which we have already examined in Lemma 2.24(b)(c). This proves the following lemma. (Note that, if $q = 2^k - 1$ then, since q is a prime power, by [44, Theorem 1] the integers q and k are primes, that is q is a *Mersenne prime*.) Recall that $d \geq 2$.

Lemma 5.3. *Let $e \in \mathbb{N}$ satisfy $d/2 < e \leq d$.*

(a) *The group $\mathrm{GL}(\mathcal{V})$ contains $\mathrm{fat}(d, q; e)$-elements.*

(b) *The group $\mathrm{GL}(\mathcal{V})$ contains $\mathrm{pppd}(d, q; e)$-elements.*

(c) *The group $\mathrm{GL}(\mathcal{V})$ contains $\mathrm{ppd}(d, q; e)$-elements unless $(q, e) = (2, 6)$, or $e = 2$ and q is a Mersenne prime (that is a prime of the form $2^k - 1$ with k a prime).*

Lemma 5.4. *Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. If $g \in \mathrm{GL}(\mathcal{V})$ is a $\mathrm{fat}(d, q; e)$-element, then $|g|$ is divisible by some primitive divisor of $q^e - 1$.*

Proof. Suppose that g is a $\mathrm{fat}(d, q; e)$-element. Let $\mathcal{U}$ be the (uniquely determined) e-dimensional and $\langle g \rangle$-irreducible subspace of $\mathcal{V}$. Let r be the order of the restriction $g|_{\mathcal{U}}$. (Then r is a divisor of $|g|$.) Since $g|_{\mathcal{U}}$ is an irreducible element of $\mathrm{GL}(\mathcal{U})$, by Lemma 4.11(b) we have $\mathrm{ord}(q; r) = e$, that is r is a primitive divisor of $q^e - 1$. □

We point out that Lemma 5.4 cannot be turned into an "if and only if" statement, even if we assume $|g|$ to be divisible by a minimal primitive divisor of $q^e - 1$, as introduced in Definition 2.25. We verify this in the following example. (Things look different if we assume that the order of g is divisible by a primitive divisor of $q^e - 1$ which is a prime power, that is if g is a $\mathrm{pppd}(d, q; e)$-element for some integer $e > d/2$. In that case, g is in fact fat; see Lemma 5.8 below.)

Example 5.5. Suppose that $d = 6$ and $q = 29$, whence $\mathcal{V}$ is a 6-dimensional $\mathbb{F}_{29}$-vector space. Let $\mathfrak{B}$ be a basis of $\mathcal{V}$ and let $g \in \mathrm{GL}(\mathcal{V})$ be such that the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & 3 & \cdot & \cdot & \cdot \\ \cdot & 1 & 12 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 28 & \cdot \\ \cdot & \cdot & \cdot & 1 & 5 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{pmatrix} \in \mathrm{GL}(6, 29).$$

(Here the symbol "$\cdot$" denotes the zero element in $\mathbb{F}_{29}$.) One can check that $|g| = 65 = 13 \times 5$ and $\mathrm{ord}(29; 13) = 3$, $\mathrm{ord}(29; 5) = 2$. By Lemma 2.15, we get

$$\mathrm{ord}(29; 65) = \mathrm{lcm}\big\{\mathrm{ord}(29; 13), \mathrm{ord}(29; 5)\big\} = 6,$$

whence 65 is a minimal primitive divisor of $29^6 - 1$. However, the block diagonal form of $g_{\mathfrak{B}}$ shows that g is not a $\mathrm{fat}(6, 29; 6)$-element.

Our next lemma is a useful tool for showing that a given element in $\mathrm{GL}(\mathcal{V})$ is not fat. Recall from Section 2.1 (p. 13) the definition of the Carmichael function $\lambda : \mathbb{N} \to \mathbb{N}$. Recall further that $d \geq 2$ and that $\mathcal{V}$ is a d-dimensional $\mathbb{F}_q$-vector space.

Lemma 5.6. *Let $g \in \mathrm{GL}(\mathcal{V})$ be fat. Then $d < 2\lambda(|g|)$. Moreover, if q is a square, then $d < \lambda(|g|)$.*

Proof. Assume that g is a $\mathrm{fat}(d, q; e)$-element (for some $e > d/2$) and that $q = p^b$. By Lemma 5.4 the order of g is divisible by a primitive divisor of $q^e - 1$, that is by an integer r such that $e = \mathrm{ord}\big(p^b; r\big)$. Thus, by Lemma 2.13 the integer e divides, and thus is less than or equal to, $\lambda(r)/\gcd(\lambda(r), b)$. Recalling that $e > d/2$, we obtain

$$d < \frac{2\lambda(r)}{\gcd\big(\lambda(r), b\big)} = \frac{2\lambda(|g|)}{\frac{\lambda(|g|)}{\lambda(r)}\gcd\big(\lambda(r), b\big)}. \tag{5.1}$$

Since r is a divisor of $|g|$, using Lemma 2.4 we see that $\lambda(r)$ divides $\lambda(|g|)$, that is $\lambda(|g|)/\lambda(r) \in \mathbb{N}$. Then (5.1) yields

$$d < \frac{2\lambda(|g|)}{\gcd\big(\lambda(|g|), \frac{\lambda(|g|)}{\lambda(r)}b\big)},$$

and hence

$$d < \frac{2\lambda(|g|)}{\gcd\big(\lambda(|g|), b\big)}. \tag{5.2}$$

In particular, $d < 2\lambda(|g|)$, as asserted.

In order to verify the "moreover" part, suppose that q is a square (that is b is even). Since $d \geq 2$, (5.2) implies that $2 < 2\lambda(|g|)$. Then (as we may deduce from Lemma 2.4) we have $|g| \geq 3$ and thus $\lambda(|g|)$ is even. The assertion now follows from (5.2). □

Lemma 5.7. *Let $g \in \mathrm{GL}(\mathcal{V})$ and let $e, \ell \in \mathbb{N}$. Suppose that $d/2 < e \leq d$.*

(a) *If g^ℓ is a $\mathrm{fat}(d, q; e)$-element, then g is a $\mathrm{fat}(d, q; e)$-element.*

(b) *If g is a $\mathrm{fat}(d, q; e)$-element, then the characteristic polynomial of g^ℓ has an irreducible factor of degree $e_0 \geq e/\ell$.*

Proof. (a) Suppose that g^ℓ is a $\mathrm{fat}(d, q; e)$-element. Let $\mathcal{U}$ be the (uniquely determined) e-dimensional and $\langle g^\ell \rangle$-irreducible subspace of $\mathcal{V}$. According to Lemma 5.2 the characteristic polynomial of g^ℓ has an irreducible factor, say f, of degree e. As shown in the (second paragraph of the) proof of Lemma 5.2 we have $\mathcal{U} = \ker(f(g^\ell))$. Since g commutes with g^ℓ, we obtain $(ug)f(g^\ell) = uf(g^\ell)g = 0g = 0$ for all $u \in \mathcal{U}$, which shows that $\mathcal{U}$ is $\langle g \rangle$-invariant. Then (recalling that $\mathcal{U}$ is $\langle g^\ell \rangle$-irreducible) we see that $\mathcal{U}$ is $\langle g \rangle$-irreducible.

(*b*) Suppose that g is a $\mathrm{fat}(d,q;e)$-element. By Lemma 5.2 the characteristic polynomial of g has an irreducible factor of degree e. Let ω be a root of that factor. By Lemma 3.4 we have

$$\mathrm{ord}(q;|\omega|) = e. \tag{5.3}$$

Since $|\omega^\ell| = |\omega|/\gcd(\ell,|\omega|)$ we have $\mathrm{ord}(q;|\omega|) = \mathrm{ord}\big(q;|\omega^\ell|\gcd(\ell,|\omega|)\big)$, and thus by Lemma 2.17, $\mathrm{ord}(q;|\omega|) \le \mathrm{ord}\big(q;|\omega^\ell|\big)\gcd(\ell,|\omega|)$. Hence,

$$\mathrm{ord}(q;|\omega|) \le \mathrm{ord}\big(q;|\omega^\ell|\big)\ell. \tag{5.4}$$

Now, let $h \in \mathbb{F}_q[x]$ be the characteristic polynomial of g^ℓ. Then ω^ℓ is a root of h. Let $h_0 \in \mathbb{F}_q[x]$ be an irreducible factor of h such that $h_0(\omega^\ell) = 0$. By Lemma 3.4 the degree of h_0 is equal to $\mathrm{ord}\big(q;|\omega^\ell|\big)$. According to (5.3) and (5.4) we have $\mathrm{ord}\big(q;|\omega^\ell|\big) \ge e/\ell$. □

By definition any $\mathrm{ppd}(d,q;e)$-element is a $\mathrm{pppd}(d,q;e)$-element. We next show that, in turn, every $\mathrm{pppd}(d,q;e)$-element is fat (with respect to the same integer $e > d/2$).

Lemma 5.8. *Let $e \in \mathbb{N}$ be such that $d/2 < e \le d$ and let $g \in \mathrm{GL}(\mathcal{V})$ be a $\mathrm{pppd}(d,q;e)$-element. Then g is a $\mathrm{fat}(d,q;e)$-element.*

Proof. Let r be a primitive prime power divisor of $q^e - 1$ dividing $|g|$. Let $\ell = |g|/r$. Consider the element g^ℓ of order r. By [21, Theorem 1.1.3], g^ℓ is a $\mathrm{fat}(d,q;e)$-element, and hence by Lemma 5.7(*a*) so is g. □

Remark 5.9. In his PhD thesis [21] as well as in his subsequent article [22], DiMuro defines a $\mathrm{pppd}(d,q;e)$-element to be an element $g \in \mathrm{GL}(\mathcal{V})$ such that g has order *equal* to a primitive prime power divisor of $q^e - 1$, where $e \ge \lfloor d/3 \rfloor$. By [21, Theorem 1.1.3] the group generated by such an element acts irreducibly on an e-dimensional subspace of $\mathcal{V}$. In contrast to that, our definition of $\mathrm{pppd}(d,q;e)$-elements allows the integer e to only reach values between $\lfloor d/2 \rfloor + 1$ and d. Setting $e > d/2$ enables us to let "our" $\mathrm{pppd}(d,q;e)$-elements have orders *divisible* by primitive prime power divisors of $q^e - 1$, without loosing the crucial property that each such element g determines an e-dimensional subspace of $\mathcal{V}$ on which $\langle g \rangle$ acts irreducibly. (For $e \le d/2$, the fact that an element $g \in \mathrm{GL}(\mathcal{V})$ has order divisible by a primitive prime power divisor of $q^e - 1$ only guarantees that $\langle g \rangle$ acts irreducibly on a subspace of $\mathcal{V}$ of dimension divisible by e.)

Although DiMuro views "his" pppd-elements as a generalisation of ppd-elements as originally introduced in [48] (see [22, p. 222]), it is not the case that every such ppd-element is a pppd-element in DiMuro's sense. For example, an

element $g \in \mathrm{GL}(3,3)$ of order 26 is a $\mathrm{ppd}(3,3;3)$-element (as the order of g is a multiple of the primitive prime divisor 13 of $3^3-1=26$) but it is not a pppd-element according to DiMuro's definition (as $|g|$ is not a prime power). Our definition of pppd-elements truly generalises the concept of ppd-elements, as first introduced in [48, Definition 2.3].

In Lemma 5.8 we saw that the set of all $\mathrm{pppd}(d,q;e)$-elements in $\mathrm{GL}(\mathcal{V})$ forms a subset of the set of all $\mathrm{fat}(d,q;e)$-elements in $\mathrm{GL}(\mathcal{V})$. The following example demonstrates that, depending on the triple (d,q,e), this subset may, but does not need to, be proper. In fact, in the situation of Example 5.10(b) below, all $\mathrm{fat}(d,q;e)$-elements in $\mathrm{GL}(\mathcal{V})$ turn out to be ppd-elements.

Example 5.10. Suppose that $d=7$ and $q=29$, whence $\mathcal{V}$ is a 7-dimensional $\mathbb{F}_{29}$-vector space.

(a) Let $\mathfrak{B}$ be a basis of $\mathcal{V}$. Let $g \in \mathrm{GL}(\mathcal{V})$ be such that the matrix of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} h & \mathbf{0}_{6,1} \\ \mathbf{0}_{1,6} & 1 \end{pmatrix} \in \mathrm{GL}(7,29),$$

where $\mathbf{0}_{6,1}$ and $\mathbf{0}_{1,6}$ are the (6×1)-zero matrix, and respectively the (1×6)-zero matrix, over $\mathbb{F}_{29}$, and where $h \in \mathrm{GL}(6,29)$ is the companion matrix of the polynomial

$$f(x) = x^6 + 15x^5 + 24x^4 + 12x^3 + 17x^2 + 27x + 1 \in \mathbb{F}_{29}[x].$$

We may verify (for example using GAP [24]) that $65 = |h| = |g|$ and that the polynomial f is irreducible (over $\mathbb{F}_{29}$). Since $(x-1)f$ is the characteristic polynomial of g, by Lemma 5.2, g is a $\mathrm{fat}(7,29;6)$-element. However, g is not a pppd-element, because the only prime divisors of $|g|$ are 5 and 13, and we have $\mathrm{ord}(29;5)=2$ and $\mathrm{ord}(29;13)=3$.

Hence, the set of all $\mathrm{pppd}(7,29;6)$-elements in $\mathrm{GL}(\mathcal{V})$ is properly contained in the set of all $\mathrm{fat}(7,29;6)$-elements in $\mathrm{GL}(\mathcal{V})$.

(b) Let $g \in \mathrm{GL}(\mathcal{V})$ be a $\mathrm{fat}(7,29;5)$-element. By Lemma 5.4 the order of g is divisible by a primitive divisor r of 29^5-1. Now, one can check that the primitive divisors of 29^5-1 are given by

$$\underbrace{732541}_{\text{prime}},\ \underbrace{1465082}_{2\times 732541},\ \underbrace{2930164}_{2^2\times 732541},\ \underbrace{5127787}_{7\times 732541},\ \underbrace{10255574}_{2\times 7\times 732541},\ \underbrace{20511148}_{2^2\times 7\times 732541}.$$

Hence, all primitive divisors of 29^5-1 are divisible by the primitive prime divisor 732541 of 29^5-1. Thus, g is a $\mathrm{ppd}(7,29;5)$-element.

Thus, every $\mathrm{fat}(7,29;5)$-element in $\mathrm{GL}(\mathcal{V})$ is a $\mathrm{ppd}(7,29;5)$-element.

Recall that q is a power of p. Recall further (from Definition 4.14) that we write $g_{p'}$ and g_p for the p'-part, and respectively the p-part, of an element $g \in \mathrm{GL}(\mathcal{V})$.

Lemma 5.11. *Let $g \in \mathrm{GL}(\mathcal{V})$ and let $e \in \mathbb{N}$ satisfy $d/2 < e \leq d$.*

(*a*) *The element g is a $\mathrm{fat}(d, q; e)$-element if and only if $g_{p'}$ is a $\mathrm{fat}(d, q; e)$-element.*

(*b*) *The element g is a $\mathrm{pppd}(d, q; e)$-element if and only if $g_{p'}$ is a $\mathrm{pppd}(d, q; e)$-element.*

(*c*) *The element g is a $\mathrm{ppd}(d, q; e)$-element if and only if $g_{p'}$ is a $\mathrm{ppd}(d, q; e)$-element.*

Proof. (*a*) Suppose that g is a $\mathrm{fat}(d, q; e)$-element. Let $\mathcal{U}$ be the (uniquely determined) e-dimensional and $\langle g \rangle$-irreducible subspace of $\mathcal{V}$. By (the "in particular" part of) Lemma 4.15 the subspace $\mathcal{U}$ is $\langle g_{p'} \rangle$-irreducible. Then $g_{p'}$ is a $\mathrm{fat}(d, q; e)$-element.

Conversely, if $g_{p'}$ is a $\mathrm{fat}(d, q; e)$-element, then (since $g_{p'}$ is a power of g) by Lemma 5.7(*a*), g is a $\mathrm{fat}(d, q; e)$-element.

(*b*) Suppose that g is a $\mathrm{pppd}(d, q; e)$-element. Let r be a primitive prime power divisor of $q^e - 1$ which divides $|g|$. (Then r and q are coprime, whence $p \nmid r$.) Since $g = g_{p'} g_p = g_p g_{p'}$, the prime power r divides the least common multiple of $|g_{p'}|$ and $|g_p|$. Because $|g_p|$ is a power of p (and $p \nmid r$) it follows that r is a divisor of $|g_{p'}|$. Hence, $g_{p'}$ is a $\mathrm{pppd}(d, q; e)$-element.

Conversely, if $g_{p'}$ is a $\mathrm{pppd}(d, q; e)$-element, then the order of $g_{p'}$, and hence also the order of g, is divisible by a primitive prime power divisor of $q^e - 1$, which means that g is a $\mathrm{pppd}(d, q; e)$-element.

(*c*) The proof works analogously to the proof of part (*b*). (Exchange the term "primitive prime power divisor" by "primitive prime divisor" and "$\mathrm{pppd}(d, q; e)$-element" by $\mathrm{ppd}(d, q; e)$-element".) □

5.2 Counting fat elements

The set of all non-singular linear mappings $g \in \mathrm{GL}(\mathcal{V})$ with determinant 1 forms a subgroup of $\mathrm{GL}(\mathcal{V})$, the *special linear group* $\mathrm{SL}(\mathcal{V})$. Being the kernel of the surjective group homomorphism

$$\det : \mathrm{GL}(\mathcal{V}) \to \mathbb{F}_q^*, \quad g \mapsto \det(g),$$

the group $\mathrm{SL}(\mathcal{V})$ is normal in $\mathrm{GL}(\mathcal{V})$ and has order equal to $|\mathrm{GL}(\mathcal{V})|/(q-1)$. The question we want to answer in this section is the following. Given a subgroup $G \leq \mathrm{GL}(\mathcal{V})$ which contains $\mathrm{SL}(\mathcal{V})$ and an integer e satisfying $d/2 < e \leq d$, what is the proportion of all $\mathrm{fat}(d,q;e)$-elements in G. In [48] Niemeyer and Praeger answer the analogous question for ppd-elements. More precisely, they show the following.

Lemma 5.12 (Niemeyer & Praeger [48, Theorem 5.7(i)])**.** *Let $d \geq 3$, let G be a group satisfying $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$, and let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Let $\mathrm{ppd}(G;e)$ be the proportion (in G) of all $\mathrm{ppd}(d,q;e)$-elements in G. Then*

$$\frac{1}{e+1} \leq \mathrm{ppd}(G;e) < \frac{1}{e}.$$

In this section we calculate the precise number of all $\mathrm{fat}(d,q;e)$-elements in G and show that the bounds given in Lemma 5.12 also hold for the proportion of all $\mathrm{fat}(d,q;e)$-elements in G; see Theorem 5.18. Since (as we may recall from Lemma 5.8) every ppd-element is fat, this means that the number of those fat elements in G which are not ppd-elements is comparatively small.

We begin in Subsection 5.2.1 by counting irreducible elements (that is we first consider the special case $e = d$). The general case is treated in Subsection 5.2.2.

5.2.1 Proportion of irreducible elements

Recall from Definition 3.5 the notion of $N_q^*(d)$. The precise value of $N_q^*(d)$ can be calculated through Lemma 3.7.

Lemma 5.13. *Let $g \in \mathrm{GL}(\mathcal{V})$. The group $\mathrm{GL}(\mathcal{V})$ acts via conjugation on the set of all irreducible elements in $g\mathrm{SL}(\mathcal{V})$. This action has $N_q^*(d)/(q-1)$ orbits, each of them of length $|\mathrm{GL}(\mathcal{V})|/(q^d-1)$.*

Proof. The coset $g\mathrm{SL}(\mathcal{V})$ consists of all elements in $\mathrm{GL}(\mathcal{V})$ with determinant equal to $\det(g)$. Consider an irreducible element $h \in g\mathrm{SL}(\mathcal{V})$. Since conjugation by elements from $\mathrm{GL}(\mathcal{V})$ neither changes the determinant of h, nor the fact that h is irreducible, it follows that $\mathrm{GL}(\mathcal{V})$ acts via conjugation on the set of all irreducible elements in $g\mathrm{SL}(\mathcal{V})$. Let $\mathfrak{I}$ be the set of all orbits of this action.

Let f_h be the characteristic polynomial of h. Clearly, f_h is a monic polynomial of degree d over $\mathbb{F}_q$. By Lemma 4.8(a) the characteristic polynomial of h is irreducible. By [34, Bemerkung 5.4.3] we have $f_h(0) = (-1)^d \det(h) = (-1)^d \det(g)$. Hence, by mapping each orbit $O \in \mathfrak{I}$ onto the characteristic

polynomial of a representative of O we obtain the mapping

$$\iota : \mathfrak{I} \to \big\{ f \in \mathbb{F}_q[x] \mid f \text{ monic, irreducible}, \deg(f) = d, f(0) = (-1)^d \det(g) \big\}.$$

By Lemma 4.8(b), ι is injective. In order to see that ι is surjective, fix a monic, irreducible polynomial $f \in \mathbb{F}_q[x]$ with $\deg(f) = d$ and $f(0) = (-1)^d \det(g)$. Let ℓ be an element of $\mathrm{GL}(\mathcal{V})$ whose matrix with respect to some basis of $\mathcal{V}$ is the companion matrix of f. Then f is the characteristic polynomial of ℓ. By [34, Bemerkung 5.4.3] we have $\det(\ell) = (-1)^d f(0) = \det(g)$, whence ℓ lies in $g\mathrm{SL}(\mathcal{V})$. This proves that ι is surjective, and thus bijective. Then Proposition 3.12 reveals that

$$|\mathfrak{I}| = \frac{N_q^*(d)}{q-1}.$$

Let $O \in \mathfrak{I}$ be the orbit containing the irreducible element $h \in g\mathrm{SL}(\mathcal{V})$. According to the orbit-stabiliser-theorem the length of O is given by the index $|\mathrm{GL}(\mathcal{V}) : C_{\mathrm{GL}(\mathcal{V})}(h)|$, where $C_{\mathrm{GL}(\mathcal{V})}(h)$ is the centraliser of $\langle h \rangle$ in $\mathrm{GL}(\mathcal{V})$. Thus, by Proposition 4.18 we have $|O| = |\mathrm{GL}(\mathcal{V})|/(q^d - 1)$. □

Recall from Definition 4.20 that, given a subgroup $G \leq \mathrm{GL}(\mathcal{V})$, we write $\mathrm{irr}(G)$ for the proportion (in G) of all irreducible elements in G. The following lemma determines the proportion of all irreducible elements in subgroups of $\mathrm{GL}(\mathcal{V})$ which contain $\mathrm{SL}(\mathcal{V})$, and thus generalises Corollary 4.21 (for $d \geq 2$). The "moreover" part of Proposition 5.14 is proved also in [45, Lemma 2.3].

Proposition 5.14. *Let G be a group satisfying $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$. Then*

$$\mathrm{irr}(G) = \frac{N_q^*(d)}{q^d - 1}.$$

Moreover,

$$\frac{1}{d+1} \leq \mathrm{irr}(G) < \frac{1}{d}.$$

Proof. The group G contains $|G : \mathrm{SL}(\mathcal{V})|$ cosets of $\mathrm{SL}(\mathcal{V})$. From Lemma 5.13 it follows that each of these cosets contains $N_q^*(d)(q-1)^{-1}|\mathrm{GL}(\mathcal{V})|(q^d-1)^{-1}$ irreducible elements. Hence, the number of all irreducible elements in G is given by

$$\mathrm{irr}(G)|G| = \frac{|G : \mathrm{SL}(\mathcal{V})| \; N_q^*(d) \; |\mathrm{GL}(\mathcal{V})|}{(q-1)(q^d-1)}.$$

Then $\mathrm{irr}(G) = N_q^*(d)/(q^d-1)$, as asserted. The "moreover" part follows from Lemma 3.9(c). (Recall that $d \geq 2$.) □

5.2.2 Proportion of fat elements

In order to pull back the results of Subsection 5.2.1 to the general case of fat elements, we require two facts about (overgroups of) the special linear group, which are presented in Lemmas 5.15, 5.16 below. Both are basic and well-known. However, since they are among the main ingredients to prove Theorem 5.18, we provide a proof here.

Lemma 5.15. *Let $e \leq d$ be a positive integer and let G be a group satisfying $\mathrm{SL}(\mathcal{V}) \leq G \leq \Gamma\mathrm{L}(\mathcal{V})$. The group G acts transitively on the set of all e-dimensional subspaces of $\mathcal{V}$ via*

$$\big\{\mathcal{X} \leq \mathcal{V} \mid \dim(\mathcal{X}) = e\big\} \times G \to \big\{\mathcal{X} \leq \mathcal{V} \mid \dim(\mathcal{X}) = e\big\}, \quad (\mathcal{X}, g) \mapsto \mathcal{X}g.$$

Proof. Consider two e-dimensional subspaces $\mathcal{U}, \mathcal{W}$ of $\mathcal{V}$. Choose two bases $\{u_1, \ldots, u_d\}$, $\{w_1, \ldots, w_d\}$ of $\mathcal{V}$ so that $\mathcal{U}$ and $\mathcal{W}$ are spanned by the vectors $u_1, \ldots, u_e$ and $w_1, \ldots, w_e$, respectively. First, define an element $h \in \mathrm{GL}(\mathcal{V})$ by $u_i h = w_i$, $i \in \{1, \ldots, d\}$. Then consider the mapping $g \in \mathrm{GL}(\mathcal{V})$ given by $u_1 g = \det(h)^{-1} w_1$ and $u_i g = w_i$, $i \in \{2, \ldots, d\}$. According to our construction we have $\mathcal{U}g = \mathcal{W}$. Moreover, g has determinant $\det(g) = \det(h)^{-1} \det(h) = 1$, which is why $g \in \mathrm{SL}(\mathcal{V})$. This proves that the group $\mathrm{SL}(\mathcal{V})$ acts transitively on the set of all e-dimensional subspaces of $\mathcal{V}$ (via $(\mathcal{X}, g) \mapsto \mathcal{X}g$) . In order to complete the proof, recall from Section 4.1 that non-singular, semilinear mappings on $\mathcal{V}$ map e-dimensional subspaces of $\mathcal{V}$ again onto e-dimensional subspaces of $\mathcal{V}$. □

Recall that, given a subspace $\mathcal{U} \leq \mathcal{V}$, we write $\mathrm{SL}(\mathcal{V})_\mathcal{U}$ for the subspace stabiliser of $\mathcal{U}$ in $\mathrm{SL}(\mathcal{V})$, that is $\mathrm{SL}(\mathcal{V})_\mathcal{U} = \{g \in \mathrm{SL}(\mathcal{V}) \mid \mathcal{U}g = \mathcal{U}\}$. Recall also that $g|_\mathcal{U}$ means the restriction of g to $\mathcal{U}$.

Lemma 5.16. *Let $\mathcal{U}$ be a non-trivial and proper subspace of $\mathcal{V}$. Then the mapping*

$$\mathrm{SL}(\mathcal{V})_\mathcal{U} \to \mathrm{GL}(\mathcal{U}), \quad g \mapsto g|_\mathcal{U}$$

is a surjective group homomorphism.

Proof. Consider an element $g \in \mathrm{SL}(\mathcal{V})$. The restriction $g|_\mathcal{U}$ is an invertible linear mapping on $\mathcal{U}$. Moreover, we have $(gg')|_\mathcal{U} = (g|_\mathcal{U})(g'|_\mathcal{U})$ for all $g' \in \mathrm{SL}(\mathcal{V})_\mathcal{U}$. Hence, the mapping $\mathrm{SL}(\mathcal{V})_\mathcal{U} \to \mathrm{GL}(\mathcal{U}), g \mapsto g|_\mathcal{U}$ is a well-defined group homomorphism. In order to see that this homomorphism is surjective, fix an element $h \in \mathrm{GL}(\mathcal{U})$. Let $e = \dim(\mathcal{U})$. Then (by assumption) we have $1 \leq e \leq d-1$. Let $\{v_1, \ldots, v_d\}$ be a basis of $\mathcal{V}$ such that the vectors $v_1, \ldots, v_e$

span $\mathcal{U}$. Define $\widehat{h} \in \mathrm{GL}(\mathcal{V})$ by

$$v_i\widehat{h} = \begin{cases} v_i h, & \text{if } 1 \leq i \leq e, \\ \det(h)^{-1} v_i, & \text{if } i = e+1, \\ v_i, & \text{if } e+2 \leq i \leq d. \end{cases}$$

Then $\det(\widehat{h}) = \det(h)\det(h)^{-1} = 1$ and $\mathcal{U}\widehat{h} = \mathcal{U}h = \mathcal{U}$, whence $\widehat{h} \in \mathrm{SL}(\mathcal{V})_{\mathcal{U}}$. Moreover, $\widehat{h}|_{\mathcal{U}} = h$ as needed. □

Definition 5.17. Let A be a subset of $\mathrm{GL}(\mathcal{V})$, and let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. We write $\mathrm{fat}(A; e)$ for the proportion (in A) of all $\mathrm{fat}(d, q; e)$-elements in A.

We are now able to determine the proportion of all $\mathrm{fat}(d, q; e)$-elements in linear groups containing the special linear group. The following result generalises and sharpens [47, Lemma 4.3]. The key idea of its proof relies on [48, proof of Lemma 5.4]. Recall that we write $N_q^*(e)$ for the number of all monic, irreducible polynomials $f \neq x$ of degree e over $\mathbb{F}_q$. The precise value of $N_q^*(e)$ is given in Lemma 3.7.

Theorem 5.18. *Let G be a group satisfying $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$ and let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Then*

$$\mathrm{fat}(G; e) = \frac{N_q^*(e)}{q^e - 1}.$$

Moreover,

$$\frac{1}{e+1} \leq \mathrm{fat}(G; e) < \frac{1}{e}.$$

Proof. If $e = d$, then the assertion holds by Proposition 5.14. So we may assume that $d/2 < e < d$. Since each $\mathrm{fat}(d, q; e)$-element in G uniquely determines an e-dimensional and $\langle g \rangle$-irreducible subspace of $\mathcal{V}$, it follows that the number of all $\mathrm{fat}(d, q; e)$-elements in G is given by

$$\mathrm{fat}(G; e)|G| = \sum_{\substack{\mathcal{U} \leq \mathcal{V}, \\ \dim(\mathcal{U}) = e}} \mathrm{fat}(G_{\mathcal{U}}; e)|G_{\mathcal{U}}|. \tag{5.5}$$

Consider an e-dimensional subspace $\mathcal{U}$ of $\mathcal{V}$. By Lemma 5.16, the mapping

$$\delta : G_{\mathcal{U}} \to \mathrm{GL}(\mathcal{U}), \quad g \mapsto g|_{\mathcal{U}}$$

is a surjective group homomorphism. Now, $g \in G_{\mathcal{U}}$ is a $\mathrm{fat}(d, q; e)$-element if and only if $g|_{\mathcal{U}}$ is irreducible. Moreover, since elements in $\ker(\delta)$ act trivially

on $\mathcal{U}$, the restriction $g|_{\mathcal{U}}$ is irreducible if and only if all elements in the coset $\ker(\delta)g$ are $\mathrm{fat}(d,q;e)$-elements. Thus the number of all $\mathrm{fat}(d,q;e)$-elements in $G_{\mathcal{U}}$ is equal to $|\ker(\delta)|$ times the number of all irreducible elements in $\mathrm{im}(\delta) = \mathrm{GL}(\mathcal{U})$, that is

$$\mathrm{fat}(G_{\mathcal{U}};e)|G_{\mathcal{U}}| = \underbrace{|\ker(\delta)||\mathrm{im}(\delta)|}_{=|G_{\mathcal{U}}|}\mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big).$$

Then $\mathrm{fat}(G_{\mathcal{U}};e) = \mathrm{irr}(\mathrm{GL}(\mathcal{U}))$ and (5.5) simplifies to

$$\mathrm{fat}(G;e)|G| = \sum_{\substack{\mathcal{U}\leq\mathcal{V},\\ \dim(\mathcal{U})=e}} \mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big)|G_{\mathcal{U}}|.$$

Since (by Proposition 5.14) the value of $\mathrm{irr}(\mathrm{GL}(\mathcal{U}))$ only depends on the integers e and q, and since by Lemma 5.15 (and the orbit-stabiliser-theorem) the number of all e-dimensional subspaces of $\mathcal{V}$ is equal to $|G : G_{\mathcal{U}}|$, we conclude that

$$\mathrm{fat}(G;e)|G| = |G : G_{\mathcal{U}}|\,\mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big)|G_{\mathcal{U}}|.$$

Thus, $\mathrm{fat}(G;e) = \mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big)$ and the assertion holds by Proposition 5.14. (Note that since $d \geq 2$ we have $e > d/2 \geq 1$.) □

Lemma 5.12 and Theorem 5.18 enable us to bound from above the proportion of all $\mathrm{fat}(d,q;e)$-elements with orders not divisible by any primitive prime divisor of $q^e - 1$.

Corollary 5.19. *Let $d \geq 3$. Let G satisfy $\mathrm{SL}(\mathcal{V}) \leq G \leq \mathrm{GL}(\mathcal{V})$ and let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. The proportion (in G) of all $\mathrm{fat}(d,q;e)$-elements in G which are not $\mathrm{ppd}(d,q;e)$-elements is less than $e^{-1}(e+1)^{-1}$.*

Proof. By Lemma 5.12 and Theorem 5.18 the number of all $\mathrm{fat}(d,q;e)$-elements in G which are not $\mathrm{ppd}(d;q;e)$-elements is less than $|G|/e - |G|/(e+1)$. Hence, the proportion of such elements in G is less than $1/e - 1/(e+1) = 1/(e(e+1))$. □

5.3 Exceptional fat elements

By Lemma 5.12 and Corollary 5.19 the proportion of fat elements in $\mathrm{GL}(\mathcal{V})$ which are not ppd-elements is rather small. This means all the more that there exist relatively few fat elements in $\mathrm{GL}(\mathcal{V})$ which are not pppd-elements, and motivating the following definition.

Definition 5.20. Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. An element $g \in \mathrm{GL}(\mathcal{V})$ is said to be an *exceptional fat element*, or more precisely an *exceptional* $\mathrm{fat}(d, q; e)$*-element*, if g is a $\mathrm{fat}(d, q; e)$-element but not a $\mathrm{pppd}(d, q; e)$-element. In this case we also refer to g as a $\mathrm{fat}^*(d, q; e)$-element.

As illustrated in Example 5.10, depending on the dimension d of $\mathcal{V}$, the size q of the underlying field, and the integer e, the group $\mathrm{GL}(\mathcal{V})$ might or might not contain $\mathrm{fat}^*(d, q; e)$-elements.

Recall that q is a power of the prime p and that we write $g_{p'}$ for the p'-part of an element $g \in \mathrm{GL}(\mathcal{V})$. The following result is a direct consequence of Lemma 5.11$(a)(b)$.

Lemma 5.21. *Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$ and let $g \in \mathrm{GL}(\mathcal{V})$. Then g is a $\mathrm{fat}^*(d, q; e)$-element if and only if $g_{p'}$ is a $\mathrm{fat}^*(d, q; e)$-element.*

According to Lemma 5.4 any $\mathrm{fat}(d, q; e)$-element g in $\mathrm{GL}(\mathcal{V})$ has order divisible by a primitive divisor r of $q^e - 1$ as introduced in Definition 2.23. If we assume that g is an exceptional fat element, then (because g is not a pppd-element) r is not a prime power and thus has at least two distinct prime factors.

As we may verify by looking at Example 5.5, the fact that the order of an element g in $\mathrm{GL}(\mathcal{V})$ is divisible by a suitable "primitive *non* prime power divisor" does not guarantee that g is an exceptional fat element (or any fat element at all). However, we can rule out that some element in $\mathrm{GL}(\mathcal{V})$ is an exceptional fat element by checking that its order does not contain any minimal "primitive *non* prime power divisors" of $q^e - 1$. To some extend this method can be applied in a very general way, independently of the choice of d, q and e. That is, in some cases, we can deduce from just looking at the order of g (and without having any information on d, q or e) that g is not an exceptional fat element.

Lemma 5.22. *Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$ and let $g \in \mathrm{GL}(\mathcal{V})$ be a $\mathrm{fat}^*(d, q; e)$-element. Then the following hold.*

(a) *Neither $|g|$ nor $|g|/2$ are prime powers, and $|g| \notin \{1, 12, 15, 20, 24, 30, 40, 48, 51, 60, 68, 80, 85, 96\}$. In particular, $|g| \geq 21$.*

(b) *Suppose that q is a square and $|g| \leq 100$. Then $|g| \in \{35, 45, 55, 63, 65, 70, 77, 90, 91, 95, 99\}$.*

Proof. By Lemma 5.4 the order of g is divisible by a primitive divisor r of $q^e - 1$. We may assume that r is a minimal primitive divisor of $q^e - 1$, as

introduced in Definition 2.25. By definition (of exceptional fat elements) the integer r has at least two distinct prime divisors. In particular, $|g| \neq 1$.

(a) If $|g|$ is a prime power, then r is a prime power, and that is not true. Suppose that $|g|$ is not a prime power, but $|g|/2$ is. Then $|g|/2$ is odd. It follows that r is not divisible by 4. Hence, by Lemma 2.28(a) the integer r is odd. This reveals that r is a divisor of the prime power $|g|/2$. Thus, r is a prime power, which is not true.

Suppose that $|g| \in \{12, 15, 20, 24, 30, 40, 48, 51, 60, 68, 80, 85, 96\}$. Recalling that r is divisible by (at least) two distinct primes, one can check that $r \in \{6, 10, 12, 15, 20, 24, 30, 34, 40, 48, 51, 60, 68, 80, 85, 96\}$. Since r is a minimal primitive divisor of $q^e - 1$, by Lemma 2.28(a)(b) we have $\gcd(r, 4) \in \{1, 4\}$ and $r \notin \{12, 15, 20, 24, 40, 48, 51, 60, 68, 80, 85, 96\}$. This yields the contradiction $r \in \emptyset$.

(b) Seeking a contradiction assume that $|g| \notin \{35, 45, 55, 63, 65, 70, 77, 90, 91, 95, 99\}$. Since $|g| \leq 100$, by part (a) of the current lemma we get $|g| \in \{21, 28, 33, 36, 39, 42, 44, 52, 56, 57, 66, 69, 72, 75, 76, 78, 84, 87, 88, 92, 93, 100\}$. Since r is a divisor of $|g|$ which is divisible by (at least) two distinct primes, we may verify that $r \in \{6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 33, 36, 38, 39, 42, 44, 46, 50, 52, 56, 57, 66, 69, 72, 75, 76, 78, 84, 87, 88, 92, 93, 100\}$. Recalling that r is a minimal primitive divisor of $q^e - 1$ and that q is a square, according to Lemma 2.28(c) we have $\gcd(r, 16) \in \{1, 16\}$ and $\gcd(r, 9) \in \{1, 9\}$. Then $r \in \emptyset$. Contradiction. □

The following lemma is another useful tool for showing that some given $g \in \mathrm{GL}(\mathcal{V})$ is not an exceptional fat element.

Lemma 5.23. *Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Let $g \in \mathrm{GL}(\mathcal{V})$ be a $\mathrm{fat}^*(d, q; e)$-element and let ℓ be a prime dividing $|g|$. Then the following hold.*

(a) *We have*

$$d < \frac{(\ell - 1)(|g| - \ell)}{\ell} < (\sqrt{|g|} - 1)^2 < |g| - 8.$$

In particular, if $|g|$ is even, then $d < (|g| - 2)/2$.

(b) *Suppose that q is a square. Then*

$$d < \frac{(\ell - 1)(|g| - \ell)}{2\ell} < \frac{(\sqrt{|g|} - 1)^2}{2} < \frac{|g|}{2} - 5.$$

In particular, if $|g|$ is even, then $d < (|g| - 2)/4$.

Proof. By Lemma 5.4 the order of g is divisible by a primitive divisor r of $q^e - 1$. We may assume that r is a minimal primitive divisor of $q^e - 1$. By

definition (of exceptional fat elements) the integer r has at least two distinct prime divisors. From Lemma 2.28(a) we know that either 4 divides r, or r is odd. We can thus choose coprime integers $r_1, r_2 \geq 3$ such that $r = r_1 r_2$. Recall that we write $\varphi : \mathbb{N} \to \mathbb{N}$ to denote Euler's totient function. Observe that, since $r_1, r_2 \geq 3$, Lemma 2.1 implies that $\varphi(r_1)$ and $\varphi(r_2)$ are both even. Recall from Lemma 2.15 that

$$e = \operatorname{ord}(q; r) = \operatorname{lcm}\big\{\operatorname{ord}(q; r_1), \operatorname{ord}(q; r_2)\big\}. \tag{5.6}$$

(i) Using (5.6), (the "in particular" part of) Lemma 2.13, and recalling that $\varphi(r_1), \varphi(r_2)$ are even, we obtain $e \mid \operatorname{lcm}\big\{\varphi(r_1), \varphi(r_2)\big\} \mid \varphi(r_1)\varphi(r_2)/2$. Then (by Lemma 2.1) e is a divisor of $\varphi(r)/2$, and hence also a divisor of $\varphi(|g|)/2$. In particular,

$$e \leq \frac{\varphi(|g|)}{2}.$$

(ii) Suppose that q is a square. Then, combining (5.6) with Lemma 2.13 and the fact that $\varphi(r_1), \varphi(r_2)$ are even, reveals that e is a divisor of $\operatorname{lcm}\{\varphi(r_1)/2, \varphi(r_2)/2\}$. Thus, (by Lemma 2.1) the integer e divides $\varphi(r)/4$ and hence also $\varphi(|g|)/4$. In particular,

$$e \leq \frac{\varphi(|g|)}{4}.$$

Now, since $e > d/2$, we conclude that $d < \varphi(|g|)$ and that moreover, in case q is a square, we have $d < \varphi(|g|)/2$. Then by Lemma 2.3 we obtain

$$d < \frac{(\ell - 1)(|g| - \ell)}{\ell} < (\sqrt{|g|} - 1)^2,$$

and if q is a square, then

$$d < \frac{(\ell - 1)(|g| - \ell)}{2\ell} < \frac{(\sqrt{|g|} - 1)^2}{2}.$$

The remainder of the "main" assertion follows from Lemma 5.22, according to which we have $|g| \geq 21$, and in case q is a square even $|g| \geq 35$. The "in particular" parts follow from the "main" assertion by setting $\ell = 2$. □

II

FAT ELEMENTS IN THE MAXIMAL SUBGROUPS OF THE FINITE GENERAL LINEAR GROUP

Consider a finite vector space $\mathcal{V}$ of dimension $d \geq 2$. In [2] Aschbacher describes eight classes $\mathscr{C}_1, \ldots, \mathscr{C}_8$ of subgroups of $\mathrm{GL}(\mathcal{V})$ and proves the following (see also [30, Theorem 3.2] applied to $X_0 = \mathrm{SL}(\mathcal{V})$ and $X = \mathrm{GL}(\mathcal{V})$). Every subgroup of $\mathrm{GL}(\mathcal{V})$, which does not contain $\mathrm{SL}(\mathcal{V})$, either is contained in a member of one of these classes, or belongs to a certain family of subgroups which we specify in Definition 12.1 below.[(I)] Even though Aschbacher does not explicitly define a ninth class of subgroups, the latter family of subgroups is often referred to as Aschbacher's class $\mathscr{S}$. Members of the classes $\mathscr{C}_1, \ldots, \mathscr{C}_8$ are known as *geometric subgroups*, because they "preserve some geometric structure" in their natural action on the underlying vector space $\mathcal{V}$. For $i \in \{1, \ldots, 8\}$, the class $\mathscr{C}_i$ consists (roughly) of stabilisers in $\mathrm{GL}(\mathcal{V})$ of

$(i = 1)$ subspaces of $\mathcal{V}$;

$(i = 2)$ direct sum decompositions $\mathcal{V} = \bigoplus_{i=1}^{t} \mathcal{V}_i$, $\dim(\mathcal{V}_i) = d/t$;

$(i = 3)$ extension fields of prime index;

$(i = 4)$ tensor product decompositions $\mathcal{V} = \mathcal{V}_1 \otimes \mathcal{V}_2$;

$(i = 5)$ subfields of prime index;

$(i = 6)$ symplectic-type groups in absolutely irreducible representations;

$(i = 7)$ tensor decompositions $\mathcal{V} = \bigotimes_{i=1}^{t} \mathcal{V}_i$, $d = \dim(\mathcal{V}_i)^t$;

$(i = 8)$ non-degenerate classical form.

While not every geometric subgroup $G \in \mathscr{C}_i$ $(i \in \{1, \ldots, 8\})$ needs to be maximal in $\mathrm{GL}(\mathcal{V})$, according to [10,38] most of them turn out to be maximal.

In this part we investigate the occurrence of fat elements in various geometric subgroups of $\mathrm{GL}(\mathcal{V})$ and several members of $\mathscr{S}$. Guralnick et al. [30] classify all subgroups of $\mathrm{GL}(\mathcal{V})$ containing ppd-elements, which (as we may recall from Lemma 5.8) are examples of fat elements. Since the Aschbacher classes are partly overlapping, in order to avoid repetitions, [30] does not explicitly list all geometric subgroups which contain ppd-elements, like those belonging to $\mathscr{C}_5$. Nonetheless, the list of all geometric subgroups containing ppd-elements is rather short. This is because the geometric structure preserved often entails a factorisation of the group order, making the existence of ppd-elements highly restricted or even impossible. For example, members of $\mathscr{C}_2$ contain ppd-elements only if the corresponding direct sum decomposition consists of 1-dimensional subspaces; see [30, Lemma 4.1]. Members of $\mathscr{C}_4 \cup \mathscr{C}_7$ do not contain ppd-elements at all; see [30, first paragraph on p. 181]. DiMuro [21]

[(I)] In fact, Aschbacher formulates his statement in a more general setting for the group of all κ-semisimilarities on $\mathcal{V}$ with respect to a classical from κ; see [2, Theorem Γ, p. 503] or [30, Theorem 3.2].

generalises the results in [30] to pppd$(d, q; e)$-elements (as introduced in Definition 5.1(b)) with $e \geq \lfloor d/3 \rfloor$. He, too, obtains a comparatively short list of examples – especially if we assume e to be strictly bigger than $d/2$. Neither [30] nor [21] specify the number of all ppd-elements, and respectively all pppd-elements, in a given geometric subgroup.

We present a classification of geometric subgroups $G \in \mathscr{C}_i$ containing fat elements for $i \in \{1, 2, 3, 4, 5, 7\}$. Our results are presented in Chapters 6, 7, 8, 9, 10, and 11, respectively. (Classes $\mathscr{C}_6, \mathscr{C}_8$ will be considered in future work and are not investigated in this dissertation.) This not only involves deciding whether or not G contains fat elements, but also determining the precise number of such elements in G. What is more, in Chapter 6 (covering Aschbacher's $\mathscr{C}_1$-class, that is reducible groups) we examine the occurrence of fat elements in groups $G \cap H$, where $G \in \mathscr{C}_1$ and H is a subgroup of $\mathrm{GL}(\mathcal{V})$ containing $\mathrm{SL}(\mathcal{V})$. Additionally, for such groups H, we consider pairs of fat elements in $H \times H$ which generate a reducible group.

Chapter 12 examines the occurrence of exceptional fat elements (that is fat elements which are not pppd-elements) in covering groups of the sporadic simple groups and in covering groups of the finite simple linear, unitary, and symplectic groups in non-defining characteristic.

In contrast to [30] we follow a class-by-class approach, meaning that we deal with each of the classes $\mathscr{C}_1, \ldots, \mathscr{C}_5, \mathscr{C}_7, \mathscr{S}$ individually. For the sake of a clear structure we reserve a separate chapter for each Aschbacher class under consideration.

Chapter 6

Aschbacher's $\mathscr{C}_1$-class (Reducible subgroups)

The aim of this chapter is to examine fat elements in members of Aschbacher's $\mathscr{C}_1$-class.[(I)] More precisely, given a finite vector space $\mathcal{V} \neq \{0\}$, we are interested in the occurrence of fat elements in the stabiliser $\mathrm{GL}(\mathcal{V})_{\mathcal{W}}$ of a non-trivial and proper subspace $\mathcal{W}$ of $\mathcal{V}$. In fact, we widen the focus of our analysis to groups $H_{\mathcal{W}}$, where H is a subgroup of $\mathrm{GL}(\mathcal{V})$ containing $\mathrm{SL}(\mathcal{V})$. The corresponding findings are featured in Section 6.1. The main result is presented in Theorem 6.4.

Section 6.2 investigates *fat pairs*, that is pairs of fat elements, in $H \times H$, where $\mathrm{SL}(\mathcal{V}) \leq H \leq \mathrm{GL}(\mathcal{V})$. In Theorem 6.11 we give an explicit upper bound for the proportion of all fat pairs generating a reducible group in the set of all pairs in $H \times H$. Theorem 6.12 specifies an upper bound for the proportion of all pairs of elements generating a reducible group in the set of all fat pairs in $H \times H$. The latter can be interpreted as the (conditional) probability that, on a single random selection from the set of all fat pairs in $H \times H$, we obtain a pair generating a reducible group.

Throughout this chapter, even where not explicitly stated, we shall be working under the following hypothesis.

Hypothesis 6.1. let $d \in \mathbb{N}$, let q be a prime power, and let $\mathcal{V}$ be an $\mathbb{F}_q$-vector space of dimension d. Let H be a group satisfying $\mathrm{SL}(\mathcal{V}) \leq H \leq \mathrm{GL}(\mathcal{V})$.

[(I)] Large parts of this chapter have been published by Niemeyer, Praeger and the author in [47]. Here, we add some more details and refine [47, Lemma 4.4].

6.1 Proportion of fat elements

Consider a subspace $\mathcal{W}$ of $\mathcal{V}$. Recall that $H_{\mathcal{W}} = \{h \in H \mid \mathcal{W}h = \mathcal{W}\}$ denotes the subspace stabiliser of $\mathcal{W}$ in H. If $\mathcal{U}$ is another subspace of $\mathcal{V}$, then we write

$$(H_{\mathcal{W}})_{\mathcal{U}} = H_{\mathcal{W},\mathcal{U}}.$$

Recall further Definition 5.1(a) of fat elements. Our method to determine the proportion (in $H_{\mathcal{W}}$) of all fat elements in $H_{\mathcal{W}}$ follows the approach taken in Subsection 5.2.2. The findings presented in this section are essentially refinements of Lemmas 5.15, 5.16 and Theorem 5.18, and we can retrieve their statements by setting $\mathcal{W} = \{0\}$ and $\mathcal{W} = \mathcal{V}$, respectively.

We do not assume $\mathcal{W}$ to be a non-trivial and proper subspace of $\mathcal{V}$ (even though the group $\mathrm{GL}(\mathcal{V})_{\mathcal{V}} = \mathrm{GL}(\mathcal{V})_{\{0\}} = \mathrm{GL}(\mathcal{V})$ does not belong to Aschbacher's $\mathscr{C}_1$-class), as the results in this section also hold for $\mathcal{W} \in \{\{0\}, \mathcal{V}\}$.

Lemma 6.2. *Suppose that Hypothesis 6.1 holds. Let $\mathcal{W}$ be a w-dimensional subspace of $\mathcal{V}$ and let $e \in \mathbb{N}$.*

(a) *If $e + w \leq d$, then $H_{\mathcal{W}}$ acts transitively on the set of all e-dimensional subspaces $\mathcal{U} \leq \mathcal{V}$ such that $\mathcal{U} \cap \mathcal{W} = \{0\}$.*

(b) *If $e \leq w \leq d$, then $H_{\mathcal{W}}$ acts transitively on the set of all e-dimensional subspaces $\mathcal{U} \leq \mathcal{W}$.*

Proof. Let $\mathcal{U}, \mathcal{U}'$ be subspaces in $\mathcal{V}$ such that $\dim(\mathcal{U}) = \dim(\mathcal{U}') = e$, and

$$\begin{cases} \mathcal{U} \cap \mathcal{W} = \mathcal{U}' \cap \mathcal{W} = \{0\}, & \text{in case } (a), \\ \mathcal{U}, \mathcal{U}' \leq \mathcal{W}, & \text{in case } (b). \end{cases}$$

Choose two bases $\{v_1, \ldots, v_d\}$ and $\{v'_1, \ldots, v'_d\}$ for $\mathcal{V}$ such that

$$\begin{aligned} \mathcal{W} &= \langle v_1, \ldots, v_w \rangle = \langle v'_1, \ldots, v'_w \rangle, \\ \mathcal{U} &= \langle v_{t+1}, \ldots, v_{t+e} \rangle, \\ \mathcal{U}' &= \langle v'_{t+1}, \ldots, v'_{t+e} \rangle, \end{aligned}$$

where $t = w$ in case (a), and $t = 0$ in case (b). We first define $\ell \in \mathrm{GL}(\mathcal{V})$ by $v_i\ell = v'_i$ for $i \in \{1, \ldots, d\}$. Next, we define $h \in \mathrm{GL}(\mathcal{V})$ by $v_1 h = \det(\ell)^{-1} v'_1$ and $v_i h = v'_i$ for $i = \{2, \ldots, d\}$. Then $\mathcal{W}h = \mathcal{W}$ and $\det(h) = \det(\ell)^{-1} \det(\ell) = 1$, that is $h \in \mathrm{SL}(\mathcal{V})_{\mathcal{W}} \leq H_{\mathcal{W}}$. Moreover, $\mathcal{U}h = \mathcal{U}'$. □

Lemma 6.3. *Suppose that Hypothesis 6.1 holds with $d \geq 2$, and let $\mathcal{W} \leq \mathcal{V}$. Let $\mathcal{U}$ be a non-trivial and proper subspace of $\mathcal{V}$ satisfying either $\mathcal{U} \leq \mathcal{W}$ or $\mathcal{U} \cap \mathcal{W} = \{0\}$. Then the mapping*

$$H_{\mathcal{W},\mathcal{U}} \to \mathrm{GL}(\mathcal{U}), \quad g \mapsto g|_{\mathcal{U}}$$

is a surjective group homomorphism.

Proof. We only prove that the mapping $\delta : H_{\mathcal{W},\mathcal{U}} \to \mathrm{GL}(\mathcal{U})$ given by $g \mapsto g|_{\mathcal{U}}$ is surjective. If $\mathcal{W} \in \{\{0\}, \mathcal{V}\}$ or $\mathcal{W} = \mathcal{U}$, then $H_{\mathcal{W},\mathcal{U}} = H_{\mathcal{U}}$ and the assertion holds by Lemma 5.16. Hence, assume that

$$\mathcal{W} \notin \{\{0\}, \mathcal{V}\} \quad \text{and} \quad \mathcal{W} \neq \mathcal{U}.$$

First suppose that $\mathcal{U}$ is a (proper) subspace of $\mathcal{W}$. Consider the group homomorphisms

$$\delta_1 : H_{\mathcal{W},\mathcal{U}} \to \mathrm{GL}(\mathcal{W}), \quad g \mapsto g|_{\mathcal{W}},$$
$$\delta_2 : \mathrm{im}(\delta_1) \to \mathrm{GL}(\mathcal{U}), \quad g \mapsto g|_{\mathcal{U}}.$$

Observe that $\mathrm{im}(\delta) = \mathrm{im}(\delta_2)$. Since $\mathrm{SL}(\mathcal{V}) \leq H$, by Lemma 5.16 the mapping $H_{\mathcal{W}} \to \mathrm{GL}(\mathcal{W})$, $g \mapsto g|_{\mathcal{W}}$ is surjective. Hence, $\mathrm{GL}(\mathcal{W})_{\mathcal{U}} \leq \mathrm{im}(\delta_1)$, and again using Lemma 5.16 (applied to $\mathcal{V} = \mathcal{W}$) it follows that $\mathrm{im}(\delta_2) = \mathrm{GL}(\mathcal{U})$.

Now, suppose that $\mathcal{U} \cap \mathcal{W} = \{0\}$. Let $e = \dim(\mathcal{U})$ and $w = \dim(\mathcal{W})$ (whence $e + w \leq d$). Since $\mathcal{U}$ and $\mathcal{W}$ intersect trivially, we may choose a basis $\{v_1, \ldots, v_d\}$ of $\mathcal{V}$ such that $\mathcal{U} = \langle v_1, \ldots, v_e \rangle$ and $\mathcal{W} = \langle v_{e+1}, \ldots, v_{e+w} \rangle$. (Recall that $\mathcal{W} \neq \{0\}$, whence $w \geq 1$.) Let $\ell \in \mathrm{GL}(\mathcal{U})$. Define $\widehat{\ell} \in \mathrm{GL}(\mathcal{V})$ by

$$v_i\widehat{\ell} = \begin{cases} v_i\ell, & \text{if } 1 \leq i \leq e, \\ \det(\ell)^{-1}v_i, & \text{if } i = e+1, \\ v_i, & \text{if } e+2 \leq i \leq d. \end{cases}$$

Then $\det(\widehat{\ell}) = \det(\ell)\det(\ell)^{-1} = 1$, $\mathcal{U}\widehat{\ell} = \mathcal{U}\ell = \mathcal{U}$, and $\mathcal{W}\widehat{\ell} = \mathcal{W}$. Hence, $\widehat{\ell} \in \mathrm{SL}(\mathcal{V})_{\mathcal{W},\mathcal{U}} \leq H_{\mathcal{W},\mathcal{U}}$. Moreover, $\widehat{\ell}|_{\mathcal{U}} = \ell$. This completes the proof. □

Consider an integer e such that $d/2 < e \leq d$. As introduced in Definition 5.17, we write $\mathrm{fat}(H_{\mathcal{W}}; e)$ for the proportion (in $H_{\mathcal{W}}$) of all $\mathrm{fat}(d, q; e)$-elements in $H_{\mathcal{W}}$. The following theorem determines the precise value of, and also gives good lower and upper bounds for, the proportion $\mathrm{fat}(H_{\mathcal{W}}; e)$.

Recall from Definition 3.5 the meaning of $N_q^*(e)$. A formula for $N_q^*(e)$ is given in Lemma 3.7. Note that we write $\mathrm{SL}(e, q)$ for the subgroup of $\mathrm{GL}(e, q)$ consisting of all invertible $(e \times e)$-matrices over $\mathbb{F}_q$ with determinant 1. In view of the group isomorphism (4.2) on p. 52, Definition 4.4(*b*) and Lemma 4.8(*a*), we call a matrix in $\mathrm{GL}(e, q)$ *irreducible* if its characteristic polynomial is irreducible. By Proposition 5.14, the group $\mathrm{SL}(e, q)$ contains irreducible elements.

Theorem 6.4. *Suppose that Hypothesis 6.1 holds with $d \geq 2$. Let $\mathcal{W} \leq \mathcal{V}$ and let e be an integer satisfying $d/2 < e \leq d$.*

(a) We have $\mathrm{fat}(H_{\mathcal{W}}; e) \neq 0$ if and only if $\dim(\mathcal{W}) \in [0, d-e] \cup [e, d]$.

(b) Suppose that $\mathrm{fat}(H_{\mathcal{W}}; e) \neq 0$. Then $\mathrm{fat}(H_{\mathcal{W}}; e) = \mathrm{fat}(H; e)$, that is

$$\mathrm{fat}(H_{\mathcal{W}}; e) = \frac{N_q^*(e)}{q^e - 1}$$

and moreover,

$$\frac{1}{e+1} \leq \mathrm{fat}(H_{\mathcal{W}}; e) < \frac{1}{e}.$$

Proof. First, suppose that $\dim(\mathcal{W}) \in [0, d-e] \cup [e, d]$. Then there exists a basis $\mathfrak{B} = \{v_1, \ldots, v_d\}$ of $\mathcal{V}$ such that, writing $w = \dim(\mathcal{W})$, we have

$$\mathcal{W} = \begin{cases} \langle v_1, \ldots, v_w \rangle, & \text{if } e \leq \dim(\mathcal{W}) \leq d, \\ \langle v_{e+1}, \ldots, v_{e+w} \rangle, & \text{if } 0 \leq \dim(\mathcal{W}) \leq d-e. \end{cases}$$

Let s be an irreducible element of $\mathrm{SL}(e, q)$ and let $g \in \mathrm{GL}(\mathcal{V})$ be such that the matrix of g with respect to $\mathfrak{B}$ is equal to

$$g_{\mathfrak{B}} = \begin{pmatrix} s & \mathbf{0}_{e,d-e} \\ \mathbf{0}_{d-e,e} & \mathbf{1} \end{pmatrix} \in \mathrm{GL}(d, q),$$

where $\mathbf{1}$ is the identity in $\mathrm{GL}(d-e, q)$ and $\mathbf{0}_{a,b}$ denotes the $(a \times b)$-zero matrix over $\mathbb{F}_q$ $(a, b \in \{e, d-e\})$. Then $\det(g) = \det(s) = 1$ and $\mathcal{W}g = \mathcal{W}$, whence $g \in \mathrm{SL}(\mathcal{V})_{\mathcal{W}} \leq H_{\mathcal{W}}$. Since the characteristic polynomial of g contains an irreducible factor of degree e (namely that characteristic polynomial of s), applying Lemma 5.2 we see that g is a $\mathrm{fat}(d, q; e)$-element.

Conversely, suppose that $H_{\mathcal{W}}$ contains a $\mathrm{fat}(d, q; e)$-element g. Let $\mathcal{U}'$ be the uniquely determined $\langle g \rangle$- irreducible subspace of $\mathcal{V}$ with $\dim(\mathcal{U}') = e$. Since $\mathcal{W}$ is $\langle g \rangle$-invariant, we see that the intersection $\mathcal{U}' \cap \mathcal{W}$ is a $\langle g \rangle$-invariant subspace of $\mathcal{U}'$, which (due to the fact that $\mathcal{U}'$ is $\langle g \rangle$-irreducible) must be either trivial or equal to $\mathcal{U}'$. Hence,

$$\mathcal{U}' \cap \mathcal{W} = \{0\} \quad \text{or} \quad \mathcal{U}' \leq \mathcal{W}.$$

In particular, $\dim(\mathcal{W}) \leq d - e$ or $\dim(\mathcal{W}) \geq e$. (This completes the proof of part (a).) It follows that the number of all $\mathrm{fat}(d, q; e)$-elements in $H_{\mathcal{W}}$ satisfies

$$\underbrace{\mathrm{fat}(H_{\mathcal{W}}; e)||H_{\mathcal{W}}|}_{\substack{\text{number of } \mathrm{fat}(d,q;e)\text{-} \\ \text{elements in } H_{\mathcal{W}}}} = \sum_{\mathcal{U} \in \mathbf{U}} \underbrace{\mathrm{fat}(H_{\mathcal{W},\mathcal{U}}; e)|H_{\mathcal{W},\mathcal{U}}|}_{\substack{\text{number of } \mathrm{fat}(d,q;e)\text{-} \\ \text{elements in } H_{\mathcal{W},\mathcal{U}}}}, \tag{6.1}$$

where

$$\mathbf{U} := \begin{cases} \{\mathcal{U} \leq \mathcal{V} \mid \dim(\mathcal{U}) = e, \mathcal{U} \cap \mathcal{W} = \{0\}\}, & \text{if } \dim(\mathcal{W}) \leq d - e, \\ \{\mathcal{U} \leq \mathcal{V} \mid \dim(\mathcal{U}) = e, \mathcal{U} \leq \mathcal{W}\}, & \text{if } \dim(\mathcal{W}) \geq e. \end{cases}$$

Fix a subspace $\mathcal{U} \in \mathbf{U}$. By Lemma 6.3 the mapping

$$\delta : H_{\mathcal{W},\mathcal{U}} \to \mathrm{GL}(\mathcal{U}), \quad g \mapsto g|_{\mathcal{U}}$$

is a surjective group homomorphism. Observe that $g \in H_{\mathcal{W},\mathcal{U}}$ is a $\mathrm{fat}(d, q; e)$-element if and only if $g|_{\mathcal{U}}$ is irreducible. Moreover, since elements of $\ker(\delta)$ act trivially on $\mathcal{U}$, the restriction $g|_{\mathcal{U}}$ is irreducible if and only if all elements contained in the coset $\ker(\delta)g$ are $\mathrm{fat}(d, q; e)$-elements. If follows that the number of all $\mathrm{fat}(d, q; e)$-elements in $H_{\mathcal{W},\mathcal{U}}$ is equal to $|\ker(\delta)|$ times the number of all irreducible elements in $\mathrm{im}(\delta) = \mathrm{GL}(\mathcal{U})$. That is,

$$\mathrm{fat}(H_{\mathcal{W},\mathcal{U}}; e)|H_{\mathcal{W},\mathcal{U}}| = \underbrace{|\ker(\delta)||\mathrm{im}(\delta)|}_{=|H_{\mathcal{W},\mathcal{U}}|} \mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big),$$

where $\mathrm{irr}(\mathrm{GL}(\mathcal{U}))$ is the proportion (in $\mathrm{GL}(\mathcal{U})$) of all irreducible element in $\mathrm{GL}(\mathcal{U})$, as introduced in Definition 4.20. Then $\mathrm{fat}(H_{\mathcal{W},\mathcal{U}}; e) = \mathrm{irr}(\mathrm{GL}(\mathcal{U}))$ and Equation (6.1) simplifies to

$$\mathrm{fat}(H_{\mathcal{W}}; e)|H_{\mathcal{W}}| = \sum_{\mathcal{U} \in \mathbf{U}} \mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big)|H_{\mathcal{W},\mathcal{U}}|.$$

Since (by Proposition 5.14) the value of $\mathrm{irr}(\mathrm{GL}(\mathcal{U}))$ only depends on the integers e and q, and since by Lemma 6.2 (and the orbit-stabiliser-theorem) we have $|\mathbf{U}| = |H_{\mathcal{W}} : H_{\mathcal{W},\mathcal{U}}|$, we conclude that

$$\mathrm{fat}(H_{\mathcal{W}}; e)|H_{\mathcal{W}}| = |H_{\mathcal{W}} : H_{\mathcal{W},\mathcal{U}}| \, \mathrm{irr}\big(\mathrm{GL}(\mathcal{U})\big)|H_{\mathcal{W},\mathcal{U}}|.$$

Then $\mathrm{fat}(H_{\mathcal{W}}; e) = \mathrm{irr}(\mathrm{GL}(\mathcal{U}))$. The assertion now follows from Proposition 5.14. (Note that since $d \geq 2$ we have $e > d/2 \geq 1$.) □

6.2 Reducible fat pairs

In this section we study pairs of fat elements in $H \times H$ which generate a reducible group. Recall Definitions 4.4(*b*), 5.1(*a*), 5.17.

Definition 6.5. Suppose that Hypothesis 6.1 holds.

(*a*) We say that $(g_1, g_2) \in \mathrm{GL}(\mathcal{V}) \times \mathrm{GL}(\mathcal{V})$ is *reducible* if the group $\langle g_1, g_2 \rangle$ generated by g_1 and g_2 is reducible.

(*b*) We call $(g_1, g_2) \in \mathrm{GL}(\mathcal{V}) \times \mathrm{GL}(\mathcal{V})$ a *fat pair*, or more precisely a $\mathrm{fat}(d, q; e_1, e_2)$-*pair* if, for $i \in \{1, 2\}$, g_i is a $\mathrm{fat}(d, q; e_i)$-element for some $e_i \in \mathbb{N}$ satisfying $d/2 \leq e_i \leq d$.

(*c*) Let $e_1, e_2 \in \mathbb{N}$ be such that $d/2 < e_1, e_2 \leq d$. We write $\mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2)$ for the proportion of all reducible $\mathrm{fat}(d, q; e_1, e_2)$-pairs in the set of all pairs in $H \times H$.

(*d*) We define

$$\mathrm{red}\mathit{and}\mathrm{fat}(H) = \sum_{d/2<e_1,e_2\leq d} \mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2)$$

and

$$\mathrm{red}\mathit{if}\mathrm{fat}(H) = \frac{\sum_{d/2<e_1,e_2\leq d} \mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2)}{\sum_{d/2<e_1,e_2\leq d} \mathrm{fat}(H; e_1)\mathrm{fat}(H; e_2)}.$$

By definition $\mathrm{red}\mathit{and}\mathrm{fat}(H)$ is the proportion of all reducible fat pairs in the set of all pairs in $H \times H$, and $\mathrm{red}\mathit{if}\mathrm{fat}(H)$ is the proportion of all reducible pairs in the set of all fat pairs in $H \times H$. The aim of this section is to calculate explicit upper bounds for $\mathrm{red}\mathit{and}\mathrm{fat}(H)$ and $\mathrm{red}\mathit{if}\mathrm{fat}(H)$. The results are presented in Theorems 6.11, 6.12. The proofs of both theorems involve counting certain subspaces in $\mathcal{V}$. It is common practice to denote the number of all w-dimensional subspaces in $\mathcal{V}$ (for $0 \leq w \leq d$) by the *Gaussian coefficients* (see for example [14, p. 124]).

Definition 6.6. Let $\mathcal{V}$ be as in Hypothesis 6.1 and let $w \leq d$ be a non-negative integer. The *Gaussian coefficient* $\binom{d}{w}_q$ is the number of w-dimensional subspaces in $\mathcal{V}$.

An explicit formula for $\binom{d}{w}_q$ is given for example in [14, (9.2.2)].

Lemma 6.7. *Let d, q be as in Hypothesis 6.1 and let $w \leq d$ be a non-negative integer. Then*

$$\binom{d}{w}_q = \frac{\prod_{i=d-w+1}^{d}(q^i - 1)}{\prod_{i=1}^{w}(q^i - 1)}.$$

In particular, we have (see for example [14, Proposition 9.2.4]) the following.

Lemma 6.8. *In the situation of Lemma 6.7 we have $\binom{d}{w}_q = \binom{d}{d-w}_q$.*

Recall that, for a rational number r, we write $\lceil r \rceil$ to denote the smallest integer which is at least equal to r.

Lemma 6.9. *For d, q as in Hypothesis 6.1 we have $\sum_{i=1}^{\lceil d/2 \rceil - 1} \binom{d}{i}_q^{-1} < q^{-d+1}$.*

Proof. If $d \in \{1, 2\}$, then $\sum_{i=1}^{\lceil d/2 \rceil - 1} \binom{d}{i}_q^{-1} = 0 < q^{-d+1}$. So assume that $d \geq 3$. By Lemma 6.7 we get $\binom{d}{2}_q < \binom{d}{i}_q$ for $2 < i \leq \lceil d/2 \rceil - 1$. Hence,

$$\sum_{i=1}^{\lceil d/2 \rceil - 1} \frac{q^{d-1}}{\binom{d}{i}_q} \leq \frac{q^{d-1}}{\binom{d}{1}_q} + \left(\left\lceil \frac{d}{2} \right\rceil - 2 \right) \frac{q^{d-1}}{\binom{d}{2}_q}. \tag{6.2}$$

Again, using Lemma 6.7, we have

$$\frac{q^{d-1}}{\binom{d}{1}_q} = \frac{q^{d-1}(q-1)}{q^d - 1} = 1 - q^{-1} + q^{-d} - \frac{q^{-1} - q^{-d}}{q^d - 1} < 1 - q^{-1} + q^{-d},$$

and (recalling that $d \geq 3$)

$$\begin{aligned} \frac{q^{d-1}}{\binom{d}{2}_q} &= \frac{q^{d-1}(q-1)(q^2-1)}{(q^d-1)(q^{d-1}-1)} \\ &= q^{-d+3} - \frac{q^{d+1} + q^d - q^{d-1} - q^3 - q^2 + q^{-d+3}}{(q^d-1)(q^{d-1}-1)} \\ &< q^{-d+3}, \end{aligned}$$

which combined with (6.2) yield

$$\sum_{i=1}^{\lceil d/2 \rceil - 1} \frac{q^{d-1}}{\binom{d}{i}_q} < 1 - q^{-1} + q^{-d} + \left(\left\lceil \frac{d}{2} \right\rceil - 2 \right) q^{-d+3} =: \mu(d, q).$$

We prove the assertion by showing that $\mu(d, q) < 1$.

If $d \in \{3, 4\}$, then $\mu(d, q) = 1 - q^{-1} + q^{-d} < 1$. For $d \geq 5$ we use induction on d to show that $\mu(d, q) < 1$. Now, $\mu(5, q) = 1 - q^{-1} + q^{-5} + q^{-2} < 1$. Next, assuming $\mu(d, q) < 1$, we have

$$\begin{aligned} \mu(d+1, q) &= 1 - q^{-1} + q^{-d-1} + \left(\left\lceil \frac{d+1}{2} \right\rceil - 2 \right) q^{-d+2} \\ &< 1 - q^{-1} + q^{-d} + \left(\left\lceil \frac{d}{2} \right\rceil - 1 \right) q^{-d+2} \\ &= 1 - q^{-1} + q^{-d} + \left(\left\lceil \frac{d}{2} \right\rceil - 1 \right) q^{-d+2} + \\ &\quad + \underbrace{\left(\left\lceil \frac{d}{2} \right\rceil - 2 \right) q^{-d+3} - \left(\left\lceil \frac{d}{2} \right\rceil - 2 \right) q^{-d+3}}_{=0}. \end{aligned}$$

By assumption, $\mu(d,q) = 1 - q^{-1} + q^{-d} + (\lceil d/2 \rceil - 2)q^{-d+3} < 1$, and thus

$$\mu(d+1,q) < 1 + \left(\left\lceil \frac{d}{2} \right\rceil - 1\right) q^{-d+2} - \left(\left\lceil \frac{d}{2} \right\rceil - 2\right) q^{-d+3}.$$

Using $q \geq 2$ and $d \geq 5$, we obtain

$$\begin{aligned}\mu(d+1,q) &< 1 + \left(\left\lceil \frac{d}{2} \right\rceil - 1\right) q^{-d+2} - 2\left(\left\lceil \frac{d}{2} \right\rceil - 2\right) q^{-d+2} \\ &= 1 - q^{-d+2} \underbrace{\left(\left\lceil \frac{d}{2} \right\rceil - 3\right)}_{\geq 0} \\ &\leq 1\end{aligned}$$

as needed. □

We next calculate an upper bound for the proportion red*and*fat$(H; e_1, e_2)$, as introduced in Definition 6.5(*c*). Note that $(h_1, h_2) \in H \times H$ is a reducible fat$(d, q; e_1, e_2)$ pair if and only if there exists a non-trivial and proper subspace $\mathcal{W} \leq \mathcal{V}$ such that h_i is a fat$(d, q; e_i)$-element in $H_{\mathcal{W}}$. If $\max\{e_1, e_2\} = d$, then $\langle h_1, h_2 \rangle$ is irreducible. Hence, in order that $\mathcal{W}$ exists, we need $e_i < d$ for $i \in \{1, 2\}$, and (since $e_i > d/2$) particularly $d \geq 3$. Recall from Definition 5.17 that fat$(H; e)$ is the proportion (in H) of all fat$(d, q; e)$-elements in H.

Lemma 6.10. *Suppose that Hypothesis 6.1 holds with $d \geq 3$. Let $e_1, e_2 \in \mathbb{N}$ be such that $d/2 < e_1, e_2 < d$. Then*

$$\begin{aligned}\text{red}\textit{and}\text{fat}(H; e_1, e_2) &< 2\,\text{fat}(H; e_1)\,\text{fat}(H; e_2) q^{-d+1} \\ &< \frac{2}{e_1 e_2} q^{-d+1} \leq \frac{8}{(d+1)^2} q^{-d+1}.\end{aligned}$$

Proof. Suppose that $H \times H$ contains a reducible fat$(d, q; e_1, e_2)$-pair (h_1, h_2). Then there exists at least one non-trivial and proper subspace $\mathcal{W} \leq \mathcal{V}$ such that h_i is a fat$(d, q; e_i)$-element in $H_{\mathcal{W}}$, $i \in \{1, 2\}$. For $i \in \{1, 2\}$ we obtain the following. There exists a (uniquely determined) $\langle h_i \rangle$-irreducible subspace $\mathcal{U}_i$ of $\mathcal{V}$ with $\dim(\mathcal{U}_i) = e_i$. The intersection $\mathcal{W} \cap \mathcal{U}_i$ is a $\langle h_i \rangle$-invariant subspace of $\mathcal{U}_i$. Since $\mathcal{U}_i$ is irreducible it follows that $\mathcal{W} \cap \mathcal{U}_i$ is either trivial or equal to $\mathcal{U}_i$. Suppose that we have $\mathcal{W} \cap \mathcal{U}_i = \{0\}$ and $\mathcal{W} \cap \mathcal{U}_{3-i} = \mathcal{U}_{3-i}$. Then $\mathcal{U}_1 \cap \mathcal{U}_2 = \{0\}$ which contradicts $\dim(\mathcal{U}_i) = e_i > d/2$. Thus either $\mathcal{W} \cap \mathcal{U}_1 = \mathcal{W} \cap \mathcal{U}_2 = \{0\}$, or $\mathcal{W} \cap \mathcal{U}_1 = \mathcal{U}_1$ and $\mathcal{W} \cap \mathcal{U}_2 = \mathcal{U}_2$. Hence, (recalling that $\dim(\mathcal{W}) \notin \{0, d\}$) we have either $1 \leq \dim(\mathcal{W}) \leq d - \max\{e_1, e_2\}$ or $\max\{e_1, e_2\} \leq \dim(\mathcal{W}) \leq d - 1$.

We thus obtain the following upper bound for the number of all reducible fat$(d, q; e_1, e_2)$-pairs in $H \times H$.

$$\text{red}\textit{and}\text{fat}(H; e_1, e_2)|H|^2 \leq \sum_{w} \sum_{\mathcal{W}} \prod_{i=1,2} \text{fat}(H_{\mathcal{W}}; e_i)|H_{\mathcal{W}}|,$$

where $w \in [1, d-\max\{e_1,e_2\}] \cup [\max\{e_1,e_2\}, d-1]$, and where the second sum runs over all $\mathcal{W} \leq \mathcal{V}$ with $\dim(\mathcal{W}) = w$. According to Theorem 6.4(b) we have $\prod_{i=1,2} \mathrm{fat}(H_{\mathcal{W}}; e_i) = \prod_{i=1,2} \mathrm{fat}(H; e_i)$. Thus,

$$\mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2) \leq \mathrm{fat}(H; e_1)\mathrm{fat}(H; e_2) \sum_{w} \sum_{\mathcal{W}} |H : H_{\mathcal{W}}|^{-2},$$

with $w, \mathcal{W}$ as before. Since H acts transitively on the set of all w-dimensional subspaces in $\mathcal{V}$ (see Lemma 5.15), there is a total of $|H : H_{\mathcal{W}}|$ such subspaces whence

$$\begin{aligned}
&\mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2) \\
&\quad \leq \mathrm{fat}(H; e_1)\mathrm{fat}(H; e_2) \sum_{\substack{1 \leq w \leq d-\max\{e_1,e_2\} \\ \max\{e_1,e_2\} \leq w \leq d-1}} \binom{d}{w}_q^{-1} \\
&\quad = \mathrm{fat}(H; e_1)\mathrm{fat}(H; e_2) \sum_{1 \leq w \leq d-\max\{e_1,e_2\}} \left(\binom{d}{w}_q^{-1} + \binom{d}{d-w}_q^{-1} \right).
\end{aligned}$$

Then, since $\binom{d}{w}_q = \binom{d}{d-w}_q$ by Lemma 6.8 and since $d - \max\{e_1, e_2\} \leq \lceil d/2 \rceil - 1$, we obtain

$$\mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2) \leq 2\,\mathrm{fat}(H; e_1)\,\mathrm{fat}(H; e_2) \sum_{w=1}^{\lceil d/2 \rceil - 1} \binom{d}{w}_q^{-1}.$$

Using Lemma 6.9, it follows that

$$\mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2) < 2\,\mathrm{fat}(H; e_1)\mathrm{fat}(H; e_2) q^{-d+1}.$$

By (the "moreover" part of) Theorem 5.18, for $i = 1, 2$, $\mathrm{fat}(H; e_i) < 1/e_i$. We get $2e_1^{-1}e_2^{-1}q^{-d+1} \leq 8(d+1)^{-2}q^{-d+1}$ as $e_i \geq (d+1)/2$. □

We now have all ingredients to prove the main results of this section. Recall Definition 6.5(d).

Theorem 6.11. *Suppose that Hypothesis 6.1 holds with $d \geq 3$. Then*

$$\mathrm{red}\mathit{and}\mathrm{fat}(H) < q^{-d+1}.$$

Proof. In the case $d = \max\{e_1, e_2\}$ any $\mathrm{fat}(d, q; e_1, e_2)$-pair generates an irreducible group, and thus $\mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_1) = 0$. Hence,

$$\mathrm{red}\mathit{and}\mathrm{fat}(H) = \sum_{\lceil (d+1)/2 \rceil \leq e_1, e_2 \leq d-1} \mathrm{red}\mathit{and}\mathrm{fat}(H; e_1, e_2).$$

Using Lemma 6.10 we obtain

$$\mathrm{red}\mathit{and}\mathrm{fat}(H) < \sum_{\lceil (d+1)/2\rceil \le e_1,e_2 \le d-1} \frac{2}{e_1 e_2} q^{-d+1}.$$

Consider $s = \sum_{i=\lceil (d+1)/2\rceil}^{d-1} i^{-1}$. If d is odd, then

$$s = \sum_{i=(d+1)/2}^{d-1} \frac{1}{i} < \int_{(d-1)/2}^{d-1} \frac{dx}{x} = \ln(d-1) - \ln\left(\frac{d-1}{2}\right) = \ln(2).$$

If d is even, we have $\lceil (d+1)/2\rceil = (d+2)/2$, and then

$$s = \sum_{i=(d+2)/2}^{d-1} \frac{1}{i} < \int_{d/2}^{d-1} \frac{dx}{x} < \int_{d/2}^{d} \frac{dx}{x} = \ln(d) - \ln\left(\frac{d}{2}\right) = \ln(2).$$

Hence, $\mathrm{red}\mathit{and}\mathrm{fat}(H) < 2s^2 q^{-d+1} < 2\big(\ln(2)\big)^2 q^{-d+1} < q^{-d+1}$, as required. □

Recall from Definition 6.5(d) that $\mathrm{red}\mathit{if}\mathrm{fat}(H)$ is the proportion of all reducible fat pairs in the set of fat pairs from $H \times H$. Equivalently, we may define $\mathrm{red}\mathit{if}\mathrm{fat}(H)$ to be the (conditional) probability that, on a single random selection from the set of fat pairs in $H \times H$, we obtain a reducible pair.

Theorem 6.12. *Suppose that Hypothesis 6.1 holds with $d \ge 3$. Then*

$$\mathrm{red}\mathit{if}\mathrm{fat}(H) < 2q^{-d+1}.$$

Proof. According to Definition 6.5(d) we have

$$\mathrm{red}\mathit{if}\mathrm{fat}(H) = \frac{\sum_{d/2<e_1,e_2\le d} \mathrm{red}\mathit{and}\mathrm{fat}(H;e_1,e_2)}{\sum_{d/2<e_1,e_2\le d} \mathrm{fat}(H;e_1)\,\mathrm{fat}(H;e_2)}.$$

If $\max\{e_1,e_2\} = d$, then every $\mathrm{fat}(d,q;e_1,e_2)$-pair in $H \times H$ generates an irreducible group, and hence $\mathrm{red}\mathit{and}\mathrm{fat}(H;e_1,e_2) = 0$ in that case. If e_1, e_2 are integers satisfying $d/2 < e_1, e_2 < d$, then by Lemma 6.10 we have

$$\mathrm{red}\mathit{and}\mathrm{fat}(H;e_1,e_2) < 2\,\mathrm{fat}(H;e_1)\,\mathrm{fat}(H;e_2)\,q^{-d+1}.$$

Note that, being a proportion, $\mathrm{fat}(H;e_i)$ is greater than or equal to zero, which is why $\sum_{d/2<e_1,e_2\le d} \mathrm{fat}(H;e_1)\mathrm{fat}(H;e_2) \ge \sum_{d/2<e_1,e_2<d} \mathrm{fat}(H;e_1)\mathrm{fat}(H;e_2)$. We conclude that

$$\mathrm{red}\mathit{if}\mathrm{fat}(H) < \frac{\sum_{d/2<e_1,e_2<d} 2\,\mathrm{fat}(H;e_1)\,\mathrm{fat}(H;e_2)\,q^{-d+1}}{\sum_{d/2<e_1,e_2<d} \mathrm{fat}(H;e_1)\,\mathrm{fat}(H;e_2)} = 2q^{-d+1}.$$

□

Chapter 7

Aschbacher's $\mathscr{C}_2$-class (Imprimitive subgroups)

In this chapter we are concerned with fat elements in linear groups belonging to Aschbacher's $\mathscr{C}_2$-class. More precisely, given a finite vector space $\mathcal{V}$ and a divisor t of $\dim(\mathcal{V})$, we investigate fat elements in $\mathrm{GL}(\mathcal{V})$ which stabilise a direct sum decomposition

$$\mathcal{V} = \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_t \tag{7.1}$$

of $\dim(\mathcal{V})/t$-dimensional subspaces $\mathcal{V}_1, \ldots, \mathcal{V}_t \leq \mathcal{V}$ by permuting these subspaces amongst themselves. We call the set $\mathfrak{F} = \{\mathcal{V}_1, \ldots, \mathcal{V}_t\}$ a *$\mathscr{C}_2$-frame*, write $\mathrm{C}_2(\mathfrak{F})$ for the maximal (with respect to inclusion) subgroup of $\mathrm{GL}(\mathcal{V})$ which stabilises (7.1), and refer to elements of $\mathrm{C}_2(\mathfrak{F})$ as *$\mathscr{C}_2$-maps* in $\mathfrak{F}$. If $m = \dim(\mathcal{V})/t$ and $\mathbb{F}_q$ is the underlying field, then $\mathrm{C}_2(\mathfrak{F})$ is isomorphic to the wreath product

$$\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(m, q) \wr S_t.$$

In Section 7.1 we introduce the notions of $\mathscr{C}_2$-frames and $\mathscr{C}_2$-subframes. A set $\mathfrak{D}$ consisting of non-trivial, equal dimensional subspaces of $\mathcal{V}$ is called a *$\mathscr{C}_2$-subframe of* $\mathfrak{F}$ (written as $\mathfrak{D} \sqsubseteq \mathfrak{F}$) if there exists an injective mapping $\iota : \mathfrak{D} \to \mathfrak{F}$ such that $\mathcal{Y} \leq \iota(\mathcal{Y})$ for all $\mathcal{Y} \in \mathfrak{D}$. In such a case we have $\langle v \in \mathcal{Y} \mid \mathcal{Y} \in \mathfrak{D} \rangle = \bigoplus_{\mathcal{Y} \in \mathfrak{D}} \mathcal{Y}$, and $g \in \mathrm{C}_2(\mathfrak{F})$ *preserves* $\mathfrak{D}$ if $\bigoplus_{\mathcal{Y} \in \mathfrak{D}} \mathcal{Y}$ is $\langle g \rangle$-invariant. Section 7.2 investigates various properties of $\mathscr{C}_2$-maps. We particularly focus on elements in $\mathrm{C}_2(\mathfrak{F})$ which *conserve* $\mathfrak{F}$, that is which do not preserve any $\mathscr{C}_2$-subframe of $\mathfrak{F}$ other than $\mathfrak{F}$ itself. In Section 7.3 we show that the study of fat $\mathscr{C}_2$-maps boils down to the investigation of fat $\mathscr{C}_2$-maps which conserve the underlying $\mathscr{C}_2$-frame. We hence first consider elements in $\mathrm{C}_2(\mathfrak{F})$ conserving $\mathfrak{F}$, which (thanks to our findings in Section 7.2) can be handled more easily than arbitrary fat $\mathscr{C}_2$-maps in $\mathfrak{F}$. Then we turn to the general case. The main results of this

chapter (concerning the existence and proportion of fat elements in $\mathrm{C}_2(\mathfrak{F})$) are presented in Theorems 7.40, 7.42.

Notation. Throughout this chapter we let q be a power of a prime p.

7.1 Introducing $\mathscr{C}_2$-frames

Definition 7.1. Let $\mathcal{V} \neq \{0\}$ be a finite $\mathbb{F}_q$-vector space. A *$\mathscr{C}_2$-frame* in $\mathcal{V}$ is a non-empty set $\mathfrak{F}$ consisting of non-trivial subspaces of $\mathcal{V}$ such that the following hold.

(a) For all $\mathcal{X}, \mathcal{Y} \in \mathfrak{F}$ we have $\dim(\mathcal{X}) = \dim(\mathcal{Y})$.

(b) If $|\mathfrak{F}| \geq 2$, then $\mathcal{X} \cap \langle v \in \mathcal{Y} \mid \mathcal{Y} \in \mathfrak{F} \setminus \mathcal{X} \rangle = \{0\}$ for all $\mathcal{X} \in \mathfrak{F}$.

A *$\mathscr{C}_2$-frame* (over $\mathbb{F}_q$) is a $\mathscr{C}_2$-frame in some unspecified ($\mathbb{F}_q$-)vector space.

Given a $\mathscr{C}_2$-frame $\mathfrak{F}$, we have $\langle v \in \mathcal{X} \mid \mathcal{X} \in \mathfrak{F} \rangle = \bigoplus_{\mathcal{X} \in \mathfrak{F}} \mathcal{X}$. Hence, for each $w \in \langle v \in \mathcal{X} \mid \mathcal{X} \in \mathfrak{F} \rangle$ there are uniquely determined elements $w_{\mathcal{X}}$, $\mathcal{X} \in \mathfrak{F}$, such that $w = \sum_{\mathcal{X} \in \mathfrak{F}} w_{\mathcal{X}}$.

Definition 7.2. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame.

(a) We write $\langle \mathfrak{F} \rangle = \bigoplus_{\mathcal{X} \in \mathfrak{F}} \mathcal{X}$ and call $\langle \mathfrak{F} \rangle$ the *$\mathscr{C}_2$-span* of $\mathfrak{F}$.

(b) For $\mathcal{X} \in \mathfrak{F}$, we denote by $\pi_{\mathcal{X}}$ the *natural projection* $\langle \mathfrak{F} \rangle \to \mathcal{X}$ given by $\sum_{\mathcal{Y} \in \mathfrak{F}} v_{\mathcal{Y}} \mapsto v_{\mathcal{X}}$, where $v_{\mathcal{Y}} \in \mathcal{Y}$ for each $\mathcal{Y} \in \mathfrak{F}$.

(c) The *size* of $\mathfrak{F}$ is the pair (m, t), where m is the common dimension of the subspaces $\mathcal{X} \in \mathfrak{F}$ and $t = |\mathfrak{F}|$. We write $\mathrm{size}(\mathfrak{F})$ for the size of $\mathfrak{F}$.

Observe that, if (m, t) is the size of a $\mathscr{C}_2$-frame $\mathfrak{F}$, then $\dim(\langle \mathfrak{F} \rangle) = mt$.

Example 7.3. Let $\mathcal{V}$ be a finite vector space with basis $\{v_1, \ldots, v_4\}$ and le

$$\mathfrak{F}_1 = \big\{\langle v_1, v_2\rangle, \langle v_3, v_4\rangle\big\}, \qquad \mathfrak{F}_2 = \big\{\langle v_1\rangle, \langle v_3\rangle\big\},$$
$$\mathfrak{F}_3 = \big\{\langle v_1\rangle\big\}, \qquad \mathfrak{F}_4 = \big\{\langle v_1 + v_2\rangle\big\},$$
$$\mathfrak{F}_5 = \big\{\langle v_1\rangle, \langle v_2\rangle\big\}, \qquad \mathfrak{F}_6 = \big\{\{0\}\big\},$$
$$\mathfrak{F}_7 = \big\{\langle v_1, v_2\rangle, \langle v_3\rangle\big\}, \qquad \mathfrak{F}_8 = \big\{\langle v_1\rangle, \langle v_2\rangle, \langle v_1 + v_2\rangle\big\}.$$

The sets $\mathfrak{F}_1, \ldots, \mathfrak{F}_5$ are $\mathscr{C}_2$-frames in $\mathcal{V}$ with sizes $(2,2), (1,2), (1,1), (1,1)$, and $(1,2)$, respectively. The set $\mathfrak{F}_6$ is not a $\mathscr{C}_2$-frame, because it contains the trivial subspace $\{0\}$. The sets $\mathfrak{F}_7, \mathfrak{F}_8$ violate condition (a), and respectively condition (b), of Definition 7.1, and thus are not $\mathscr{C}_2$-frames either.

Definition 7.4. Let $\mathcal{V} \neq \{0\}$ be a finite $\mathbb{F}_q$-vector space. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame in $\mathcal{V}$. A *$\mathscr{C}_2$-subframe* of $\mathfrak{F}$ is a $\mathscr{C}_2$-frame $\mathfrak{D}$ in $\mathcal{V}$ such that the following hold.

(a) For all $\mathcal{Y} \in \mathfrak{D}$ there exists a unique $\mathcal{X} \in \mathfrak{F}$ satisfying $\mathcal{Y} \leq \mathcal{X}$.

(b) For all $\mathcal{X} \in \mathfrak{F}$ there is at most one $\mathcal{Y} \in \mathfrak{D}$ satisfying $\mathcal{Y} \leq \mathcal{X}$.

We write $\mathfrak{D} \sqsubseteq \mathfrak{F}$ to indicate that $\mathfrak{D}$ is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$. A $\mathscr{C}_2$-subframe $\mathfrak{D}$ of $\mathfrak{F}$ is called *proper* if $\mathfrak{D} \neq \mathfrak{F}$.

Consider a $\mathscr{C}_2$-frame $\mathfrak{F}$. The relation "$\sqsubseteq$" is a *partial order* on the set of all $\mathscr{C}_2$-subframes of $\mathfrak{F}$ as it is *reflexive* ($\mathfrak{D} \sqsubseteq \mathfrak{D}$ for all $\mathfrak{D} \sqsubseteq \mathfrak{F}$), *antisymmetric* ($\mathfrak{E} \sqsubseteq \mathfrak{D}$, $\mathfrak{D} \sqsubseteq \mathfrak{E}$ implies that $\mathfrak{E} = \mathfrak{D}$ for all $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$), and *transitive* (if $\mathfrak{A} \sqsubseteq \mathfrak{D}$ and $\mathfrak{D} \sqsubseteq \mathfrak{E}$, then $\mathfrak{A} \sqsubseteq \mathfrak{E}$ for all $\mathfrak{A}, \mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$).

We can think of the $\mathscr{C}_2$-frame $\mathfrak{F}$ as a vector space equipped with the structure of a direct sum decomposition, namely $\bigoplus_{\mathcal{X} \in \mathfrak{F}} \mathcal{X}$. In this sense, $\mathscr{C}_2$-subframes of $\mathfrak{F}$ are subspaces which inherit some of this structure. Observe that, if $\mathfrak{F}$ has size (m, t), then $\mathfrak{F}$ contains a $\mathscr{C}_2$-subframe of size (m_0, t_0) if and only if $1 \leq m_0 \leq m$ and $1 \leq t_0 \leq t$.

Example 7.5. In the situation of Example 7.3 we have $\mathfrak{F}_3 \sqsubseteq \mathfrak{F}_2 \sqsubseteq \mathfrak{F}_1$, $\mathfrak{F}_3 \sqsubseteq \mathfrak{F}_5$, $\mathfrak{F}_4 \sqsubseteq \mathfrak{F}_1$. Note that $\mathfrak{F}_5$ is not a $\mathscr{C}_2$-subframe of $\mathfrak{F}_1$. However, $\langle \mathfrak{F}_5 \rangle \leq \langle \mathfrak{F}_1 \rangle$.

Recall from Definition 7.2(b) the notion of $\pi_{\mathcal{X}}$.

Lemma 7.6. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$.*

(a) *Let $\mathcal{Y} \in \mathfrak{D}$, $\mathcal{X} \in \mathfrak{F}$ be such that $\mathcal{Y} \leq \mathcal{X}$. Then $\mathcal{Y} = \langle \mathfrak{D} \rangle \cap \mathcal{X} = \langle \mathfrak{D} \rangle \pi_{\mathcal{X}}$.*

(b) *We have $\langle \mathfrak{D} \rangle = \bigoplus_{\mathcal{X} \in \mathfrak{F}} \langle \mathfrak{D} \rangle \pi_{\mathcal{X}} = \bigoplus_{\mathcal{X} \in \mathfrak{F}} (\langle \mathfrak{D} \rangle \cap \mathcal{X})$.*

(c) *The $\mathscr{C}_2$-subframe $\mathfrak{D}$ consists of all non-trivial intersections $\langle \mathfrak{D} \rangle \cap \mathcal{X}$, $\mathcal{X} \in \mathfrak{F}$.*

Proof. Parts (b) and (c) follow directly from part (a), which is why we only prove assertion (a). Let $\mathcal{Y} \in \mathfrak{D}$ and $\mathcal{X} \in \mathfrak{F}$ be such that $\mathcal{Y} \leq \mathcal{X}$. Since (by definition) $\mathcal{Y} \leq \langle \mathfrak{D} \rangle$ and (by assumption) $\mathcal{Y} \leq \mathcal{X}$, we get

$$\mathcal{Y} \leq \langle \mathfrak{D} \rangle \cap \mathcal{X}.$$

Elements of $\mathcal{X}$ are mapped by $\pi_{\mathcal{X}}$ onto themselves. We thus have $\langle \mathfrak{D} \rangle \cap \mathcal{X} = (\langle \mathfrak{D} \rangle \cap \mathcal{X}) \pi_{\mathcal{X}}$, and hence

$$\langle \mathfrak{D} \rangle \cap \mathcal{X} \leq \langle \mathfrak{D} \rangle \pi_{\mathcal{X}}.$$

Suppose that (for some $t, t_0 \in \mathbb{N}$) we have $\mathfrak{F} = \{\mathcal{X}_1, \ldots, \mathcal{X}_t\}$, $\mathfrak{D} = \{\mathcal{Y}_1, \ldots, \mathcal{Y}_{t_0}\}$. We may assume that $\mathcal{Y}_i \leq \mathcal{X}_i$ for all $i \in \{1, \ldots, t_0\}$, and that $\mathcal{Y} = \mathcal{Y}_1$. (Then

$\mathcal{X} = \mathcal{X}_1$.) Consider an element $v \in \langle\mathfrak{D}\rangle$. Since $\langle\mathfrak{D}\rangle = \mathcal{Y}_1 \oplus \cdots \oplus \mathcal{Y}_{t_0}$, there exist elements $v_i \in \mathcal{Y}_i$ ($i \in \{1, \ldots, t_0\}$), such that $v = v_1 + \cdots + v_{t_0}$. Then, for all $i \in \{1, \ldots, t_0\}$, we have $v_i \in \mathcal{X}_i$, whence $v\pi_{\mathcal{X}_i} = v_i$. In particular, $v\pi_{\mathcal{X}} = v_1 \in \mathcal{Y}$. This shows that

$$\langle\mathfrak{D}\rangle\pi_{\mathcal{X}} \leq \mathcal{Y}$$

and completes the proof (of (a)). □

Lemma 7.7. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame, and let $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$.*

(a) We have $\mathfrak{E} = \mathfrak{D}$ if and only if $\langle\mathfrak{E}\rangle = \langle\mathfrak{D}\rangle$.

(b) The intersection $\langle\mathfrak{D}\rangle \cap \langle\mathfrak{E}\rangle$ is equal to $\bigoplus_{\mathcal{Y}\in\mathfrak{D}} \bigoplus_{\mathcal{Z}\in\mathfrak{E}} \mathcal{Y} \cap \mathcal{Z}$.

Proof. (a) If $\mathfrak{E} = \mathfrak{D}$, then trivially $\langle\mathfrak{E}\rangle = \langle\mathfrak{D}\rangle$. So, assume that $\langle\mathfrak{E}\rangle = \langle\mathfrak{D}\rangle$. Then $\langle\mathfrak{E}\rangle \cap \mathcal{X} = \langle\mathfrak{D}\rangle \cap \mathcal{X}$ for all $\mathcal{X} \in \mathfrak{F}$, which according to Lemma 7.6(c) means that $\mathfrak{E} = \mathfrak{D}$.

(b) Let $\mathrm{size}(\mathfrak{F}) = (m, t)$ and $\mathfrak{F} = \{\mathcal{X}_1, \ldots, \mathcal{X}_t\}$. For $i \in \{1, \ldots, t\}$ let $\mathcal{Y}_i = \langle\mathfrak{D}\rangle \cap \mathcal{X}_i$ and $\mathcal{Z}_i = \langle\mathfrak{E}\rangle \cap \mathcal{X}_i$. By Lemma 7.6$(b)$ we have

$$\langle\mathfrak{D}\rangle = \bigoplus_{i=1}^{t} \mathcal{Y}_i, \quad \langle\mathfrak{E}\rangle = \bigoplus_{i=1}^{t} \mathcal{Z}_i. \tag{7.2}$$

From Lemma 7.6(c) we get $\bigoplus_{\mathcal{Y}\in\mathfrak{D}} \bigoplus_{\mathcal{Z}\in\mathfrak{E}} \mathcal{Y} \cap \mathcal{Z} = \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{t} \mathcal{Y}_i \cap \mathcal{Z}_j$, and hence

$$\bigoplus_{\mathcal{Y}\in\mathfrak{D}} \bigoplus_{\mathcal{Z}\in\mathfrak{E}} \mathcal{Y} \cap \mathcal{Z} = \bigoplus_{i=1}^{t} \mathcal{Y}_i \cap \mathcal{Z}_i. \tag{7.3}$$

According to Equations (7.2), (7.3) the assertion translates to $\left(\bigoplus_{i=1}^{t} \mathcal{Y}_i\right) \cap \left(\bigoplus_{i=1}^{t} \mathcal{Z}_i\right) = \bigoplus_{i=1}^{t} \mathcal{Y}_i \cap \mathcal{Z}_i$. Since $\bigcup_{i=1}^{t} (\mathcal{Y}_i \cap \mathcal{Z}_i) \subseteq \left(\bigoplus_{i=1}^{t} \mathcal{Y}_i\right) \cap \left(\bigoplus_{i=1}^{t} \mathcal{Z}_i\right)$ it follows that $\bigoplus_{i=1}^{t} \mathcal{Y}_i \cap \mathcal{Z}_i$ is a subspace of $\left(\bigoplus_{i=1}^{t} \mathcal{Y}_i\right) \cap \left(\bigoplus_{i=1}^{t} \mathcal{Z}_i\right)$. In order to see that $\left(\bigoplus_{i=1}^{t} \mathcal{Y}_i\right) \cap \left(\bigoplus_{i=1}^{t} \mathcal{Z}_i\right)$ is a subspace of $\bigoplus_{i=1}^{t} \mathcal{Y}_i \cap \mathcal{Z}_i$, choose an element v in $\left(\bigoplus_{i=1}^{t} \mathcal{Y}_i\right) \cap \left(\bigoplus_{i=1}^{t} \mathcal{Z}_i\right)$. Then there exist $x_i \in \mathcal{Y}_i$ and $y_i \in \mathcal{Z}_i$ ($i \in \{1, \ldots, t\}$) such that

$$v = x_1 + \cdots + x_t = y_1 + \cdots + y_t.$$

For $j \in \{1, \ldots, t\}$ we have

$$\underbrace{x_j - y_j}_{\in \mathcal{X}_j} = \underbrace{(y_1 + \cdots + y_t - y_j) - (x_1 + \cdots + x_t - x_j)}_{\in \bigoplus_{i\in\{1,\ldots,t\}\setminus\{j\}} \mathcal{X}_i},$$

which (using $\mathcal{X}_j \cap \bigoplus_{i\in\{1,\ldots,t\}\setminus\{j\}} \mathcal{X}_i = \{0\}$) yields $x_j - y_j = 0$, that is $x_j = y_j$, and thus $x_j \in \mathcal{Y}_j \cap \mathcal{Z}_j$. It follows that $v \in \bigoplus_{i=1}^{t} \mathcal{Y}_i \cap \mathcal{Z}_i$. □

Suppose that we are in the situation of Lemma 7.7. We point out that, while (by part (b) of that lemma) $\langle\mathfrak{D}\rangle \cap \langle\mathfrak{E}\rangle = \bigoplus_{\mathcal{Y}\in\mathfrak{D}} \bigoplus_{\mathcal{Z}\in\mathfrak{E}} \mathcal{Y} \cap \mathcal{Z}$, the set $\{\mathcal{Y} \cap \mathcal{Z} \mid \mathcal{Y} \in \mathfrak{D}, \mathcal{Z} \in \mathfrak{E}\}$ does not need to be a $\mathscr{C}_2$-frame (even if we only consider the non-trivial intersections $\mathcal{Y} \cap \mathcal{Z} \neq \{0\}$), because its elements may have different dimensions.

7.2 Linear groups acting on $\mathscr{C}_2$-frames

Definition 7.8. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame. A *$\mathscr{C}_2$-map* in $\mathfrak{F}$ is a non-singular linear mapping g on $\langle\mathfrak{F}\rangle$ such that $\mathcal{X}g \in \mathfrak{F}$ for all $\mathcal{X} \in \mathfrak{F}$.

The set of all $\mathscr{C}_2$-maps in a $\mathscr{C}_2$-frame $\mathfrak{F}$ forms a subgroup of $\mathrm{GL}(\langle\mathfrak{F}\rangle)$.

Definition 7.9. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame.

(a) We define $\mathrm{C}_2(\mathfrak{F})$ to be the group of all $\mathscr{C}_2$-maps in $\mathfrak{F}$.

(b) Let $(m, t) = \mathrm{size}(\mathfrak{F})$. A *basis* of $\mathfrak{F}$ is a basis $\{v_1, \ldots, v_{mt}\}$ of $\langle\mathfrak{F}\rangle$ such that $\langle v_{(i-1)m+1}, \ldots, v_{im}\rangle \in \mathfrak{F}$ for all $i \in \{1, \ldots, t\}$.

Consider a $\mathscr{C}_2$-frame $\mathfrak{F}$ of size (m, t) over $\mathbb{F}_q$, and let $\mathfrak{B}$ be basis of $\mathfrak{F}$. By definition, a non-singular linear mapping g on $\langle\mathfrak{F}\rangle$ lies in $\mathrm{C}_2(\mathfrak{F})$ if and only if $\langle g\rangle$ permutes the elements of $\mathfrak{F}$ amongst themselves (by acting on $\mathfrak{F}$ via multiplication from the right). Thus, $g \in \mathrm{GL}(\langle\mathfrak{F}\rangle)$ is an element of $\mathrm{C}_2(\mathfrak{F})$ if and only if the matrix of g with respect to $\mathfrak{B}$ is a $(t\times t)$-block monomial matrix, by which we mean a $(t\times t)$-block matrix containing precisely one non-zero block in each row, and each column, of blocks. This implies that

$$\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(m, q) \wr S_t.$$

The characteristic polynomial of an element $g \in \mathrm{C}_2(\mathfrak{F})$ is a product of factors, each of them corresponding to a $\langle g\rangle$-orbit on $\mathfrak{F}$. For each $\langle g\rangle$-orbit the respective factor can be computed using Proposition 4.23; see Example 7.10. (This method generalises the results in [25] where the authors compute the characteristic polynomials of monomial matrices over finite fields, that is cover the case $m = 1$.)

Example 7.10. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size $(m, 6)$ over $\mathbb{F}_q$ and let $g \in \mathrm{C}_2(\mathfrak{F})$. Suppose that there are three $\langle g\rangle$-orbits on $\mathfrak{F}$ of length 3, 2, and 1, respectively. Then there exist a basis $\mathfrak{B}$ of $\mathfrak{F}$ and elements $g_1, \ldots, g_6 \in \mathrm{GL}(m, q)$ such that

the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \cdot & g_1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & g_2 & \cdot & \cdot & \cdot \\ g_3 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & g_4 & \cdot \\ \cdot & \cdot & \cdot & g_5 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & g_6 \end{pmatrix}.$$

(Here "$\cdot$" denotes the $(m \times m)$-zero matrix over $\mathbb{F}_q$.) Let $f_1, f_2, f_3 \in \mathbb{F}_q[x]$ be the characteristic polynomials of $g_1g_2g_3$, g_4g_5, and g_6, respectively. By Proposition 4.23, the characteristic polynomial of g is given by $f_1(x^3)f_2(x^2)f_3(x)$.

Let $\mathfrak{D}$ be a $\mathscr{C}_2$-subframe of $\mathfrak{F}$. For $g \in \mathrm{C}_2(\mathfrak{F})$ the set $\mathfrak{D}g = \{\mathcal{X}g \mid \mathcal{X} \in \mathfrak{D}\}$ is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$ and $\mathfrak{D}g$ has the same size as $\mathfrak{D}$. Conversely, given $\mathfrak{E} \sqsubseteq \mathfrak{F}$ with $\mathrm{size}(\mathfrak{E}) = \mathrm{size}(\mathfrak{D})$ there exists a $\mathscr{C}_2$-map in $\mathfrak{F}$ such that $\mathfrak{E}g = \mathfrak{D}$. Using Lemma 5.15, we conclude the following.

Lemma 7.11. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame. The group $\mathrm{C}_2(\mathfrak{F})$ acts on the set of all $\mathscr{C}_2$-subframes of $\mathfrak{F}$ via*

$$\{\mathfrak{D} \mid \mathfrak{D} \sqsubseteq \mathfrak{F}\} \times \mathrm{C}_2(\mathfrak{F}) \to \{\mathfrak{D} \mid \mathfrak{D} \sqsubseteq \mathfrak{F}\}, \quad (\mathfrak{D}, g) \mapsto \mathfrak{D}g.$$

Each orbit consists of all $\mathscr{C}_2$-subframes of a given size.

7.2.1 Linear mappings preserving $\mathscr{C}_2$-subframes

Definition 7.12. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$.

(*a*) An element $g \in \mathrm{C}_2(\mathfrak{F})$ *preserves* $\mathfrak{D}$ if $\mathfrak{D}g = \mathfrak{D}$. We say that $G \leq \mathrm{C}_2(\mathfrak{F})$ *preserves* $\mathfrak{D}$ if all elements in G preserve $\mathfrak{D}$.

(*b*) We write $\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}$ for the maximal (with respect to inclusion) subgroup of $\mathrm{C}_2(\mathfrak{F})$ preserving $\mathfrak{D}$.

Thus, (in the situation of Definition 7.12) the group $\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}$ is the stabiliser in $\mathrm{C}_2(\mathfrak{F})$ of $\mathfrak{D}$ with respect to the action specified in Lemma 7.11. As we may deduce from our next lemma, the group $\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}$ is equal to the subspace stabiliser of $\langle\mathfrak{D}\rangle$ in $\mathrm{C}_2(\mathfrak{F})$.

Lemma 7.13. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. An element $g \in C_2(\mathfrak{F})$ preserves $\mathfrak{D}$ if and only $\langle\mathfrak{D}\rangle$ is $\langle g\rangle$-invariant.*

Proof. Note that $\langle\mathfrak{D}\rangle g = \langle\mathfrak{D}g\rangle$. Hence, $\langle\mathfrak{D}\rangle$ is $\langle g\rangle$-invariant if and only if $\langle\mathfrak{D}g\rangle = \langle\mathfrak{D}\rangle$. By Lemma 7.7($a$) the latter holds if and only if $\mathfrak{D}g = \mathfrak{D}$, that is if and only if g preserves $\mathfrak{D}$. □

As shown below, the group $\mathrm{C}_2(\mathfrak{F})_\mathfrak{D}$ induces on $\langle\mathfrak{D}\rangle$ the entire group $\mathrm{C}_2(\mathfrak{D})$.

Lemma 7.14. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. Then*

$$\mathrm{C}_2(\mathfrak{F})_\mathfrak{D} \to \mathrm{C}_2(\mathfrak{D}), \quad g \mapsto g|_{\langle\mathfrak{D}\rangle}$$

is a surjective group homomorphism.

Proof. Consider an element $g \in \mathrm{C}_2(\mathfrak{F})_\mathfrak{D}$. By Lemma 7.13 the $\mathscr{C}_2$-span $\langle\mathfrak{D}\rangle$ is $\langle g\rangle$-invariant, which is why the restriction $g|_{\langle\mathfrak{D}\rangle}$ is an element of $\mathrm{GL}(\langle\mathfrak{D}\rangle)$. Moreover, since g preserves $\mathfrak{D}$, for all $\mathcal{X} \in \mathfrak{D}$ we have $\mathcal{X}g \in \mathfrak{D}$ and thus $\mathcal{X}g|_{\langle\mathfrak{D}\rangle} \in \mathfrak{D}$. It follows that $g \mapsto g|_{\langle\mathfrak{D}\rangle}$ defines a mapping from $\mathrm{C}_2(\mathfrak{F})_\mathfrak{D}$ to $\mathrm{C}_2(\mathfrak{D})$ and this mapping is clearly a group homomorphism.

In order to show that this homomorphism is onto, let $h \in \mathrm{C}_2(\mathfrak{D})$. Let $(m,t) = \mathrm{size}(\mathfrak{F})$ and $(m_0,t_0) = \mathrm{size}(\mathfrak{D})$. Suppose that $\mathfrak{D} = \{\mathcal{Y}_1,\dots,\mathcal{Y}_{t_0}\}$. We assume that the underlying field is $\mathbb{F}_q$. For $i \in \{1,\dots,t_0\}$ let

$$\mathfrak{B}_i = \{v_{(i-1)m+1},\dots,v_{(i-1)m+m_0}\}$$

be bases of $\mathcal{Y}_i$. Then $\mathfrak{B} = \bigcup_{i=1}^{t_0}\mathfrak{B}_i$ is a basis of $\mathfrak{D}$ (as introduced in Definition 7.9(b)), and with respect to $\mathfrak{B}$ the matrix $h_\mathfrak{B}$ of h is a $(t_0 \times t_0)$-block monomial matrix over $\mathbb{F}_q$ (where each block is an $(m_0 \times m_0)$-matrix). We extend the element $h_\mathfrak{B}$ (in three steps) in order to obtain a $(t\times t)$-block monomial matrix $H \in \mathrm{GL}(mt,q)$. We

(i) exchange each $(m_0 \times m_0)$-zero-block by a $(m \times m)$-zero-block;

(ii) exchange each $(m_0 \times m_0)$-block $\ell \in \mathrm{GL}(m_0,q)$ by the matrix

$$\begin{pmatrix} \ell & \mathbf{0}_{m_0,m-m_0} \\ \mathbf{0}_{m-m_0,m_0} & \mathbf{1} \end{pmatrix},$$

where $\mathbf{1}$ is the identity in $\mathrm{GL}(m-m_0,q)$, and $\mathbf{0}_{a,b}$ denotes the $(a\times b)$-zero matrix over $\mathbb{F}_q$ $(a,b \in \{m_0, m-m_0\})$;

(iii) "fill up" the remaining entries of H so that H becomes a $(t \times t)$-block monomial matrix in $\mathrm{GL}(mt,q)$.

Since $\mathfrak{D} \sqsubseteq \mathfrak{F}$ we can extend $\mathfrak{B}$ to a basis $\widehat{\mathfrak{B}} = \{v_1,\dots,v_{mt}\}$ of $\mathfrak{F}$. Let $g \in \mathrm{GL}(\langle\mathfrak{F}\rangle)$ be such that the matrix of g with respect to $\widehat{\mathfrak{B}}$ equals H. According to our construction, g permutes the elements of $\mathfrak{F}$ and $\mathfrak{D}$ amongst themselves, whence $g \in \mathrm{C}_2(\mathfrak{F})_\mathfrak{D}$. Moreover, we have $g|_{\langle\mathfrak{D}\rangle} = h$. □

7.2.2 Linear mappings conserving $\mathscr{C}_2$-subframes

Consider a finite vector space $\mathcal{V} \neq \{0\}$ and an element $h \in \mathrm{GL}(\mathcal{V})$. Similar to the definition of $\langle h \rangle$-irreducible subspaces of $\mathcal{V}$, that is non-trivial subspaces of $\mathcal{V}$ which are $\langle h \rangle$-invariant and which do not contain any non-trivial and proper, $\langle h \rangle$-invariant subspaces, we next consider $\mathscr{C}_2$-subframes $\mathfrak{D}$ of a given $\mathscr{C}_2$-frame $\mathfrak{F}$, which are preserved by an element $g \in \mathrm{C}_2(\mathfrak{F})$ and which do not contain any proper $\mathscr{C}_2$-subframes preserved by g.

Definition 7.15. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. An element $g \in \mathrm{C}_2(\mathfrak{F})$ *conserves* $\mathfrak{D}$ if g preserves $\mathfrak{D}$ and g does not preserve any proper $\mathscr{C}_2$-subframe of $\mathfrak{D}$.

Elements of $\mathrm{C}_2(\mathfrak{F})$ conserving the entire underlying $\mathscr{C}_2$-frame $\mathfrak{F}$ behave similarly to irreducible elements in $\mathrm{GL}(\mathcal{V})$. (For example, two elements in $\mathrm{C}_2(\mathfrak{F})$ which conserve $\mathfrak{F}$ are conjugate in $\mathrm{C}_2(\mathfrak{F})$ if and only if they have the same characteristic polynomial; see Lemma 7.22.) Such elements can be characterised as follows.

Lemma 7.16. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) and let $\mathcal{X} \in \mathfrak{F}$. An element $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$ if and only if $\mathfrak{F} = \{\mathcal{X}g^i \mid 0 \leq i \leq t-1\}$ and $\mathcal{X}$ is $\langle g^t \rangle$-irreducible.*

Proof. First, suppose that g conserves $\mathfrak{F}$. Since $g \in \mathrm{C}_2(\mathfrak{F})$, the group $\langle g \rangle$ acts on $\mathfrak{F}$ via $(\mathcal{Y}, h) \mapsto \mathcal{Y}h$, $\mathcal{Y} \in \mathfrak{F}$, $h \in \langle g \rangle$. If this action is not transitive, then each orbit is a proper $\mathscr{C}_2$-subframe of $\mathfrak{F}$ which is preserved by g. As this contradicts g conserving $\mathfrak{F}$, we conclude that $\mathfrak{F} = \{\mathcal{X}g^i \mid 0 \leq i \leq t-1\}$ and $\mathcal{X}$ is $\langle g^t \rangle$-invariant. Seeking a contradiction assume that $\mathcal{X}$ contains a non-trivial and proper, $\langle g^t \rangle$-invariant subspace $\mathcal{X}_0$. In such a case the set $\{\mathcal{X}_0 g^i \mid 0 \leq i \leq t-1\}$ is a proper $\mathscr{C}_2$-subframe of $\mathfrak{F}$ which is preserved by g. This again contradicts our assumption that g conserves $\mathfrak{F}$, whence $\mathcal{X}$ is $\langle g^t \rangle$-irreducible.

Conversely, suppose that $\mathfrak{F} = \{\mathcal{X}g^i \mid 0 \leq i \leq t-1\}$ and $\mathcal{X}$ is $\langle g^t \rangle$-irreducible. Let $\mathfrak{D} \sqsubseteq \mathfrak{F}$ be preserved by g. Since $\langle g \rangle$ transitively permutes the elements of $\mathfrak{F}$ amongst themselves, it follows that $|\mathfrak{D}| = t$. Then each element in $\mathfrak{D}$ is $\langle g^t \rangle$-invariant and there exists $\mathcal{Y} \in \mathfrak{D}$ such that $\mathcal{Y} \leq \mathcal{X}$. Recalling that $\mathcal{X}$ is $\langle g^t \rangle$-irreducible (and that $\mathcal{Y}g^t = \mathcal{Y} \neq \{0\}$) we conclude that $\mathcal{X} = \mathcal{Y}$. Thus, $\mathfrak{D} = \mathfrak{F}$, whence g conserves $\mathfrak{F}$. □

In Lemma 7.17 below we present a matrix formulation of Lemma 7.16. Recall from Definition 7.9(*b*) the meaning of a basis of a $\mathscr{C}_2$-frame. Recall that a matrix $h \in \mathrm{GL}(m, q)$ is said to be irreducible if its characteristic polynomial is irreducible.

Lemma 7.17. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$. An element $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$ if and only if there exist a basis $\mathfrak{B}$ of $\mathfrak{F}$ and an irreducible element $h \in \mathrm{GL}(m,q)$ such that the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies*

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & \mathbf{1} \\ h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix}, \tag{7.4}$$

where $\mathbf{0}$ is the $(m \times m)$-zero matrix over $\mathbb{F}_q$ and $\mathbf{1}$ denotes the identity element in $\mathrm{GL}(m,q)$.

Proof. Suppose that $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$. Let $\mathcal{X} \in \mathfrak{F}$ and let $\{v_1, \ldots, v_m\}$ be a basis of $\mathcal{X}$. By Lemma 7.16 we have $\mathfrak{F} = \{\mathcal{X}g^i \mid 0 \leq i \leq t-1\}$. Hence,

$$\mathfrak{B} = \{\underbrace{v_1, \ldots, v_m}_{\text{basis of } \mathcal{X}}, \underbrace{v_1 g, \ldots, v_m g}_{\text{basis of } \mathcal{X}g}, \ldots, \underbrace{v_1 g^{t-1}, \ldots, v_m g^{t-1}}_{\text{basis of } \mathcal{X}g^{t-1}}\}$$

is a basis of $\mathfrak{F}$. Moreover (Lemma 7.16 also states that) $\mathcal{X}$ is $\langle g^t \rangle$-invariant. Let $h \in \mathrm{GL}(m,q)$ be the matrix of $g^t|_{\mathcal{X}}$ with respect to $\{v_1, \ldots, v_m\}$. Then the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies (7.4). Since by Lemma 7.16 the element $g^t|_{\mathcal{X}}$ is irreducible (and since h and $g^t|_{\mathcal{X}}$ have the same characteristic polynomial) Lemma 4.8(a) reveals that h is irreducible.

Conversely, let $\mathfrak{B} = \{v_1, \ldots, v_{mt}\}$ be a basis of $\mathfrak{F}$, let h be an irreducible element in $\mathrm{GL}(m,q)$, and let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies (7.4). Let $\mathcal{X} = \langle v_1, \ldots, v_m \rangle$. By Definition 7.9($b$) we have $\mathcal{X} \in \mathfrak{F}$. Further, (7.4) implies that

$$\mathfrak{F} = \{\mathcal{X}g^i \mid 0 \leq i \leq t-1\}$$

and that the matrix of $g^t|_{\mathcal{X}}$ with respect to $\{v_1, \ldots, v_m\}$ is equal to h. (In particular, the characteristic polynomial of $g^t|_{\mathcal{X}}$ is irreducible.) Then $g^t|_{\mathcal{X}}$ is irreducible by Lemma 4.8(a). By Lemma 7.16 it follows that g conserves $\mathfrak{F}$. □

Recall that q is a power of the prime p. Recall Definition 4.14 of the p'-part of a group element. Consider a finite $\mathbb{F}_q$-vector space $\mathcal{V}$ and an element $h \in \mathrm{GL}(\mathcal{V})$. Suppose that h is reducible. Then, being a power of h, the element $h_{p'}$ is also reducible, and thus $\mathcal{V}$ contains a non-trivial and proper $\langle h_{p'} \rangle$-invariant subspace $\mathcal{V}_0$. In fact, we may choose $\mathcal{V}_0$ such that $\dim(\mathcal{V}_0) \geq \dim(\mathcal{V})/2$. This is because by Maschke's Theorem (see for example [35, Theorem 1.9]) $\mathcal{V}$ is *completely reducible* as an $\mathbb{F}_q\langle h_{p'} \rangle$-module, meaning that every $\langle h_{p'} \rangle$-invariant subspace of $\mathcal{V}$ has a $\langle h_{p'} \rangle$-invariant complement in $\mathcal{V}$. Hence, either $\mathcal{V}_0$ or its $\langle h_{p'} \rangle$-invariant complement has dimension bigger than or equal to $\dim(\mathcal{V})/2$.

We next prove an analogous result for $\mathscr{C}_2$-maps which do not conserve the underlying $\mathscr{C}_2$-frame.

Lemma 7.18. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame over $\mathbb{F}_q$. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that g does not conserve $\mathfrak{F}$. Then $g_{p'}$ preserves a proper $\mathscr{C}_2$-subframe $\mathfrak{E} \sqsubseteq \mathfrak{F}$ with $\dim(\langle\mathfrak{E}\rangle) \geq \dim(\langle\mathfrak{F}\rangle)/2$.*

Proof. Since g does not conserve $\mathfrak{F}$, g preserves a proper $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$. Being a power of g, the element $g_{p'}$ also preserves $\mathfrak{D}$. Let (m,t) and (m_0,t_0) be the sizes of $\mathfrak{F}$ and $\mathfrak{D}$, respectively. Then $\dim(\langle\mathfrak{F}\rangle) = mt$ and $\dim(\langle\mathfrak{D}\rangle) = m_0t_0$. If $m_0t_0 \geq mt/2$, then the assertion holds by setting $\mathfrak{E} = \mathfrak{D}$. So, suppose that

$$1 \leq m_0t_0 < \frac{mt}{2}. \tag{7.5}$$

We assume that $\mathfrak{F} = \{\mathcal{X}_1,\dots,\mathcal{X}_t\}$, $\mathfrak{D} = \{\mathcal{Y}_1,\dots,\mathcal{Y}_{t_0}\}$, and that $\mathcal{W}_i \leq \mathcal{V}_i$ for all $i \in \{1,\dots,t_0\}$. If $t_0 < t$, then $g_{p'}$ preserves the proper $\mathscr{C}_2$-subframes $\{\mathcal{X}_1,\dots,\mathcal{X}_{t_0}\}, \{\mathcal{X}_{t_0+1},\dots,\mathcal{X}_t\} \sqsubseteq \mathfrak{F}$. In such a case the $\mathscr{C}_2$-span of (at least) one of these $\mathscr{C}_2$-subframes has dimension greater or equal to $mt/2$, and the assertion holds. Thus, assume that $t_0 = t$. Then, using (7.5), we obtain

$$1 \leq m_0 < \frac{m}{2}. \tag{7.6}$$

If $g_{p'}$ does not transitively permute the $\mathcal{Y}_1,\dots,\mathcal{Y}_t$, then there exists a proper subset $I \subsetneq \{1\dots,t\}$ such that $|I| \geq t/2$ and $g_{p'}$ preserves $\{\mathcal{Y}_i \mid i \in I\}$. In this case, $g_{p'}$ preserves $\{\mathcal{X}_i \mid i \in I\}$, which is a proper $\mathscr{C}_2$-subframe of $\mathfrak{F}$ with a $\mathscr{C}_2$-span of dimension $m|I| \geq mt/2$, and the assertion holds.

So, assume that $g_{p'}$ transitively permutes the subspaces $\mathcal{Y}_1,\dots,\mathcal{Y}_t$, and hence also the subspaces $\mathcal{X}_1,\dots,\mathcal{X}_t$. Then $\mathcal{Y}_1$ and $\mathcal{X}_1$ are $\langle g_{p'}^t\rangle$-invariant. By [35, Theorem 1.9] (Maschke) there exists a $\langle g_{p'}^t\rangle$-invariant complement $\mathcal{X}$ of $\mathcal{Y}_1$ in $\mathcal{X}_1$. Then $\mathfrak{E} = \{\mathcal{X}g^{i-1} \mid 1 \leq i \leq t\}$ is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$ which is preserved by g. Observe that $\dim(\langle\mathfrak{E}\rangle) = (m-m_0)t$. Thus, by (7.6) we have $mt/2 < \dim(\langle\mathfrak{E}\rangle) \leq (m-1)t$, and the proof is complete. □

Lemma 7.19. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame and let $g \in \mathrm{C}_2(\mathfrak{F})$. Let $\mathfrak{D},\mathfrak{E} \sqsubseteq \mathfrak{F}$ be such that $\langle\mathfrak{D}\rangle \cap \langle\mathfrak{E}\rangle \neq \{0\}$. Then the following hold.*

(a) If g conserves $\mathfrak{D}$ and g preserves $\mathfrak{E}$, then $\mathfrak{D} \sqsubseteq \mathfrak{E}$.

(b) If g conserves $\mathfrak{D}$ and $\mathfrak{E}$, then $\mathfrak{D} = \mathfrak{E}$.

Proof. Since $\langle\mathfrak{D}\rangle \cap \langle\mathfrak{E}\rangle \neq \{0\}$, by Lemma 7.7(*b*) there exist $\mathcal{X} \in \mathfrak{D}$ and $\mathcal{Y} \in \mathfrak{E}$ such that $\mathcal{X} \cap \mathcal{Y} \neq \{0\}$.

(a) Suppose that $\mathfrak{D}$ is conserved, and $\mathfrak{E}$ is preserved, by g. Let $t = |\mathfrak{D}|$ and let $0 \neq v \in \mathcal{X} \cap \mathcal{Y}$. Since g conserves $\mathfrak{D}$, by Lemma 7.16, $\mathcal{X}$ is $\langle g^t \rangle$-invariant, whence $vg^t \in \mathcal{X}$. Since g preserves $\mathfrak{E}$, vg^t also lies in some element of $\mathfrak{E}$, namely $\mathcal{Y}$ (for the remaining elements of $\mathfrak{E}$ intersect $\mathcal{X}$ trivially). Hence, $vg^t \in \mathcal{X} \cap \mathcal{Y}$, and it follows that $\mathcal{X} \cap \mathcal{Y}$ is $\langle g^t \rangle$-invariant.

Consider the set $\mathfrak{A} = \{(\mathcal{X} \cap \mathcal{Y})g^i \mid 0 \leq i \leq t-1\}$. We have $\mathfrak{A} \sqsubseteq \mathfrak{D}$ and $\mathfrak{A} \sqsubseteq \mathfrak{E}$. Moreover, recalling that $\mathcal{X} \cap \mathcal{Y}$ is $\langle g^t \rangle$-invariant, we see that g preserves $\mathfrak{A}$. Since g conserves $\mathfrak{D}$ we conclude that $\mathfrak{D} = \mathfrak{A} \sqsubseteq \mathfrak{E}$.

(b) Suppose that g conserves $\mathfrak{D}$ and $\mathfrak{E}$. Then by part (a) we have $\mathfrak{D} \sqsubseteq \mathfrak{E}$ and $\mathfrak{E} \sqsubseteq \mathfrak{D}$. Hence, $\mathfrak{D} = \mathfrak{E}$. □

Lemma 7.20. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame over $\mathbb{F}_q$ and let $g, h \in \mathrm{C}_2(\mathfrak{F})$. Then g conserves $\mathfrak{F}$ if and only if $h^{-1}gh$ conserves $\mathfrak{F}$.*

Proof. Seeking a contradiction suppose that g conserves $\mathfrak{F}$ and that $h^{-1}gh$ preserves a proper $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$. Then $\mathfrak{D}(h^{-1}gh) = \mathfrak{D}$, that is $(\mathfrak{D}h^{-1})g = \mathfrak{D}h^{-1}$. Thus, g preserves the proper $\mathscr{C}_2$-subframe $\mathfrak{D}h^{-1} \sqsubseteq \mathfrak{F}$. This contradicts g conserving $\mathfrak{F}$, and hence proves the assertion. □

Lemma 7.21. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$.*

(a) *Let $g \in \mathrm{C}_2(\mathfrak{F})$ conserve $\mathfrak{F}$, and let $f \in \mathbb{F}_q[x]$ be the minimal polynomial of g^t. Then $f \neq x$, f is irreducible, $\deg(f) = m$, and $f(x^t)$ is the characteristic polynomial of g.*

Moreover, if ω is a root of f, then $|g| = |\omega|t = |g^t|t \mid (q^m - 1)t$.

(b) *Let $f \neq x$ be a monic, irreducible polynomial of degree m over $\mathbb{F}_q$. Then there exists an element $g \in \mathrm{C}_2(\mathfrak{F})$ such that g conserves $\mathfrak{F}$ and $f(x^t)$ is the characteristic polynomial of g.*

Proof. (a) By Lemma 7.17 there exist a basis $\mathfrak{B}$ of $\mathfrak{F}$ and an irreducible element $h \in \mathrm{GL}(m, q)$ such that the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies (7.4). Let $f_h \in \mathbb{F}_q[x]$ be the characteristic polynomial of h. (Then $f_h \neq x$ is a monic, irreducible polynomial of degree m over $\mathbb{F}_q$.) Note that $g_{\mathfrak{B}}^t$ is a block diagonal matrix with all diagonal blocks equal to h. Thus,

(i) the polynomial f_h annihilates $g_{\mathfrak{B}}^t$ (and hence also g^t);

(ii) for all $\mathcal{X} \in \mathfrak{F}$ the matrix of $g^t|_{\mathcal{X}}$ with respect to the basis $\mathfrak{B} \cap \mathcal{X}$ is equal to h;

(iii) we have $|g| = t|h|$ and $|g^t| = |h|$.

Since f_h is monic and irreducible, (i) implies that f_h is the minimal polynomial of g^t, that is $f_h = f$. Then $\deg(f) = m$, $f \neq x$, f is irreducible, and by (ii) the polynomial

$$f \text{ is the characteristic polynomial of } g^t|_{\mathcal{X}}.$$

Using Proposition 4.23 and Lemma 7.16 we see that the characteristic polynomial of g is given by $f(x^t)$.

By Lemma 4.8(a) the element $g^t|_{\mathcal{X}}$ is irreducible. Thus, according to Lemma 4.11$(a)(b)$ we have $|g^t|_{\mathcal{X}}| = |\omega| \mid q^m - 1$. Note that $|h| = |g^t|_{\mathcal{X}}|$ by (ii). Then (iii) yields $|g| = |\omega|t \mid (q^m - 1)t$ and $|g^t| = |\omega|$.

(b) Let $\mathfrak{B}$ be a basis of $\mathfrak{F}$, let $h \in \mathrm{GL}(m, q)$ be the companion matrix of f, and let $g \in \mathrm{GL}(\langle\mathfrak{F}\rangle)$ be such that $g_{\mathfrak{B}}$ satisfies (7.4). Since $g_{\mathfrak{B}}$ is a $(t \times t)$-block monomial matrix, we have $g \in \mathrm{C}_2(\mathfrak{F})$. By Lemma 7.17 the element g conserves $\mathfrak{F}$. □

Lemma 7.22. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t), and let $g_1, g_2 \in \mathrm{C}_2(\mathfrak{F})$ conserve $\mathfrak{F}$. The following are equivalent.*

(a) *The elements g_1, g_2 are conjugate in $\mathrm{C}_2(\mathfrak{F})$.*

(b) *The elements g_1, g_2 have the same characteristic polynomial.*

(c) *The elements g_1^t, g_2^t have the same minimal polynomial.*

Proof. The equivalence of (b) and (c) holds by Lemma 7.21(a). If (a) holds, then g_1, g_2 are conjugate in $\mathrm{GL}(\langle\mathfrak{F}\rangle)$, and hence (b) holds.

It remains to show that (b) implies (a). Suppose that $\mathfrak{F}$ is defined over $\mathbb{F}_q$ and that the characteristic polynomials of g_1 and g_2 coincide. For $i \in \{1, 2\}$, by Lemma 7.17 there exist a basis $\mathfrak{B}_i$ of $\mathfrak{F}$ and an irreducible element $h_i \in \mathrm{GL}(m, q)$ such that (writing $\mathbf{0}$ for the $(m \times m)$-zero matrix over $\mathbb{F}_q$ and $\mathbf{1}$ for the identity element in $\mathrm{GL}(m, q)$) the matrix of g_i with respect to $\mathfrak{B}_i$ equals

$$(g_i)_{\mathfrak{B}_i} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & \mathbf{1} \\ h_i & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix}.$$

Let $f_i \in \mathbb{F}_q[x]$ be the characteristic polynomial of h_i. Then, as we may deduce from Proposition 4.23 (or Lemma 7.21(a)), the characteristic polynomial of g_i is given by $f_i(x^t)$. Thus (by assumption) we have $f_1(x^t) = f_2(x^t)$ and hence

$f_1 = f_2$. Recalling that h_1 and h_2 are irreducible, from Lemma 4.8(a) it follows that h_1 and h_2 are conjugate in $\mathrm{GL}(m, q)$. Say,

$$h_1 = a^{-1} h_2 a$$

for some $a \in \mathrm{GL}(m, q)$. Let A be the $(t \times t)$-block diagonal matrix over $\mathbb{F}_q$ with all diagonal blocks equal to a. Then

$$(g_1)_{\mathfrak{B}_1} = A^{-1} (g_2)_{\mathfrak{B}_2} A.$$

We conclude that $(g_1)_{\mathfrak{B}_1}$ and $(g_2)_{\mathfrak{B}_1}$ are conjugate by a $(t \times t)$-block monomial matrix, namely by the product of A and the $(t \times t)$-block permutation matrix representing the basis change from $\mathfrak{B}_2$ to $\mathfrak{B}_1$. (The fact that the basis change matrix from $\mathfrak{B}_2$ to $\mathfrak{B}_1$ is a $(t \times t)$-block permutation matrix follows from Definition 7.9(b).) Hence, g_1, g_2 are conjugate in $\mathrm{C}_2(\mathfrak{F})$. □

Lemma 7.20 implies that $\mathrm{C}_2(\mathfrak{F})$ acts via conjugation on the set of all elements in $\mathfrak{F}$ which conserve $\mathfrak{F}$. As a direct consequence of Lemmas 7.21, 7.22 we obtain the following.

Lemma 7.23. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$. Let $\mathfrak{C}$ be the set of all orbits in $\{g \in \mathrm{C}_2(\mathfrak{F}) \mid g \text{ conserves } \mathfrak{F}\}$ under conjugation by $\mathrm{C}_2(\mathfrak{F})$. By mapping each orbit $O \in \mathfrak{C}$ onto the characteristic polynomial of a representative of O, we obtain a bijection*

$$\mathfrak{C} \to \{f(x^t) \mid f \in \mathbb{F}_q[x] \text{ monic and irreducible}, \deg(f) = m, f \neq x\}.$$

Recall that, given a group G and an element $g \in G$, we write $C_G(g)$ for the centraliser of g in G. In contrast to centralisers of irreducible elements, centralisers of conserving elements in $\mathrm{C}_2(\mathfrak{F})$ do not need to be cyclic. However, as shown below, centralisers of conserving elements have the same order.

Let S_t denote the symmetric group on $\{1, \ldots, t\}$.

Lemma 7.24. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$. If g conserves $\mathfrak{F}$, then $|C_{\mathrm{C}_2(\mathfrak{F})}(g)| = (q^m - 1)t$.*

Proof. Let $\mathfrak{F} = \{\mathcal{X}_1, \ldots, \mathcal{X}_t\}$. For $c \in C_{\mathrm{C}_2(\mathfrak{F})}(g)$ let $\psi(c) \in S_t$ be the permutation on $\{1, \ldots, t\}$ given by $\mathcal{X}_{\psi(c)} = \mathcal{X}_i c$. Let Ψ denote the group homomorphism

$$\Psi : C_{\mathrm{C}_2(\mathfrak{F})}(g) \to S_t, \quad c \mapsto \psi(c).$$

Since $\psi(c)\psi(g) = \psi(g)\psi(c)$ for all $c \in C_{\mathrm{C}_2(\mathfrak{F})}(g)$, we have $\mathrm{im}(\Psi) \leq C_{S_t}(\psi(g))$. Since by Lemma 7.16 the element $\psi(g)$ is a t-cycle, the centraliser of $\psi(g)$ in S_t is equal to $\langle \psi(g) \rangle$ (see [54, p. 16]). Then $\psi(g) \in \mathrm{im}(\Psi) \leq C_{S_t}(\psi(g)) = \langle \psi(g) \rangle$, and we conclude that $\mathrm{im}(\Psi) = \langle \psi(g) \rangle$. In particular, $|\mathrm{im}(\Psi)| = t$. Since $|C_{\mathrm{C}_2(\mathfrak{F})}(g)| = |\mathrm{im}(\Psi)| \times |\ker(\Psi)|$ it remains to show that $|\ker(\Psi)| = q^m - 1$.

(Recall from Definition 7.9(b) the notion of a basis of $\mathfrak{F}$.) By Lemma 7.17 there exist a basis $\mathfrak{B}$ of $\mathfrak{F}$ and an irreducible element $h \in \mathrm{GL}(m,q)$ such that the matrix $g_{\mathfrak{B}}$ of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & \mathbf{1} \\ h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix}.$$

Now, the group $\mathrm{C}_2(\mathfrak{F})$ consists of all elements in $\mathrm{GL}(\langle\mathfrak{F}\rangle)$ whose matrices with respect to $\mathfrak{B}$ are a $(t \times t)$-block monomial matrix. Hence, $\ker(\Psi)$ consists of all elements $c \in \mathrm{GL}(\langle\mathfrak{F}\rangle)$ such that $c_{\mathfrak{B}}$ is a $(t \times t)$-block diagonal matrix commuting with $g_{\mathfrak{B}}$. In fact, since for $c_1, \ldots, c_t \in \mathrm{GL}(m,q)$ we have

$$\begin{pmatrix} c_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & c_t \end{pmatrix} \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & \mathbf{1} \\ h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix} = \begin{pmatrix} \mathbf{0} & c_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & c_2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & c_{t-1} \\ c_t h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix},$$

$$\begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & \mathbf{1} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & \mathbf{1} \\ h & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix} \begin{pmatrix} c_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & c_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & c_t \end{pmatrix} = \begin{pmatrix} \mathbf{0} & c_2 & \mathbf{0} & \cdots & \mathbf{0} \\ \vdots & \mathbf{0} & c_3 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \mathbf{0} \\ \mathbf{0} & \vdots & & \ddots & c_t \\ h c_1 & \mathbf{0} & \cdots & \cdots & \mathbf{0} \end{pmatrix}$$

(which implies that $c_1 = \cdots = c_t$ and $c_t h = h c_1$), it follows that the kernel of Ψ consists of all elements $c \in \mathrm{GL}(\langle\mathfrak{F}\rangle)$ such that $c_{\mathfrak{B}}$ is a $(t \times t)$-block diagonal matrix with all diagonal blocks equal to some $c_0 \in C_{\mathrm{GL}(m,q)}(h)$. Then $|\ker(\Psi)| = |C_{\mathrm{GL}(m,q)}(h)|$. Recalling that h is irreducible, Proposition 4.18 yields $|\ker(\Psi)| = q^m - 1$. □

Recall from Definition 3.5 that $N_q^*(m)$ is the number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$. The precise value of $N_q^*(m)$ can be calculated using a formula presented in Lemma 3.7.

Proposition 7.25. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$. Let $\mathrm{con}(\mathfrak{F})$ be the proportion in $\mathrm{C}_2(\mathfrak{F})$ of all elements conserving $\mathfrak{F}$. Then*

$$\mathrm{con}(\mathfrak{F}) = \frac{N_q^*(m)}{t(q^m - 1)}.$$

Moreover,

$$\frac{1}{(m+1)t} \leq \operatorname{con}(\mathfrak{F}) \leq \frac{1}{mt}.$$

If $m \geq 2$, then the upper bound is not strict, that is $\operatorname{con}(\mathfrak{F}) < 1/(mt)$. If $m = 1$, then $\operatorname{con}(\mathfrak{F}) = 1/t$.

Proof. According to Lemmas 7.23 and 7.24, and the orbit-stabiliser-theorem the number $\operatorname{con}(\mathfrak{F})|\mathrm{C}_2(\mathfrak{F})|$ of all elements in $\mathrm{C}_2(\mathfrak{F})$ which conserve $\mathfrak{F}$ is equal to $N_q^*(m)|\mathrm{C}_2(\mathfrak{F})|t^{-1}(q^m-1)^{-1}$. Hence, $\operatorname{con}(\mathfrak{F}) = N_q^*(m)t^{-1}(q^m-1)^{-1}$. The "moreover"-part follows from Lemma 3.9(c). □

7.3 Fat $\mathscr{C}_2$-maps

We now turn our attention to $\mathscr{C}_2$-maps which are fat. Consider a $\mathscr{C}_2$-frame $\mathfrak{F}$ of size (m,t) over $\mathbb{F}_q$. Recall from Definition 5.1(a) that we refer to an element $g \in \mathrm{C}_2(\mathfrak{F})$ as being fat, or more precisely as a $\operatorname{fat}(mt,q;e)$-element, if $\langle g\rangle$ acts irreducibly on an e-dimensional subspace of $\langle\mathfrak{F}\rangle$, where e is a positive integer satisfying $mt/2 < e \leq mt$. Because $e > mt/2$, the e-dimensional, $\langle g\rangle$-irreducible subspace is uniquely determined. A prominent example of fat elements are irreducible elements (in which case $e = mt$). Fix a $\operatorname{fat}(mt,q;e)$-element $g \in \mathrm{C}_2(\mathfrak{F})$ (for some $e > mt/2$), and let $\mathcal{U}$ be the e-dimensional and $\langle g\rangle$-irreducible subspace of $\langle\mathfrak{F}\rangle$. There are two cases to distinguish.

(i) The subspace $\mathcal{U}$ intersects (at least) one of the $\mathcal{X} \in \mathfrak{F}$ non-trivially. Then $\bigoplus_{\mathcal{X}\in\mathfrak{F}} \mathcal{U}\cap\mathcal{X}$ is a non-trivial, $\langle g\rangle$-invariant subspace of $\mathcal{U}$. Hence, (recalling that $\mathcal{U}$ is $\langle g\rangle$-irreducible) we obtain

$$\mathcal{U} = \bigoplus_{\mathcal{X}\in\mathfrak{F}} \mathcal{U}\cap\mathcal{X}.$$

Now, the irreducibility of $\mathcal{U}$ implies that g transitively permutes the non-trivial intersections $\mathcal{U}\cap\mathcal{X}$, $\mathcal{X}\in\mathfrak{F}$, amongst themselves. This is why all non-trivial intersections have equal dimension, and hence

$$\mathfrak{D} = \{\mathcal{U}\cap\mathcal{X} \mid \mathcal{X}\in\mathfrak{F}, \mathcal{U}\cap\mathcal{X} \neq \{0\}\}$$

is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$. We thus get $\mathcal{U} = \langle\mathfrak{D}\rangle$. By Lemma 7.6($a$) we further have $\mathfrak{D} = \{\mathcal{U}\pi_\mathcal{X} \mid \mathcal{X}\in\mathfrak{F}, \mathcal{U}\pi_\mathcal{X} \neq \{0\}\}$. (The projections $\pi_\mathcal{X}$, $\mathcal{X}\in\mathfrak{F}$, are introduced in Definition 7.2(b).)

(ii) The subspace $\mathcal{U}$ intersects all $\mathcal{X}\in\mathfrak{F}$ trivially. In such a case (as shown in Lemma 7.27 below) the set

$$\mathfrak{D} = \{\mathcal{U}\pi_\mathcal{X} \mid \mathcal{X}\in\mathfrak{F}, \mathcal{U}\pi_\mathcal{X} \neq \{0\}\}$$

is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$. If $\mathcal{U} = \langle \mathfrak{D} \rangle$, then for all $\mathcal{X} \in \mathfrak{F}$ we get $\langle \mathfrak{D} \rangle \cap \mathcal{X} = \mathcal{U} \cap \mathcal{X} = \{0\}$, which contradicts $\mathfrak{D}$ being a $\mathscr{C}_2$-subframe of $\mathfrak{F}$. Hence, $\mathcal{U} \leq \langle \mathfrak{D} \rangle$ and $\mathcal{U}$ lies "diagonally" in $\langle \mathfrak{D} \rangle$.

As shown in Example 7.26 below, both cases can occur. In Lemma 7.27 we prove that (in both cases (i) and (ii)) the $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ specified above is conserved by g. Hence, $\mathfrak{D}$ is the smallest (with respect to "$\sqsubseteq$") $\mathscr{C}_2$-subframe of $\mathfrak{F}$ which contains $\mathcal{U}$.

Example 7.26. Let $\mathcal{V}$ be a 9-dimensional vector space over $\mathbb{F}_2$ with basis $\mathfrak{B} = \{v_1, \ldots, v_9\}$. Let $\mathcal{X}_1 = \langle v_1, v_2, v_3 \rangle$, $\mathcal{X}_2 = \langle v_4, v_5, v_6 \rangle$, and $\mathcal{X}_3 = \langle v_7, v_8, v_9 \rangle$. Consider the $\mathscr{C}_2$-frame

$$\mathfrak{F} = \{\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3\}$$

in $\mathcal{V}$. Note that $\mathrm{size}(\mathfrak{F}) = (3,3)$, $\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(3,2) \wr S_3$, and $\mathfrak{B}$ is a basis of $\mathfrak{F}$ (as introduced in Definition 7.9(b)).

We write "$\cdot$" for the zero element in $\mathbb{F}_2$, denote by $\mathbf{1}$ be the identity matrix in $\mathrm{GL}(3,2)$, and let $\mathbf{0}$ be the (3×3)-zero matrix over $\mathbb{F}_2$.

(a) Let

$$h = \begin{pmatrix} \cdot & 1 & \cdot \\ 1 & 1 & \cdot \\ \cdot & \cdot & 1 \end{pmatrix} \in \mathrm{GL}(3,2).$$

The characteristic polynomial of h is given by $f(x) = x^3 + 1 \in \mathbb{F}_2[x]$. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that the matrix of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \\ h & \mathbf{0} & \mathbf{0} \end{pmatrix} \in \mathrm{GL}(9,2).$$

(That is, $v_i g = v_{i+3}$ for $i \in \{1, \ldots, 6\}$, $v_7 g = v_2$, $v_8 g = v_1 + v_2$, $v_9 g = v_3$.) By Proposition 4.23 the characteristic polynomial of g is given by

$$f(x^3) = x^9 + 1 = (x+1) \underbrace{(x^2 + x + 1)}_{\text{irreducible over } \mathbb{F}_2} \underbrace{(x^6 + x^3 + 1)}_{\text{irreducible over } \mathbb{F}_2}.$$

Thus, $g \in \mathrm{C}_2(\mathfrak{F})$ is a $\mathrm{fat}(9,2;6)$-element. Consider the subspace

$$\mathcal{U} = \langle \overbrace{v_1}^{\in \mathcal{X}_1}, \underbrace{\overbrace{v_2}^{\in \mathcal{X}_1}}_{= v_1 g^3}, \overbrace{\underbrace{v_4}_{= v_1 g}}^{\in \mathcal{X}_2}, \underbrace{\overbrace{v_5}^{\in \mathcal{X}_2}}_{= v_1 g^4}, \overbrace{\underbrace{v_7}_{= v_1 g^2}}^{\in \mathcal{X}_3}, \underbrace{\overbrace{v_8}^{\in \mathcal{X}_3}}_{= v_1 g^5} \rangle \leq \mathcal{V} = \langle \mathfrak{F} \rangle.$$

Since $\mathcal{U} = \langle v_1 g^i \mid 0 \leq i \leq 5 \rangle$ and since $v_1 g^6 = v_1 + v_2 = v_1 + v_1 g^3 \in \mathcal{U}$, we see that $\mathcal{U}$ is $\langle g \rangle$-invariant. The matrix of $g|_{\mathcal{U}}$ with respect to the basis $\{v_1, v_1 g, v_1 g^2, v_1 g^3, v_1 g^4, v_1 g^5\}$ of $\mathcal{U}$ is the companion matrix of the

polynomial $x^6+x^3+1 \in \mathbb{F}_2[x]$. Since x^6+x^3+1 is irreducible over $\mathbb{F}_2$, the restriction $g|_{\mathcal{U}}$ is irreducible by Lemma 4.8(a). Hence, $\mathcal{U}$ is the (uniquely determined) 6-dimensional, $\langle g\rangle$-irreducible subspace of $\mathcal{V}$.
(The element g conserves the $\mathscr{C}_2$-subframe $\{\langle v_1, v_2\rangle, \langle v_4, v_5\rangle, \langle v_7, v_8\rangle\}$ of $\mathfrak{F}$. In particular, g does not conserve $\mathfrak{F}$.)

(b) Let h be the companion matrix of the polynomial $f(x) = x^3+x+1 \in \mathbb{F}_2[x]$, that is let

$$h = \begin{pmatrix} \cdot & 1 & \cdot \\ \cdot & \cdot & 1 \\ 1 & 1 & \cdot \end{pmatrix} \in \mathrm{GL}(2,3).$$

Since f is irreducible, h is an irreducible element in $\mathrm{GL}(3,2)$. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that the matrix of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \\ h & \mathbf{0} & \mathbf{0} \end{pmatrix} \in \mathrm{GL}(9,2).$$

(That is, $v_i g = v_{i+3}$ for $i \in \{1,\dots,6\}$, $v_7 g = v_2$, $v_8 g = v_3$, $v_9 g = v_1 + v_2$.) Since h is irreducible, by Lemma 7.17 the element g conserves $\mathfrak{F}$. By Proposition 4.23 the characteristic polynomial of g is given by

$$f(x^3) = x^9 + x^3 + 1 = \underbrace{(x^3+x^2+1)}_{\text{irreducible over } \mathbb{F}_2}\underbrace{(x^6+x^5+x^4+x^2+1)}_{\text{irreducible over } \mathbb{F}_2}.$$

Thus, $g \in \mathrm{C}_2(\mathfrak{F})$ is a fat$(9,2;6)$-element which conserves $\mathfrak{F}$. Let $w = v_1+v_6$. Consider the subspace

$$\mathcal{U} = \langle \underbrace{v_1+v_6}_{w}, \underbrace{v_4+v_9}_{wg}, \underbrace{v_1+v_2+v_7}_{wg^2}, \underbrace{v_2+v_4+v_5}_{wg^3}, \underbrace{v_5+v_7+v_8}_{wg^4}, \underbrace{v_2+v_3+v_8}_{wg^5} \rangle$$

of $\mathcal{V}$. We get $wg^6 = v_3+v_5+v_6 = w+wg^2+wg^4+wg^5 \in \mathcal{U}$. Hence, $\mathcal{U}$ is $\langle g\rangle$-invariant. The matrix of $g|_{\mathcal{U}}$ with respect to the basis $\{w, wg, wg^2, wg^3, wg^4, wg^5\}$ is the companion matrix of the polynomial $x^6+x^5+x^4+x^2+1 \in \mathbb{F}_2[x]$. Since the latter is irreducible, using Lemma 4.8(a) we conclude that $g|_{\mathcal{U}}$ is irreducible. Hence, $\mathcal{U}$ is the (uniquely determined) 6-dimensional, $\langle g\rangle$-irreducible subspace of $\mathcal{V}$.

In contrast to Example 7.26(a), one can check that $\mathcal{U} \cap \mathcal{X}_i = \{0\}$ for all $i \in \{1,2,3\}$: Seeking a contradiction, assume that $\mathcal{U}$ intersects one of the $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3$ non-trivially. Say, $\mathcal{U} \cap \mathcal{X}_1 \neq \{0\}$. Because g conserves $\mathfrak{F}$, Lemma 7.16 implies that g transitively permutes the intersections $\mathcal{U} \cap \mathcal{X}_i$, $i \in \{1,2,3\}$, amongst themselves. Then $\dim(\mathcal{U} \cap \mathcal{X}_1) = \dim(\mathcal{U} \cap \mathcal{X}_2) = \dim(\mathcal{U} \cap \mathcal{X}_3)$ and

$$\mathfrak{D} = \{\mathcal{U} \cap \mathcal{X}_i \mid i \in \{1,2,3\}\}$$

is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$ which is preserved by g. Note that $\langle\mathfrak{D}\rangle \leq \mathcal{U}$. Since g conserves $\mathfrak{F}$ it follows that $\mathfrak{D} = \mathfrak{F}$. This yields the contradiction $\mathcal{V} = \langle\mathfrak{F}\rangle = \langle\mathfrak{D}\rangle \leq \mathcal{U}$.

Lemma 7.27. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) and $g \in \mathrm{C}_2(\mathfrak{F})$. Let $\mathcal{U} \leq \langle\mathfrak{F}\rangle$ satisfy $\dim(\mathcal{U}) > mt/2$ and let $\mathfrak{D} = \{\mathcal{U}\pi_{\mathcal{X}} \mid \mathcal{X} \in \mathfrak{F},\ \mathcal{U}\pi_{\mathcal{X}} \neq \{0\}\}$. Suppose that $\mathcal{U}$ is $\langle g\rangle$-irreducible. Then $\mathfrak{D} \sqsubseteq \mathfrak{F}$, g conserves $\mathfrak{D}$, and $\mathcal{U} \leq \langle\mathfrak{D}\rangle$.*

Proof. Observe that each $u \in \mathcal{U} \leq \langle\mathfrak{F}\rangle$ satisfies $u = \sum_{\mathcal{X}\in\mathfrak{F}} u\pi_{\mathcal{X}}$, whence

$$\mathcal{U} \leq \bigoplus_{\mathcal{X}\in\mathfrak{F}} \mathcal{U}\pi_{\mathcal{X}} = \langle\mathfrak{D}\rangle.$$

Observe further that $\mathcal{U}(\pi_{\mathcal{X}})g = \mathcal{U}g(\pi_{\mathcal{X}g})$ for all $\mathcal{X} \in \mathfrak{F}$. Recalling that $\mathcal{U}$ is $\langle g\rangle$-invariant, we thus get

$$\mathcal{U}(\pi_{\mathcal{X}})g = \mathcal{U}\pi_{\mathcal{X}g}, \quad \text{for all } \mathcal{X} \in \mathfrak{F}.$$

Hence, $\langle g\rangle$ permutes the elements of $\mathfrak{D}$ among themselves. Seeking a contradiction, assume that this action is not transitive. For a subset $\mathfrak{S} \subseteq \mathfrak{D}$ let $\langle\mathfrak{S}\rangle$ denote the subspace $\langle v \in \mathcal{X} \mid \mathcal{X} \in \mathfrak{S}\rangle$. (We have been using this notation for $\mathscr{C}_2$-frames. However, we do not know yet that $\mathfrak{D}$ is a $\mathscr{C}_2$-frame.) Let $\mathfrak{D}_0$ be a $\langle g\rangle$-orbit on $\mathfrak{D}$ which is minimal with respect to the dimension of $\langle\mathfrak{D}_0\rangle$. Then $\langle g\rangle$ permutes the elements in $\mathfrak{D}\setminus\mathfrak{D}_0$ among themselves (whence $\langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle$ is a $\langle g\rangle$-invariant subspace of $\langle\mathfrak{D}\rangle$) and $\dim(\langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle) \geq \dim(\langle\mathfrak{D}\rangle)/2$. Since $\mathcal{U}$ is a $\langle g\rangle$-invariant subspace of $\langle\mathfrak{D}\rangle$, and since $\dim(\mathcal{U}) > \dim(\langle\mathfrak{D}\rangle)/2$, the intersection $\mathcal{U} \cap \langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle$ is non-trivial and $\langle g\rangle$-invariant. Recalling that $\mathcal{U}$ is $\langle g\rangle$-irreducible, we conclude that $\mathcal{U} \cap \langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle = \mathcal{U}$, that is $\mathcal{U} \leq \langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle$. Then

$$\overbrace{\bigoplus_{\mathcal{X}\in\mathfrak{F}} \mathcal{U}\pi_{\mathcal{X}}}^{=\langle\mathfrak{D}\rangle} \leq \bigoplus_{\mathcal{X}\in\mathfrak{F}} \langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle\pi_{\mathcal{X}}. \tag{7.7}$$

Because $\langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle$ is a direct sum of some of the $\mathcal{U}\pi_{\mathcal{X}}$ ($\mathcal{X} \in \mathfrak{F}$), the right hand-side of Equation (7.7) is equal to $\langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle$. Hence, (7.7) simplifies to $\langle\mathfrak{D}\rangle \leq \langle\mathfrak{D}\setminus\mathfrak{D}_0\rangle$. As this is not true it follows that $\langle g\rangle$ transitively permutes the elements of $\mathfrak{D}$. Then all $\mathcal{X} \in \mathfrak{D}$ have the same dimension. We conclude that $\mathfrak{D}$ is a $\mathscr{C}_2$-subframe of $\mathfrak{F}$ which is preserved by g.

It remains to prove that g conserves $\mathfrak{D}$. Suppose that $\mathfrak{F}$ is defined over $\mathbb{F}_q$. Seeking a contradiction, assume that g does not conserve $\mathfrak{D}$. By Lemma 7.18 (applied to $\mathfrak{D}$ and $g|_{\langle\mathfrak{D}\rangle}$) the p'-part of $g|_{\langle\mathfrak{D}\rangle}$, and hence also the p'-part of g, preserve a proper $\mathscr{C}_2$-subframe $\mathfrak{E} \sqsubseteq \mathfrak{D}$ with $\dim(\langle\mathfrak{E}\rangle) \geq \dim(\langle\mathfrak{D}\rangle)/2$. Now, since

$g_{p'}$ preserves $\mathfrak{E}$, the subspace $\langle\mathfrak{E}\rangle$ is $\langle g_{p'}\rangle$-invariant by Lemma 7.13. Then, since $\mathcal{U}$ is also a $\langle g_{p'}\rangle$-invariant subspace of $\langle\mathfrak{D}\rangle$ and since $\dim(\mathcal{U}) > \dim(\langle\mathfrak{D}\rangle)/2$, we see that the intersection $\mathcal{U} \cap \langle\mathfrak{E}\rangle$ is $\langle g_{p'}\rangle$-invariant and non-trivial. Since, by (the "in particular" part of) Lemma 4.15, the subspace $\mathcal{U}$ is $\langle g_{p'}\rangle$-irreducible, it follows that $\mathcal{U} \cap \langle\mathfrak{E}\rangle = \mathcal{U}$, that is $\mathcal{U} \leq \langle\mathfrak{E}\rangle$. Then

$$\overbrace{\bigoplus_{\mathcal{X}\in\mathfrak{F}} \mathcal{U}\pi_{\mathcal{X}}}^{=\langle\mathfrak{D}\rangle} \leq \bigoplus_{\mathcal{X}\in\mathfrak{F}} \langle\mathfrak{E}\rangle\pi_{\mathcal{X}}. \tag{7.8}$$

Because $\mathfrak{E} \sqsubseteq \mathfrak{F}$, Lemma 7.6($b$) yields $\bigoplus_{\mathcal{X}\in\mathfrak{F}} \langle\mathfrak{E}\rangle\pi_{\mathcal{X}} = \langle\mathfrak{E}\rangle$. Hence, (7.8) simplifies to $\langle\mathfrak{D}\rangle \leq \langle\mathfrak{E}\rangle$, which contradicts $\mathfrak{E}$ being a proper $\mathscr{C}_2$-subframe of $\mathfrak{D}$. Thus, g does not preserve any proper $\mathscr{C}_2$ -subframe of $\mathfrak{D}$, whence g conserves $\mathfrak{D}$. □

Remark 7.28. In the situation of Lemma 7.27, $\mathcal{U}$ can be a proper subspace of $\langle\mathfrak{D}\rangle$. Otherwise, any fat element in $\mathrm{C}_2(\mathfrak{F})$ which conserves $\mathfrak{F}$ would be irreducible, which according to Example 7.26(b) is not true.

7.3.1 Fat $\mathscr{C}_2$-maps conserving the underlying frame

We first consider fat elements in $\mathrm{C}_2(\mathfrak{F})$ which conserve $\mathfrak{F}$. As presented below, this comprises the investigation of irreducible elements in $\mathrm{C}_2(\mathfrak{F})$.

Lemma 7.29. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame. An irreducible element in $\mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$.*

Proof. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be irreducible. If g does not conserve $\mathfrak{F}$, then g preserves a proper $\mathscr{C}_2$-subframe $\mathfrak{D}$ of $\mathfrak{F}$. Then $\langle\mathfrak{D}\rangle$ is a non-trivial and proper subspace of $\langle\mathfrak{F}\rangle$, which by Lemma 7.13 is $\langle g\rangle$-invariant. This contradicts the irreducibility of g. □

According to Lemma 7.29 any irreducible element $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$. The converse implication is not true. That is, the condition that $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$ does not force $\langle g\rangle$ to act irreducibly on $\langle\mathfrak{F}\rangle$. As shown in Example 7.31(b) an element $g \in \mathrm{C}_2(\mathfrak{F})$ conserving $\mathfrak{F}$ does not even need to be fat. Whether or not such an element g is fat, can be determined by looking at its order. Recall Definition 2.7.

Proposition 7.30. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$, let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$.*

(a) *Suppose that $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{F}$. Then g is a $\mathrm{fat}(mt, q; e)$-element if and only if $\gcd(q,t) = 1$ and $\mathrm{ord}(q; |g|) = e$.*

(b) *The group $\mathrm{C}_2(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements conserving $\mathfrak{F}$ if and only if $\gcd(q,t) = 1$ and $\mathrm{ord}(q; (q^m - 1)t) = e$.*

Proof. (a) Let f be the minimal polynomial of g^t and let ω be a root of f. By Lemma 7.21(a), f is irreducible of degree m, the characteristic polynomial of g is given by $f(x^t)$, and $|g| = |\omega|t$. By Lemma 5.2, g is a fat$(mt, q; e)$-element if and only if $f(x^t)$ has an irreducible factor of degree e. (Note that, being the minimal polynomial of a non-singular linear mapping, f satisfies $f(0) \neq 0$.) Then the assertion holds by Lemma 3.26.

(b) By Lemmas 7.23 and 5.2 the group $\mathrm{C}_2(\mathfrak{F})$ contains fat$(mt, q; e)$-elements conserving $\mathfrak{F}$ if and only if the polynomial ring $\mathbb{F}_q[x]$ contains monic, irreducible polynomials f of degree m such that $f(x^t)$ has an irreducible factor of degree e. According to Proposition 3.28 this is equivalent to saying that $\gcd(q, t) = 1$ and $\mathrm{ord}(q; (q^m - 1)t) = e$. □

Example 7.31. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size $(5, t)$ over $\mathbb{F}_5$, whence

$$\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(5, 5) \wr S_t.$$

Let $\mathfrak{B}$ be a basis of $\mathfrak{F}$ as introduced in Definition 7.9(b). Let $h \in \mathrm{GL}(5, 5)$ be an irreducible matrix of order $5^5 - 1 = 4 \times 11 \times 71$. (The existence of h follows from Proposition 4.18.) Let $\mathbf{0}$ denote the (5×5)-zero matrix over $\mathbb{F}_5$.

(a) Suppose that $t = 2$. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that the matrix of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ h & \mathbf{0} \end{pmatrix}.$$

By Lemma 7.17, g conserves $\mathfrak{F}$. Note that $|g^2| = |h|$, whence $|g| = 2(5^5 - 1)$. Note further that $\mathrm{ord}(5; (5^5 - 1)2) = 10$. (This can be deduced from Proposition 2.19 or calculated in GAP [24], see Remark 2.8.) Clearly, $\gcd(5, t) = 1$. Thus, by Proposition 7.30(a), g is an irreducible element (conserving $\mathfrak{F}$).

(b) Let $t = 2$ and let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that the matrix of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} \\ h^2 & \mathbf{0} \end{pmatrix}.$$

We may check that $\mathrm{ord}(5; |h^2|) = \mathrm{ord}(5; (5^5 - 1)/2) = 5$. Thus, by Lemma 4.12, h^2 is irreducible. Hence, by Lemma 7.17 the element g conserves $\mathfrak{F}$. We have $|g| = 2|h^2| = |h| = 5^5 - 1$, and thus $\mathrm{ord}(5; |g|) = 5 = \dim(\langle\mathfrak{F}\rangle)/2$. If g was fat, then according to Proposition 7.30(a) we would get $\mathrm{ord}(q; |g|) > \dim(\langle\mathfrak{F}\rangle)/2$. As this is not true, g is not fat (but conserves $\mathfrak{F}$).

(c) Suppose that $t = 3$. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be such that the matrix of g with respect to $\mathfrak{B}$ satisfies

$$g_{\mathfrak{B}} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \\ h & \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

By Lemma 7.17, g conserves $\mathfrak{F}$. We have $|g^3| = |h|$, and thus $|g| = 3(5^5 - 1)$. Hence, (as we may verify in GAP [24], see Remark 2.8) we get $\mathrm{ord}(5; |g|) = 10$. Clearly, $\gcd(5, t) = 1$. Then by Proposition 7.30(a), g is a $\mathrm{fat}(15, 5; 10)$-element (conserving $\mathfrak{F}$).

The following result is obtained by combining Lemma 7.29, Proposition 7.30 and (in part (b) additionally) Proposition 2.19. Recall that, given a $\mathscr{C}_2$-frame $\mathfrak{F}$ of size (m, t) over $\mathbb{F}_q$, the irreducible elements in $\mathrm{C}_2(\mathfrak{F})$ are precisely the $\mathrm{fat}(mt, q; mt)$-elements in $\mathrm{C}_2(\mathfrak{F})$.

Corollary 7.32. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$.*

(a) *An element $g \in \mathrm{C}_2(\mathfrak{F})$ is irreducible if and only if g conserves $\mathfrak{F}$ and $\gcd(q, t) = 1$, $\mathrm{ord}(q; |g|) = mt$.*

(b) *The following are equivalent.*

- (i) *The group $\mathrm{C}_2(\mathfrak{F})$ contains irreducible elements.*
- (ii) *We have $\gcd(q, t) = 1$ and $\mathrm{ord}(q; (q^m - 1)t) = mt$.*
- (iii) *The integer $q^m - 1$ is divisible by every prime divisor of t and by $\gcd(4, t)$.*

Example 7.33. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$. By Corollary 7.32(b) the group $\mathrm{C}_2(\mathfrak{F})$ contains irreducible elements if and only if $\gcd(q, t) = 1$ and $\mathrm{ord}(q; (q^m - 1)t) = mt$. Using Example 2.20 we obtain the following.

(a) If $m = 10$ and $t = 100$, then $\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(10, q) \wr S_{100}$ contains irreducible elements if and only if $q \equiv \pm 1 \pmod{10}$.

(b) If $t = 2$, then $\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(m, q) \wr S_2$ contains irreducible elements if and only if $2 \nmid q$.

Definition 7.34. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame over $\mathbb{F}_q$ of size (m, t), and let $e \in \mathbb{N}$ be such that $mt/2 < e \leq mt$. We define $\mathrm{confat}(\mathfrak{F}; e)$ to be the proportion in $\mathrm{C}_2(\mathfrak{F})$ of all $\mathrm{fat}(mt, q; e)$-elements which conserve $\mathfrak{F}$.

Recall from Definition 3.5 that $N_q^*(m)$ is the number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$. Recall from Definition 2.16 the notion of the s'-part of an integer. As introduced in Section 2.1, φ denotes Euler's totient function.

Proposition 7.35. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$, and let $e \in \mathbb{N}$ be such that $mt/2 < e \leq mt$. Suppose that* $\operatorname{confat}(\mathfrak{F}; e) \neq 0$.

(a) *If $e = mt$, then*

$$\operatorname{confat}(\mathfrak{F}; e) = \frac{N_q^*(m,t)}{t(q^m-1)}$$

and

$$\frac{\varphi(t)}{(m+1)t^2} \leq \operatorname{confat}(\mathfrak{F}; e) \leq \frac{\varphi(t)}{mt^2}.$$

(b) *If $e < mt$, then $m \mid e$ and $t/\gcd\left(\frac{e}{m}, t\right)$ is an odd prime. Moreover, writing $s = t/\gcd\left(\frac{e}{m}, t\right)$, we have*

$$\operatorname{confat}(\mathfrak{F}; e) = \frac{N_q^*(m,(t)_{s'})}{t(q^m-1)},$$

and

$$\frac{\varphi\big((t)_{s'}\big)}{(m+1)(t)_{s'}t} \leq \operatorname{confat}(\mathfrak{F}; e) \leq \frac{\varphi\big((t)_{s'}\big)}{m(t)_{s'}t}.$$

Proof. As we may deduce from Lemma 7.20, the group $\mathrm{C}_2(\mathfrak{F})$ acts by conjugation on the set of all elements in $\mathrm{C}_2(\mathfrak{F})$ which conserve $\mathfrak{F}$. Since conjugation does not alter the characteristic polynomial, Lemma 5.2 implies that $\mathrm{C}_2(\mathfrak{F})$ acts by conjugation on the set of all $\operatorname{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})$ conserving $\mathfrak{F}$. By Lemma 7.24 (and the orbit-stabiliser-theorem) the length of each orbit is given by $|\mathrm{C}_2(\mathfrak{F})|t^{-1}(q^m-1)^{-1}$. By Lemma 5.2 and Lemma 7.23 the number of all orbits is equal to the number, say T, of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q[x]$ such that $f(x^t)$ has an irreducible factor of degree e. Thus, the number $\operatorname{confat}(\mathfrak{F}; e)|\mathrm{C}_2(\mathfrak{F})|$ of all $\operatorname{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})$ conserving $\mathfrak{F}$ is equal to $T|\mathrm{C}_2(\mathfrak{F})|t^{-1}(q^m-1)^{-1}$. Hence,

$$\operatorname{confat}(\mathfrak{F}; e) = \frac{T}{t(q^m-1)}.$$

Then the assertion holds by Propositions 3.29, 3.31, and Theorem 3.24. □

Recall from Definition 4.20 that we write $\operatorname{irr}(\mathrm{C}_2(\mathfrak{F}))$ for the proportion (in $\mathrm{C}_2(\mathfrak{F})$) of all irreducible $\mathscr{C}_2$-maps in a $\mathscr{C}_2$-frame $\mathfrak{F}$. If $(m,t) = \operatorname{size}(\mathfrak{F})$, in which case $\dim(\langle\mathfrak{F}\rangle) = mt$, then by Lemma 7.29 we obtain

$$\operatorname{irr}\big(\mathrm{C}_2(\mathfrak{F})\big) = \operatorname{confat}(\mathfrak{F}; mt).$$

Because irreducible elements are such a prominent example of fat elements, we restate Proposition 7.35(a) in terms of irreducible elements.

Corollary 7.36. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$. Suppose that* $\operatorname{irr}(\mathrm{C}_2(\mathfrak{F})) \neq 0$. *Then*

$$\operatorname{irr}\big(\mathrm{C}_2(\mathfrak{F})\big) = \frac{N_q^*(m,t)}{t(q^m-1)}$$

and

$$\frac{\varphi(t)}{t^2(m+1)} \leq \operatorname{irr}\big(\mathrm{C}_2(\mathfrak{F})\big) \leq \frac{\varphi(t)}{t^2 m}.$$

Example 7.37. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_5$. Let $e = 110$.

(a) Suppose that $(m,t) = (5,22)$, whence $\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(5,5) \wr S_{22}$. Note that $e = mt$, which is why $\operatorname{confat}(\mathfrak{F};e)$ is the proportion of irreducible elements in $\mathrm{C}_2(\mathfrak{F})$, that is

$$\operatorname{confat}(\mathfrak{F};e) = \operatorname{irr}(\mathrm{C}_2(\mathfrak{F})).$$

Since $22 \mid 5^5 - 1 = 4 \times 11 \times 71$, by Corollary 7.32($b$) the group $\mathrm{C}_2(\mathfrak{F})$ contains irreducible elements. Corollary 7.36 yields

$$\frac{\varphi(22)}{22^2 \times 6} \leq \operatorname{irr}\big(\mathrm{C}_2(\mathfrak{F})\big) \leq \frac{\varphi(22)}{22^2 \times 5}, \tag{7.9}$$

whence

$$0.0034 < \operatorname{irr}\big(\mathrm{C}_2(\mathfrak{F})\big) < 0.0042.$$

Using Corollary 7.36 and Theorem 3.23 we can also calculate the precise value of $\operatorname{irr}\big(\mathrm{C}_2(\mathfrak{F})\big)$, which turns out to be the upper bound in (7.9).

(b) Suppose that $m = 5$ and $t \in \{23, 33\}$. Since

$$\operatorname{ord}\big(5;(5^5-1)23\big) = 110 = \operatorname{ord}\big(5;(5^5-1)33\big)$$

(which we can verify in GAP [24], see Remark 2.8), by Proposition 7.30(b) the group $\mathrm{C}_2(\mathfrak{F})$ contains $\operatorname{fat}(mt,q;e)$-elements which conserve $\mathfrak{F}$, that is $\operatorname{confat}(\mathfrak{F};e) \neq 0$. We have

$$\frac{t}{\gcd\big(\frac{e}{m};t\big)} = \begin{cases} 23, & \text{if } (m,t) = (5,23), \\ 3, & \text{if } (m,t) = (5,33). \end{cases}$$

Then by Proposition 7.35(b),

$$\frac{\varphi((23)_{23'})}{6 \times (23)_{23'} 23} \leq \operatorname{confat}\big(\mathrm{C}_2(\mathfrak{F})\big) \leq \frac{\varphi((23)_{23'})}{5 \times (23)_{23'} \times 23}, \quad \text{if } t = 23, \tag{7.10}$$

$$\frac{\varphi((33)_{3'})}{6 \times (33)_{3'} \times 33} \leq \operatorname{confat}\big(\mathrm{C}_2(\mathfrak{F})\big) \leq \frac{\varphi((33)_{3'})}{5 \times (33)_{3'} \times 33}, \quad \text{if } t = 33, \tag{7.11}$$

whence

$$\begin{aligned} 0.0072 < \operatorname{confat}\big(\mathrm{C}_2(\mathfrak{F})\big) < 0.0087, &\quad \text{if } t = 23, \\ 0.0045 < \operatorname{confat}\big(\mathrm{C}_2(\mathfrak{F})\big) < 0.0056, &\quad \text{if } t = 33. \end{aligned}$$

Using Proposition 7.35(b) and Theorem 3.23 we can verify that the exact value of $\operatorname{confat}\big(\mathrm{C}_2(\mathfrak{F})\big)$ is given by the upper bound in (7.10) and (7.11), respectively.

7.3.2 The general case

The following lemma provides the link between (arbitrary) fat $\mathscr{C}_2$-maps and fat $\mathscr{C}_2$-maps which conserve the underlying $\mathscr{C}_2$-frame. It suggests that the study of (arbitrary) fat elements in $\mathrm{C}_2(\mathfrak{F})$ reduces to the investigation of fat elements in $\mathrm{C}_2(\mathfrak{F})$ which conserve $\mathfrak{F}$.

Lemma 7.38. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$, let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$, and let $g \in \mathrm{C}_2(\mathfrak{F})$ be a $\operatorname{fat}(mt, q; e)$-element. Then there exists a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that $\dim(\langle\mathfrak{D}\rangle) \geq e$, g conserves $\mathfrak{D}$, and the restriction $g|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_2(\mathfrak{D})$ is a $\operatorname{fat}(\dim(\langle\mathfrak{D}\rangle), q; e)$-element (conserving $\mathfrak{D}$).*

Proof. Let $\mathcal{U}$ be the (uniquely determined) subspace of $\langle\mathfrak{F}\rangle$ which is $\langle g\rangle$-irreducible and e-dimensional. By Lemma 7.27 there exists a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that g conserves $\mathfrak{D}$ and $\mathcal{U} \leq \langle\mathfrak{D}\rangle$. By Lemma 7.13 the subspace $\langle\mathfrak{D}\rangle$ is $\langle g\rangle$-invariant. By Lemma 7.14 we have $g|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_2(\mathfrak{D})$. Since $\langle\mathfrak{D}\rangle$ contains $\mathcal{U}$, $g|_{\langle\mathfrak{D}\rangle}$ is a $\operatorname{fat}(\dim(\langle\mathfrak{D}\rangle), q; e)$-element. And because g conserves $\mathfrak{D}$, the restriction $g|_{\langle\mathfrak{D}\rangle}$ also has this property. □

Before we proceed to prove the main results of this chapter, we apply Lemma 7.38 in order to show that, writing (m,t) for the size of $\mathfrak{F}$, the group $\mathrm{C}_2(\mathfrak{F})$ cannot contain both a $\operatorname{fat}(mt, q; mt)$-element and a $\operatorname{fat}(mt, q; mt-1)$-element unless either m or t is equal to 1. (This is also shown in [45, Proposition 3.2] but our line of argument is different.) Recall Definition 2.7.

Lemma 7.39. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m,t) over $\mathbb{F}_q$. Suppose that the group $\mathrm{C}_2(\mathfrak{F})$ contains a $\operatorname{fat}(mt, q; mt)$-element and a $\operatorname{fat}(mt; q, mt-1)$ element. Then $1 \in \{m, t\}$.*

Proof. Seeking a contradiction, assume that $m, t \geq 2$. Since $\mathrm{C}_2(\mathfrak{F})$ contains a $\operatorname{fat}(mt, q; mt)$-element (that is an irreducible element), Corollary 7.32(b) yields

$$\operatorname{ord}(q; (q^m - 1)t) = mt.$$

Let $g \in \mathrm{C}_2(\mathfrak{F})$ be a $\mathrm{fat}(mt, q; mt-1)$-element. By Lemma 7.38 the element g conserves a $\mathscr{C}_2$-subframe $\mathfrak{D}$ of $\mathfrak{F}$ with $\dim(\langle\mathfrak{D}\rangle) \geq mt-1$. Let $\mathrm{size}(\mathfrak{D}) = (m_0, t_0)$. Since m_0, t_0 are positive integers satisfying $m_0 \leq m$ and $t_0 \leq t$, and since

$$\underbrace{\dim\big(\langle\mathfrak{D}\rangle\big)}_{\geq mt-1} = m_0 t_0,$$

(recalling that $m, t \geq 2$) we conclude that $(m_0, t_0) = (m, t)$. Thus $\mathfrak{D} = \mathfrak{F}$, whence g conserves $\mathfrak{F}$. Then by Proposition 7.30(b) we obtain the contradiction $\mathrm{ord}(q; (q^m - 1)t) = mt - 1$. □

We next give necessary and sufficient conditions for the existence of fat elements in $\mathrm{C}_2(\mathfrak{F})$.

Theorem 7.40. *Let $\mathfrak{F}$ be $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$, and let $e \in \mathbb{N}$ be such that $mt/2 < e \leq mt$.*

(a) *An element $g \in \mathrm{C}_2(\mathfrak{F})$ is a $\mathrm{fat}(mt, q; e)$-element if and only if g conserves a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that, writing $(m_0, t_0) = \mathrm{size}(\mathfrak{D})$ and $h = g|_{\langle\mathfrak{D}\rangle}$, we have $\gcd(q, t_0) = 1$ and $\mathrm{ord}(q; |h|) = e$.*

(b) *The group $\mathrm{C}_2(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements if and only if there exist positive integers $m_0 \leq m$, $t_0 \leq t$ such that $\gcd(q, t_0) = 1$ and $\mathrm{ord}(q; (q^{m_0} - 1)t_0) = e$.*

Proof. (a) If $g \in \mathrm{C}_2(\mathfrak{F})$ is a $\mathrm{fat}(mt, q; e)$-element, then by Lemma 7.38, $\mathfrak{F}$ contains a $\mathscr{C}_2$-subframe $\mathfrak{D}$, say of size (m_0, t_0), such that g conserves $\mathfrak{D}$ and the restriction $h = g|_{\langle\mathfrak{D}\rangle}$ is a $\mathrm{fat}(m_0 t_0, q; e)$-element in $\mathrm{C}_2(\mathfrak{D})$ (which conserves $\mathfrak{D}$). Applying Proposition 7.30(a) to $h \in \mathrm{C}_2(\mathfrak{D})$ yields $\gcd(q, t_0) = 1$, $\mathrm{ord}(q; |h|) = e$.

Conversely, let $g \in \mathrm{C}_2(\mathfrak{F})$ conserve a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ of size (m_0, t_0). Let h be the restriction $g|_{\langle\mathfrak{D}\rangle}$. Observe that $h \in \mathrm{C}_2(\mathfrak{D})$ by Lemma 7.14. Now, if $\gcd(q, t_0) = 1$ and $\mathrm{ord}(q; |h|) = e$, then by Proposition 7.30(a), applied to $h \in \mathrm{C}_2(\mathfrak{D})$, h is a $\mathrm{fat}(m_0 t_0, q; e)$-element. Then g is a $\mathrm{fat}(mt, q; e)$-element.

(b) Suppose that $\mathrm{C}_2(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements. Then according to Lemma 7.38 there exists a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that $\mathrm{C}_2(\mathfrak{D})$ contains $\mathrm{fat}(\dim(\langle\mathfrak{D}\rangle), q; e)$-elements which conserve $\mathfrak{D}$. Let $(m_0, t_0) = \mathrm{size}(\mathfrak{D})$. Since $\mathfrak{D} \sqsubseteq \mathfrak{F}$ we have $1 \leq m_0 \leq m$ and $1 \leq t_0 \leq t$. Further, Proposition 7.30(b) (applied to $\mathrm{C}_2(\mathfrak{D})$) reveals that $\gcd(q, t_0) = 1$ and that $\mathrm{ord}(q; (q^{m_0} - 1)t_0) = e$.

Conversely, assume that there exist positive integers $m_0 \leq m$, $t_0 \leq t$ satisfying $\gcd(q, t_0) = 1$ and $\mathrm{ord}(q; (q^{m_0} - 1)t_0) = e$. (Then $e \leq m_0 t_0$ by

Lemma 2.17.) Let $\mathfrak{D} \sqsubseteq \mathfrak{F}$ be a $\mathscr{C}_2$-subframe of size (m_0, t_0). By Proposition 7.30(b) the group $\mathrm{C}_2(\mathfrak{D})$ contains $\mathrm{fat}(m_0t_0, q; e)$-elements. Then, as we may deduce from Lemma 7.14, the group $\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}} \leq \mathrm{C}_2(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements. □

Example 7.41. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size $(5, 33)$ over $\mathbb{F}_5$, whence

$$\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(5, 5) \wr S_{33}.$$

By Theorem 7.40(b) the group $\mathrm{C}_2(\mathfrak{F})$ contains $\mathrm{fat}(165, 5; e)$-elements for some integer e satisfying

$$\frac{165}{2} < e \leq 165 \tag{7.12}$$

if and only if there exist positive integers m_0, t_0 such that

$$m_0 \leq m, \quad t_0 \leq t, \quad \gcd(5, t_0) = 1, \quad \mathrm{ord}(5; (5^{m_0} - 1)t_0) = e. \tag{7.13}$$

Using GAP [24] we verify that $m_0, t_0, e \in \mathbb{N}$ satisfy (7.12) and (7.13) if and only if the triple (m_0, t_0, e) is among the following.

$$(3, 31, 93), (3, 32, 96), (4, 24, 96), (4, 26, 104), (4, 27, 108), (4, 32, 128),$$
$$(5, 22, 110), (5, 23, 110), (5, 27, 90), (5, 32, 160), (5, 33, 110).$$

Hence, $\mathrm{C}_2(\mathfrak{F})$ contains $\mathrm{fat}(165, 5; e)$-elements (precisely) for

$$e \in \{90, 93, 96, 104, 108, 110, 128, 160\}.$$

Recall Definitions 5.17, 7.34. Consider a $\mathscr{C}_2$-frame $\mathfrak{F}$ of size (m, t) over $\mathbb{F}_q$ and let e be an integer satisfying $mt/2 < e \leq mt$. The final result of this chapter demonstrates how to calculate the proportion $\mathrm{fat}(\mathrm{C}_2(\mathfrak{F}); e)$ of $\mathrm{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})$. Recall that, in Proposition 7.35 we gave a formula for the precise value of, and also presented good estimates for, the proportion $\mathrm{confat}(\mathfrak{F}; e)$ of all $\mathrm{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})$ conserving $\mathfrak{F}$.

Theorem 7.42. *Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size (m, t) over $\mathbb{F}_q$, and let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$. Let $S = \{(m_0, t_0) \in \mathbb{N} \times \mathbb{N} \mid m_0 \leq m, t_0 \leq t, \gcd(q, t_0) = 1, \mathrm{ord}(q; (q^{m_0} - 1)t_0) = e\}$. Suppose that $\mathrm{fat}(\mathrm{C}_2(\mathfrak{F}); e) \neq 0$. Then $S \neq \emptyset$ and*

$$\mathrm{fat}\big(\mathrm{C}_2(\mathfrak{F}); e\big) = \sum_{\mathfrak{D} \in \mathbf{D}} \mathrm{confat}(\mathfrak{D}; e),$$

where $\mathbf{D}$ is a set of $\mathscr{C}_2$-subframes of $\mathfrak{F}$ containing precisely one $\mathscr{C}_2$-frame of size (m_0, t_0) for all pairs $(m_0, t_0) \in S$.

Proof. Let $g \in \mathrm{C}_2(\mathfrak{F})$ be a $\mathrm{fat}(mt, q; e)$-element. Then by Lemma 7.38 there exists a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$, say of size (m_0, t_0), such that $g \in \mathrm{C}_2(\mathfrak{F})$ conserves $\mathfrak{D}$ and the restriction $g|_{\langle\mathfrak{D}\rangle}$ is a $\mathrm{fat}(m_0t_0, q; e)$-element (conserving $\mathfrak{D}$). By Proposition 7.30(*b*) we have $\gcd(q, t_0) = 1$ and $\mathrm{ord}(q; (q^{m_0} - 1)t_0) = e$, that is $(m_0, t_0) \in S$. Hence, the set of all $\mathrm{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})$ is the union

$$\bigcup_{\substack{\mathfrak{D}\sqsubseteq\mathfrak{F},\\ \mathrm{size}(\mathfrak{D})\in S}} \big\{g \in \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \mathrm{fat}(mt, q; e)\text{-element conserving } \mathfrak{D}\big\}.$$

We show that the union above is disjoint. To see that this is true, suppose that a $\mathrm{fat}(mt, q; e)$-element in $\mathrm{C}_2(\mathfrak{F})$ conserves two $\mathscr{C}_2$-subframes $\mathfrak{D}_1, \mathfrak{D}_2 \sqsubseteq \mathfrak{F}$ with $\mathrm{size}(\mathfrak{D}_1), \mathrm{size}(\mathfrak{D}_2) \in S$. For $i \in \{1, 2\}$, let $(m_i, t_i) = \mathrm{size}(\mathfrak{D}_i)$. From Lemma 2.17 we obtain $\mathrm{ord}(q; (q^{m_i} - 1)t_i) \leq m_it_i$, and thus (recalling that $\mathrm{ord}(q; (q^{m_i} - 1)t_i) = e$) we have $e \leq m_it_i = \dim(\langle\mathfrak{D}_i\rangle)$. Since $e > mt/2 = \dim(\langle\mathfrak{F}\rangle)/2$, we see that $\langle\mathfrak{D}_1\rangle$ and $\langle\mathfrak{D}_2\rangle$ intersect non-trivially. Then by Lemma 7.19(*b*), $\mathfrak{D}_1 = \mathfrak{D}_2$.

It follows that the number of all $\mathrm{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})$ satisfies

$$\begin{aligned}&\mathrm{fat}\big(\mathrm{C}_2(\mathfrak{F}); e\big)|\mathrm{C}_2(\mathfrak{F})|\\ &= \sum_{\substack{\mathfrak{D}\sqsubseteq\mathfrak{F},\\ \mathrm{size}(\mathfrak{D})\in S}} \big|\{g \in \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \mathrm{fat}(mt, q; e)\text{-element conserving } \mathfrak{D}\}\big|. \qquad (7.14)\end{aligned}$$

Fix a $\mathscr{C}_2$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ with $\mathrm{size}(\mathfrak{D}) \in S$. By Lemma 7.14 the mapping

$$\delta : \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_2(\mathfrak{D}), \quad g \mapsto g|_{\langle\mathfrak{D}\rangle}$$

is a surjective group homomorphism. Since elements of $\ker(\delta)$ act trivially on $\langle\mathfrak{D}\rangle$ we conclude the following. If for $g \in \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}$ the coset $\ker(\delta)g$ contains a $\mathrm{fat}(mt, q; e)$-element conserving $\mathfrak{D}$, then every element in $\ker(\delta)g$ is a $\mathrm{fat}(mt, q; e)$-element conserving $\mathfrak{D}$. It follows that the number of $\mathrm{fat}(mt, q; e)$-elements in $\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}$ which conserve $\mathfrak{D}$ is equal to $|\ker(\delta)|$ times the number of $\mathrm{fat}(\dim(\langle\mathfrak{D}\rangle), q; e)$-elements in $\mathrm{im}(\delta)$ conserving $\mathfrak{D}$. That is,

$$\begin{aligned}&\big|\{g \in \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \mathrm{fat}(mt, q; e)\text{-element conserving } \mathfrak{D}\}\big|\\ &= |\ker(\delta)| \times \underbrace{\big|\{g \in \overbrace{\mathrm{im}(\delta)}^{\mathrm{C}_2(\mathfrak{D})} \mid g \text{ a } \mathrm{fat}(\dim(\langle\mathfrak{D}\rangle), q; e)\text{-element conserving } \mathfrak{D}\}\big|}_{=\mathrm{confat}(\mathfrak{D};e)|\mathrm{C}_2(\mathfrak{D})|}.\end{aligned}$$

Recalling that δ is onto (which is why $\mathrm{im}(\delta) = \mathrm{C}_2(\mathfrak{D})$ and $|\mathrm{im}(\delta)||\ker(\delta)| = |\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}|$) it follows that

$$\begin{aligned}&|\{g \in \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \mathrm{fat}(mt, q; e)\text{-element conserving } \mathfrak{D}\}|\\ &\quad = \mathrm{confat}(\mathfrak{D}; e)|\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}|.\end{aligned}$$

Hence, (7.14) simplifies to

$$\operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});e\big)|\mathrm{C}_2(\mathfrak{F})| = \sum_{\substack{\mathfrak{D}\sqsubseteq\mathfrak{F},\\ \operatorname{size}(\mathfrak{D})\in S}} \operatorname{confat}(\mathfrak{D};e)|\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}|.$$

By Proposition 7.35, the value of $\operatorname{confat}(\mathfrak{D};e)$ is the same for all $\mathfrak{D}\sqsubseteq\mathfrak{F}$ of a fixed size. By Lemma 7.11 the group $\mathrm{C}_2(\mathfrak{F})$ acts transitively (via multiplication from the right) on the set of all $\mathscr{C}_2$-subframes of $\mathfrak{F}$ of a given size. Since $\mathbf{D}$ (as specified in the assertion) is a set of representatives of the orbits, using the orbit-stabiliser-theorem we conclude that

$$\operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});e\big)|\mathrm{C}_2(\mathfrak{F})| = \sum_{\mathfrak{D}\in\mathbf{D}} |\mathrm{C}_2(\mathfrak{F}) : \mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}| \operatorname{confat}(\mathfrak{D};e)\,|\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}|.$$

Then $\operatorname{fat}(\mathrm{C}_2(\mathfrak{F});e) = \sum_{\mathfrak{D}\in\mathbf{D}} \operatorname{confat}(\mathfrak{D};e)$, as asserted. □

Example 7.43. Let $\mathfrak{F}$ be a $\mathscr{C}_2$-frame of size $(5,33)$ over $\mathbb{F}_5$, whence

$$\mathrm{C}_2(\mathfrak{F}) \cong \mathrm{GL}(5,5) \wr S_{33}.$$

By Example 7.41, $\mathrm{C}_2(\mathfrak{F})$ contains $\operatorname{fat}(165,5;e)$-elements (for some integer $165/2 < e \le 165$) if and only if $e \in \{90, 93, 96, 104, 108, 110, 128, 160\}$. Here we determine the proportion $\operatorname{fat}(\mathrm{C}_2(\mathfrak{F});110)$ of $\operatorname{fat}(165,5;110)$-elements in $\mathrm{C}_2(\mathfrak{F})$.

According to Example 7.41 there are precisely three pairs (m_0,t_0) of positive integers such that $m_0 \le 5$, $t_0 \le 33$, $\gcd(5,t_0)=1$ and $\operatorname{ord}(5;(5^{m_0}-1)t_0) = 110$, namely $(5,22),(5,23),(5,33)$.

Let $\mathfrak{D}_1,\mathfrak{D}_2,\mathfrak{D}_3 \sqsubseteq \mathfrak{F}$ be $\mathscr{C}_2$-subframes of size $(5,22)$, $(5,23)$, and $(5,33)$, respectively. Then by Theorem 7.42,

$$\operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});110\big) = \sum_{i=1}^{3} \operatorname{confat}(\mathfrak{D}_i;110).$$

In (7.9), (7.10), and (7.11) (see Example 7.37) we derived a lower and upper bound for $\operatorname{confat}(\mathfrak{D}_i;110)$, $i\in\{1,2,3\}$. Using these result we obtain

$$\operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});110\big) \le \frac{\varphi(22)}{22^2\times 5} + \frac{\varphi(1)}{5\times 23} + \frac{\varphi(11)}{5\times 11\times 33} = \frac{1531}{83490},$$
$$\operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});110\big) \ge \frac{\varphi(22)}{22^2\times 6} + \frac{\varphi(1)}{6\times 23} + \frac{\varphi(11)}{6\times 11\times 33} = \frac{1531}{100188},$$

and hence

$$0.0152 < \operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});110\big) < 0.0184.$$

We remark that (by Example 7.37) the precise value of $\operatorname{fat}\big(\mathrm{C}_2(\mathfrak{F});110\big)$ is given by $1531/83490 \approx 0.0183$.

Chapter 8

Aschbacher's $\mathscr{C}_3$-class (Field extension subgroups)

Notation. Throughout this chapter we let q be a power of a prime p.

For positive integers m, t, consider an m-dimensional vector space $\mathcal{X}$ over $\mathbb{F}_{q^t}$. We can naturally turn $\mathcal{X}$ into an mt-dimensional vector space over $\mathbb{F}_q$ by restricting scalar multiplication on $\mathcal{X}$ to $\mathbb{F}_q$. Recall from Definition 4.1(a) that we denote the resulting $\mathbb{F}_q$-vector space by $\mathcal{X}_{\mathbb{F}_q}$. Then

$$\begin{aligned} \Gamma\mathrm{L}(\mathcal{X}) &\cong \Gamma\mathrm{L}(m, q^t), \\ \mathrm{GL}(\mathcal{X}) &\cong \mathrm{GL}(m, q^t), \\ \mathrm{GL}(\mathcal{X}_{\mathbb{F}_q}) &\cong \mathrm{GL}(mt, q). \end{aligned}$$

If h is a non-singular semilinear mapping on $\mathcal{X}$, then (according to Definition 4.1(b)) we write $h_{\mathbb{F}_q}$ for h viewed as a mapping on $\mathcal{X}_{\mathbb{F}_q}$.

This chapter surveys the occurrence of fat elements in linear groups belonging to Aschbacher's $\mathscr{C}_3$-class. That is, we assume that

$$t \text{ is prime}$$

and investigate fat elements g in $\mathrm{GL}(\mathcal{X}_{\mathbb{F}_q})$ which retain on $\mathcal{X}$ the structure of an $\mathbb{F}_{q^t}$-vector space in the sense that

$$g = h_{\mathbb{F}_q} \quad \text{for some } h \in \Gamma\mathrm{L}(\mathcal{X}). \tag{8.1}$$

The largest subgroup H of $\Gamma\mathrm{L}(\mathcal{X})$ which embeds into $\mathrm{GL}(\mathcal{X}_{\mathbb{F}_q})$ via $h \mapsto h_{\mathbb{F}_q}$, consists of all elements in $\Gamma\mathrm{L}(\mathcal{X})$ whose associated field automorphisms lie in the Galois group $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$, and is isomorphic to the semi-direct product

$$H \cong \mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q) \ltimes \mathrm{GL}(\mathcal{X}).$$

If q is prime, then $\mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q) = \mathrm{Aut}(\mathbb{F}_{q^t})$, and hence $H = \Gamma\mathrm{L}(\mathcal{X})$. In general, writing $q = p^b$ (with p prime), we have $|\mathrm{Aut}(\mathbb{F}_{q^t}) : \mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)| = b$, and hence H is a subgroup of index b in $\Gamma\mathrm{L}(\mathcal{X})$. In the literature we often find H being denoted as $\Gamma\mathrm{L}(mt/t, q^t)$ or $\Gamma\mathrm{L}_{mt/t}(q^t)$. As pointed out in [10, p. 65], this is convenient but might cause confusion because, for example, $\Gamma\mathrm{L}(6/3, 4^3) \ncong \Gamma\mathrm{L}(4/2, 8^2)$. We shall not use this notation here. Instead, in line with Chapter 7, we introduce the concept of $\mathscr{C}_3$-frames and $\mathscr{C}_3$-maps. Several lemmas and definitions in this chapter will be very similar, or even identical, to corresponding parts in Chapter 7. This underlines the close resemblance of the approaches used to investigate fat elements in groups belonging to Aschbacher's $\mathscr{C}_2$- and $\mathscr{C}_3$-class.[I] We intentionally decided not to combine both chapters, as we believe that a class-by-class study improves the readability.

In the situation above, the pair $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ is a *$\mathscr{C}_3$-frame* and $G = \{h_{\mathbb{F}_q} \mid h \in H\} \leq \mathrm{GL}(\mathcal{X}_{\mathbb{F}_q})$ is the group of all *$\mathscr{C}_3$-maps* in $\mathfrak{F}$. We write

$$G = \mathrm{C}_3(\mathfrak{F}).$$

An element $h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$ *conserves* the $\mathscr{C}_3$-frame $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ if $h \in \Gamma\mathrm{L}(\mathcal{X})$ is irreducible. We show that the existence and proportion of fat elements in $\mathrm{C}_3(\mathfrak{F})$ depends on, and can be deduced from, the existence and proportion of fat elements in $\mathrm{C}_3(\mathfrak{F})$ conserving $\mathfrak{F}$. This is good news, because we can handle such elements using results from Chapter 4.

We set up this chapter according to the structure of Chapter 7. In Section 8.1 we introduce $\mathscr{C}_3$-frames and prove some of their properties. Section 8.2 investigates $\mathscr{C}_3$-maps in general. Finally, Section 8.3 is devoted to the study of $\mathscr{C}_3$-maps which are fat. The main results of this chapter (concerning the existence and proportion of fat elements in $\mathrm{C}_3(\mathfrak{F})$) are presented in Theorems 8.31 and 8.33.

8.1 Introducing $\mathscr{C}_3$-frames

Definition 8.1. Let m be a positive integer, let t be a prime, and let $\mathcal{X}$ be an m-dimensional $\mathbb{F}_{q^t}$-vector space. We call the pair $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ a *$\mathscr{C}_3$-frame*, or more precisely a *$\mathscr{C}_3$-frame over $\mathbb{F}_q$*.

In this context, the *size* of $\mathfrak{F}$ is given by $\mathrm{size}(\mathfrak{F}) = (m, t)$. Moreover, $\langle\mathfrak{F}\rangle$ denotes the $\mathbb{F}_q$-vector space $\mathcal{X}_{\mathbb{F}_q}$ obtained by restricting scalar multiplication on $\mathcal{X}$ to $\mathbb{F}_q$. We refer to $\langle\mathfrak{F}\rangle$ as the *$\mathscr{C}_3$-span* of $\mathfrak{F}$.

Consider a $\mathscr{C}_3$-frame $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ of size (m, t). According to our definition, $\mathcal{X}$ is an $\mathbb{F}_{q^t}$-vector space and $\langle\mathfrak{F}\rangle$ is an $\mathbb{F}_q$-vector space. Thus, $\mathcal{Y} \leq \mathcal{X}$ indicates

[I] We also use the "frame terminology" when dealing with fat elements in Aschbacher's $\mathscr{C}_4$-class; see Chapter 9.

that $\mathcal{Y}$ is an $\mathbb{F}_{q^t}$-subspace of $\mathcal{X}$, while $\mathcal{U} \leq \langle\mathfrak{F}\rangle$ means that $\mathcal{U}$ is an $\mathbb{F}_q$-subspace of $\langle\mathfrak{F}\rangle$. In order to avoid ambiguity, we add the order of the underlying field as a subscript of "$\leq$", that is, we write $\mathcal{Y} \leq_{q^t} \mathcal{X}$ and $\mathcal{U} \leq_q \langle\mathfrak{F}\rangle$. Similarly, we use the expressions $\dim_{q^t}(\mathcal{X})$, $\dim_q(\langle\mathfrak{F}\rangle)$ instead of $\dim(\mathcal{X})$ and $\dim(\langle\mathfrak{F}\rangle)$.

Definition 8.2. Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ be a $\mathscr{C}_3$-frame. A *$\mathscr{C}_3$-subframe* of $\mathfrak{F}$ is a $\mathscr{C}_3$-frame $(\mathcal{Y}, \mathbb{F}_q)$ such that $\mathcal{Y} \leq_{q^t} \mathcal{X}$. We write $\mathfrak{D} \sqsubseteq \mathfrak{F}$ to denote that $\mathfrak{D}$ is a $\mathscr{C}_3$-subframe of $\mathfrak{F}$. A $\mathscr{C}_3$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ is called *proper* if $\mathfrak{D} \neq \mathfrak{F}$.

Just like with $\mathscr{C}_2$-frames (see comments after Definitions 7.2, 7.4) we have

$$\dim_q\big(\langle\mathfrak{F}\rangle\big) = mt,$$

and the relation "$\sqsubseteq$" is a partial order on the set of all $\mathscr{C}_3$-subframes of $\mathfrak{F}$. Note that $\mathfrak{F}$ contains $\mathscr{C}_3$-subframes of size (m_0, t_0) if and only if

$$1 \leq m_0 \leq m \quad \text{and} \quad t_0 = t.$$

(This differs from $\mathscr{C}_2$-frames, where t_0 can be any positive integer less than or equal to t.) Note further that two $\mathscr{C}_3$-subframes $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$ have the same $\mathscr{C}_3$-span if and only if $\mathfrak{D} = \mathfrak{E}$.

Definition 8.3. Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ be a $\mathscr{C}_3$-frame.

(*a*) Let $\mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q)$ and $\mathfrak{E} = (\mathcal{Z}, \mathbb{F}_q)$ be $\mathscr{C}_3$-subframes of $\mathfrak{F}$. The *intersection* of $\mathfrak{D}$ and $\mathfrak{E}$ is defined as $\mathfrak{D} \cap \mathfrak{E} = (\mathcal{Y} \cap \mathcal{Z}, \mathbb{F}_q)$.

(*b*) Let $\mathcal{U} \leq_q \langle\mathfrak{F}\rangle$. We call $\bigcap_{\mathfrak{D} \sqsubseteq \mathfrak{F}, \mathcal{U} \leq_q \langle\mathfrak{D}\rangle} \mathfrak{D}$ the *$\mathscr{C}_3$-cover* of $\mathcal{U}$ in $\mathfrak{F}$.

Clearly, the intersection $\mathfrak{D} \cap \mathfrak{E}$ of two $\mathscr{C}_3$-subframes $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$ is a $\mathscr{C}_3$-subframe of $\mathfrak{F}$. Thus, the $\mathscr{C}_3$-cover in $\mathfrak{F}$ of a subspace $\mathcal{U} \leq_q \langle\mathfrak{F}\rangle$ is the smallest (with respect to "$\sqsubseteq$") $\mathscr{C}_3$-subframe of $\mathfrak{F}$ whose $\mathscr{C}_3$-span contains $\mathcal{U}$.

Lemma 8.4. *If $\mathfrak{F}$ is a $\mathscr{C}_3$-frame and $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$, then $\langle\mathfrak{D} \cap \mathfrak{E}\rangle = \langle\mathfrak{D}\rangle \cap \langle\mathfrak{E}\rangle$.*

Proof. Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$, $\mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q)$, $\mathfrak{E} = (\mathcal{Z}, \mathbb{F}_q)$ such that $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$. Then $(\mathcal{Y} \cap \mathcal{Z})_{\mathbb{F}_q} = \mathcal{Y}_{\mathbb{F}_q} \cap \mathcal{Z}_{\mathbb{F}_q}$, that is $\langle\mathfrak{D} \cap \mathfrak{E}\rangle = \langle\mathfrak{D}\rangle \cap \langle\mathfrak{E}\rangle$. □

8.2 Linear groups acting on $\mathscr{C}_3$-frames

Recall the terminology and notation introduced in Section 4.1. In particular recall that, given a (finite) vector space $\mathcal{X}$ over $\mathbb{F}_{q^t}$ and an element $h \in \Gamma\mathrm{L}(\mathcal{X})$, we write $h_{\mathbb{F}_q}$ to denote h viewed as a mapping on $\mathcal{X}_{\mathbb{F}_q}$. Conversely, by saying that $h_{\mathbb{F}_q}$ is a mapping on $\mathcal{X}_{\mathbb{F}_q}$, we implicitly assume that h is a mapping on $\mathcal{X}$.

Definition 8.5. Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ be a $\mathscr{C}_3$-frame of size (m, t).

(*a*) A *$\mathscr{C}_3$-map* in $\mathfrak{F}$ is an element $g \in \mathrm{GL}(\langle\mathfrak{F}\rangle)$ such that $g = h_{\mathbb{F}_q}$ for some $h \in \Gamma\mathrm{L}(\mathcal{X})$.

(*b*) We write $\mathrm{C}_3(\mathfrak{F})$ for the group of all $\mathscr{C}_3$-maps in $\mathfrak{F}$, and denote by $\mathrm{K}_3(\mathfrak{F})$ the group of all $\mathscr{C}_3$-maps $h_{\mathbb{F}_q}$ in $\mathfrak{F}$ with $h \in \mathrm{GL}(\mathcal{X})$.

Thus, in the situation of Definition 8.5 we have

$$\begin{aligned} \mathrm{C}_3(\mathfrak{F}) &= \mathrm{GL}\big(\langle\mathfrak{F}\rangle\big) \cap \big\{h_{\mathbb{F}_q} \mid h \in \Gamma\mathrm{L}(\mathcal{X})\big\}, \\ \mathrm{K}_3(\mathfrak{F}) &= \big\{h_{\mathbb{F}_q} \mid h \in \mathrm{GL}(\mathcal{X})\big\}. \end{aligned} \tag{8.2}$$

For an $\mathbb{F}_{q^t}$-semilinear mapping $h \in \Gamma\mathrm{L}(\mathcal{X})$, the element $h_{\mathbb{F}_q}$ is $\mathbb{F}_q$-linear, that is lies in $\mathrm{GL}(\langle\mathfrak{F}\rangle)$, if and only if $\mathbb{F}_q$ is contained in the fixed field of the field automorphism σ associated with h. This is equivalent to saying that $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$, and hence implies that the group homomorphism

$$\mathrm{C}_3(\mathfrak{F}) \to \mathrm{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q),$$

assigning to each element $h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$ the field automorphism associated with $h \in \Gamma\mathrm{L}(\mathcal{X})$, is surjective. Since $\mathrm{K}_3(\mathfrak{F})$ is the kernel of that homomorphism, it follows that

$$|\mathrm{C}_3(\mathfrak{F}) : \mathrm{K}_3(\mathfrak{F})| = t.$$

Observe that $\mathrm{GL}(m, q^t) \cong \mathrm{K}_3(\mathfrak{F}) \lhd \mathrm{C}_3(\mathfrak{F}) \leq \mathrm{GL}(\langle\mathfrak{F}\rangle) \cong \mathrm{GL}(mt, q)$.

Definition 8.6. Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ be a $\mathscr{C}_3$-frame, let $\mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q) \sqsubseteq \mathfrak{F}$, and let $g = h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$. We write $\mathfrak{D}g = (\mathcal{Y}h, \mathbb{F}_q)$.

Lemma 8.7. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame, let $\mathfrak{D} \sqsubseteq \mathfrak{F}$, and let $g \in \mathrm{C}_3(\mathfrak{F})$. Then $\mathfrak{D}g \sqsubseteq \mathfrak{F}$ and $\langle\mathfrak{D}\rangle g = \langle\mathfrak{D}g\rangle$.*

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ and $\mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q)$. Let $(m, t) = \mathrm{size}(\mathfrak{F})$ and let $h \in \Gamma\mathrm{L}(\mathcal{X})$ be such that $g = h_{\mathbb{F}_q}$. Since elements of $\Gamma\mathrm{L}(\mathcal{X})$ map subspaces of $\mathcal{X}$ again onto subspaces of $\mathcal{X}$, we have $\mathcal{Y}h \leq_{q^t} \mathcal{X}$, and thus $\mathfrak{D}g \sqsubseteq \mathfrak{F}$. Further, observe that $(\mathcal{Y}_{\mathbb{F}_q})h_{\mathbb{F}_q} = (\mathcal{Y}h)_{\mathbb{F}_q}$, whence $\langle\mathfrak{D}\rangle g = \langle\mathfrak{D}g\rangle$. □

The natural action of the general semilinear group on the subspaces of its underlying vector space induces an action of $\mathrm{C}_3(\mathfrak{F})$ on the set of all $\mathscr{C}_3$-subframes of $\mathfrak{F}$. By Lemma 5.15 we obtain the following.

Lemma 8.8. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame and let G satisfy $\mathrm{K}_3(\mathfrak{F}) \leq G \leq \mathrm{C}_3(\mathfrak{F})$. The group G acts on the set of all $\mathscr{C}_3$-subframes of $\mathfrak{F}$ via*

$$\{\mathfrak{D} \mid \mathfrak{D} \sqsubseteq \mathfrak{F}\} \times G \to \{\mathfrak{D} \mid \mathfrak{D} \sqsubseteq \mathfrak{F}\}, \quad (\mathfrak{D}, g) \mapsto \mathfrak{D}g.$$

Each orbit consists of all $\mathscr{C}_3$-subframes of a given size.

8.2.1 Linear mappings preserving $\mathscr{C}_3$-subframes

Consider a $\mathscr{C}_3$-map $g = h_{\mathbb{F}_q}$ in some $\mathscr{C}_3$-frame $\mathfrak{F}$ over $\mathbb{F}_q$. Let $\mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q)$ be a $\mathscr{C}_3$-subframe of $\mathfrak{F}$. If $\mathcal{Y}$ is $\langle h \rangle$-invariant, then g is said to *preserve* $\mathfrak{D}$.

Definition 8.9. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame, let $\mathfrak{D} \sqsubseteq \mathfrak{F}$, and let $G \leq \mathrm{C}_3(\mathfrak{F})$.

(*a*) An element $g \in \mathrm{C}_3(\mathfrak{F})$ is said to *preserve* $\mathfrak{D}$ if $\mathfrak{D}g = \mathfrak{D}$. The group G *preserves* $\mathfrak{D}$ if all elements of G preserve $\mathfrak{D}$.

(*b*) The maximal (with respect to inclusion) subgroup of G which preserves $\mathfrak{D}$ is denoted by $G_{\mathfrak{D}}$.

Hence, for G satisfying $\mathrm{K}_3(\mathfrak{F}) \leq G \leq \mathrm{C}_3(\mathfrak{F})$, the group $G_{\mathfrak{D}}$ is the stabiliser of $\mathfrak{D} \sqsubseteq \mathfrak{F}$ in the action described in Lemma 8.8 above. In fact, according to our next lemma, $G_{\mathfrak{D}}$ is also the (subspace) stabiliser of $\langle \mathfrak{D} \rangle$ in G.

Lemma 8.10. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame, let $\mathfrak{D} \sqsubseteq \mathfrak{F}$, and let $g \in \mathrm{C}_3(\mathfrak{F})$. The element g preserves $\mathfrak{D}$ if and only if $\langle \mathfrak{D} \rangle$ is $\langle g \rangle$-invariant.*

Proof. By Lemma 8.7, we have $\langle \mathfrak{D} \rangle g = \langle \mathfrak{D}g \rangle$. Hence, $\langle \mathfrak{D} \rangle$ is $\langle g \rangle$-invariant if and only if $\langle \mathfrak{D}g \rangle = \langle \mathfrak{D} \rangle$, that is if and only if $\mathfrak{D}g = \mathfrak{D}$. □

Lemma 8.11. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. The mappings*

$$\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_3(\mathfrak{D}), \quad g \mapsto g|_{\langle \mathfrak{D} \rangle},$$
$$\mathrm{K}_3(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{K}_3(\mathfrak{D}), \quad g \mapsto g|_{\langle \mathfrak{D} \rangle}$$

are surjective group homomorphisms.

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ and $\mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q)$. Let $(m, t) = \mathrm{size}(\mathfrak{F})$. By Lemma 8.10, the group $\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}$ is equal to the subspace stabiliser $\mathrm{C}_3(\mathfrak{F})_{\langle \mathfrak{D} \rangle}$. By (8.2) we thus have $\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} = \big(\mathrm{GL}\big(\langle \mathfrak{F} \rangle\big) \cap \big\{h_{\mathbb{F}_q} \mid h \in \Gamma\mathrm{L}(\mathcal{X})\big\}\big)_{\langle \mathfrak{D} \rangle}$. Hence,

$$\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} = \mathrm{GL}\big(\langle \mathfrak{F} \rangle\big)_{\langle \mathfrak{D} \rangle} \cap \big\{h_{\mathbb{F}_q} \mid h \in \Gamma\mathrm{L}(\mathcal{X})_{\mathcal{Y}}\big\}.$$

Thus, using

$$\begin{aligned}\big\{g|_{\langle\mathfrak{D}\rangle} \mid g \in \mathrm{GL}\big(\langle\mathfrak{F}\rangle\big)_{\langle\mathfrak{D}\rangle}\big\} &= \mathrm{GL}\big(\langle\mathfrak{D}\rangle\big),\\ \big\{h_{\mathbb{F}_q}|_{\langle\mathfrak{D}\rangle} \mid h \in \Gamma\mathrm{L}(\mathcal{X})_{\mathcal{Y}}\big\} &= \big\{(h|_{\mathcal{Y}})_{\mathbb{F}_q} \mid h \in \Gamma\mathrm{L}(\mathcal{X})_{\mathcal{Y}}\big\}\\ &= \big\{h_{\mathbb{F}_q} \mid h \in \Gamma\mathrm{L}(\mathcal{Y})\big\},\end{aligned}$$

we conclude that

$$\big\{g|_{\langle\mathfrak{D}\rangle} \mid g \in \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}\big\} = \mathrm{GL}\big(\langle\mathfrak{D}\rangle\big) \cap \big\{h_{\mathbb{F}_q} \mid h \in \Gamma\mathrm{L}(\mathcal{Y})\big\} = \mathrm{C}_3(\mathfrak{D}).$$

This shows that the mapping $\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_3(\mathfrak{D})$, $g \mapsto g|_{\langle\mathfrak{D}\rangle}$ is well-defined and surjective. Now, if for $g = h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$ the element $(h_0)_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{D})$ denotes the restriction of g to $\langle\mathfrak{D}\rangle$, then h and h_0 are associated with the same field automorphism. It follows that $\mathrm{K}_3(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{K}_3(\mathfrak{D})$, $g \mapsto g|_{\langle\mathfrak{D}\rangle}$ is also well-defined and surjective. (Clearly, both mappings are group homomorphisms.) □

8.2.2 Linear mappings conserving $\mathscr{C}_3$-subframes

Definition 8.12. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. An element $g \in \mathrm{C}_3(\mathfrak{F})$ *conserves* $\mathfrak{D}$ if g preserves $\mathfrak{D}$ and g does not preserve any proper $\mathscr{C}_3$-subframe of $\mathfrak{D}$.

Elements which conserve the underlying frame can be characterised as follows.

Lemma 8.13. *Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q), \mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q)$ be $\mathscr{C}_3$-frames such that $\mathfrak{D} \sqsubseteq \mathfrak{F}$. An element $h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$ conserves $\mathfrak{D}$ if and only if $\mathcal{Y}$ is $\langle h\rangle$-irreducible.*

Proof. The element $h_{\mathbb{F}_q}$ conserves $\mathfrak{D}$ if and only if $\mathcal{Y}$ is the only non-trivial and $\langle h\rangle$-invariant subspace of $\mathcal{Y}$. This is the same as saying that $\mathcal{Y}$ is $\langle h\rangle$-irreducible. □

Recall from Definition 3.5 that $N_q^*(m)$ is the number of all monic, irreducible polynomials $f \neq x$ over $\mathbb{F}_q$. The precise value of $N_q^*(m)$ can be calculated using the formula given in Lemma 3.7. Recall further from Definition 8.1 that, if (m, t) is the size of some $\mathscr{C}_3$-frame, then t is a prime.

Proposition 8.14. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime). Let $\mathrm{con}(\mathfrak{F})$ be the proportion (in $\mathrm{C}_3(\mathfrak{F})$) of all elements from $\mathrm{C}_3(\mathfrak{F})$ conserving $\mathfrak{F}$. Then*

$$\mathrm{con}(\mathfrak{F}) = \frac{N_{q^t}^*(m)}{(q^{mt}-1)t} + \frac{(t-1)N_q^*(m)}{(q^m-1)t}.$$

Moreover,

$$\frac{1}{m+1} \leq \operatorname{con}(\mathfrak{F}) \leq \frac{1}{m}.$$

If $m \geq 2$, then the upper bound is not strict, that is $\operatorname{con}(\mathfrak{F}) < 1/m$. If $m = 1$, then $\operatorname{con}(\mathfrak{F}) = 1$.

Proof. Let $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$, and let $H = \{h \in \Gamma\mathrm{L}(\mathcal{X}) \mid h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})\}$. Recall from Definition 4.20 the notion of $\operatorname{irr}(H)$. By Lemma 8.13 we have

$$\operatorname{con}(\mathfrak{F}) = \operatorname{irr}(H).$$

Since $\mathrm{GL}(\mathcal{X}) \leq H \leq \Gamma\mathrm{L}(\mathcal{X})$ and $|H : \mathrm{GL}(\mathcal{X})| = |\mathrm{C}_3(\mathfrak{F}) : \mathrm{K}_3(\mathfrak{F})| = t$, (recalling that t is a prime) the assertion holds by Theorem 4.22. □

Combining Lemma 8.13 with Lemma 4.5 yields the following.

Lemma 8.15. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame and let $g, \ell \in \mathrm{C}_3(\mathfrak{F})$. Then g conserves $\mathfrak{F}$ if and only if $\ell^{-1}g\ell$ conserves $\mathfrak{F}$.*

Consider a $\mathscr{C}_3$-frame $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$. Let $g = h_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$, and let σ be the field automorphism associated with h. The coset $g\mathrm{K}_3(\mathfrak{F})$ consists of all elements $u_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})$ such that u is σ-semilinear. The group $\mathrm{K}_3(\mathfrak{F})$ acts via conjugation on $g\mathrm{K}_3(\mathfrak{F})$. Because of Lemma 8.15, the group $\mathrm{K}_3(\mathfrak{F})$ also acts (via conjugation) on the set $\{\ell \in g\mathrm{K}_3(\mathfrak{F}) \mid \ell \text{ conserves } \mathfrak{F}\}$. Our next result identifies a set of polynomials over $\mathbb{F}_q$ which is in a one-to-one correspondence with the orbits of the latter action.

Lemma 8.16. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime). Let $g \in \mathrm{C}_3(\mathfrak{F})$ and let $\mathfrak{C}$ be the set of all orbits in $\{\ell \in g\mathrm{K}_3(\mathfrak{F}) \mid \ell \text{ conserves } \mathfrak{F}\}$ under conjugation by $\mathrm{K}_3(\mathfrak{F})$. By mapping each orbit $O \in \mathfrak{C}$ onto the characteristic polynomial of a representative of O, we obtain a bijection*

$$\mathfrak{C} \to \begin{cases} \{\prod_{\xi \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\xi \mid f \neq x \text{ is a monic,} \\ \quad \text{irreducible polynomial of degree } m \text{ over } \mathbb{F}_{q^t}\}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \{f(x^t) \mid f \neq x \text{ is a monic, irreducible} \\ \quad \text{polynomial of degree } m \text{ over } \mathbb{F}_q\}, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

Proof. Recall Definitions 3.37, 4.2. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ and $g = h_{\mathbb{F}_q}$. Let

$$\mathbb{K} = \begin{cases} \mathbb{F}_{q^t}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \mathbb{F}_q, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

Note (recalling that t is a prime) that $\mathbb{K}$ is the fixed field of the field automorphism associated with h. Consider an element $\ell = u_{\mathbb{F}_q} \in g\mathrm{K}_3(\mathfrak{F})$. Then $\mathbb{K}$ is also the fixed field of the field automorphism associated with u. Recall from Lemma 8.13, that ℓ conserves $\mathfrak{F}$ if and only if the element $u \in \Gamma\mathrm{L}(\mathcal{X})$ is irreducible.

Now, if $f \in \mathbb{K}[x]$ is the minimal polynomial on $\mathcal{X}_{\mathbb{K}}$ of the ($\mathbb{F}_{q^t}$-)linear part of u (which is u itself in case $g \in \mathrm{K}_3(\mathfrak{F})$), then by Lemma 4.16, and respectively by Proposition 4.26, the characteristic polynomial of ℓ is given by

$$\begin{cases} \prod_{\xi \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^{\xi}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ f(x^t), & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

Then the assertion follows from Lemma 4.17. □

Recall that, given a group G and an element $g \in G$, we write $C_G(g)$ for the centraliser of $\langle g \rangle$ in G.

Lemma 8.17. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m,t) over $\mathbb{F}_q$ (so t is prime) and let $g \in \mathrm{C}_3(\mathfrak{F})$ conserve $\mathfrak{F}$. Then*

$$|C_{\mathrm{K}_3(\mathfrak{F})}(g)| = \begin{cases} q^{mt} - 1, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ q^m - 1, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$ and $g = h_{\mathbb{F}_q}$. Since g conserves $\mathfrak{F}$, by Lemma 8.13 the element $h \in \Gamma\mathrm{L}(\mathcal{X})$ is irreducible. Let $\mathbb{K}$ be the fixed field of the field automorphism associated with h. Then

$$\mathbb{K} = \begin{cases} \mathbb{F}_{q^t}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \mathbb{F}_q, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

By Proposition 4.18 the order of $C_{\mathrm{GL}(\mathcal{X})}(h)$ is given by $|\mathbb{K}|^m - 1$. Since $|C_{\mathrm{K}_3(\mathfrak{F})}(g)| = |C_{\mathrm{GL}(\mathcal{X})}(h)|$, the assertion follows. □

Recall from Definition 8.3(b) the notion of a $\mathscr{C}_3$-cover.

Lemma 8.18. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m,t) over $\mathbb{F}_q$. Let $g \in \mathrm{C}_3(\mathfrak{F})$, let $\mathcal{U} \leq_q \langle \mathfrak{F} \rangle$, and let $\mathfrak{U}$ be the $\mathscr{C}_3$-cover of $\mathcal{U}$ in $\mathfrak{F}$.*

(a) *If $\mathcal{U}$ is $\langle g \rangle$-invariant, then g preserves $\mathfrak{U}$.*

(b) *Suppose that $\mathcal{U}$ is $\langle g \rangle$-irreducible and $\dim_q(\mathcal{U}) > mt/2$. Then g conserves $\mathfrak{U}$. Moreover, if $g \in \mathrm{K}_3(\mathfrak{F})$, then $\langle \mathfrak{U} \rangle = \mathcal{U}$.*

Proof. (a) Suppose that $\mathcal{U}$ is $\langle g\rangle$-invariant. Since $\mathcal{U} \leq_q \langle\mathfrak{U}\rangle$ and $\mathcal{U}g = \mathcal{U}$, we get $\mathcal{U} \leq_q \langle\mathfrak{U}\rangle g$. Then Lemma 8.7 yields $\mathcal{U} \leq_q \langle\mathfrak{U}g\rangle$. We thus obtain $\mathcal{U} \leq_q \langle\mathfrak{U}\rangle \cap \langle\mathfrak{U}g\rangle$, that is according to Lemma 8.4,

$$\mathcal{U} \leq_q \langle\mathfrak{U} \cap \mathfrak{U}g\rangle.$$

Since $\mathfrak{U}\cap\mathfrak{U}g \sqsubseteq \mathfrak{F}$ and since (being the $\mathscr{C}_3$-cover of $\mathcal{U}$ in $\mathfrak{F}$) $\mathfrak{U}$ is the smallest (with respect to "$\sqsubseteq$") $\mathscr{C}_3$-subframe of $\mathfrak{F}$ whose $\mathscr{C}_3$-span contains $\mathcal{U}$, it follows that $\mathfrak{U} \sqsubseteq \mathfrak{U} \cap \mathfrak{U}g$. Hence, $\mathfrak{U} = \mathfrak{U}g$ as asserted.

(b) Suppose that $\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q)$, $\mathfrak{U} = (\mathcal{Y}, \mathbb{F}_q)$, and $g = h_{\mathbb{F}_q}$. Since $\mathcal{U}$ is $\langle g\rangle$-invariant, from part (a) of the current lemma we know that g preserves $\mathfrak{U}$, that is $\mathcal{Y}$ is $\langle h\rangle$-invariant. Recall that q is a power of the prime p. Recall that we write $h_{p'}$ for the p'-part of h (as introduced in Definition 4.14). Seeking a contradiction, assume that there exists a non-trivial, proper, $\langle h_{p'}\rangle$-invariant subspace $\mathcal{Y}_0$ of $\mathcal{Y}$. Then by [35, Theorem 1.9] (Maschke) there exists an $\langle h_{p'}\rangle$-invariant complement of $\mathcal{Y}_0$ in $\mathcal{Y}$. Replacing $\mathcal{Y}_0$ by this complement if necessary, we may assume that $\dim_{q^t}(\mathcal{Y}_0) \geq \dim_{q^t}(\mathcal{Y})/2$, whence

$$\dim_q\big((\mathcal{Y}_0)_{\mathbb{F}_q}\big) \geq \dim_q(\mathcal{Y}_{\mathbb{F}_q})/2.$$

(Observe that $(\mathcal{Y}_0)_{\mathbb{F}_q}$ is $\langle(h_{p'})_{\mathbb{F}_q}\rangle$-invariant.) Since $\dim_q(\mathcal{U}) > mt/2 \geq \dim_q(\mathcal{Y}_{\mathbb{F}_q})/2$ and $\mathcal{U} \leq_q \mathcal{Y}_{\mathbb{F}_q}$, it follows that

$$\mathcal{U} \cap (\mathcal{Y}_0)_{\mathbb{F}_q} \neq \{0\}.$$

Note that $g_{p'} = (h_{\mathbb{F}_q})_{p'} = (h_{p'})_{\mathbb{F}_q}$. Then, recalling that $(\mathcal{Y}_0)_{\mathbb{F}_q}$ is $\langle(h_{p'})_{\mathbb{F}_q}\rangle$-invariant and using (the "in particular" part of) Lemma 4.15, by which the subspace $\mathcal{U}$ is $\langle(h_{p'})_{\mathbb{F}_q}\rangle$-irreducible, we obtain $\mathcal{U} \cap (\mathcal{Y}_0)_{\mathbb{F}_q} = \mathcal{U}$, that is

$$\mathcal{U} \leq_q (\mathcal{Y}_0)_{\mathbb{F}_q}.$$

Now, $(\mathcal{Y}_0, \mathbb{F}_q)$ is a $\mathscr{C}_3$-subframe of $\mathfrak{F}$. Since (being the $\mathscr{C}_3$-cover of $\mathcal{U}$ in $\mathfrak{F}$) $\mathfrak{U} = (\mathcal{Y}, \mathbb{F}_q)$ is the smallest $\mathscr{C}_3$-subframe of $\mathfrak{F}$ whose $\mathscr{C}_3$-span contains $\mathcal{U}$, (recalling that $\mathcal{U} \leq_q (\mathcal{Y}_0)_{\mathbb{F}_q}$) we conclude that $\mathfrak{U} \sqsubseteq (\mathcal{Y}_0, \mathbb{F}_q)$. This is not true, because $\mathcal{Y} \not\leq_{q^t} \mathcal{Y}_0$. Hence, $\mathcal{Y}$ is $\langle h_{p'}\rangle$-irreducible and thus also $\langle h\rangle$-irreducible. Then by Lemma 8.13, g conserves $\mathfrak{U}$.

It remains to prove the "moreover" part. To this end, suppose $g \in \mathrm{K}_3(\mathfrak{F})$. Since g preserves $\mathfrak{U}$, by Lemma 8.10 the subspace $\langle\mathfrak{U}\rangle$ is $\langle g\rangle$-invariant. Let $\widehat{f} \in \mathbb{F}_q[x]$ be the characteristic polynomial of the restriction $g|_{\langle\mathfrak{U}\rangle}$. By Lemma 8.11 we have $g|_{\langle\mathfrak{U}\rangle} \in \mathrm{K}_3(\mathfrak{U})$. Hence, by Lemma 8.16 there exists a monic, irreducible polynomial $f \in \mathbb{F}_{q^t}[x]$ such that

$$\widehat{f} = \prod_{\xi \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^{\xi}.$$

Now, (since $\mathcal{U}$ is $\langle g\rangle$-irreducible) by Lemma 4.8(a) the characteristic polynomial of $g|_{\mathcal{U}}$ is irreducible (over $\mathbb{F}_q$). Since that polynomial has degree $\dim_q(\mathcal{U}) > mt/2$ and is a divisor of $\widehat{f}$, using Lemma 3.38 we conclude that $\widehat{f}$ is irreducible (over $\mathbb{F}_q$). Then by Lemma 4.8(a), $g|_{\langle\mathfrak{U}\rangle}$ is irreducible, or in other words, $\langle\mathfrak{U}\rangle$ is $\langle g\rangle$-irreducible. Since $\mathcal{U}$ is also $\langle g\rangle$-irreducible (and since $\mathcal{U} \leq_q \langle\mathfrak{U}\rangle$) it follows that $\mathcal{U} = \langle\mathfrak{U}\rangle$. □

Remark 8.19. We emphasise that the "moreover" part of Lemma 8.18(b) does not hold for all elements in $\mathrm{C}_3(\mathfrak{F})$. That is, if in the situation of Lemma 8.18(b) we have $g \in \mathrm{C}_3(\mathfrak{F})\backslash\mathrm{K}_3(\mathfrak{F})$, then $\mathcal{U}$ may be a proper subspace of $\langle\mathfrak{U}\rangle$. Otherwise, any fat element in $\mathrm{C}_3(\mathfrak{F})$ (see Definition 5.1(a)) which conserves $\mathfrak{F}$ would be irreducible, which is not true by Example 8.22 with $m = 3$.

8.3 Fat $\mathscr{C}_3$-maps

Consider a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$. Let $e \leq mt$ be an integer strictly bigger than $mt/2$. Recall from Definition 5.1(a) that we call an element $g \in \mathrm{C}_3(\mathfrak{F})$ fat, or more precisely a $\mathrm{fat}(mt, q; e)$-element, if $\langle g\rangle$ acts irreducibly on an e-dimensional subspace of $\langle\mathfrak{F}\rangle$. Observe that $\mathrm{fat}(mt, q; mt)$-elements in $\mathrm{C}_3(\mathfrak{F})$ are precisely the irreducible elements in $\mathrm{C}_3(\mathfrak{F})$.

8.3.1 Fat $\mathscr{C}_3$-maps conserving the underlying frame

As in the case of $\mathscr{C}_2$-maps (see Lemma 7.29), any irreducible $\mathscr{C}_3$-map conserves the underlying frame.

Lemma 8.20. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame. An irreducible element in $\mathrm{C}_3(\mathfrak{F})$ conserves $\mathfrak{F}$.*

Proof. Let $g \in \mathrm{C}_3(\mathfrak{F})$ be irreducible. If g preserves a proper $\mathscr{C}_3$-subframe $\mathfrak{D}$ of $\mathfrak{F}$, then by Lemma 8.10 the non-trivial and proper subspace $\langle\mathfrak{D}\rangle$ of $\langle\mathfrak{F}\rangle$ is $\langle g\rangle$-invariant. This contradicts the irreducibility of g. □

Proposition 8.21. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime). Let $g \in \mathrm{C}_3(\mathfrak{F})$ and let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$. Then the following hold.*

(a) The coset $g\mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements conserving $\mathfrak{F}$ if and only if

$$\begin{cases} e = mt, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \gcd(q, t) = 1 \text{ and } e = \mathrm{ord}(q; (q^m - 1)t), & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

(b) Suppose that $g \notin \mathrm{K}_3(\mathfrak{F})$ and $g\mathrm{K}_3(\mathfrak{F})$ contains a $\mathrm{fat}(mt, q; e)$-element conserving $\mathfrak{F}$. Then $e \in \{mt, m(t-1)\}$.

Proof. (a) Suppose that $g \in \mathrm{K}_3(\mathfrak{F})$, whence $g\mathrm{K}_3(\mathfrak{F}) = \mathrm{K}_3(\mathfrak{F})$. According to Lemmas 5.2, 8.16 the group $\mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements conserving $\mathfrak{F}$ if and only if the polynomial ring $\mathbb{F}_{q^t}[x]$ contains monic, irreducible polynomials $f \neq x$ of degree m such that the Galois-twist $\prod_{\xi \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\xi \in \mathbb{F}_q[x]$ of f over $\mathbb{F}_q$ has an irreducible factor (over $\mathbb{F}_q$) of degree e. According to Proposition 3.39 this is the case if and only if $e = mt$.

Suppose that $g \notin \mathrm{K}_3(\mathfrak{F})$. Then by Lemmas 5.2, 8.16 the coset $g\mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements conserving $\mathfrak{F}$ if and only if the polynomial ring $\mathbb{F}_q[x]$ contains monic, irreducible polynomials $f \neq x$ of degree m such that $f(x^t)$ has an irreducible factor of degree e. According to Proposition 3.28 the latter is equivalent to saying that $\gcd(q, t) = 1$, $\mathrm{ord}(q; (q^m - 1)t) = e$.

(b) Since $g \notin \mathrm{K}_3(\mathfrak{F})$ and $g\mathrm{K}_3(\mathfrak{F})$ contains a $\mathrm{fat}(mt, q; e)$-element conserving $\mathfrak{F}$, part (a) of the current lemma yields $\gcd(q, t) = 1$, $\mathrm{ord}(q; (q^m - 1)t) = e$. Then, because t is a prime, the assertion holds by Lemma 2.21. □

The following example shows that, in the situation of Proposition 8.21(b), the integer e can take both values, mt and $m(t-1)$.

Example 8.22. Let $m \in \{2, 3\}$ and $t = 3$. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_2$, whence $\mathrm{C}_3(\mathfrak{F}) \cong \Gamma\mathrm{L}(m, 8)$ and $\mathrm{K}_3(\mathfrak{F}) \cong \mathrm{GL}(m, 8)$.

Since $(2^m - 1)3 \in \{9, 21\}$ divides $2^6 - 1 = 63$ but $(2^m - 1)3$ does not divide $2^1 - 1$, $2^2 - 1$, and $2^3 - 1$, Lemma 2.11 yields $\mathrm{ord}(2; (2^m - 1)3) = 6$. Then by Proposition 8.21(a) the set $\mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(3m, 2; 6)$-elements which conserve $\mathfrak{F}$. Note that $6 = mt$ if $m = 2$ and $6 = m(t-1)$ if $m = 3$.

Corollary 8.23. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime). The following hold.*

(a) *The group $\mathrm{K}_3(\mathfrak{F})$ contains irreducible elements.*

(b) *If $g \in \mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$, then the coset $g\mathrm{K}_3(\mathfrak{F})$ contains irreducible elements if and only if $t \mid q^m - 1$.*

Proof. By Lemma 8.20, any irreducible element of $\mathrm{C}_3(\mathfrak{F})$ conserves $\mathfrak{F}$. Thus, using Proposition 8.21(a), we obtain the following.

(a) The group $\mathrm{K}_3(\mathfrak{F})$ contains irreducible elements.

(b) For $g \in \mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$, the coset $g\mathrm{K}_3(\mathfrak{F})$ contains irreducible elements if and only if

$$\gcd(q, t) = 1, \quad \mathrm{ord}(q; (q^m - 1)t) = mt. \tag{8.3}$$

Recall that t is a prime. According to Proposition 2.19 (applied to $a = q$ and $r = q^m - 1$) condition (8.3) is equivalent to $t \mid q^m - 1$. □

Example 8.24. Let $m \in \mathbb{N}$. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size $(m, 2)$ over $\mathbb{F}_q$. By Corollary 8.23(a) the group $\mathrm{K}_3(\mathfrak{F}) \cong \mathrm{GL}(m, q^2)$ contains irreducible elements for any q. By Corollary 8.23(b), the set $\mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$ contains irreducible elements if and only if q is odd.

We next determine the number of all irreducible elements in a given coset $g\mathrm{K}_3(\mathfrak{F})$, $g \in \mathrm{C}_3(\mathfrak{F})$. This yields the number of all irreducible elements in $\mathrm{C}_3(\mathfrak{F})$. As usual, we present our results in terms of proportions. Recall Definition 4.20. Recall further from Definitions 3.5, 3.22 the meaning of $N_q^*(m)$ and $N_q^*(m, t)$. The precise values of $N_q^*(m)$, $N_q^*(m, t)$ can be calculated through Lemma 3.7 and Theorem 3.23, respectively.

Proposition 8.25. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime).*

(a) *Let $g \in \mathrm{C}_3(\mathfrak{F})$. Then*

$$\mathrm{irr}\big(g\mathrm{K}_3(\mathfrak{F})\big) = \begin{cases} \dfrac{N_q^*(mt)t}{q^{mt}-1} \neq 0, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \dfrac{N_q^*(m,t)}{q^m-1} \neq 0, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}) \text{ and } t \mid q^m-1, \\ 0, & \text{else.} \end{cases}$$

Moreover,

$$\begin{cases} \dfrac{t}{mt+1} \leq \mathrm{irr}\big(g\mathrm{K}_3(\mathfrak{F})\big) \leq \dfrac{1}{m}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \dfrac{t-1}{(m+1)t} \leq \mathrm{irr}\big(g\mathrm{K}_3(\mathfrak{F})\big) \leq \dfrac{t-1}{mt}, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}) \text{ and } t \mid q^m-1. \end{cases}$$

(b) *We have*

$$\mathrm{irr}\big(\mathrm{C}_3(\mathfrak{F})\big) = \begin{cases} \dfrac{N_q^*(mt)}{q^{mt}-1} + \dfrac{(t-1)N_q^*(m,t)}{t(q^m-1)} \neq 0, & \text{if } t \mid q^m-1, \\ \dfrac{N_q^*(mt)}{q^{mt}-1} \neq 0, & \text{if } t \nmid q^m-1. \end{cases}$$

Moreover,

$$\begin{cases} \dfrac{1}{mt+1} + \dfrac{(t-1)^2}{(m+1)t^2} \leq \mathrm{irr}\big(\mathrm{C}_3(\mathfrak{F})\big) \leq \dfrac{1}{mt} + \dfrac{(t-1)^2}{mt^2}, & \text{if } t \mid q^m-1, \\ \dfrac{1}{mt+1} \leq \mathrm{irr}\big(\mathrm{C}_3(\mathfrak{F})\big) \leq \dfrac{1}{mt}, & \text{if } t \nmid q^m-1. \end{cases}$$

Proof. Since $|\mathrm{C}_3(\mathfrak{F}) : \mathrm{K}_3(\mathfrak{F})| = t$, part (b) follows directly from part (a) by adding up the numbers of irreducible elements in each of the cosets of $\mathrm{K}_3(\mathfrak{F})$ in $\mathrm{C}_3(\mathfrak{F})$ and dividing the result by $|\mathrm{C}_3(\mathfrak{F})|$. We thus only prove assertion (a).

The group $\mathrm{K}_3(\mathfrak{F})$ acts via conjugation on the set of all irreducible elements in $g\mathrm{K}_3(\mathfrak{F})$. Recall from Lemma 8.20 that every irreducible element in $g\mathrm{K}_3(\mathfrak{F})$ conserves $\mathfrak{F}$. Thus, using Lemmas 4.8(a), 8.16 we deduce the following. If $g \in \mathrm{K}_3(\mathfrak{F})$, then the number of all orbits is equal to the number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_{q^t}$ such that $\prod_{\xi \in \mathrm{Gal}(\mathbb{F}_{q^t}:\mathbb{F}_q)} f^\xi$ is irreducible over $\mathbb{F}_q$. If $g \notin \mathrm{K}_3(\mathfrak{F})$, then the number of all orbits is equal to the number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$ such that $f(x^t)$ is irreducible over $\mathbb{F}_q$. Thus, by Proposition 3.39 and Definition 3.22 there is a total of

$$\begin{cases} N_q^*(mt)t, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ N_q^*(m,t), & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}) \end{cases}$$

orbits. By Lemma 8.17 (and the orbit-stabiliser-theorem) each orbit has length

$$\begin{cases} \dfrac{|\mathrm{K}_3(\mathfrak{F})|}{q^{mt}-1}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \dfrac{|\mathrm{K}_3(\mathfrak{F})|}{q^{m}-1}, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

Hence, the number of all irreducible elements in $g\mathrm{K}_3(\mathfrak{F})$ is equal to

$$\mathrm{irr}\big(g\mathrm{K}_3(\mathfrak{F})\big)|g\mathrm{K}_3(\mathfrak{F})| = \begin{cases} \dfrac{N_q^*(mt)t|\mathrm{K}_3(\mathfrak{F})|}{q^{mt}-1}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \dfrac{N_q^*(m,t)|\mathrm{K}_3(\mathfrak{F})|}{q^{m}-1}, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

This yields

$$\mathrm{irr}\big(g\mathrm{K}_3(\mathfrak{F})\big) = \begin{cases} \dfrac{N_q^*(mt)t}{q^{mt}-1}, & \text{if } g \in \mathrm{K}_3(\mathfrak{F}), \\ \dfrac{N_q^*(m,t)}{q^{m}-1}, & \text{if } g \notin \mathrm{K}_3(\mathfrak{F}). \end{cases}$$

If $g \notin \mathrm{K}_3(\mathfrak{F})$, then by Corollary 8.23$(b)$ we have $\mathrm{irr}\big(g\mathrm{K}_3(\mathfrak{F})\big) \neq 0$ if and only if $t \mid q^m - 1$. This completes the proof of the first part of assertion (a). The "moreover" part of assertion (a) holds by Lemma 3.9(c) and Theorem 3.24. (Recall that t is a prime, whence $\varphi(t) = t - 1$.) □

Example 8.26. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size $(2,3)$ over $\mathbb{F}_2$, whence

$$\mathrm{C}_3(\mathfrak{F}) \cong \Gamma\mathrm{L}(2,8).$$

Since $3 \mid 2^2-1$, Proposition 8.25(b) yields

$$\operatorname{irr}(\mathrm{C}_3(\mathfrak{F})) = \frac{N_2^*(6)}{2^6-1} + \frac{2N_2^*(2,3)}{3(2^2-1)}.$$

Using Lemma 3.7 and Theorem 3.23 we obtain $\operatorname{irr}(\mathrm{C}_3(\mathfrak{F})) = 1/7+2/9 = 23/63$.

Definition 8.27. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m,t) over $\mathbb{F}_q$, and let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$. We write $\operatorname{confat}(\mathfrak{F}; e)$ for the proportion (in $\mathrm{C}_3(\mathfrak{F})$) of all $\operatorname{fat}(mt, q; e)$-elements in $\mathrm{C}_3(\mathfrak{F})$ which conserve $\mathfrak{F}$.

Proposition 8.28. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m,t) over $\mathbb{F}_q$ (so t is prime), and let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$.*

(a) *If $e = mt$, then* $\operatorname{confat}(\mathfrak{F}; e) = \operatorname{irr}(\mathrm{C}_3(\mathfrak{F}))$.[(II)]

(b) *Suppose that $e < mt$ and* $\operatorname{confat}(\mathrm{C}_3(\mathfrak{F}); e) \neq 0$. *Then*

$$\operatorname{confat}(\mathfrak{F}; e) = \frac{(t-1)N_q^*(m)}{(q^m-1)t}.$$

Moreover,

$$\frac{t-1}{(m+1)t} \leq \operatorname{confat}(\mathfrak{F}; e) \leq \frac{t-1}{mt}.$$

If $m \geq 2$, then the upper bound is not strict, that is $\operatorname{confat}(\mathfrak{F}; e) < (t-1)/(mt)$. *If $m = 1$, then* $\operatorname{confat}(\mathfrak{F}; e) = (t-1)/t$.

Proof. (a) The assertion holds by Lemma 8.20.

(b) Since $e < mt$, by Proposition 8.21(a) the group $\mathrm{K}_3(\mathfrak{F})$ does not contain any $\operatorname{fat}(mt, q; e)$-elements which conserve $\mathfrak{F}$. Let $g \in \mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$. Consider the coset $g\mathrm{K}_3(\mathfrak{F})$. The group $\mathrm{K}_3(\mathfrak{F})$ acts by conjugation on the set of all elements in $g\mathrm{K}_3(\mathfrak{F})$ which conserve $\mathfrak{F}$. Since conjugation does not change the characteristic polynomial, Lemma 5.2 implies that $\mathrm{K}_3(\mathfrak{F})$ also acts by conjugation on the set of all $\operatorname{fat}(mt, q; e)$-elements in $g\mathrm{K}_3(\mathfrak{F})$ conserving $\mathfrak{F}$. By Lemmas 5.2, 8.16 the number, say T, of all orbits (of the latter action) is the number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$ such that $f(x^t)$ has an irreducible (over $\mathbb{F}_q$) factor of degree e. By Proposition 3.29(b) there exists an odd prime divisor s of t such that $T = N_q^*(m, (t)_{s'})$. Recalling that t is a prime itself, we get

[(II)] See Proposition 8.25(b).

$t = s$, whence $T = N_q^*(m,1) = N_q^*(m)$. According to Lemma 8.17 (and the orbit-stabiliser-theorem) each orbit has length $|\mathrm{K}_3(\mathfrak{F})|/(q^m-1)$. It follows that the number of all $\mathrm{fat}(mt,q;e)$-elements in $g\mathrm{K}_3(\mathfrak{F})$ which conserve $\mathfrak{F}$ is equal to $N_q^*(m)|\mathrm{K}_3(\mathfrak{F})|/(q^m-1)$. Since $\mathrm{C}_3(\mathfrak{F})$ has $t-1$ cosets of $\mathrm{K}_3(\mathfrak{F})$ which are not equal to $\mathrm{K}_3(\mathfrak{F})$, we get

$$\underbrace{\mathrm{confat}(\mathfrak{F};e)|\mathrm{C}_3(\mathfrak{F})|}_{\substack{\text{number of } \mathrm{fat}(mt,q;e)\text{-elements}\\ \text{in } \mathrm{C}_3(\mathfrak{F}) \text{ which conserve } \mathfrak{F}}} = \frac{(t-1)N_q^*(m)|\mathrm{K}_3(\mathfrak{F})|}{q^m-1}.$$

Hence,

$$\mathrm{confat}(\mathfrak{F};e) = \frac{(t-1)N_q^*(m)}{(q^m-1)t},$$

as asserted. The "moreover" part holds by Lemma 3.9(c). □

Example 8.29. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size $(3,3)$ over $\mathbb{F}_2$, whence

$$\mathrm{C}_3(\mathfrak{F}) \cong \Gamma\mathrm{L}(3,8).$$

By Example 8.22 the group $\mathrm{C}_3(\mathfrak{F})$ contains $\mathrm{fat}(9,2;6)$-elements which conserve $\mathfrak{F}$. That is, $\mathrm{confat}(\mathfrak{F};6) \neq 0$. Then by Proposition 8.28(b) and Lemma 3.7 we get

$$\mathrm{confat}(\mathfrak{F};6) = \frac{2N_2^*(3)}{(2^3-1)3} = \frac{4}{21}.$$

8.3.2 The general case

Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame. As in the case of $\mathscr{C}_2$-frames, we will derive the existence and the proportion of fat elements in $\mathrm{C}_3(\mathfrak{F})$ from the existence and the proportion of fat elements in $\mathrm{C}_3(\mathfrak{F})$ which conserve $\mathfrak{F}$. The following lemma justifies this reduction.

Lemma 8.30. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m,t) over $\mathbb{F}_q$. Let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$, and let $g \in \mathrm{C}_3(\mathfrak{F})$ be a $\mathrm{fat}(mt,q;e)$-element. There exists a uniquely determined $\mathscr{C}_3$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that $\dim_q(\langle\mathfrak{D}\rangle) \geq e$, g conserves $\mathfrak{D}$, and the restriction $g|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_3(\mathfrak{D})$ is a $\mathrm{fat}(\dim_q(\langle\mathfrak{D}\rangle),q;e)$-element (conserving $\mathfrak{D}$).*

Proof. Let $\mathcal{U}$ be the (uniquely determined) e-dimensional and $\langle g\rangle$-irreducible ($\mathbb{F}_q$-)subspace of $\langle\mathfrak{F}\rangle$. Let $\mathfrak{D}$ be the $\mathscr{C}_3$-cover of $\mathcal{U}$ in $\mathfrak{F}$ (see Definition 8.3(b)). Then $\mathfrak{D}$ is a $\mathscr{C}_3$-subframe of $\mathfrak{F}$, which according to Lemma 8.18(b) is conserved by g. We have $\mathcal{U} \leq_q \langle\mathfrak{D}\rangle$, whence $e \leq \dim_q(\langle\mathfrak{D}\rangle)$. Since g preserves $\mathfrak{D}$, by

Lemma 8.11 we get $g|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_3(\mathfrak{D})$. Since $\langle\mathfrak{D}\rangle$ contains the $\langle g\rangle$-irreducible subspace $\mathcal{U}$, it follows that $g|_{\langle\mathfrak{D}\rangle}$ is a $\mathrm{fat}(\dim_q(\langle\mathfrak{D}\rangle), q; e)$-element. Since g conserves $\mathfrak{D}$, the restriction $g|_{\langle\mathfrak{D}\rangle}$ also conserves $\mathfrak{D}$.

Seeking a contradiction, assume that there exists another $\mathscr{C}_3$-subframe $\mathfrak{D}' \sqsubseteq \mathfrak{F}$ such that $\dim_q(\langle\mathfrak{D}'\rangle) \geq e$ and g conserves $\mathfrak{D}'$. Assume that

$$\mathfrak{F} = (\mathcal{X}, \mathbb{F}_q), \quad \mathfrak{D} = (\mathcal{Y}, \mathbb{F}_q), \quad \mathfrak{D}' = (\mathcal{Y}', \mathbb{F}_q), \quad g = h_{\mathbb{F}_q}.$$

Now (by assumption) we have $\dim_q(\langle\mathfrak{D}\rangle), \dim_q(\langle\mathfrak{D}'\rangle) > \dim_q(\langle\mathfrak{F}\rangle)/2$. Then $\dim_{q^t}(\mathcal{Y}), \dim_{q^t}(\mathcal{Y}') > \dim_{q^t}(\mathcal{X})/2$, which is why $\mathcal{Y} \cap \mathcal{Y}' \neq \{0\}$. Since by Lemma 8.13 the subspaces $\mathcal{Y}, \mathcal{Y}'$ are $\langle h\rangle$-irreducible, we conclude that $\mathcal{Y} = \mathcal{Y}'$, and thus $\mathfrak{D} = \mathfrak{D}'$. □

Consider a $\mathscr{C}_3$-frame $\mathfrak{F}$ of size (m, t) over $\mathbb{F}_q$. (Recall from Definition 8.1 that, in such a case t is a prime.) We show that $\mathrm{C}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements if and only if either e is divisible by t, or $t \nmid q$ and $e = \mathrm{ord}(q; (q^{m_0}-1)t)$ for some positive integer $m_0 \leq m$.

Theorem 8.31. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime). Let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$.*

(*a*) *The group $\mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements if and only if $t \mid e$.*

(*b*) *Let $g \notin \mathrm{K}_3(\mathfrak{F})$. The coset $g\mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements if and only if $\gcd(q, t) = 1$ and $e = \mathrm{ord}(q; (q^{m_0} - 1)t)$ for some integer $m_0 \leq m$.*

Proof. (*a*) Suppose that the group $\mathrm{K}_3(\mathfrak{F})$ contains a $\mathrm{fat}(mt, q; e)$-element k. By Lemma 8.30 there exists a $\mathscr{C}_3$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that the restriction $k|_{\langle\mathfrak{D}\rangle}$ is a $\mathrm{fat}(\dim_q(\langle\mathfrak{D}\rangle), q; e)$-element which conserves $\mathfrak{D}$. By Lemma 8.11 we have $k|_{\langle\mathfrak{D}\rangle} \in \mathrm{K}_3(\mathfrak{D})$. Let $(m_0, t) = \mathrm{size}(\mathfrak{D})$. Then Proposition 8.21(*a*) (applied to $\mathrm{K}_3(\mathfrak{D})$) reveals that $e = m_0 t$, whence $t \mid e$.

Conversely, assume that $t \mid e$. Let $m_0 = e/t$, and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$ be such that $\mathrm{size}(\mathfrak{D}) = (m_0, t)$. By Corollary 8.23(*a*) the group $\mathrm{K}_3(\mathfrak{D})$ contains irreducible elements (that is $\mathrm{fat}(m_0 t, q; m_0 t)$-elements). Then, as we may deduce from Lemma 8.11, the group $\mathrm{K}_3(\mathfrak{F})_{\mathfrak{D}} \leq \mathrm{K}_3(\mathfrak{F})$ contains $\mathrm{fat}(mt, q; e)$-elements.

(*b*) Suppose that the coset $g\mathrm{K}_3(\mathfrak{F}) \neq \mathrm{K}_3(\mathfrak{F})$ contains a $\mathrm{fat}(mt, q; e)$-element ℓ. By Lemma 8.30 there exists a $\mathscr{C}_3$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that the restriction $\ell|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_3(\mathfrak{D})$ is a $\mathrm{fat}(\dim_q(\langle\mathfrak{D}\rangle), q; e)$-element which conserves $\mathfrak{D}$. By Lemma 8.11 we have $\ell|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_3(\mathfrak{D})$. Suppose that $\ell = h_{\mathbb{F}_q}$ and $\ell|_{\langle\mathfrak{D}\rangle} = (h_0)_{\mathbb{F}_q}$. Now, (since h_0 is a restriction of h) the elements h and h_0 are associated with the same field automorphism. Hence, (recalling that $\ell \notin \mathrm{K}_3(\mathfrak{F})$) it follows that $\ell|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_3(\mathfrak{D}) \setminus \mathrm{K}_3(\mathfrak{D})$. Being a $\mathscr{C}_3$-subframe

of $\mathfrak{F}$, $\mathfrak{D}$ has size (m_0, t) for some positive integer $m_0 \leq m$. Then Proposition 8.21(a) yields $\gcd(q,t) = 1$ and $\operatorname{ord}(q; (q^{m_0}-1)t) = e$.

Conversely, assume that $\gcd(q,t) = 1$ and that there exists a positive integer m_0 satisfying $\operatorname{ord}(q; (q^{m_0}-1)t) = e$. Let $\mathfrak{D} \sqsubseteq \mathfrak{F}$ with $\operatorname{size}(\mathfrak{D}) = (m_0, t)$. Assume that $g = h_{\mathbb{F}_q}$ and let $\sigma \in \operatorname{Gal}(\mathbb{F}_{q^t} : \mathbb{F}_q)$ be the field automorphism associated with h. (Since $g \notin \mathrm{K}_3(\mathfrak{F})$ we have $\sigma \neq \mathrm{id}_{\mathbb{F}_{q^t}}$.) Now, let $g_0 = (h_0)_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{D})$ be such that h_0 is σ-semilinear. By Proposition 8.21(a), the coset $g_0\mathrm{K}_3(\mathfrak{D})$ contains a $\operatorname{fat}(m_0 t, q; e)$-element, say ℓ_0. By Lemma 8.11 there exists an element $\ell = u_{\mathbb{F}_q} \in \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}$ such that $\ell|_{\langle\mathfrak{D}\rangle} = \ell_0$. Then ℓ is a $\operatorname{fat}(mt, q; e)$-element. Moreover, in order that the restriction of ℓ to $\langle\mathfrak{D}\rangle$ lies in $g_0\mathrm{K}_3(\mathfrak{D})$, u must be σ-semilinear. Hence, $\ell \in g\mathrm{K}_3(\mathfrak{F})$. □

Example 8.32. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size $(25, 5)$ over $\mathbb{F}_2$, whence

$$\left.\begin{matrix}\Gamma\mathrm{L}(25, 2^5) \cong \mathrm{C}_3(\mathfrak{F}) \\ \mathrm{GL}(25, 2^5) \cong \mathrm{K}_3(\mathfrak{F})\end{matrix}\right\} \leq \mathrm{GL}\big(\langle\mathfrak{F}\rangle\big) \cong \mathrm{GL}(125, 2).$$

Let $e \in \mathbb{N}$ be such that $63 \leq e \leq 125$.

(a) By Theorem 8.31(a) the group $\mathrm{K}_3(\mathfrak{F})$ contains $\operatorname{fat}(125, 2; e)$-elements if and only if $5 \mid e$, that is if and only if $e \in \{65, 70, 75, \ldots, 125\}$.

(b) By Theorem 8.31(b) the set $\mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$ contains $\operatorname{fat}(125, 2; e)$-elements if and only if there exists a positive integer $m_0 \leq 25$ satisfying $\operatorname{ord}(2; (2^{m_0}-1)5) = e$. Using GAP [24] (see Remark 2.8) we verify that this is the case if and only if (m_0, e) is among the following.

$$(25, 100), (24, 120), (23, 92), (21, 84), (20, 100), (19, 76), (17, 68), (16, 80)$$

In particular, $\mathrm{C}_3(\mathfrak{F}) \setminus \mathrm{K}_3(\mathfrak{F})$ contains $\operatorname{fat}(125, 2; e)$-elements if and only if

$$e \in \{68, 76, 80, 84, 92, 100, 120\}.$$

Let e be a positive integer such that $mt/2 < e \leq mt = \dim_q(\langle\mathfrak{F}\rangle)$. We are now in the position to compute the proportion of all $\operatorname{fat}(mt, q; e)$-elements in $\mathrm{C}_3(\mathfrak{F})$, which (as introduced in Definition 5.17) is denoted by $\operatorname{fat}(\mathrm{C}_3(\mathfrak{F}); e)$. Recall from Definition 8.27 the notion of $\operatorname{confat}(\mathfrak{F}; e)$. The value of $\operatorname{confat}(\mathfrak{F}; e)$ is specified in Proposition 8.28.

Theorem 8.33. *Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_q$ (so t is prime) and let $e \in \mathbb{N}$ satisfy $mt/2 < e \leq mt$. Let M be the set of all positive integers $m_0 \leq m$ such that (at least) one of the following hold:*

(*i*) *We have* $m_0 t = e$.

(*ii*) *We have* $\gcd(q,t) = 1$ *and* $\operatorname{ord}(q;(q^{m_0}-1)t) = e$.

Suppose that $\operatorname{fat}(\mathrm{C}_3(\mathfrak{F});e) \neq 0$. *Then* $\emptyset \neq M \subseteq \{e/t, e/(t-1)\}$ *and*

$$\operatorname{fat}\big(\mathrm{C}_3(\mathfrak{F});e\big) = \sum_{\mathfrak{D}\in\mathbf{D}} \operatorname{confat}(\mathfrak{D};e),$$

where $\mathbf{D}$ *is a set of* $\mathscr{C}_3$*-subframes of* $\mathfrak{F}$ *containing precisely one* $\mathscr{C}_3$*-frame of size* (m_0,t) *for all* $m_0 \in M$.

Proof. As a first step, we show that $M \subseteq \{e/t, e/(t-1)\}$. Let $m_0 \leq m$ be a positive integer. If m_0 satisfies condition (i), then $m_0 = e/t$. Suppose that m_0 satisfies condition (ii). Since by Lemma 2.17 we have $\operatorname{ord}(q;(q^{m_0}-1)t) \leq m_0 t$, and since $m_0 t/2 \leq mt/2 < e = \operatorname{ord}(q;(q^{m_0}-1)t)$, we get

$$m_0 t/2 < \operatorname{ord}(q;(q^{m_0}-1)t) \leq m_0 t.$$

Then (recalling that t is a prime) we may apply Lemma 2.21 (to $a = q$ and $m = m_0$) and obtain $e = \operatorname{ord}(q;(q^{m_0}-1)t) \in \{m_0 t, m_0(t-1)\}$.

(The rest of the proof is almost identical to the proof of Theorem 7.42.) Let $g \in \mathrm{C}_3(\mathfrak{F})$ be a $\operatorname{fat}(mt,q;e)$-element. Then by Lemma 8.30 there exists a unique $\mathscr{C}_3$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$, say of size (m_0,t), such that $g \in \mathrm{C}_3(\mathfrak{F})$ conserves $\mathfrak{D}$ and the restriction $g|_{\langle\mathfrak{D}\rangle}$ is a $\operatorname{fat}(m_0 t,q;e)$-element (conserving $\mathfrak{D}$). By Proposition 8.21(a) one of the conditions (i) or (ii) hold. It follows that $M \neq \emptyset$ and the number of all $\operatorname{fat}(mt,q;e)$-elements in $\mathrm{C}_3(\mathfrak{F})$ is equal to

$$\begin{aligned}&\operatorname{fat}\big(\mathrm{C}_3(\mathfrak{F});e\big)\,|\mathrm{C}_3(\mathfrak{F})| \\ &= \sum_{\mathfrak{D}\in\widehat{\mathbf{D}}} \big|\big\{g \in \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \operatorname{fat}(mt,q;e)\text{-element conserving } \mathfrak{D}\big\}\big|, \end{aligned} \tag{8.4}$$

where $\widehat{\mathbf{D}}$ is the set of all $\mathscr{C}_3$-subframes of $\mathfrak{F}$ of size (m_0,t) for all $m_0 \in M$.

Fix an element $\mathfrak{D} \in \widehat{\mathbf{D}}$. By Lemma 8.11 the mapping

$$\delta : \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_3(\mathfrak{D}), \quad g \mapsto g|_{\langle\mathfrak{D}\rangle}$$

is a surjective group homomorphism. Since elements of $\ker(\delta)$ act trivially on $\langle\mathfrak{D}\rangle$ we conclude the following. If for $g \in \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}$ the coset $\ker(\delta)g$ contains a $\operatorname{fat}(mt,q;e)$-element which conserves $\mathfrak{D}$, then every element in $\ker(\delta)g$ is a $\operatorname{fat}(mt,q;e)$-element which conserves $\mathfrak{D}$. Thus, the number of $\operatorname{fat}(mt,q;e)$-elements in $\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}$ conserving $\mathfrak{D}$ is equal to $|\ker(\delta)|$ times the number of all

$\mathrm{fat}(\dim_q(\langle\mathfrak{D}\rangle), q; e)$-elements in $\mathrm{im}(\delta)$ which conserve $\mathfrak{D}$. That is,

$$\begin{aligned}&\big|\{g \in \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \mathrm{fat}(mt, q; e)\text{-element conserving } \mathfrak{D}\}\big| \\ &= |\ker(\delta)|\ \underbrace{\big|\{g \in \overbrace{\mathrm{im}(\delta)}^{\mathrm{C}_3(\mathfrak{D})} \mid g \text{ a } \mathrm{fat}(\dim_q(\langle\mathfrak{D}\rangle), q; e)\text{-element conserving } \mathfrak{D}\}\big|}_{=\mathrm{confat}(\mathfrak{D};e)|\mathrm{C}_3(\mathfrak{D})|}.\end{aligned}$$

Recall that δ is onto, which is why we have $\mathrm{im}(\delta) = \mathrm{C}_3(\mathfrak{D})$ and $|\mathrm{im}(\delta)||\ker(\delta)| = |\mathrm{C}_2(\mathfrak{F})_{\mathfrak{D}}|$. Then

$$\begin{aligned}&\big|\{g \in \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}} \mid g \text{ a } \mathrm{fat}(mt, q; e)\text{-element conserving } \mathfrak{D}\}\big| \\ &\quad = \mathrm{confat}(\mathfrak{D}; e)|\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}|.\end{aligned}$$

Hence, (8.4) simplifies to

$$\mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); e\big)|\mathrm{C}_3(\mathfrak{F})| = \sum_{\mathfrak{D}\in\widehat{\mathbf{D}}} \mathrm{confat}(\mathfrak{D}; e)|\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}|.$$

By Proposition 8.28, the value of $\mathrm{confat}(\mathfrak{D}; e)$ only depends on the size of $\mathfrak{D}$ (and q). By Lemma 8.8 the group $\mathrm{C}_3(\mathfrak{F})$ acts transitively on the set of all $\mathscr{C}_3$-subframes of $\mathfrak{F}$ of a given size. Since $\mathbf{D}$ (as specified in the assertion) is a set of representatives of the orbits (of this action), and since $\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}$ is the stabiliser of $\mathfrak{D} \in \widehat{\mathbf{D}}$, using the orbit-stabiliser-theorem we conclude that

$$\mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); e\big)|\mathrm{C}_3(\mathfrak{F})| = \sum_{\mathfrak{D}\in\mathbf{D}} |\mathrm{C}_3(\mathfrak{F}) : \mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}|\,\mathrm{confat}(\mathfrak{D}; e)\,|\mathrm{C}_3(\mathfrak{F})_{\mathfrak{D}}|.$$

Then $\mathrm{fat}(\mathrm{C}_3(\mathfrak{F}); e) = \sum_{\mathfrak{D}\in\mathbf{D}} \mathrm{confat}(\mathfrak{D}; e)$, as asserted. □

We conclude this chapter with an example.

Example 8.34. Let $\mathfrak{F}$ be a $\mathscr{C}_3$-frame of size (m, t) over $\mathbb{F}_2$, whence

$$\mathrm{C}_3(\mathfrak{F}) \cong \Gamma\mathrm{L}(m, 2^t).$$

Let $e \in \mathbb{N}$ be such that $mt/2 < e \leq mt$. Let M be as in Theorem 8.33.

(*a*) Suppose that $(m, t) = (3, 3)$ and $e = 6$. Then $M = \{2, 3\}$. Hence, by Theorem 8.33 we have

$$\mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); 6\big) = \mathrm{confat}(\mathfrak{D}; 6) + \mathrm{confat}(\mathfrak{E}; 6),$$

where $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$ are such that $\mathrm{size}(\mathfrak{D}) = (2, 3)$ and $\mathrm{size}(\mathfrak{E}) = (3, 3)$. Then according to Examples 8.26, 8.29 we get

$$\mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); 6\big) = \frac{23}{63} + \frac{4}{21} = \frac{5}{9}.$$

(b) Suppose that $(m,t) = (25,5)$ and $e = 100$. Then $M = \{20,25\}$ (see Example 8.32(b)). Let $\mathfrak{D}, \mathfrak{E} \sqsubseteq \mathfrak{F}$ be such that $\mathrm{size}(\mathfrak{D}) = (20,5)$ and $\mathrm{size}(\mathfrak{E}) = (25,5)$. According to Theorem 8.33 we have

$$\mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); 100\big) = \mathrm{confat}(\mathfrak{D}; 100) + \mathrm{confat}(\mathfrak{E}; 100).$$

Note that $5 \mid 2^{20}-1$. Then, using Proposition 8.28(a) (and the "moreover" part of Proposition 8.25(b)), we obtain

$$\frac{1}{101} + \frac{16}{525} \leq \mathrm{confat}(\mathfrak{D}; 100) \leq \frac{1}{100} + \frac{16}{500}.$$

By the "moreover" part of Proposition 8.28(b) we have

$$\frac{4}{130} \leq \mathrm{confat}(\mathfrak{E}; 100) \leq \frac{4}{125}.$$

Thus,

$$\begin{aligned}\mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); 100\big) &\leq \frac{1}{100} + \frac{16}{500} + \frac{4}{125} = 0.0740,\\ \mathrm{fat}\big(\mathrm{C}_3(\mathfrak{F}); 100\big) &\geq \frac{1}{101} + \frac{16}{525} + \frac{4}{130} > 0.0711.\end{aligned}$$

Chapter 9

Aschbacher's $\mathscr{C}_4$-class (Tensor product subgroups)

Notation. Throughout this chapter we let q be a power of a prime p.

The aim of this chapter is to study fat elements in members of Aschbacher's $\mathscr{C}_4$-class. To this end, we need to introduce the concept of a tensor product of (finite) vector spaces. Consider two finite $\mathbb{F}_q$-vector spaces $\mathcal{V}$ and $\mathcal{W}$. An $\mathbb{F}_q$-vector space $\mathcal{T}$ is called a *tensor product* of $\mathcal{V}$ and W if there exists a bilinear mapping $\beta : \mathcal{V} \times \mathcal{W} \to \mathcal{T}$ satisfying the following *universal property*. For each bilinear mapping $\beta' : \mathcal{V} \times \mathcal{W} \to \mathcal{T}'$ (where $\mathcal{T}'$ is some $\mathbb{F}_q$-vector space) there exists a unique linear mapping $f : \mathcal{T} \to \mathcal{T}'$ such that

$$f\big(\beta(v, w)\big) = \beta'(v, w), \quad \text{for all } v \in \mathcal{V}, w \in \mathcal{W}.$$

According to [33, Sätze 9.2, 9.3, pp. 508, 509] tensor products of $\mathcal{V}$ and $\mathcal{W}$ exist, and they are all mutually isomorphic. For the purposes of this chapter, we thus pick our favourite tensor product of $\mathcal{V}$ and $\mathcal{W}$ (for example the one constructed in [33, proof of Satz 9.3, p. 509]) and denote it by

$$\mathcal{V} \otimes \mathcal{W}.$$

Fix a bilinear mapping $\beta : \mathcal{V} \times \mathcal{W} \to \mathcal{V} \otimes \mathcal{W}$ satisfying the universal property above. We refer to the elements of $\mathrm{im}(\beta)$ as *simple tensors* and write

$$v \otimes w = \beta(v, w), \quad \text{for all } v \in \mathcal{V}, w \in \mathcal{W}.$$

Since β is bilinear, we have

$$\varepsilon(v \otimes w) = (\varepsilon v) \otimes w = v \otimes (\varepsilon w),$$
$$(v_1 + v_2) \otimes (w_1 + w_2) = (v_1 \otimes w_1) + (v_1 \otimes w_2) + (v_2 \otimes w_1) + (v_2 \otimes w_2)$$

for all $\varepsilon \in \mathbb{F}_q$, $v, v_1, v_2 \in \mathcal{V}$, and $w, w_1, w_2 \in \mathcal{W}$. If $\dim(\mathcal{V}), \dim(\mathcal{W}) \geq 2$, then $\mathcal{V} \otimes \mathcal{W}$ contains elements which are not simple tensors (that is we have $\mathrm{im}(\beta) \subsetneq \mathcal{V} \otimes \mathcal{W}$). For example, given linearly independent vectors $v_1, v_2 \in \mathcal{V}$ and linearly independent vectors $w_1, w_2 \in \mathcal{W}$, the element $(v_1 \otimes w_1) + (v_2 \otimes w_2) \in \mathcal{V} \otimes \mathcal{W}$ is not a simple tensor. However, every element of $\mathcal{V} \otimes \mathcal{W}$ can be written as a sum of simple tensors. The latter is due to the following fact.

Given bases $\mathfrak{B}_\mathcal{V}, \mathfrak{B}_\mathcal{W}$ of $\mathcal{V}$ and $\mathcal{W}$, respectively, the elements $v \otimes w$, $v \in \mathfrak{B}_\mathcal{V}, w \in \mathfrak{B}_\mathcal{W}$ form a basis of $\mathcal{V} \otimes \mathcal{W}$. This also implies that

$$\dim(\mathcal{V} \otimes \mathcal{W}) = \dim(\mathcal{V}) \dim(\mathcal{W}).$$

For $a \in \mathrm{GL}(\mathcal{V})$ and $b \in \mathrm{GL}(\mathcal{W})$ the expression $a \otimes b$ denotes the $\mathbb{F}_q$-linear extension of $v \otimes w \mapsto va \otimes wb$ ($v \in \mathfrak{B}_\mathcal{V}, w \in \mathfrak{B}_\mathcal{W}$). In such a case we have $a \otimes b \in \mathrm{GL}(\mathcal{V} \otimes \mathcal{W})$ and

$$\varepsilon(a \otimes b) = \varepsilon a \otimes b = a \otimes \varepsilon b, \quad \text{for all } \varepsilon \in \mathbb{F}_q^*.$$

If $\mathcal{X} \leq \mathcal{V}$ and $\mathcal{Y} \leq \mathcal{W}$, then we write $\mathcal{X} \otimes \mathcal{Y}$ for the subspace of $\mathcal{V} \otimes \mathcal{W}$ spanned by all simple tensors $x \otimes y$, $x \in \mathcal{X}, y \in \mathcal{Y}$. The subspace $\mathcal{X} \otimes \mathcal{Y}$ has a basis consisting of simple tensors. In fact, any pair $\mathfrak{B}_\mathcal{X}, \mathfrak{B}_\mathcal{Y}$, where $\mathfrak{B}_\mathcal{X}$ is a basis of $\mathcal{X}$ and $\mathfrak{B}_\mathcal{Y}$ is a basis of $\mathcal{Y}$, yields a basis $\{x \otimes y \mid x \in \mathfrak{B}_\mathcal{X}, y \in \mathfrak{B}_\mathcal{Y}\}$ of $\mathcal{X} \otimes \mathcal{Y}$ consisting of simple tensors.

In this chapter we investigate the occurrence of fat elements in the subgroup $G \leq \mathrm{GL}(\mathcal{V} \otimes \mathcal{W})$ given by

$$G = \big\{a \otimes b \mid a \in \mathrm{GL}(\mathcal{V}), b \in \mathrm{GL}(\mathcal{W})\big\}.$$

Extending Aschbacher's original definition of the $\mathscr{C}_4$-class, we allow the spaces $\mathcal{V}, \mathcal{W}$ to have the same dimension. (We shall refer to the case $\dim(\mathcal{V}) = \dim(\mathcal{W})$ in Chapter 11.)

The group G is isomorphic to the quotient of $\mathrm{GL}(\mathcal{V}) \times \mathrm{GL}(\mathcal{W})$ by its normal subgroup $N = \{(\varepsilon \,\mathrm{id}_\mathcal{V}, \varepsilon^{-1} \,\mathrm{id}_\mathcal{W}) \mid \varepsilon \in \mathbb{F}_q^*\}$ and is an example of a central product.[I] We write $\mathrm{GL}(\mathcal{V}) \circ \mathrm{GL}(\mathcal{W}) = (\mathrm{GL}(\mathcal{V}) \times \mathrm{GL}(\mathcal{W}))/N$. Hence,

$$G \cong \mathrm{GL}(\mathcal{V}) \circ \mathrm{GL}(\mathcal{W}).$$

In line with Chapters 7, 8, we define G in terms of objects named $\mathscr{C}_4$-frames. More precisely, we call the pair $\mathfrak{F} = (\mathcal{V}, \mathcal{W})$ a *$\mathscr{C}_4$-frame*, refer to elements in G as *$\mathscr{C}_4$-maps* in $\mathfrak{F}$, and write

$$G = \mathrm{C}_4(\mathfrak{F}).$$

The structure of this chapter follows the set-ups of Chapters 7, 8. We begin in Section 9.1 by introducing $\mathscr{C}_4$-frames. Section 9.2 deals with $\mathscr{C}_4$-maps in general, while Section 9.3 investigates properties of fat $\mathscr{C}_4$-maps. Our main results of this chapter (concerning the existence and proportion of fat elements in $\mathrm{C}_4(\mathfrak{F})$) are presented in Theorems 9.25, 9.26.

[I] For a (general) definition of the central product see [40, Definition 2.2.6] or [3, (11.1)].

9.1 Introducing $\mathscr{C}_4$-frames

Definition 9.1. Let $\mathcal{V}, \mathcal{W} \neq \{0\}$ be finite vector spaces over $\mathbb{F}_q$ and let $\mathcal{V} \otimes \mathcal{W}$ be the tensor product of $\mathcal{V}$ and $\mathcal{W}$ introduced on p. 151 above.

(*a*) A *$\mathscr{C}_4$-frame in $\mathcal{V} \otimes \mathcal{W}$* is a pair $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ such that $\{0\} \neq \mathcal{X} \leq \mathcal{V}$ and $\{0\} \neq \mathcal{Y} \leq \mathcal{W}$. In this context, the *size* of $\mathfrak{F}$ is given by $\operatorname{size}(\mathfrak{F}) = (\dim(\mathcal{X}), \dim(\mathcal{Y}))$ and $\langle \mathfrak{F} \rangle = \mathcal{X} \otimes \mathcal{Y} \leq \mathcal{V} \otimes \mathcal{W}$ is called the *$\mathscr{C}_4$-span* of $\mathfrak{F}$. We also say that $\mathfrak{F}$ *spans* $\langle \mathfrak{F} \rangle$.

A *$\mathscr{C}_4$-frame*, or more precisely a *$\mathscr{C}_4$-frame over $\mathbb{F}_q$*, is a $\mathscr{C}_4$-frame in some unspecified tensor product of two finite $\mathbb{F}_q$-vector spaces.

(*b*) Let $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ be a $\mathscr{C}_4$-frame in $\mathcal{V} \otimes \mathcal{W}$. A *$\mathscr{C}_4$-subframe* of $\mathfrak{F}$ is a $\mathscr{C}_4$-frame $(\mathcal{X}_0, \mathcal{Y}_0)$ in $\mathcal{V} \otimes \mathcal{W}$ such that $\mathcal{X}_0 \leq \mathcal{X}$ and $\mathcal{Y}_0 \leq \mathcal{Y}$. We write $\mathfrak{D} \sqsubseteq \mathfrak{F}$ to indicate that $\mathfrak{D}$ is a $\mathscr{C}_4$-frame of $\mathfrak{F}$. A $\mathscr{C}_4$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ is said to be *proper* if $\mathfrak{D} \neq \mathfrak{F}$.

Consider a $\mathscr{C}_4$-frame $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ of size (m, t). Analogously to $\mathscr{C}_2$-frames and $\mathscr{C}_3$-frames, $\mathfrak{F}$ spans a vector space of dimension

$$\dim\big(\langle \mathfrak{F} \rangle\big) = mt.$$

Note also that, being reflexive, antisymmetric, and transitive, the relation "$\sqsubseteq$" is a partial order on the set of all $\mathscr{C}_4$-subframes of $\mathfrak{F}$. The $\mathscr{C}_4$-frame $\mathfrak{F}$ contains $\mathscr{C}_4$-subframes of size (m_0, t_0) if and only if

$$1 \leq m_0 \leq m \quad \text{and} \quad 1 \leq t_0 \leq t.$$

If a subspace $\mathcal{U} \leq \langle \mathfrak{F} \rangle$ is spanned by a $\mathscr{C}_4$-subframe of $\mathfrak{F}$, that is if $\mathcal{U} = \mathcal{X}_0 \otimes \mathcal{Y}_0$ for some $\mathcal{X}_0 \leq \mathcal{X}$ and $\mathcal{Y}_0 \leq \mathcal{Y}$, then $\mathcal{U}$ has a basis consisting of simple tensors. The converse is not true. For example, if ($m, t \geq 2$ and) x_1, x_2 and y_1, y_2 are linearly independent elements of $\mathcal{X}$ and $\mathcal{Y}$, respectively, then the subspace $\mathcal{U} = \langle x_1 \otimes y_1, x_2 \otimes y_2 \rangle \leq \langle \mathfrak{F} \rangle$ is not spanned by any $\mathscr{C}_4$-subframe of $\mathfrak{F}$. To see that this is true, observe that the smallest (with respect to "$\sqsubseteq$") $\mathscr{C}_4$-subframe of $\mathfrak{F}$ whose $\mathscr{C}_4$-span contains $\mathcal{U}$ is given by $\mathfrak{D} = (\langle x_1, x_2 \rangle, \langle y_1, y_2 \rangle)$. Then $\operatorname{size}(\mathfrak{D}) = (2, 2)$, whence $\dim(\langle \mathfrak{D} \rangle) = 4 > \dim(\mathcal{U})$, and thus $\mathcal{U} \lneq \langle \mathfrak{D} \rangle$.

Definition 9.2. Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and $\mathfrak{D}_1 = (\mathcal{X}_1, \mathcal{Y}_1), \mathfrak{D}_2 = (\mathcal{X}_2, \mathcal{Y}_2) \sqsubseteq \mathfrak{F}$.

(*a*) The *intersection* of $\mathfrak{D}_1$ and $\mathfrak{D}_2$ is defined by $\mathfrak{D}_1 \cap \mathfrak{D}_2 = (\mathcal{X}_1 \cap \mathcal{X}_2, \mathcal{Y}_1 \cap \mathcal{Y}_2)$.

(*b*) Let $\mathcal{U} \leq \langle \mathfrak{F} \rangle$. We call $\bigcap_{\mathfrak{D} \sqsubseteq \mathfrak{F}, \mathcal{U} \leq \langle \mathfrak{D} \rangle} \mathfrak{D}$ the *$\mathscr{C}_4$-cover* of $\mathcal{U}$ in $\mathfrak{F}$.

Suppose that we are in the situation of Definition 9.2(b) and let $\mathfrak{U}$ be the $\mathscr{C}_4$-cover of $\mathcal{U}$ in $\mathfrak{F}$. Clearly, $\mathfrak{U}$ is a $\mathscr{C}_4$-subframe of $\mathfrak{F}$. As shown (in Lemma 9.3(b)) below, we have $\mathcal{U} \leq \langle \mathfrak{U} \rangle$. Thus, $\mathfrak{U}$ is the smallest (with respect to "$\sqsubseteq$") $\mathscr{C}_4$-subframe of $\mathfrak{F}$ whose $\mathscr{C}_4$-span contains $\mathcal{U}$. This fact justifies the name *$\mathscr{C}_4$-cover*. Our next lemma further verifies that $(\mathcal{X}_1 \otimes \mathcal{Y}_1) \cap (\mathcal{X}_2 \otimes \mathcal{Y}_2) = (\mathcal{X}_1 \cap \mathcal{X}_2) \otimes (\mathcal{Y}_1 \cap \mathcal{Y}_2)$.

Lemma 9.3. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $\mathfrak{D}_1, \mathfrak{D}_2 \sqsubseteq \mathfrak{F}$.*

(a) *We have $\langle \mathfrak{D}_1 \rangle \cap \langle \mathfrak{D}_2 \rangle = \langle \mathfrak{D}_1 \cap \mathfrak{D}_2 \rangle$.*

(b) *Let $\mathcal{U} \leq \langle \mathfrak{F} \rangle$ and let $\mathfrak{U}$ be the $\mathscr{C}_4$-cover of $\mathcal{U}$ in $\mathfrak{F}$. Then $\mathcal{U} \leq \langle \mathfrak{U} \rangle$.*

Proof. (a) Suppose that $\mathfrak{D}_1 = (\mathcal{X}_1, \mathcal{Y}_1)$ and $\mathfrak{D}_2 = (\mathcal{X}_2, \mathcal{Y}_2)$. Let $\mathcal{X}'$ and $\mathcal{Y}'$ be the vector spaces spanned by (all vectors in) $\mathcal{X}_1 \cup \mathcal{X}_2$ and $\mathcal{Y}_1 \cup \mathcal{Y}_2$, respectively. Let $\mathfrak{F}' = (\mathcal{X}', \mathcal{Y}')$. Then

$$\mathfrak{D}_i \sqsubseteq \mathfrak{F}' \sqsubseteq \mathfrak{F}, \quad i \in \{1, 2\}.$$

For $i \in \{1, 2\}$, let $\mathcal{X}_i^\circ$ be a complement of $\mathcal{X}_1 \cap \mathcal{X}_2$ in $\mathcal{X}_i$, and let $\mathcal{Y}_i^\circ$ denote a complement of $\mathcal{Y}_1 \cap \mathcal{Y}_2$ in $\mathcal{Y}_i$. For $\mathcal{Z} \in \{\mathcal{X}_1 \cap \mathcal{X}_2, \mathcal{Y}_1 \cap \mathcal{Y}_2, \mathcal{X}_1^\circ, \mathcal{X}_2^\circ, \mathcal{Y}_1^\circ, \mathcal{Y}_2^\circ\}$ let $\mathfrak{B}_\mathcal{Z}$ be a basis of $\mathcal{Z}$. Then

$$\mathfrak{B}_{\mathfrak{F}'} = \{x \otimes y \mid x \in \underbrace{\mathfrak{B}_{\mathcal{X}_1 \cap \mathcal{X}_2} \cup \mathfrak{B}_{\mathcal{X}_1^\circ} \cup \mathfrak{B}_{\mathcal{X}_2^\circ}}_{\text{basis of } \mathcal{X}'},\ y \in \underbrace{\mathfrak{B}_{\mathcal{Y}_1 \cap \mathcal{Y}_2} \cup \mathfrak{B}_{\mathcal{Y}_1^\circ} \cup \mathfrak{B}_{\mathcal{Y}_2^\circ}}_{\text{basis of } \mathcal{Y}'}\},$$

$$\mathfrak{B}_{\mathfrak{D}_1} = \{x \otimes y \mid x \in \underbrace{\mathfrak{B}_{\mathcal{X}_1 \cap \mathcal{X}_2} \cup \mathfrak{B}_{\mathcal{X}_1^\circ}}_{\text{basis of } \mathcal{X}_1},\ y \in \underbrace{\mathfrak{B}_{\mathcal{Y}_1 \cap \mathcal{Y}_2} \cup \mathfrak{B}_{\mathcal{Y}_1^\circ}}_{\text{basis of } \mathcal{Y}_1}\},$$

$$\mathfrak{B}_{\mathfrak{D}_2} = \{x \otimes y \mid x \in \underbrace{\mathfrak{B}_{\mathcal{X}_1 \cap \mathcal{X}_2} \cup \mathfrak{B}_{\mathcal{X}_2^\circ}}_{\text{basis of } \mathcal{X}_2},\ y \in \underbrace{\mathfrak{B}_{\mathcal{Y}_1 \cap \mathcal{Y}_2} \cup \mathfrak{B}_{\mathcal{Y}_2^\circ}}_{\text{basis of } \mathcal{Y}_2}\},$$

$$\mathfrak{B}_{\mathfrak{D}_1 \cap \mathfrak{D}_2} = \{x \otimes y \mid x \in \mathfrak{B}_{\mathcal{X}_1 \cap \mathcal{X}_2},\ y \in \mathfrak{B}_{\mathcal{Y}_1 \cap \mathcal{Y}_2}\}$$

are bases of $\langle \mathfrak{F}' \rangle$, $\langle \mathfrak{D}_1 \rangle$, $\langle \mathfrak{D}_2 \rangle$, and $\langle \mathfrak{D}_1 \cap \mathfrak{D}_2 \rangle$, respectively.

Since $\mathfrak{B}_{\mathfrak{D}_1 \cap \mathfrak{D}_2} \subseteq \mathfrak{B}_{\mathfrak{D}_i}$ ($i \in \{1, 2\}$), it follows that $\langle \mathfrak{D}_1 \cap \mathfrak{D}_2 \rangle \leq \langle \mathfrak{D}_1 \rangle \cap \langle \mathfrak{D}_2 \rangle$.

Conversely, looking at the bases $\mathfrak{B}_{\mathfrak{F}'}, \mathfrak{B}_{\mathfrak{D}_1}, \mathfrak{B}_{\mathfrak{D}_2}$, we see that an element in $\langle \mathfrak{F}' \rangle$ lies in $\langle \mathfrak{D}_1 \rangle \cap \langle \mathfrak{D}_2 \rangle$ if and only if it is a linear combination of elements $x \otimes y$ with $x \in \mathfrak{B}_{\mathcal{X}_1 \cap \mathcal{X}_2}$, $y \in \mathfrak{B}_{\mathcal{Y}_1 \cap \mathcal{Y}_2}$. Thus, $\langle \mathfrak{D}_1 \rangle \cap \langle \mathfrak{D}_2 \rangle \leq \langle \mathfrak{D}_1 \cap \mathfrak{D}_2 \rangle$.

(b) By (definition of the $\mathscr{C}_4$-cover and) part (a) of the current lemma we have

$$\langle \mathfrak{U} \rangle = \bigcap_{\mathfrak{D} \sqsubseteq \mathfrak{F}, \mathcal{U} \leq \langle \mathfrak{D} \rangle} \langle \mathfrak{D} \rangle.$$

This proves the assertion (because, being a subspace of each $\langle \mathfrak{D} \rangle$, $\mathcal{U}$ also lies in their intersection). □

Lemma 9.4. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $\mathfrak{D}_1, \mathfrak{D}_2 \sqsubseteq \mathfrak{F}$. Then $\mathfrak{D}_1 = \mathfrak{D}_2$ if and only if $\langle \mathfrak{D}_1 \rangle = \langle \mathfrak{D}_2 \rangle$.*

Proof. If $\mathfrak{D}_1 = \mathfrak{D}_2$ then, clearly, $\langle \mathfrak{D}_1 \rangle = \langle \mathfrak{D}_2 \rangle$. So, suppose that $\langle \mathfrak{D}_1 \rangle = \langle \mathfrak{D}_2 \rangle$. Then, for $i \in \{1, 2\}$, we have $\langle \mathfrak{D}_1 \rangle \cap \langle \mathfrak{D}_2 \rangle = \langle \mathfrak{D}_\mathrm{i} \rangle$, that is by Lemma 9.3$(a)$,

$$\langle \mathfrak{D}_1 \cap \mathfrak{D}_2 \rangle = \langle \mathfrak{D}_i \rangle, \quad i \in \{1, 2\}.$$

In particular, the dimension of $\langle \mathfrak{D}_1 \cap \mathfrak{D}_2 \rangle$ is equal to $\dim(\langle \mathfrak{D}_i \rangle)$, $i \in \{1, 2\}$. Writing $\mathfrak{D}_1 = (\mathcal{X}_1, \mathcal{Y}_1)$ and $\mathfrak{D}_2 = (\mathcal{X}_2, \mathcal{Y}_2)$, the latter translates to

$$\dim(\mathcal{X}_1 \cap \mathcal{X}_2) \dim(\mathcal{Y}_1 \cap \mathcal{Y}_2) = \dim(\mathcal{X}_i) \dim(\mathcal{Y}_i), \quad i \in \{1, 2\}.$$

This implies that $\mathcal{X}_1 = \mathcal{X}_2$ and $\mathcal{Y}_1 = \mathcal{Y}_2$. □

9.2 Linear groups acting on $\mathscr{C}_4$-subframes

Let $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ be a $\mathscr{C}_4$-frame. Recall that, given $a \in \mathrm{GL}(\mathcal{X})$ and $b \in \mathrm{GL}(\mathcal{Y})$, the element $a \otimes b \in \mathrm{GL}(\mathcal{X} \otimes \mathcal{Y})$ is given by (the linear extension of)

$$(x \otimes y)(a \otimes b) = xa \otimes yb, \quad x \in \mathcal{X}, y \in \mathcal{Y}.$$

Definition 9.5. Let $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ be a $\mathscr{C}_4$-frame. A *$\mathscr{C}_4$-map* in $\mathfrak{F}$ is a non-singular linear mapping g on $\langle \mathfrak{F} \rangle$ such that $g = a \otimes b$ for some $a \in \mathrm{GL}(\mathcal{X})$ and $b \in \mathrm{GL}(\mathcal{Y})$.

The set of all $\mathscr{C}_4$-maps in a $\mathscr{C}_4$-frame $\mathfrak{F}$ forms a subgroup of $\mathrm{GL}(\langle \mathfrak{F} \rangle)$.

Definition 9.6. Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame. We write $\mathrm{C}_4(\mathfrak{F})$ for the group of all $\mathscr{C}_4$-maps in $\mathfrak{F}$.

Suppose that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ is a $\mathscr{C}_4$-frame of size (m, t) over $\mathbb{F}_q$. As mentioned at the beginning of this chapter, we have

$$\mathrm{C}_4(\mathfrak{F}) \cong \mathrm{GL}(\mathcal{X}) \circ \mathrm{GL}(\mathcal{Y}).$$

By writing $a \otimes b \in \mathrm{C}_4(\mathfrak{F})$ we implicitly assume that $a \in \mathrm{GL}(\mathcal{X})$ and $b \in \mathrm{GL}(\mathcal{Y})$. Consider elements $a \otimes b, a' \otimes b' \in \mathrm{C}_4(\mathfrak{F})$. The product of $a \otimes b$ and $a' \otimes b'$ satisfies

$$(a \otimes b)(a' \otimes b') = (aa' \otimes bb').$$

This, in particular, implies that $(a \otimes b)^{\mathrm{lcm}\{|a|,|b|\}} = a^{\mathrm{lcm}\{|a|,|b|\}} \otimes b^{\mathrm{lcm}\{|a|,|b|\}} = \mathrm{id}_\mathcal{X} \otimes \mathrm{id}_\mathcal{Y} = \mathrm{id}_{\langle \mathfrak{F} \rangle}$, and hence

$$|a \otimes b| \quad \text{divides} \quad \mathrm{lcm}\big\{|a|, |b|\big\}.$$

Recall that, given bases $\mathfrak{B}_\mathcal{X} = \{x_1, \dots, x_m\}$ of $\mathcal{X}$ and $\mathfrak{B}_\mathcal{Y} = \{y_1, \dots, y_t\}$ of $\mathcal{Y}$, the set $\mathfrak{B} = \{x_1 \otimes y_1, \dots, x_1 \otimes y_t, x_2 \otimes y_1, \dots, x_2 \otimes y_t, \dots, x_m \otimes y_1, \dots, x_m \otimes y_t\}$ is a basis of $\langle \mathfrak{F} \rangle = \mathcal{X} \otimes \mathcal{Y}$. Then, writing $A = (a_{ij})_{1 \le i \le m, 1 \le j \le t}$ for the matrix of a with respect to $\mathfrak{B}_\mathcal{X}$ and B for the matrix of b with respect to $\mathfrak{B}_\mathcal{Y}$, the matrix of $a \otimes b$ with respect to $\mathfrak{B}$ is the Kronecker product $A \otimes B$, that is

$$(a \otimes b)_\mathfrak{B} = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in \mathrm{GL}(mt, q).$$

The characteristic polynomial of $a \otimes b$ is the tensor product of the characteristic polynomials of a and b, as introduced in Definition 3.32.

For a prime r, recall from Definition 4.14 the notion of the r-part and the r'-part of a group element.

Lemma 9.7. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame, let $g = a \otimes b \in \mathrm{C}_4(\mathfrak{F})$, and let r be a prime. Then $g_r = a_r \otimes b_r$ and $g_{r'} = a_{r'} \otimes b_{r'}$.*

Proof. By Lemma 4.13 we have $g = (a_{r'}a_r) \otimes (b_{r'}b_r) = (a_r a_{r'}) \otimes (b_r b_{r'})$, that is

$$g = (a_{r'} \otimes b_{r'})(a_r \otimes b_r) = (a_r \otimes b_r)(a_{r'} \otimes b_{r'}).$$

Since the orders of the elements $a_{r'} \otimes b_{r'}, a_r \otimes b_r \in \mathrm{C}_4(\mathfrak{F})$ divide $\mathrm{lcm}\{|a_{r'}|, |b_{r'}|\}$ and $\mathrm{lcm}\{|a_r|, |b_r|\}$, respectively, we see that $|a_{r'} \otimes b_{r'}|$ is coprime to r and that $|a_r \otimes b_r|$ is a power of r. Then the assertion holds by Lemma 4.13. □

Definition 9.8. Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame, let $\mathfrak{D} = (\mathcal{X}_0, \mathcal{Y}_0) \sqsubseteq \mathfrak{F}$, and let $g = a \otimes b \in \mathrm{C}_4(\mathfrak{F})$. We write $\mathfrak{D}g = (\mathcal{X}_0 a, \mathcal{Y}_0 b)$.

Observe that (in the situation of Definition 9.8) we have $\mathfrak{D}g \sqsubseteq \mathfrak{F}$ and

$$\langle \mathfrak{D}g \rangle = \langle \mathfrak{D} \rangle g.$$

The natural action of the general linear group on the subspaces of its underlying vector space induces the action of $\mathrm{C}_4(\mathfrak{F})$ on the set of all $\mathscr{C}_4$-subframes of $\mathfrak{F}$. As a consequence of Lemma 5.15 we obtain the following.

Lemma 9.9. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame. The group $\mathrm{C}_4(\mathfrak{F})$ acts on the set of all $\mathscr{C}_4$-subframes of $\mathfrak{F}$ via*

$$\{\mathfrak{D} \mid \mathfrak{D} \sqsubseteq \mathfrak{F}\} \times \mathrm{C}_4(\mathfrak{F}) \to \{\mathfrak{D} \mid \mathfrak{D} \sqsubseteq \mathfrak{F}\}, \quad (\mathfrak{D}, g) \mapsto \mathfrak{D}g.$$

Each orbit consists of all $\mathscr{C}_4$-subframes of a given size.

9.2.1 Linear mappings preserving $\mathscr{C}_4$-subframes

Consider a $\mathscr{C}_4$-map $g = a \otimes b$ in some $\mathscr{C}_4$-frame $\mathfrak{F}$. Let $\mathfrak{D} = (\mathcal{X}_0, \mathcal{Y}_0)$ be a $\mathscr{C}_4$-subframe of $\mathfrak{F}$. If $\mathcal{X}_0$ is $\langle a \rangle$-invariant and $\mathcal{Y}_0$ is $\langle b \rangle$-invariant, then g is said to *preserve* $\mathfrak{D}$.

Definition 9.10. Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$.

(*a*) An element $g \in \mathrm{C}_4(\mathfrak{F})$ *preserves* $\mathfrak{D}$ if $\mathfrak{D}g = \mathfrak{D}$. We say that $G \leq \mathrm{C}_4(\mathfrak{F})$ *preserves* $\mathfrak{D}$ if all element in G preserve $\mathfrak{D}$.

(*b*) We write $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$ for the maximal (with respect to inclusion) subgroup of $\mathrm{C}_4(\mathfrak{F})$ preserving $\mathfrak{D}$.

Hence, (in the situation of Definition 9.10) the group $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$ is the stabiliser in $\mathrm{C}_4(\mathfrak{F})$ of $\mathfrak{D}$ with respect to the action presented in Lemma 9.9. Our next lemma implies that $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$ is equal to the subspace stabiliser of $\langle \mathfrak{D} \rangle$ in $\mathrm{C}_4(\mathfrak{F})$.

Lemma 9.11. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. An element $g \in \mathrm{C}_4(\mathfrak{F})$ preserves $\mathfrak{D}$ if and only if $\langle \mathfrak{D} \rangle$ is $\langle g \rangle$-invariant.*

Proof. Recall that $\langle \mathfrak{D}g \rangle = \langle \mathfrak{D} \rangle g$. Hence, $\langle \mathfrak{D} \rangle$ is $\langle g \rangle$-invariant if and only if $\langle \mathfrak{D}g \rangle = \langle \mathfrak{D} \rangle$. By Lemma 9.4, the latter is equivalent to $\mathfrak{D}g = \mathfrak{D}$. □

Recall from Definition 9.2(*b*) the meaning of a $\mathscr{C}_4$-cover.

Lemma 9.12. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame, let $g \in \mathrm{C}_4(\mathfrak{F})$, let $\mathcal{U} \leq \langle \mathfrak{F} \rangle$, and let $\mathfrak{U}$ be the $\mathscr{C}_4$-cover of $\mathcal{U}$ in $\mathfrak{F}$. If $\mathcal{U}$ is $\langle g \rangle$-invariant, then g preserves $\mathfrak{U}$.*

Proof. Suppose that $\mathcal{U}$ is $\langle g \rangle$-invariant. Let $\mathbf{D} = \{\mathfrak{D} \sqsubseteq \mathfrak{F} \mid \mathcal{U} \leq \langle \mathfrak{D} \rangle\}$. Then

$$\mathfrak{U} = \bigcap_{\mathfrak{D} \in \mathbf{D}} \mathfrak{D} \quad \text{and} \quad \mathfrak{U}g = \left(\bigcap_{\mathfrak{D} \in \mathbf{D}} \mathfrak{D} \right) g = \bigcap_{\mathfrak{D} \in \mathbf{D}} \mathfrak{D}g. \tag{9.1}$$

Now, if $\mathfrak{D} \in \mathbf{D}$, then $\mathfrak{D}g$ is a $\mathscr{C}_4$-subframe of $\mathfrak{F}$ and (recalling that $\mathcal{U}g = \mathcal{U}$) the subspace $\mathcal{U}$ lies in $\langle \mathfrak{D} \rangle g = \langle \mathfrak{D}g \rangle$. This shows that $\mathfrak{D}g \in \mathbf{D}$ for all $\mathfrak{D} \in \mathbf{D}$. It follows that $\bigcap_{\mathfrak{D} \in \mathbf{D}} \mathfrak{D}g = \bigcap_{\mathfrak{D} \in \mathbf{D}} \mathfrak{D}$, which according to (9.1) is equivalent to saying that $\mathfrak{U}g = \mathfrak{U}$. □

We next show that $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$ induces on $\langle \mathfrak{D} \rangle$ the entire group $\mathrm{C}_4(\mathfrak{D})$.

Lemma 9.13. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. The mapping*

$$\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_4(\mathfrak{D}), \quad g \mapsto g|_{\langle \mathfrak{D} \rangle}$$

is a surjective group homomorphism.

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ and $\mathfrak{D} = (\mathcal{X}_0, \mathcal{Y}_0)$. Let $g = a \otimes b \in \mathrm{C}_4(\mathfrak{F})$ preserve $\mathfrak{D}$. Then by definition, $a \in \mathrm{GL}(\mathcal{X})_{\mathcal{X}_0}$, $b \in \mathrm{GL}(\mathcal{Y})_{\mathcal{Y}_0}$, and

$$g|_{\langle \mathfrak{D} \rangle} = (a \otimes b)|_{\mathcal{X}_0 \otimes \mathcal{Y}_0} = a|_{\mathcal{X}_0} \otimes b|_{\mathcal{Y}_0} \in \mathrm{C}_4(\mathfrak{D}).$$

Because $\{a'|_{\mathcal{X}_0} \mid a' \in \mathrm{GL}(\mathcal{X})_{\mathcal{X}_0}\} = \mathrm{GL}(\mathcal{X}_0)$ and $\{b'|_{\mathcal{Y}_0} \mid b' \in \mathrm{GL}(\mathcal{Y})_{\mathcal{Y}_0}\} = \mathrm{GL}(\mathcal{Y}_0)$, it follows that $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_4(\mathfrak{D}), g \mapsto g|_{\langle \mathfrak{D} \rangle}$ is surjective. (Clearly, this mapping is a group homomorphism.) □

9.2.2 Linear mappings conserving $\mathscr{C}_4$-subframes

Definition 9.14. Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $\mathfrak{D} \sqsubseteq \mathfrak{F}$. An element $g \in \mathrm{C}_4(\mathfrak{F})$ is said to *conserve* $\mathfrak{D}$ if g preserves $\mathfrak{D}$ and g does not preserve any proper $\mathscr{C}_4$-subframe of $\mathfrak{D}$.

We obtain the following characterisation of elements in $\mathrm{C}_4(\mathfrak{F})$ which conserve $\mathfrak{F}$.

Lemma 9.15. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame. An element $a \otimes b \in \mathrm{C}_4(\mathfrak{F})$ conserves $\mathfrak{F}$ if and only if a and b are irreducible.*

Proof. Let $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$. By definition, $a \otimes b$ conserves $\mathfrak{F}$ if and only if $\mathcal{X}$ and $\mathcal{Y}$ are the only non-trivial subspaces of $\mathcal{X}$, and respectively of $\mathcal{Y}$, which are left invariant by $\langle a \rangle$ and $\langle b \rangle$, respectively. □

Recall that q is a power of the prime p. Recall that we write $g_{p'}, g_p$ for the p'-part, and respectively the p-part, of a group element g. Our next result is the $\mathscr{C}_4$-counterpart of Lemma 7.18.

Lemma 9.16. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame over $\mathbb{F}_q$. Let $g \in \mathrm{C}_4(\mathfrak{F})$ be such that g does not conserve $\mathfrak{F}$. Then $g_{p'}$ preserves a proper $\mathscr{C}_4$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ satisfying* $\dim(\langle \mathfrak{D} \rangle) \geq \dim(\langle \mathfrak{F} \rangle)/2$.

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ and $g = a \otimes b$. By Lemma 9.7 we have

$$g_{p'} = a_{p'} \otimes b_{p'}.$$

Let $\mathcal{X}_0$ be a non-trivial, $\langle a_{p'} \rangle$-irreducible subspace of $\mathcal{X}$, and let $\mathcal{Y}_0$ be a non-trivial, $\langle b_{p'} \rangle$-irreducible subspace of $\mathcal{Y}$. If $\mathcal{X}_0 = \mathcal{X}$ and $\mathcal{Y}_0 = \mathcal{Y}$, then the elements $a_{p'}, b_{p'}$ are irreducible. In such a case a and b are irreducible, which according to Lemma 9.15 means that g conserves $\mathfrak{F}$. As this contradicts our assumption, we conclude that either $\mathcal{X}_0 \lneq \mathcal{X}$ or $\mathcal{Y}_0 \lneq \mathcal{Y}$ (or both). Without loss of generality, we assume that

$$\mathcal{X}_0 \lneq \mathcal{X}.$$

(The case $\mathcal{Y}_0 \leq \mathcal{Y}$ can be handled analogously.) By [35, Theorem 1.9] (Maschke), $\mathcal{X}_0$ has an $\langle a_{p'} \rangle$-invariant complement in $\mathcal{X}$. By exchanging $\mathcal{X}_0$ by that complement if necessary, we get

$$\frac{\dim(\mathcal{X})}{2} \leq \dim(\mathcal{X}_0) < \dim(\mathcal{X}).$$

Then $\mathfrak{D} = (\mathcal{X}_0, \mathcal{Y})$ is a proper $\mathscr{C}_4$-subframe of $\mathfrak{F}$ which is preserved by $g_{p'}$, and $\dim(\langle \mathfrak{D} \rangle) = \dim(\mathcal{X}_0)\dim(\mathcal{Y}) \geq \dim(\mathcal{X})\dim(\mathcal{Y})/2 = \dim(\langle \mathfrak{F} \rangle)/2$. □

9.3 Fat $\mathscr{C}_4$-maps

Consider a $\mathscr{C}_4$-frame $\mathfrak{F}$. Recall from Definition 5.1(a) that we refer to an element $g \in \mathrm{C}_4(\mathfrak{F})$ as being fat if $\langle g \rangle$ acts irreducibly on a subspace of $\langle \mathfrak{F} \rangle$ of dimension strictly bigger than $\dim(\langle \mathfrak{F} \rangle)/2$. As in the cases of $\mathscr{C}_2$-maps and $\mathscr{C}_3$-maps (see Sections 7.3, 8.3) we reduce the investigation of fat elements in $\mathrm{C}_4(\mathfrak{F})$ to the study of fat elements in $\mathrm{C}_4(\mathfrak{F})$ which conserve $\mathfrak{F}$. What is special about $\mathscr{C}_4$-maps is that (as presented in Lemma 9.17 below) every fat $\mathscr{C}_4$-map in $\mathfrak{F}$ conserving the underlying frame $\mathfrak{F}$ turns out to be irreducible. This is a major difference to $\mathscr{C}_2$-maps and $\mathscr{C}_3$-maps, which being fat and conserving do not need to be irreducible; see Remarks 7.28, 8.19. In the course of this section, we thus first consider irreducible elements in $\mathrm{C}_4(\mathfrak{F})$, and then generalise our findings to fat elements in $\mathrm{C}_4(\mathfrak{F})$.

Lemma 9.17. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame over $\mathbb{F}_q$. Let $g \in \mathrm{C}_4(\mathfrak{F})$ be such that g conserves $\mathfrak{F}$ and $\langle g \rangle$ acts irreducibly on a subspace $\mathcal{U} \leq \langle \mathfrak{F} \rangle$ of dimension $\dim(\mathcal{U}) > \dim(\langle \mathfrak{F} \rangle)/2$. Then $\mathcal{U} = \langle \mathfrak{F} \rangle$ (that is, g is irreducible).*

Proof. Let $(m, t) = \mathrm{size}(\mathfrak{F})$. (Then $\dim(\langle \mathfrak{F} \rangle) = mt$.) Let $g = a \otimes b$, and let $f_a, f_b \in \mathbb{F}_q[x]$ be the characteristic polynomials of a and b, respectively. Then $f = f_a \otimes f_b$ is the characteristic polynomial of g (with $f_a \otimes f_b$ as specified in Definition 3.32). Let $f_0 \in \mathbb{F}_q[x]$ be the characteristic polynomial of the restriction $g|_{\mathcal{U}}$. Note that

$$\begin{aligned} \deg(f_0) = \dim(\mathcal{U}) &> \frac{mt}{2}, \\ \deg(f_a) &= m, \\ \deg(f_b) &= t, \\ \deg(f_a \otimes f_b) &= mt. \end{aligned}$$

By Lemma 4.8(a) the polynomial f_0 is irreducible. Since g conserves $\mathfrak{F}$, by Lemmas 9.15 and 4.8(a) the polynomials f_a, f_b are also irreducible. Since f_0 is a divisor of f, Lemma 3.34 yields

$$\deg(f_0) \mid \mathrm{lcm}\{m, t\} = \frac{mt}{\gcd(m, t)},$$

Recalling that $\deg(f_0) > mt/2$, we conclude that $\gcd(m,t) = 1$ and $\deg(f_0) = mt$. Then $f_0 = f$. Thus, f is irreducible, which by Lemma 4.8(a) is equivalent to saying that g is irreducible. □

9.3.1 Irreducible $\mathscr{C}_4$-maps

Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame and let $g = a \otimes b \in \mathrm{C}_4(\mathfrak{F})$. If f_a and f_b are the characteristic polynomials of a and b, respectively, then the characteristic polynomial of g is given by the tensor product $f_a \otimes f_b$, as introduced in Definition 3.32. Irreducible elements in $\mathrm{C}_4(\mathfrak{F})$ can be characterised as follows.

Lemma 9.18. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size (m,t).*

(a) An element $g \in \mathrm{C}_4(\mathfrak{F})$ is irreducible if and only if g conserves $\mathfrak{F}$ and $\gcd(m,t) = 1$.

(b) The group $\mathrm{C}_4(\mathfrak{F})$ contains irreducible elements if and only if $\gcd(m,t) = 1$.

Proof. (a) Let $g = a \otimes b$, and let f_a, f_b be the characteristic polynomials of a and b, respectively. Then $f_a \otimes f_b$ is the characteristic polynomial of g. Note that $\deg(f_a) = m$ and $\deg(f_b) = t$. By Lemma 4.8(a), g is irreducible if and only if $f_a \otimes f_b$ is irreducible. According to Lemma 3.35 this is the case if and only if f_a, f_b are irreducible and $\gcd(m,t) = 1$. The assertion now follows from Lemmas 4.8(a), 9.15.

(b) If $\mathrm{C}_4(\mathfrak{F})$ contains irreducible elements, then part (a) of the current lemma yields $\gcd(m,t) = 1$. Conversely suppose that $\gcd(m,t) = 1$. Assume that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$. Since the groups $\mathrm{GL}(\mathcal{X}), \mathrm{GL}(\mathcal{Y})$ contain irreducible elements (see Corollary 4.21 or Lemma 5.3(a)), from Lemma 9.15 we deduce that $\mathrm{C}_4(\mathfrak{F})$ contains elements which conserve $\mathfrak{F}$. Since $\gcd(m,t) = 1$, by part (a) of the current lemma, any such element is irreducible. □

Lemma 9.19. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame over $\mathbb{F}_q$, and let $g, g' \in \mathrm{C}_4(\mathfrak{F})$ be irreducible. Then g, g' are conjugate in $\mathrm{C}_4(\mathfrak{F})$ if and only if they have the same characteristic polynomial.*

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ and $g = a \otimes b$, $g' = a' \otimes b'$. By Lemmas 9.15 and 9.18(a) the elements $a, a' \in \mathrm{GL}(\mathcal{X})$, $b, b' \in \mathrm{GL}(\mathcal{Y})$ are irreducible and $\gcd(m,t) = 1$.

If g and g' are conjugate in $\mathrm{C}_4(\mathfrak{F}) \leq \mathrm{GL}(\langle\mathfrak{F}\rangle)$, then their characteristic polynomials coincide. Conversely, suppose that g and g' have the same characteristic polynomial, say f. Let $f_a, f_b, f'_a, f'_b \in \mathbb{F}_q[x]$ be the characteristic polynomials of a, b, a', and b', respectively. Then

$$f = f_a \otimes f_b = f'_a \otimes f'_b.$$

Let γ be a root of f. By Definition 3.32 there exist roots $\alpha, \beta, \alpha', \beta'$ of f_a, f_b, f'_a, and f'_b, respectively, such that

$$\gamma = \alpha\beta = \alpha'\beta'. \tag{9.2}$$

Since the elements a, b, a', b' are irreducible, by Lemma 4.8(a) the polynomials f_a, f_b, f'_a, f'_b are irreducible.

Let $(m, t) = \mathrm{size}(\mathfrak{F})$. Then $\deg(f_a) = \deg(f'_a) = m$ and $\deg(f_b) = \deg(f'_b) = t$. Hence, (recalling that a, b, a', b' are irreducible) Lemma 3.2(d) yields

$$\alpha, \alpha' \in \mathbb{F}^*_{q^m}, \quad \beta, \beta' \in \mathbb{F}^*_{q^t}.$$

Let $\varepsilon = \beta/\beta'$. Then by (9.2) we have $\varepsilon = \alpha'/\alpha$. It follows that $\varepsilon \in \mathbb{F}^*_{q^m} \cap \mathbb{F}^*_{q^t}$, which recalling that $\gcd(m, t) = 1$ and using Lemma 2.10 reveals that

$$\varepsilon \in \mathbb{F}^*_q.$$

Observe (using (9.2)) that $\alpha' = \varepsilon\alpha$ and $\beta' = \varepsilon^{-1}\beta$. Hence, α' and β' are roots of the characteristic polynomials of $\varepsilon a \in \mathrm{GL}(\mathcal{X})$ and $\varepsilon^{-1}b \in \mathrm{GL}(\mathcal{Y})$, respectively. Now, the elements a, b, and hence also $\varepsilon a, \varepsilon^{-1}b$ are irreducible, and have thus irreducible characteristic polynomials by Lemma 4.8(a). Since the characteristic polynomials of $\varepsilon a, a'$, and respectively of $\varepsilon^{-1}b, b'$ share a root (namely α' and β', respectively), by Lemma 3.2(e) the characteristic polynomials of $\varepsilon a, a'$, and respectively of $\varepsilon^{-1}b, b'$, coincide. Using Lemma 4.8(b), we conclude that $\varepsilon a, a'$ are conjugate in $\mathrm{GL}(\mathcal{X})$ (say by $a^* \in \mathrm{GL}(\mathcal{X})$), and that $\varepsilon^{-1}b, b'$ are conjugate in $\mathrm{GL}(\mathcal{Y})$ (say by $b^* \in \mathrm{GL}(\mathcal{Y})$). Then

$$\underbrace{\varepsilon a \otimes \varepsilon^{-1}b}_{=a\otimes b=g} \text{ and } \underbrace{a' \otimes b'}_{=g'}$$

are conjugate (by $a^* \otimes b^*$) in $\mathrm{C}_4(\mathfrak{F})$ and the proof is complete. □

Recall from Definition 3.5 that $N^*_q(m)$ is the number of all monic, irreducible polynomials $f \neq x$ of degree m over $\mathbb{F}_q$.

Lemma 9.20. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size (m, t) over $\mathbb{F}_q$. Suppose that $\gcd(m, t) = 1$. The group $\mathrm{C}_4(\mathfrak{F})$ has $N^*_q(m)N^*_q(t)/(q-1)$ conjugacy classes consisting of irreducible elements.*

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$. As we may deduce from Lemma 4.5, the group $\mathrm{C}_4(\mathfrak{F})$ acts via conjugation on the set of all irreducible elements in $\mathrm{C}_4(\mathfrak{F})$. Let $\mathfrak{I}$ be the set of all orbits of this action. (That is, let $\mathfrak{I}$ be the set of all conjugacy classes in $\mathrm{C}_4(\mathfrak{F})$ which consist of irreducible elements.) Recall that the characteristic polynomial of an element $g \in \mathrm{C}_4(\mathfrak{F})$ is equal to the tensor product $f_a \otimes f_b$ of some polynomials $f_a, f_b \in \mathbb{F}_q[x]$ with $\deg(f_a) = m$

and $\deg(f_b) = t$. If g is irreducible, then by Lemmas 9.18(a) and 4.8(a) the polynomials $f_a \otimes f_b, f_a, f_b$ are irreducible. Thus, by mapping each orbit $O \in \mathfrak{I}$ onto the characteristic polynomial of a representative of O, we obtain a mapping

$$\iota : \mathfrak{I} \to \big\{ f_a \otimes f_b \mid f_a, f_b \neq x \text{ monic and irreducible polynomials over } \mathbb{F}_q, \deg(f_a) = m, \deg(f_b) = t \big\}.$$

(The mapping ι does not depend on the choice of the respective representative.) By Lemma 9.19, ι is injective. In order to see that ι is surjective, let $f_a, f_b \neq x$ be monic, irreducible polynomials over $\mathbb{F}_q$ of degree $\deg(f_a) = m$, $\deg(f_b) = t$. Let $a \in \mathrm{GL}(\mathcal{X})$ and $b \in \mathrm{GL}(\mathcal{Y})$ by such that f_a is the characteristic polynomial of a and f_b is the characteristic polynomial of b. Then $a \otimes b \in \mathrm{C}_4(\mathfrak{F})$ and the characteristic polynomial of $a \otimes b$ is equal to $f_a \otimes f_b$. Moreover, by Lemma 4.8(a) (according to which a and b are irreducible) and Lemma 9.18(a) the element $a \otimes b \in \mathrm{C}_4(\mathfrak{F})$ is irreducible. Hence, ι is bijective and the assertion follows from Proposition 3.36. □

Recall that, given a group G and an element $g \in G$, we write $C_G(g)$ for the centraliser of $\langle g \rangle$ in G.

Lemma 9.21. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size (m, t) over $\mathbb{F}_q$ and let $g \in \mathrm{C}_4(\mathfrak{F})$ be irreducible. Then $C_{\mathrm{C}_4(\mathfrak{F})}(g)$ is cyclic of order $(q^m - 1)(q^t - 1)/(q - 1)$.*

Proof. Suppose that $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$ and $g = a \otimes b$.

According to Proposition 4.18 the centraliser $C_{\mathrm{GL}(\langle \mathfrak{F} \rangle)}(g)$ of $\langle g \rangle$ in $\mathrm{GL}(\langle \mathfrak{F} \rangle)$ is cyclic. Being a subgroup of $C_{\mathrm{GL}(\langle \mathfrak{F} \rangle)}(g)$, the group $C_{\mathrm{C}_4(\mathfrak{F})}(g)$ is also cyclic, say

$$C_{\mathrm{C}_4(\mathfrak{F})}(g) = \big\langle \widehat{a} \otimes \widehat{b} \,\big\rangle.$$

Now, $\widehat{a} \otimes \widehat{b} \in \mathrm{C}_4(\mathfrak{F})$ is irreducible. Hence, by Lemmas 9.15 and 9.18(a) the elements $\widehat{a} \in \mathrm{GL}(\mathcal{X})$, $\widehat{b} \in \mathrm{GL}(\mathcal{Y})$ are irreducible and $\gcd(m, t) = 1$. Recall that the order of $\widehat{a} \otimes \widehat{b}$ divides $\mathrm{lcm}\{|\widehat{a}|, |\widehat{b}|\}$, which by (the "in particular" part of) Lemma 4.11(b) in turn divides $\mathrm{lcm}\{q^m - 1, q^t - 1\}$. Thus, keeping in mind that $\gcd(m, t) = 1$, Lemma 2.10 implies that

$$\underbrace{|C_{\mathrm{C}_4(\mathfrak{F})}(g)|}_{|\widehat{a} \otimes \widehat{b}|} \text{ divides } \frac{(q^m - 1)(q^t - 1)}{q - 1}. \tag{9.3}$$

Next, consider the group $H = \{a' \otimes b' \mid a \in C_{\mathrm{GL}(\mathcal{X})}(a), b' \in C_{\mathrm{GL}(\mathcal{Y})}(b)\}$. Elements of H commute with $a \otimes b$. Thus, $H \leq C_{\mathrm{C}_4(\mathfrak{F})}(g)$. The group H is

isomorphic to (the central product $C_{\mathrm{GL}(\mathcal{X})}(a) \circ C_{\mathrm{GL}(\mathcal{Y})}(b)$, that is to) the quotient of the direct product $C_{\mathrm{GL}(\mathcal{X})}(a) \times C_{\mathrm{GL}(\mathcal{Y})}(b)$ modulo its normal subgroup $\{(\varepsilon \mathrm{id}_{\mathcal{X}}, \varepsilon^{-1}\mathrm{id}_{\mathcal{Y}}) \mid \varepsilon \in \mathbb{F}_q^*\}$. Thus,

$$|H| = \frac{|C_{\mathrm{GL}(\mathcal{X})}(a)|\,|C_{\mathrm{GL}(\mathcal{Y})}(b)|}{q-1}.$$

Since g is irreducible, according to Lemmas 9.15 and 9.18(a) the elements a and b are irreducible. Thus, by Proposition 4.18 we have $|C_{\mathrm{GL}(\mathcal{X})}(a)| = q^m - 1$ and $|C_{\mathrm{GL}(\mathcal{Y})}(b)| = q^t - 1$, whence

$$|H| = \frac{(q^m-1)(q^t-1)}{q-1}.$$

Recalling that $H \leq C_{\mathrm{C}_4(\mathfrak{F})}(g)$, we conclude that $(q^m-1)(q^t-1)/(q-1)$ divides $|C_{\mathrm{C}_4(\mathfrak{F})}(g)|$, which combined with (9.3) reveals that $|C_{\mathrm{C}_4(\mathfrak{F})}(g)|$ is equal to $(q^m-1)(q^t-1)/(q-1)$. □

Recall from Definition 4.20 that $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F}))$ is the proportion (in $\mathrm{C}_4(\mathfrak{F})$) of all irreducible elements in $\mathrm{C}_4(\mathfrak{F})$. Recall further from Definition 3.5 the notion of $N_q^*(m)$. The value of $N_q^*(m)$ can be calculated using the formula in Lemma 3.7.

Proposition 9.22. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size (m,t) over $\mathbb{F}_q$. Suppose that* $\gcd(m,t) = 1$. *Then*

$$\mathrm{irr}\big(\mathrm{C}_4(\mathfrak{F})\big) = \frac{N_q^*(m)N_q^*(t)}{(q^m-1)(q^t-1)}.$$

Moreover,

$$\frac{1}{(m+1)(t+1)} \leq \mathrm{irr}(\mathrm{C}_4(\mathfrak{F})) \leq \frac{1}{mt}.$$

If $mt \geq 2$, then the upper bound is not strict, that is $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F})) < 1/(mt)$. *If $mt = 1$, then* $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F})) = 1$.

Proof. Since m and t are coprime, by Lemma 9.18(a) irreducible elements in $\mathrm{C}_4(\mathfrak{F})$ are precisely the conserving elements in $\mathrm{C}_4(\mathfrak{F})$.

The group $\mathrm{C}_4(\mathfrak{F})$ acts via conjugation on the set of all irreducible elements in $\mathrm{C}_4(\mathfrak{F})$. By Lemmas 9.20 and 9.21 (and the orbit-stabiliser-theorem) this action has $N_q^*(m)N_q^*(t)/(q-1)$ orbits, each of length $|\mathrm{C}_4(\mathfrak{F})|(q-1)(q^m-1)^{-1}(q^t-1)^{-1}$. It follows that the number of all irreducible elements in $\mathrm{C}_4(\mathfrak{F})$ is equal to

$$\mathrm{irr}\big(\mathrm{C}_4(\mathfrak{F})\big)|\mathrm{C}_4(\mathfrak{F})| = \frac{N_q^*(m)N_q^*(t)|\mathrm{C}_4(\mathfrak{F})|(q-1)}{(q-1)(q^m-1)(q^t-1)}.$$

Hence, $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F})) = N_q^*(m)N_q^*(t)(q^m-1)^{-1}(q^t-1)^{-1}$. The "moreover"-part then follows from Lemma 3.9(c). □

Example 9.23. Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size $(4,3)$ over $\mathbb{F}_3$, whence

$$\mathrm{C}_4(\mathfrak{F}) \cong \mathrm{GL}(4,3) \circ \mathrm{GL}(3,3).$$

By Proposition 9.22 we have

$$\mathrm{irr}\big(\mathrm{C}_4(\mathfrak{F})\big) = \frac{N_3^*(4)N_3^*(3)}{(3^4-1)(3^3-1)}.$$

Using Lemma 3.7 we obtain

$$\mathrm{irr}\big(\mathrm{C}_4(\mathfrak{F})\big) = \frac{\frac{1}{4}(3^4-1-3^2+1)\frac{1}{3}(3^3-1-3+1)}{(3^4-1)(3^3-1)} = \frac{9}{130} \approx 0.0693.$$

9.3.2 The general case

Consider a $\mathscr{C}_4$-frame $\mathfrak{F} = (\mathcal{X}, \mathcal{Y})$. Our next result shows that, if $\mathcal{U}$ is a "large" subspace of $\mathcal{X} \otimes \mathcal{Y}$ in the sense that $\dim(\mathcal{U}) > \dim(\mathcal{X} \otimes \mathcal{Y})/2$, and if $a \in \mathrm{GL}(\mathcal{X}), b \in \mathrm{GL}(\mathcal{Y})$ are such that $\langle a \otimes b\rangle$ acts irreducibly on $\mathcal{U}$, then $\mathcal{U} = \mathcal{X}_0 \otimes \mathcal{Y}_0$ for some $\mathcal{X}_0 \leq \mathcal{X}$ and $\mathcal{Y}_0 \leq \mathcal{Y}$. This fact suggests that we can retrieve information on (arbitrary) fat elements in $\mathrm{C}_4(\mathfrak{F})$ from properties of irreducible $\mathscr{C}_4$-maps.

Recall Definition 9.2(b) of the $\mathscr{C}_4$-cover in $\mathfrak{F}$ of a subspace of $\langle\mathfrak{F}\rangle$.

Proposition 9.24. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame over $\mathbb{F}_q$, let $g \in \mathrm{C}_4(\mathfrak{F})$, let $\mathcal{U} \leq \langle\mathfrak{F}\rangle$ be such that $\dim(\mathcal{U}) > \dim(\langle\mathfrak{F}\rangle)/2$, and let $\mathfrak{U}$ be the $\mathscr{C}_4$-cover of $\mathcal{U}$ in $\mathfrak{F}$. If $\mathcal{U}$ is $\langle g\rangle$-irreducible, then $\langle\mathfrak{U}\rangle = \mathcal{U}$.*

Proof. Suppose that $\langle g\rangle$ acts irreducibly on $\mathcal{U}$. Then $\mathcal{U}$ is $\langle g\rangle$-invariant, which by Lemma 9.12 implies that g preserves $\mathfrak{U}$.

We next show that g conserves $\mathfrak{U}$. Seeking a contradiction, assume that the restriction $g|_{\langle\mathfrak{U}\rangle} \in \mathrm{C}_4(\mathfrak{U})$ does not conserve $\mathfrak{U}$. According to Lemma 9.16 (applied to $\mathfrak{U}$ and $g|_{\langle\mathfrak{U}\rangle}$) the p'-part of $g|_{\langle\mathfrak{U}\rangle}$, and hence also $g_{p'}$, preserves a proper $\mathscr{C}_4$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{U}$ satisfying

$$\dim\big(\langle\mathfrak{D}\rangle\big) \geq \frac{\dim\big(\langle\mathfrak{U}\rangle\big)}{2}.$$

Since (by assumption) we have $\dim(\mathcal{U}) > \dim(\langle\mathfrak{F}\rangle)/2 \geq \dim(\langle\mathfrak{U}\rangle)/2$, since (by Lemma 9.3($b$)) $\mathcal{U}$ is a subspace of $\langle\mathfrak{U}\rangle$, and since $\langle\mathfrak{D}\rangle \leq \langle\mathfrak{U}\rangle$, it follows that

$$\mathcal{U} \cap \langle\mathfrak{D}\rangle \neq \{0\}.$$

Now (recalling that $g_{p'}$ preserves $\mathfrak{D}$), by Lemma 9.11 the subspace $\langle\mathfrak{D}\rangle$ is $\langle g_{p'}\rangle$-invariant. By (the "in particular" part of) Lemma 4.15, $\mathcal{U}$ is $\langle g_{p'}\rangle$-irreducible. Since $\mathcal{U}$ and $\langle\mathfrak{D}\rangle$ intersect non-trivially, it follows that $\mathcal{U} \leq \langle\mathfrak{D}\rangle$. Thus, $\mathfrak{D} \in \{\mathfrak{F}_0 \sqsubseteq \mathfrak{F} \mid \mathcal{U} \leq \langle\mathfrak{F}_0\rangle\}$, and hence

$$\bigcap_{\mathfrak{F}_0 \sqsubseteq \mathfrak{F}, \mathcal{U} \leq \langle\mathfrak{F}_0\rangle} \mathfrak{F}_0 \sqsubseteq \mathfrak{D}.$$

In other words, $\mathfrak{U} \sqsubseteq \mathfrak{D}$. This contradicts $\mathfrak{D}$ being a proper $\mathscr{C}_4$-subframe of $\mathfrak{U}$. Hence, g conserves $\mathfrak{U}$. Since $\mathcal{U} \leq \langle\mathfrak{U}\rangle$, Lemma 9.17 (applied to $\mathfrak{U}$ and $g|_{\langle\mathfrak{U}\rangle} \in \mathrm{C}_4(\mathfrak{U})$) yields $\langle\mathfrak{U}\rangle = \mathcal{U}$. □

We are now ready to prove the main results of this chapter. Theorem 9.25 gives necessary and sufficient conditions for the existence of fat elements in $\mathrm{C}_4(\mathfrak{F})$. The proportion of all such elements (in $\mathrm{C}_4(\mathfrak{F})$) is specified in Theorem 9.26. Recall Definition 5.1(a).

Theorem 9.25. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size (m,t) over $\mathbb{F}_q$, and let $e \in \mathbb{N}$ be such that $mt/2 < e \leq mt$. The group $\mathrm{C}_4(\mathfrak{F})$ contains $\mathrm{fat}(mt,q;e)$-elements if and only if there exist positive integers $m_0 \leq m$, $t_0 \leq t$ such that $\gcd(m_0,t_0)=1$ and $m_0t_0 = e$.*

Proof. First, suppose that $\mathrm{C}_4(\mathfrak{F})$ contains a $\mathrm{fat}(mt,q;e)$-element g. Then $\langle g\rangle$ acts irreducibly on an e-dimensional subspace $\mathcal{U} \leq \langle\mathfrak{F}\rangle$. Let $\mathfrak{U}$ be the $\mathscr{C}_4$-cover of $\mathcal{U}$ in $\mathfrak{F}$ (as introduced in Definition 9.2(b)). Let $(m_0,t_0) = \mathrm{size}(\mathfrak{U})$. Since $\mathfrak{U}$ is a $\mathscr{C}_4$-subframe of $\mathfrak{F}$ we have $m_0 \leq m$ and $t_0 \leq t$. By Proposition 9.24 we have $\langle\mathfrak{U}\rangle = \mathcal{U}$. Thus, $\dim(\langle\mathfrak{U}\rangle) = \dim(\mathcal{U})$, that is $m_0t_0 = e$. Moreover, by Lemma 9.18(a) (applied to $\mathfrak{U}$ and $g|_{\mathcal{U}} \in \mathrm{C}_4(\mathfrak{U})$) we get $\gcd(m_0,t_0) = 1$.

Conversely, let $m_0,t_0 \in \mathbb{N}$ be such that $m_0 \leq m$, $t_0 \leq t$, $\gcd(m_0,t_0) = 1$, and $m_0t_0 = e$. Let $\mathfrak{D}$ be a $\mathscr{C}_4$-subframe of $\mathfrak{F}$ of size (m_0,t_0). By Lemma 9.18(b) the group $\mathrm{C}_4(\mathfrak{D})$ contains irreducible elements, that is $\mathrm{fat}(e,q;e)$-elements. Then by Lemma 9.13, $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \leq \mathrm{C}_4(\mathfrak{F})$ contains $\mathrm{fat}(mt,q;e)$-elements. □

Consider a $\mathscr{C}_4$-frame $\mathfrak{F}$ of size (m,t) over $\mathbb{F}_q$. Recall from Definition 5.17 that we write $\mathrm{fat}(\mathrm{C}_4(\mathfrak{F});e)$ for the proportion (in $\mathrm{C}_4(\mathfrak{F})$) of all $\mathrm{fat}(mt,q;e)$-elements in $\mathrm{C}_4(\mathfrak{F})$, $e > mt/2$. Recall further (from Definition 4.20) that $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F}))$ is the proportion of all irreducible elements in $\mathrm{C}_4(\mathfrak{F})$. If $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F})) \neq 0$, which according to Lemma 9.18(b) is equivalent to saying that m and t are coprime, then the precise value of, and also a good upper and lower bound for, $\mathrm{irr}(\mathrm{C}_4(\mathfrak{F}))$ is specified in Proposition 9.22.

Theorem 9.26. *Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size (m,t) over $\mathbb{F}_q$, let e be an integer satisfying $mt/2 < e \leq mt$, and let $S = \{(m_0,t_0) \in \mathbb{N}\times\mathbb{N} \mid m_0 \leq m, t_0 \leq t, \gcd(m_0,t_0)=1, e = m_0t_0\}$. Suppose that $\operatorname{fat}(\mathrm{C}_4(\mathfrak{F});e) \neq \emptyset$. Then $S \neq \emptyset$ and*

$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F});e\big) = \sum_{\mathfrak{D}\in\mathbf{D}} \operatorname{irr}\big(\mathrm{C}_4(\mathfrak{D})\big),$$

where $\mathbf{D}$ is a set of $\mathscr{C}_4$-subframes of $\mathfrak{F}$ containing precisely one $\mathscr{C}_4$-frame of size (m_0,t_0) for all $(m_0,t_0) \in S$.

Proof. (The proof is similar to the proofs of Theorems 7.42, 8.33.)

Let $g \in \mathrm{C}_4(\mathfrak{F})$ be a $\operatorname{fat}(mt,q;e)$-element. Let $\mathcal{U}$ be the (uniquely determined) e-dimensional, $\langle g\rangle$-irreducible subspace of $\langle\mathfrak{F}\rangle$. By Proposition 9.24 there exists a $\mathscr{C}_4$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ such that $\langle\mathfrak{D}\rangle = \mathcal{U}$ (namely the $\mathscr{C}_4$-cover of $\mathcal{U}$ in $\mathfrak{F}$). By Lemma 9.11 the element g preserves $\mathfrak{D}$, that is $g \in \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$. Let $(m_0,t_0) = \operatorname{size}(\mathfrak{D})$. Then $m_0 \leq m$ and $t_0 \leq t$. Applying Lemma 9.18(a) to the restriction $g|_{\langle\mathfrak{D}\rangle} \in \mathrm{C}_4(\mathfrak{D})$, we see that $\gcd(m_0,t_0)=1$. Further, we have $e = \dim(\mathcal{U}) = \dim(\langle\mathfrak{D}\rangle) = m_0t_0$. Hence, $(m_0,t_0) \in S$, and in particular, $S \neq \emptyset$. Observe that $\mathfrak{D}$ is the unique $\mathscr{C}_4$-subframe of $\mathfrak{F}$ such that $\operatorname{size}(\mathfrak{D}) \in S$ and $\langle\mathfrak{D}\rangle$ is $\langle g\rangle$-irreducible. (To see that this is really true, let $\mathfrak{E} \sqsubseteq \mathfrak{F}$ be such that $\operatorname{size}(\mathfrak{E}) \in S$ and $\langle g\rangle$ acts irreducibly on $\langle\mathfrak{E}\rangle$. Since $\dim(\langle\mathfrak{E}\rangle) = \dim(\langle\mathfrak{D}\rangle) = e > mt/2$, the subspaces $\langle\mathfrak{D}\rangle$ and $\langle\mathfrak{E}\rangle$ intersect non-trivially. Since $\langle g\rangle$ acts irreducibly on $\langle\mathfrak{D}\rangle$ and $\langle\mathfrak{E}\rangle$, we get $\langle\mathfrak{D}\rangle = \langle\mathfrak{E}\rangle$. By Lemma 9.4, the latter is equivalent to $\mathfrak{D} = \mathfrak{E}$.)

It follows that the number of all $\operatorname{fat}(mt,q;e)$-elements in $\mathrm{C}_4(\mathfrak{F})$ is given by

$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F});e\big)|\mathrm{C}_4(\mathfrak{F})| = \sum_{\substack{\mathfrak{D}\sqsubseteq\mathfrak{F},\\ \operatorname{size}(\mathfrak{D})\in S}} \big|\big\{h \in \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \mid \langle\mathfrak{D}\rangle \text{ is } \langle h\rangle\text{-irreducible}\big\}\big|. \quad (9.4)$$

Fix a $\mathscr{C}_4$-subframe $\mathfrak{D} \sqsubseteq \mathfrak{F}$ with $\operatorname{size}(\mathfrak{D}) \in S$. By Lemma 9.13 the mapping

$$\delta : \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \to \mathrm{C}_4(\mathfrak{D}), \quad h \mapsto h|_{\langle\mathfrak{D}\rangle}$$

is a surjective group homomorphism. Because elements of $\ker(\delta)$ act trivially on $\langle\mathfrak{D}\rangle$ we see the following. If for $h \in \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$ the coset $\ker(\delta)h$ contains $\operatorname{fat}(mt,q;e)$-elements, then each element of $\ker(\delta)h$ is a $\operatorname{fat}(mt,q;e)$-element. Hence, the number of $\operatorname{fat}(mt,q;e)$-elements in $\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}$ is equal to $|\ker(\delta)|$ times the number of $\operatorname{fat}(e,q;e)$-elements (that is irreducible elements) in $\operatorname{im}(\delta)$. In other words,

$$\begin{aligned}&\big|\big\{h \in \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \mid \langle\mathfrak{D}\rangle \text{ is } \langle h\rangle\text{-irreducible}\big\}\big| \\ &\quad = |\ker(\delta)| \underbrace{\big|\big\{h \in \overbrace{\operatorname{im}(\delta)}^{\mathrm{C}_4(\mathfrak{D})} \mid h \text{ irreducible}\big\}\big|}_{=\operatorname{irr}(\mathrm{C}_4(\mathfrak{D}))|\mathrm{C}_4(\mathfrak{D})|}. \end{aligned} \quad (9.5)$$

Since δ is onto, we have $\operatorname{im}(\delta) = \mathrm{C}_4(\mathfrak{D})$ and $|\operatorname{im}(\delta)||\ker(\delta)| = |\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}|$. Thus, (9.5) yields

$$\big|\{h \in \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}} \mid \langle\mathfrak{D}\rangle \text{ is } \langle h\rangle\text{-irreducible}\}\big| = \operatorname{irr}\big(\mathrm{C}_4(\mathfrak{D})\big)|\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}|.$$

Using (9.4) we conclude that

$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); e\big)|\mathrm{C}_4(\mathfrak{F})| = \sum_{\substack{\mathfrak{D}\sqsubseteq\mathfrak{F},\\ \operatorname{size}(\mathfrak{D})\in S}} \operatorname{irr}\big(\mathrm{C}_4(\mathfrak{D})\big)|\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}|. \tag{9.6}$$

Now, by Lemma 9.9 the group $\mathrm{C}_4(\mathfrak{F})$ acts transitively on the set of all $\mathscr{C}_4$-subframes of $\mathfrak{F}$ of a given size. Further, by Proposition 9.22 the number of all irreducible $\mathscr{C}_4$-maps in a $\mathscr{C}_4$-subframe of $\mathfrak{F}$ only depends on its size (and the size of the underlying field). Thus, using the orbit-stabiliser-theorem, (9.6) yields

$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); e\big)|\mathrm{C}_4(\mathfrak{F})| = \sum_{\mathfrak{D}\in\mathbf{D}} |\mathrm{C}_4(\mathfrak{F}) : \mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}| \operatorname{irr}\big(\mathrm{C}_4(\mathfrak{D})\big)\ |\mathrm{C}_4(\mathfrak{F})_{\mathfrak{D}}|,$$

where $\mathbf{D}$ is a set of $\mathscr{C}_4$-subframes of $\mathfrak{F}$ containing precisely one $\mathscr{C}_4$-subframe of size (m_0, t_0) for all $(m_0, t_0) \in S$. Then $\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); e\big) = \sum_{\mathfrak{D}\in\mathbf{D}} \operatorname{irr}\big(\mathrm{C}_4(\mathfrak{D})\big)$. □

Example 9.27. (*a*) Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size $(4, 4)$ over $\mathbb{F}_3$, whence

$$\mathrm{C}_4(\mathfrak{F}) \cong \mathrm{GL}(4, 3) \circ \mathrm{GL}(4, 3).$$

Let $e \in \mathbb{N}$ be such that $8 < e \leq 16$. By Theorem 9.25 the group $\mathrm{C}_4(\mathfrak{F})$ contains $\operatorname{fat}(16, 3; e)$-elements if and only if $e = 12$. In such a case Theorem 9.26 and Proposition 9.22 yield

$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); 12\big) = \sum_{(m_0,t_0)\in\{(4,3),(3,4)\}} \frac{N_3^*(m_0)N_3^*(t_0)}{(3^{m_0}-1)(3^{t_0}-1)} = \frac{2N_3^*(4)N_3^*(3)}{(3^4-1)(3^3-1)}.$$

Using Example 9.23 we conclude that $\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); 12\big) = 9/65 \approx 0.1385$.

(*b*) Let $\mathfrak{F}$ be a $\mathscr{C}_4$-frame of size $(250, 270)$ over $\mathbb{F}_q$, whence

$$\mathrm{C}_4(\mathfrak{F}) \cong \mathrm{GL}(250, q) \circ \mathrm{GL}(270, q).$$

Let $e = 11 \times 13 \times 15 \times 17 = 36465$. Note that $e > 250 \times 270/2 = 33750$. By Theorem 9.25 the group $\mathrm{C}_4(\mathfrak{F})$ contains $\operatorname{fat}(67500, q; e)$-elements. Let S be as in Theorem 9.26. Then

$$S = \big\{(\underbrace{143}_{11\times13}, \underbrace{255}_{15\times17}), (\underbrace{165}_{11\times15}, \underbrace{221}_{13\times17}), (\underbrace{187}_{11\times17}, \underbrace{195}_{13\times15}), (\underbrace{195}_{13\times15}, \underbrace{187}_{11\times17}), (\underbrace{221}_{13\times17}, \underbrace{165}_{11\times15})\big\}.$$

Hence, by Theorem 9.26 and the "moreover" part of Proposition 9.22 we have

$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); e\big) \leq \frac{5}{e} = \frac{1}{7293} \leq 0.00014$$
$$\operatorname{fat}\big(\mathrm{C}_4(\mathfrak{F}); e\big) \geq \frac{1}{36864} + \frac{2}{36852} + \frac{2}{36848} \geq 0.00013.$$

Chapter 10

Aschbacher's $\mathscr{C}_5$-class (Subfield subgroups)

Consider a finite vector space $\mathcal{V} \neq \{0\}$ defined over a (finite) field $\mathbb{F}$. Let $\mathbb{K}$ be a subfield of $\mathbb{F}$ and let $\mathcal{X}$ be the $\mathbb{K}$-span of some ($\mathbb{F}$-)basis $\mathfrak{B}$ of $\mathcal{V}$. This way, $\mathfrak{B}$ is also a ($\mathbb{K}$-)basis of $\mathcal{X}$. Every element $h \in \mathrm{GL}(\mathcal{X})$ extends uniquely to an $\mathbb{F}$-linear map on $\mathcal{V}$, and we denote this unique extension by $h^{\mathbb{F}}$. Mapping each $h \in \mathrm{GL}(\mathcal{X})$ onto $h^{\mathbb{F}}$ yields an embedding of $\mathrm{GL}(\mathcal{X})$, the group of all non-singular $\mathbb{K}$-linear mappings on $\mathcal{X}$, in the group $\mathrm{GL}(\mathcal{V})$ consisting of all non-singular $\mathbb{F}$-linear mappings on $\mathcal{V}$. Since (for $h \in \mathrm{GL}(\mathcal{X})$) the matrix of h with respect to $\mathfrak{B}$ is equal to the matrix of $h^{\mathbb{F}}$ with respect to $\mathfrak{B}$, both elements h and $h^{\mathbb{F}}$ have the same characteristic polynomial.

If $\mathbb{K}$ is a proper subfield of $\mathbb{F}$, then

$$G = \left\{\alpha h^{\mathbb{F}} \mid \alpha \in \mathbb{F}^*, h \in \mathrm{GL}(\mathcal{X})\right\} \leq \mathrm{GL}(\mathcal{V})$$

is a member of Aschbacher's $\mathscr{C}_5$-class. Observe that the mapping

$$\mathrm{GL}(\mathcal{X}) \times \mathbb{F}^* \to G, \quad (h, \alpha) \mapsto \alpha h^{\mathbb{F}},$$

is a surjective group homomorphism with kernel $N = \{(\varepsilon \mathrm{id}_{\mathcal{X}}, \varepsilon^{-1}) \mid \varepsilon \in \mathbb{K}^*\}$. Thus,

$$G \cong (\mathrm{GL}(\mathcal{X}) \times \mathbb{F}^*)/N,$$

that is G is isomorphic to a central product of $\mathrm{GL}(\mathcal{X})$ and $\mathbb{F}^*$, as specified in [40, Definition 2.2.6].

The aim of this chapter is to investigate the occurrence of fat elements in G. Our results are presented in Theorems 10.2, 10.3. Both theorems can be deduced rather quickly using results from previous chapters. We shall be working with the following hypothesis.

Hypothesis 10.1. Let d, t be positive integers. Let p be prime, let q_0 be a power of p, and let $q = q_0^t$. Define $\mathcal{V}$ to be a d-dimensional $\mathbb{F}_q$-vector space and let $\mathcal{X}$ be the $\mathbb{F}_{q_0}$-span of some ($\mathbb{F}_q$-)basis of $\mathcal{V}$. (We view $\mathcal{X}$ as an $\mathbb{F}_{q_0}$-vector space.) Further, let

$$G = \left\{\alpha h^{\mathbb{F}_q} \mid \alpha \in \mathbb{F}_q^*, h \in \mathrm{GL}(\mathcal{X})\right\} \leq \mathrm{GL}(\mathcal{V}),$$
$$H = \left\{h^{\mathbb{F}_q} \mid h \in \mathrm{GL}(\mathcal{X})\right\} \leq \mathrm{GL}(\mathcal{V}).$$

Recall Definition 5.1(a) of $\mathrm{fat}(d, q; e)$-elements.

Theorem 10.2. *Suppose that Hypothesis 10.1 holds and let e be an integer such that $d/2 < e \leq d$.*

(a) *Let $\alpha \in \mathbb{F}_q^*$ and $h \in \mathrm{GL}(\mathcal{X})$. The following are equivalent.*

- (i) *The element $\alpha h^{\mathbb{F}_q} \in G$ is a $\mathrm{fat}(d, q; e)$-element.*
- (ii) *The element $h^{\mathbb{F}_q} \in H$ is a $\mathrm{fat}(d, q; e)$-element.*
- (iii) *The element $h \in \mathrm{GL}(\mathcal{X})$ is a $\mathrm{fat}(d, q_0; e)$-element and $\gcd(e, t) = 1$.*

(b) *The group G contains $\mathrm{fat}(d, q; e)$-elements if and only if $\gcd(e, t) = 1$.*

Proof. (a) Note that a subspace of $\mathcal{V}$ is $\langle \alpha h^{\mathbb{F}_q}\rangle$-invariant if and only if it is $\langle h^{\mathbb{F}_q}\rangle$-invariant. This implies that a subspace of $\mathcal{V}$ is $\langle \alpha h^{\mathbb{F}_q}\rangle$-irreducible if and only if it is $\langle h^{\mathbb{F}_q}\rangle$-irreducible, and hence proves the equivalence of (i) and (ii).

In order to show that (ii) implies (iii), suppose that $h^{\mathbb{F}_q} \in H$ is a $\mathrm{fat}(d, q; e)$-element. Then according to Lemmas 3.4 and 5.2 the characteristic polynomial of $h^{\mathbb{F}_q}$ has a root, say ω, satisfying

$$\mathrm{ord}(q; |\omega|) = e. \tag{10.1}$$

Now, ω is also a root of the characteristic polynomial of $h \in \mathrm{GL}(\mathcal{X})$. Since the characteristic polynomial of h is defined over $\mathbb{F}_{q_0}$ and since any irreducible factor of that polynomial has degree at most equal to $\dim_{q_0}(\mathcal{X}) = \dim_q(\mathcal{V}) = d$, Lemma 3.4 implies that

$$\mathrm{ord}(q_0; |\omega|) \leq d. \tag{10.2}$$

Since $e > d/2$ and $q = q_0^t$, combining (10.1) and (10.2) with Lemma 2.9(c) reveals that $\mathrm{ord}(q_0; |\omega|) = e$ and $\gcd(e, t) = 1$. By Lemmas 3.4, 5.2 the former implies that h is a $\mathrm{fat}(d, q_0; e)$-element.

Conversely, assume that $h \in \mathrm{GL}(\mathcal{X})$ is a $\mathrm{fat}(d, q_0; e)$-element and that $\gcd(e, t) = 1$. Then by Lemmas 3.4, 5.2 the characteristic polynomial of h has a root β such that

$$\mathrm{ord}(q_0; |\beta|) = e.$$

Since $q = q_0^t$, using Lemma 2.9(*c*) we see that $\mathrm{ord}(q; |\beta|) = e/\gcd(e, t) = e$. Because β is also a root of the characteristic polynomial of $h^{\mathbb{F}_q}$, using Lemmas 3.4, 5.2 we conclude that $h^{\mathbb{F}_q}$ is a $\mathrm{fat}(d, q; e)$-element.

(*b*) By part (*a*) of the current theorem, G contains $\mathrm{fat}(d, q; e)$-elements if and only if $\mathrm{GL}(\mathcal{X})$ contains $\mathrm{fat}(d, q; e)$-elements and $\gcd(e, t) = 1$. According to Lemma 5.3(*a*) there exist $\mathrm{fat}(d, q; e)$-elements in $\mathrm{GL}(\mathcal{X})$. This completes the proof. □

Suppose that Hypothesis 10.1 holds and that e is an integer such that $d/2 < e \leq d$. Recall from Definition 5.17 that $\mathrm{fat}(G; e)|G|$ is the number of all $\mathrm{fat}(d, q; e)$-elements in G. We next determine the value of the proportion $\mathrm{fat}(G; e)$ provided that it is non-zero. Recall from Definition 3.5 the meaning of $N^*_{q_0}(e)$. The precise value of $N^*_{q_0}(e)$ can be calculated using Lemma 3.7.

Theorem 10.3. *Suppose that Hypothesis 10.1 holds and let e be an integer satisfying $d/2 < e \leq d$. Suppose that G contains $\mathrm{fat}(d, q; e)$-elements. Then*

$$\mathrm{fat}(G; e) = \frac{N^*_{q_0}(e)}{q_0^e - 1}.$$

Moreover,

$$\frac{1}{e+1} \leq \mathrm{fat}(G; e) \leq \frac{1}{e}.$$

If $d \geq 2$, then the upper bound is not strict, that is $\mathrm{fat}(G; e) \leq 1/e$. If $d = 1$, then $\mathrm{fat}(G; e) = 1$.

Proof. (Recall from Hypothesis 10.1 the definition of H.) A coset of H in G consists of all elements $\alpha h^{\mathbb{F}_q}$ for some fixed $\alpha \in \mathbb{F}_q^*$. Thus, by Theorem 10.2(*a*) each coset of H in G contains the same number of $\mathrm{fat}(d, q; e)$-elements. It follows that

$$\mathrm{fat}(G; e) = \mathrm{fat}(H; e).$$

As (by assumption) we have $\mathrm{fat}(G; e) \neq 0$, Theorem 10.2(*b*) yields $\gcd(e, t) = 1$. Then, again using Theorem 10.2(*a*), we see that the number of all $\mathrm{fat}(d, q; e)$-elements in H is equal to the number of all $\mathrm{fat}(d, q_0; e)$-elements in $\mathrm{GL}(\mathcal{X})$. Since $|H| = |\mathrm{GL}(\mathcal{X})|$ we obtain

$$\mathrm{fat}(H; e) = \mathrm{fat}\big(\mathrm{GL}(\mathcal{X}); e\big).$$

Then the assertion holds by Theorem 5.18 if $d \geq 2$. In the case $d = e = 1$ we have $\mathrm{fat}(G; e) = 1$. □

Chapter 11

Aschbacher's $\mathscr{C}_7$-class (Tensor induced subgroups)

Recall the definition of a tensor product of two vector spaces, as described in Chapter 9 (on p. 151). By using multi-linear mappings (instead of bilinear mappings) we can analogously define a tensor product of several vector spaces. Consider a finite vector space $\mathcal{X}$ and a tensor product

$$\mathcal{V} = \underbrace{\mathcal{X} \otimes \cdots \otimes \mathcal{X}}_{t \text{ components}}$$

of $t \geq 2$ copies of $\mathcal{X}$. Let S_t denote the symmetric group on $\{1, \ldots, t\}$, that is the group of all permutations of the integers $1, \ldots, t$. Consider elements $\sigma \in S_t$ and $g_1, \ldots, g_t \in \mathrm{GL}(\mathcal{X})$. If $\mathfrak{B}$ is a basis of $\mathcal{X}$, then the simple tensors $v_1 \otimes \cdots \otimes v_t$ $(v_1, \ldots, v_t \in \mathfrak{B})$ form a basis of $\mathcal{V}$, and we can thus uniquely extend

$$v_1 \otimes \cdots \otimes v_t \mapsto v_{1\sigma} g_1 \otimes \cdots \otimes v_{t\sigma} g_t \quad (v_1, \ldots, v_t \in \mathfrak{B})$$

to a mapping on $\mathcal{V}$. The resulting linear extension is non-singular and we denote it by $(\sigma, g_1 \otimes \cdots \otimes g_t)$. The subgroup G of $\mathrm{GL}(\mathcal{V})$ consisting of all elements of this form is a member of Aschbacher's $\mathscr{C}_7$-class. This chapter examines the existence of fat elements in G for the special case where $t = 2$ and $\dim(\mathcal{X}) \geq 4$. We show that, in that case, any fat element $(\sigma, g_1 \otimes g_2) \in G$ satisfies $\sigma = 1$. This is not only surprising (one might think that "adding" permutations would complicate the situation and give rise to more examples of fat elements) but also reduces the investigation of fat elements in G to a setting which we have already treated in Chapter 9. In Theorem 11.2 we present a characterisation of fat elements in G. Theorem 11.3 specifies the (precise) value of, and gives good upper and lower bounds for, the proportion (in G) of all fat elements in G.

We remark that the line of argument we use in this chapter can be generalised to handle the case $t > 2$, which (as well as the case $\dim(\mathcal{X}) \in \{2, 3\}$) is subject to future work. For now, we shall be working under the following hypothesis.

Hypothesis 11.1. Let q be a prime power and let $m \geq 4$ be a positive integer. Let $\mathcal{X}$ be an m-dimensional $\mathbb{F}_q$-vector space, let $\mathcal{V} = \mathcal{X} \otimes \mathcal{X}$ be a tensor product of two copies of $\mathcal{X}$, and define $G = \big\{(\sigma, g_1 \otimes g_2) \mid \sigma \in S_2 \text{ and } g_1, g_2 \in \mathrm{GL}(\mathcal{X})\big\}$.

Observe that we have $\dim(\mathcal{V}) = m^2$. For an integer e satisfying $m^2/2 < e \leq m^2$, recall Definition 5.1(a) of $\mathrm{fat}(m^2, q; e)$-elements in G.

Theorem 11.2. *Suppose that Hypothesis 11.1 holds and let $e \in \mathbb{N}$ be such that $m^2/2 < e \leq m^2$. Then $g = (\sigma, g_1 \otimes g_2) \in G$ is a $\mathrm{fat}(m^2, q; e)$-element if and only if all of the following hold.*

(a) *We have $\sigma = 1$.*

(b) *There are coprime integers e_1, e_2 satisfying $m/2 < e_1, e_2 \leq m$ and $e = e_1 e_2$.*

(c) *For $i \in \{1, 2\}$, the element g_i is a $\mathrm{fat}(m, q; e_i)$-element.*

Proof. First suppose that conditions $(a), (b), (c)$ hold. For $i \in \{1, 2\}$, let $f_i \in \mathbb{F}_q[x]$ be the characteristic polynomial of g_i. Since $\sigma = 1$, the characteristic polynomial of g is given by $f_1 \otimes f_2 \in \mathbb{F}_q[x]$, as introduced in Definition 3.32. Since g_i is a $\mathrm{fat}(m, q; e_i)$-element, by Lemma 5.2 the polynomial f_i has an irreducible factor $a_i \in \mathbb{F}_q[x]$ of degree e_i, $i \in \{1, 2\}$. Let $b_1, b_2 \in \mathbb{F}_q[x]$ be such that $f_i = a_i b_i$ for $i \in \{1, 2\}$. Then by Lemma 3.33 we get

$$f_1 \otimes f_2 = (a_1 b_1) \otimes (a_2 b_2) = (a_1 \otimes a_2)(a_1 \otimes b_2)(b_1 \otimes a_2)(b_1 \otimes b_2)$$

and, in particular, $a_1 \otimes a_2 \mid f_1 \otimes f_2$. Since $\deg(a_1) = e_1$ and $\deg(a_2) = e_2$ are coprime and a_1, a_2 are irreducible over $\mathbb{F}_q$, by Lemma 3.35 the factor $a_1 \otimes a_2$ of $f_1 \otimes f_2$ is irreducible. Since $\deg(a_1 \otimes a_2) = e_1 e_2 = e$, Lemma 5.2 shows that g is a $\mathrm{fat}(m^2, q; e)$-element.

Conversely, suppose that g is a $\mathrm{fat}(m^2, q; e)$-element. Seeking a contradiction, assume that $\sigma \neq 1$, that is $|\sigma| = 2$. Let e_0 be the largest degree of an irreducible factor of the characteristic polynomial of g^2. Recalling that $e > m^2/2$, by Lemma 5.7(b) we have

$$e_0 > \frac{m^2}{4}. \tag{11.1}$$

Now, (since $\sigma \neq 1$) we have $g^2 = (1, g_2 g_1 \otimes g_1 g_2)$. The elements $g_2 g_1, g_1 g_2 \in \mathrm{GL}(\mathcal{X})$ are conjugate (in $\mathrm{GL}(\mathcal{X})$), and thus have the same characteristic polynomial, say $h \in \mathbb{F}_q[x]$. Then the characteristic polynomial of g^2 is equal to

$h \otimes h \in \mathbb{F}_q[x]$. Let $h_1, \ldots, h_r \in \mathbb{F}_q[x]$ be monic irreducible polynomials such that $h = h_1 \cdots h_r$. Then by Lemma 3.33 we have $h \otimes h = \prod_{i,j\in\{1,\ldots,r\}} h_i \otimes h_j$, and thus any irreducible factor of $h \otimes h$ divides one of the $h_i \otimes h_j$. Fix two polynomials $h_i, h_j \in \{h_1, \ldots, h_r\}$ such that $h_i \otimes h_j$ contains an irreducible factor of degree e_0. Then by Lemma 3.34, e_0 divides $\operatorname{lcm}\{\deg(h_i), \deg(h_j)\}$, whence

$$e_0 \leq \operatorname{lcm}\big\{\deg(h_i), \deg(h_j)\big\} \leq \deg(h_i)\deg(h_j). \tag{11.2}$$

If $h_i = h_j$, then according to (11.2) we have $e_0 \leq \deg(h_i) \leq m$, which combined with (11.1) yields the contradiction $m < 4$. So assume that $h_i \neq h_j$. Since $h_i h_j$ divides h, we have $\deg(h_i) \leq \deg(h) - \deg(h_j) = m - \deg(h_j)$. Then by (11.2) we get

$$e_0 \leq \big(m - \deg(h_j)\big)\deg(h_j) \leq \left(\frac{m}{2}\right)^2 = \frac{m^2}{4}.$$

This contradicts (11.1) and shows that condition (a) holds. It remains to verify that (b) and (c) hold. To this end, let $\mathcal{U} \leq \mathcal{V}$ be the (uniquely determined) $\langle g\rangle$-irreducible subspace of dimension e. Then by Proposition 9.24 there exist subspace $\mathcal{X}_1, \mathcal{X}_2 \leq \mathcal{X}$ such that $\mathcal{U} = \langle x_1 \otimes x_2 \mid x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2\rangle$. By Lemma 9.12 the subspace $\mathcal{X}_i$ is $\langle g_i\rangle$-invariant for $i \in \{1, 2\}$. Let $e_1 = \dim(\mathcal{X}_1)$ and $e_2 = \dim(\mathcal{X}_2)$. Then

$$e_1, e_2 \leq m \quad \text{and} \quad e = e_1 e_2.$$

Recalling that $e > m^2/2$ it follows that

$$e_1, e_2 > \frac{m}{2}.$$

For $i \in \{1, 2\}$, let f_i be the characteristic polynomial of the restriction $g_i|_{\mathcal{X}_i}$. Then $f_1 \otimes f_2$ is the characteristic polynomial of $g|_{\mathcal{U}}$. Since $\mathcal{U}$ is $\langle g\rangle$-irreducible, from Lemma 4.8(a) we know that $f_1 \otimes f_2$ is irreducible. Then according to Lemma 3.35,

$$\gcd(e_1, e_2) = 1$$

and the polynomials f_1, f_2 are irreducible. By Lemma 5.2, the latter means that g_i is a $\operatorname{fat}(m, q; e_i)$-element, $i \in \{1, 2\}$. This completes the proof. □

Using Theorem 11.2 along with some findings from Chapter 9 we are able to determine the proportion $\operatorname{fat}(G; e)$ of all $\operatorname{fat}(m^2, q; e)$-elements in G (for some $e \in \mathbb{N}$ such that $m^2/2 < e \leq m^2$). As usual we specify the value of $\operatorname{fat}(G; e)$ in terms of $N_q^*(e)$; see Definition 3.5. A formula for $N_q^*(e)$ is given in Lemma 3.7.

Theorem 11.3. *Suppose that Hypothesis 11.1 holds and let e be an integer such that $m^2/2 < e \leq m^2$.*

(*a*) *The group G contains $\mathrm{fat}(m^2, q; e)$-elements if and only if there exist coprime integers $e_1, e_2 \leq m$ such that $e = e_1 e_2$.*

(*b*) *Suppose that $\mathrm{fat}(G; e) \neq 0$ and let $E = \{(e_1, e_2) \in \mathbb{N} \times \mathbb{N} \mid e_1, e_2 \leq m, \mathrm{lcm}\{e_1, e_2\} = e\}$. Then $E \neq \emptyset$ and*

$$\mathrm{fat}(G; e) = \sum_{(e_1,e_2)\in E} \frac{N_q^*(e_1) N_q^*(e_2)}{2(q^{e_1} - 1)(q^{e_2} - 1)}.$$

Moreover,

$$\sum_{(e_1,e_2)\in E} \frac{1}{2(e_1+1)(e_2+1)} \leq \mathrm{fat}(G; e) \leq \sum_{(e_1,e_2)\in E} \frac{1}{2e_1 e_2}.$$

Proof. (Note that, since $e > m^2/2$, any two positive integers $e_1, e_2 \leq m$ satisfy $\mathrm{lcm}\{e_1, e_2\} = e$ if and only if $\gcd(e_1, e_2) = 1$ and $e_1 e_2 = e$.)

Assertion (*a*) follows from Theorem 11.2 (and Lemma 5.3(*a*)). To see that (*b*) holds, consider the group $H = \{(1, g_1 \otimes g_2) \mid g_1, g_2 \in \mathrm{GL}(\mathcal{X})\}$. Since H is the kernel of the surjective homomorphism $G \to S_2$, assigning to each $(\sigma, g_1 \otimes g_2)$ the permutation σ, we see that H is a normal subgroup of index 2 in G. By Theorem 11.2 there are no $\mathrm{fat}(m^2, q; e)$-elements in $G \setminus H$. This means that the groups G and H contain the same number of $\mathrm{fat}(m^2, q; e)$-elements. That is, $\mathrm{fat}(G; e)|G| = \mathrm{fat}(H; e)|H|$, and thus $\mathrm{fat}(G; e) = \mathrm{fat}(H; e)/2$. Assertion (*b*) then holds by Theorem 9.26 (applied to a $\mathscr{C}_4$-frame of size (m, m) over $\mathbb{F}_q$) and Proposition 9.22. □

Chapter 12

Aschbacher's $\mathscr{S}$-class (Nearly simple subgroups)

This chapter deals with fat elements in groups belonging to Aschbacher's $\mathscr{S}$-class. Members of this class are sometimes referred to as being *nearly simple*. In Section 12.1 we discuss the general setting, explain the aim of this chapter, list what remains to be done in future work, and outline the methods we use here. After that we investigate several quasi-simple groups in $\mathscr{S}$ concerning the existence of exceptional fat elements. These groups comprise all covering groups of the sporadic simple groups (considered in Section 12.2) and all linear, symplectic, and unitary quasi-simple groups of Lie type in non-defining characteristic (covered in Section 12.3). We prove in Theorems 12.6, 12.17 that, for all such groups, the only examples containing exceptional fat elements are representations of the sporadic simple group M_{24} in $\mathrm{GL}(11,2)$[(I)] and that the corresponding exceptional fat elements are $\mathrm{fat}(11,2;6)$ elements of order 21.

Notation. Throughout this chapter we let q be a power of a prime p.

12.1 Preamble

12.1.1 Aschbacher's $\mathscr{S}$-class

In order to specify the groups of interest to us (in Definition 12.1 below) we first introduce some terminology.

Consider a finite group G. The *derived group* of G is given by $G^{(1)} = \langle g^{-1}h^{-1}gh \mid g,h \in G\rangle$. If $G = G^{(1)}$, then G is said to be *perfect*. We write

[(I)] There are two non-equivalent representations of M_{24} of degree 11 over $\mathbb{F}_2$

$G^{(\infty)}$ for the first perfect group in the *derived series* $G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright G^{(3)} \triangleright \cdots$, where $G^{(i)} = (G^{(i-1)})^{(1)}$ for $i \geq 2$. The group $G^{(\infty)}$ is the uniquely determined smallest normal subgroup of G with a solvable quotient, and we refer to $G^{(\infty)}$ as the *solvable residual* of G. The center of G is denoted by $Z(G)$. The automorphism group of G is written as $\mathrm{Aut}(G)$. Further, we write $\mathrm{Inn}(G)$ for the group of all inner automorphisms of G, and $\mathrm{Out}(G)$ for the quotient group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$. We say that G is *almost simple* if there exists a non-abelian simple group S such that $S \leq G \leq \mathrm{Aut}(S)$. (Technically, G is *almost simple* if there exists a non-abelian simple group S such that G can be embedded between $\mathrm{Inn}(S) \cong S$ and $\mathrm{Aut}(S)$.)

Let $\mathcal{V}$ be a finite $\mathbb{F}_q$-vector space and assume that G is a subgroup of $\mathrm{GL}(\mathcal{V})$. Consider an extension field $\mathbb{E}$ of $\mathbb{F}_q$. Recall (from Subsection 4.2.2) that we write $\mathbb{E}_{\mathbb{F}_q}$ for $\mathbb{E}$ viewed as a vector space over $\mathbb{F}_q$. Recall (from Chapter 9) the notion of a tensor product of two vector spaces. A tensor product $\mathbb{E}_{\mathbb{F}_q} \otimes \mathcal{V}$ can be turned into an $\mathbb{E}$-vector space by defining scalar multiplication by $\alpha(\epsilon \otimes v) = \alpha\epsilon \otimes v$ for all $\alpha \in \mathbb{E}$. We say that G is *absolutely irreducible* if, for all extension fields $\mathbb{L}$ of $\mathbb{F}_q$, the group $\{\mathrm{id}_{\mathbb{L}} \otimes g \mid g \in G\}$ acts irreducibly on $\mathbb{L}_{\mathbb{F}_q} \otimes \mathcal{V}$, viewed as an $\mathbb{L}$-vector space.[(II)] The group G is *realisable over a proper subfield* if there exist a proper subfield $\mathbb{K}$ of $\mathbb{F}_q$ and a basis $\mathfrak{B}$ of $\mathcal{V}$ such that, writing $\mathcal{X}$ for the $\mathbb{K}$-vector space given by the $\mathbb{K}$-span of $\mathfrak{B}$, we have $G \leq \mathrm{GL}(\mathcal{X})$ (or more precisely $G \leq \{h^{\mathbb{F}_q} \mid h \in \mathrm{GL}(\mathcal{X})\}$ with $h^{\mathbb{F}_q}$ as in Chapter 10). We say that G *preserves a classical form* if G consists of κ-isometries with respect to a non-degenerate symplectic, non-degenerate quadratic, or non-degenerate unitary form κ. (See [38, pp. 10–13] for more details.)

Definition 12.1. Let $\mathcal{V}$ be a finite vector space. The *class* $\mathscr{S}$ (for $\mathrm{GL}(\mathcal{V})$) consists of all subgroups $G \leq \mathrm{GL}(\mathcal{V})$ such that $\mathrm{SL}(\mathcal{V}) \not\leq \mathrm{GL}(\mathcal{V})$ and the following hold.

(*a*) The quotient $G/Z(G)$ is almost simple.

(*b*) The solvable residual $G^{(\infty)}$ is absolutely irreducible, not realisable over a proper subfield, and does not preserve any classical form.

(Note that, in this chapter, we do not make use of the condition that $G^{(\infty)}$ does not preserve any classical form, if $G \in \mathscr{S}$.)

In general it is not possible to list all groups G contained in the class $\mathscr{S}$. We can, however, name all possibilities for the corresponding solvable residuals $G^{(\infty)}$. The reason for this is explained in the following paragraph.

A *covering group* of a finite perfect group L is a perfect group H satisfying $H/Z(H) \cong L$. A group is said to be *quasi-simple* if it is a covering group

[(II)] In Section 4.2 we define irreducible linear groups only for the case where the underlying vector space is finite. A generalisation of Definition 4.4 to the infinite case (which we need here if $\mathbb{L}$ is not finite) is straightforward.

of some non-abelian simple group. According to a result by Schur [51], for any non-abelian simple group S, there exists, up to isomorphism, a unique covering group F of S of maximal order. (In fact, this applies to all finite perfect groups.) The group F is finite and is referred to as the *full covering group* of S; its centre is the *Schur multiplier* $M(S)$ of S. Every covering group of S is isomorphic to a quotient of F by a subgroup of $M(S)$. Since the structure of $M(S)$ is known (see for example [38, Theorem 5.1.4]), using the classification of the finite simple groups, we are able to list all quasi-simple groups. Our notation of quasi-simple groups follows the convention in [18]. Now, consider a member G of the class $\mathscr{S}$. Since $G/Z(G)$ is almost simple, that is $S \leq G/Z(G) \leq \mathrm{Aut}(S)$ for some non-abelian simple group S, Schreier's conjecture implies that

$$\big(G/Z(G)\big)^{(\infty)} \cong S.$$

(Note that, as a consequence of the classification of the finite simple groups, Schreier's conjecture has turned into a theorem. It states that $\mathrm{Out}(S)$ is solvable.) Observe that $(G/Z(G))^{(n)} = G^{(n)}Z(G)/Z(G)$ for all positive integers n. Hence, $(G/Z(G))^{(\infty)} = G^{(\infty)}Z(G)/Z(G) \cong G^{(\infty)}/(G^{(\infty)} \cap Z(G))$. Since $G^{(\infty)}$ is absolutely irreducible, using Schur's Lemma we get $G^{(\infty)} \cap Z(G) = Z(G^{(\infty)})$. It follows that $(G/Z(G))^{(\infty)} \cong G^{(\infty)}/Z(G^{(\infty)})$. Thus,

$$G^{(\infty)}/Z(G^{(\infty)}) \cong S,$$

and hence $G^{(\infty)}$ is quasi-simple.

12.1.2 Aim and scope

Recall that q is a power of the prime p. Let $\mathcal{V}$ be an $\mathbb{F}_q$-vector space of dimension $d \geq 1$. Recall from Definition 5.1 the notion of fat elements, ppd-elements and pppd-elements in $\mathrm{GL}(\mathcal{V})$. In [30], Guralnick, Penttila, Praeger, and Saxl describe all members of $\mathscr{S}$ containing ppd-elements. The relevant groups are conveniently listed according to their solvable residual. (Recall that the solvable residuals of groups contained in Aschbacher's $\mathscr{S}$-class are quasi-simple and that we can name all quasi-simple groups.) This is reasonable because a group G in $\mathscr{S}$ contains $\mathrm{ppd}(d, q; e)$-elements (for some $e > d/2$) if and only if $G^{(\infty)}$ contains $\mathrm{ppd}(d, q; e)$-elements. This fact relies on the following two observations. Firstly, a subgroup of $\mathrm{GL}(\mathcal{V})$ contains $\mathrm{ppd}(d, q; e)$-elements if and only if its order is divisible by a primitive prime divisor of $q^e - 1$. Secondly, the analysis carried out in [30] reveals that any primitive prime divisor r of $q^e - 1$, which divides the order of a group G in $\mathscr{S}$, also divides $|G^{(\infty)}|$.

DiMuro [21] expands the results given in [30] and, in a similar manner, describes all members of $\mathscr{S}$ which contain pppd-elements. Since (by Lemma 5.8) all pppd-elements, and hence also all ppd-elements, are fat, and since moreover (by Theorem 5.18 and Corollary 5.19)"most" fat elements are ppd-elements,

the classifications presented in [21, 30] suggest that we might also be able to specify all groups in $\mathscr{S}$ which contain fat elements. Recall from Definition 5.20 that we refer to a fat element in $\mathrm{GL}(\mathcal{V})$ which is not a pppd-element as an exceptional fat element. In light of [21,30] a classification of all members of $\mathscr{S}$ containing fat elements reduces to the following problem.

Problem 12.2. *Describe all groups in $\mathscr{S}$ containing exceptional fat elements.*

A plausible first step to solve Problem 12.2 is to

(∗) determine all quasi-simple groups in $\mathscr{S}$ containing exceptional fat elements.

After that we need to check if the existence of exceptional fat elements in members of $\mathscr{S}$ is equivalent to the existence of exceptional fat elements in their solvable residuals. Hence, the second step is to

(∗∗) determine all groups G in $\mathscr{S}$ such that G contains exceptional fat elements and $G^{(\infty)}$ does not contain any exceptional fat elements.

In this chapter we begin to tackle Step (∗). By proving Theorems 12.6 and 12.17 we settle Step (∗) for groups G in $\mathscr{S}$ which are a covering group of a sporadic simple group or a covering group of a finite simple linear/unitary/symplectic group in non-defining characteristic.

According to the classification theorem of the finite simple groups, the non-abelian finite simple groups can be found among the alternating groups, the finite simple (classical and exceptional) groups of Lie type, and the 26 sporadic simple groups. Thus, finding a complete solution to Problem 12.2 involves the following.

(1) Perform Step (∗) for all members G of $\mathscr{S}$ where G is a covering group of

   (*i*) an alternating group A_n, $n \geq 5$,

   (*ii*) a finite simple orthogonal group in non-defining characteristic,

   (*iii*) a finite simple classical (that is linear, symplectic, unitary, or orthogonal) group in defining characteristic,

   (*iv*) a finite simple exceptional group of Lie type.

(2) Perform Step (∗∗) for all members G of $\mathscr{S}$.

This remains the subject to future work.

12.1.3 Methods

Our analysis makes use of representation theory. A *representation* of a (finite) group H over $\mathbb{F}_q$ is a group homomorphism $\mathfrak{X} : H \to \mathrm{GL}(\mathcal{V})$, where $\mathcal{V}$ is a finite $\mathbb{F}_q$-vector space. The *degree* of $\mathfrak{X}$, written as $\deg(\mathfrak{X})$, is the dimension of $\mathcal{V}$. We say that $\mathfrak{X}$ is *trivial* if $\mathfrak{X}$ maps every element of H onto $\mathrm{id}_{\mathcal{V}}$. If $\mathfrak{X}$ is injective, then $\mathfrak{X}$ is said to be *faithful*. We call $\mathfrak{X}$ *irreducible*, *absolutely irreducible* or *realisable over a proper subfield* according as its image $\mathrm{im}(\mathfrak{X}) \leq \mathrm{GL}(\mathcal{V})$ has this property. For the definition of a *Brauer character* afforded by $\mathfrak{X}$ we refer to Isaacs' book [35].

Fix a finite vector space $\mathcal{V}$ over $\mathbb{F}_q$. In the two subsequent sections we mainly rule out the possibility that some given member G of the class $\mathscr{S}$ for $\mathrm{GL}(\mathcal{V})$ contains exceptional fat elements. The general idea of how we proceed is based on the approach taken in [30]. On the one hand we use (existing) results on the minimum degrees of absolutely irreducible, faithful representations of quasi-simple groups to obtain a lower bound for $\dim(\mathcal{V})$. Our sources here are [30–32,36,39,52]. On the other hand the assumption that G contains exceptional fat elements yields an upper bound for the dimension of $\mathcal{V}$. In order to derive such an upper bound, we apply our findings from Chapter 5 (more precisely Lemmas 5.6, 5.22, 5.23). If the lower and upper bounds on $\dim(\mathcal{V})$ conflict, then we have a proof that G does not contain any exceptional fat elements. Otherwise these bounds considerably narrow down the possibilities for $\dim(\mathcal{V})$ and hence also for G. In order to get a grip on the few remaining cases, it often helps to specify the size of q. This can be achieved by considering the irrationalities involved in the corresponding Brauer character. Our convention to denote these irrationalities follows the notation in [18]. The following lemma determines the value of q for the few cases that we consider in this chapter.

Occasionally, we use GAP [24] to perform certain calculations. For the most part, we do this without further explanation and refer the reader instead to the GAP manuals available at `https://www.gap-system.org/Doc/manuals.html`.

Lemma 12.3. *Let $\mathfrak{X}$ be an absolutely irreducible representation of a finite group H over $\mathbb{F}_q$. Suppose that $\mathfrak{X}$ is not realisable over a proper subfield, and let I be the set of all irrationalities involved in the Brauer character afforded by $\mathfrak{X}$. Then the following hold.*

(a) *If $p = 2$ and $I = \{z_3, b_{11}\}$, then $q = 4$.*

(b) *If $p = 2$ and $I = \{z_3, b_{17}, b_{19}\}$, then $q = 4$.*

(c) *If $p = 2$ and $I = \{b_7, i_{15}, b_{23}\}$, then $q = 2$.*

(d) *If $p = 3$ and $I = \{i_1, r_7\}$, then $q = 9$.*

(*e*) *If* $p = 5$ *and* $I = \{i_1\}$, *then* $q = 5$.

(*f*) *If* $p = 7$ *and* $I = \{i_1, r_{11}\}$, *then* $q = 49$.

(*g*) *If* $p \neq 3$ *and* $I = \{z_3\}$, *then* $q = \begin{cases} p, & \text{if } \mathrm{ord}(p;3) = 1, \\ p^2, & \text{else.} \end{cases}$

(*h*) *If* $p \neq 2, 5$ *and* $I = \{i_1, b_5\}$, *then* $q = \begin{cases} p, & \text{if } \mathrm{ord}(p;4) = 1 \text{ and} \\ & \quad \mathrm{ord}(p;5) \leq 2, \\ p^2, & \text{else.} \end{cases}$

(*i*) *If* $p \neq 3, 5$ *and* $I = \{z_3, b_5\}$, *then* $q = \begin{cases} p, & \text{if } \mathrm{ord}(p;3) = 1 \text{ and} \\ & \quad \mathrm{ord}(p;5) \leq 2, \\ p^2, & \text{else.} \end{cases}$

Proof. Since $\mathfrak{X}$ is not realisable over a proper subfield, by [35, Theorem 9.14] the field $\mathbb{F}_q$ is the extension of $\mathbb{F}_p$ obtained by adjoining the traces of all elements in $\mathrm{im}(\mathfrak{X})$. (If $\mathcal{V}$ is a finite vector space and $g \in \mathrm{GL}(\mathcal{V})$, then the *trace* of g is given by $\sum_{i=1}^{\dim(\mathcal{V})} \alpha_i$ where $\prod_{i=1}^{\dim(\mathcal{V})}(x - \alpha_i)$ is the characteristic polynomial of g.) For a concrete value of p we calculate q in GAP [24] by calling

```
gap> SizeOfFieldOfDefinition(irrat,p);
```

where `irrat` is the list of all irrationalities contained in the set I, for example `[AtlasIrrationality("z3"),AtlasIrrationality("b11")]` in (*a*). This verifies (*a*)–(*f*). In the remaining cases we proceed as follows.

(*i*) We first determine the minimal polynomial m_α over $\mathbb{Q}$ of each irrationality $\alpha \in I$. The polynomials which are relevant here are listed in [10, Table 4.2]. We get $\deg(m_\alpha) \leq 2$ for all $\alpha \in I$. (Note that all elements in I are algebraic integers, that is $m_\alpha \in \mathbb{Z}[x]$ for all $\alpha \in I$.)

(*ii*) Next, we interpret the polynomials $m_\alpha, \alpha \in I$ as polynomials over $\mathbb{F}_p$ by reducing their coefficients modulo p.

(*iii*) If the p-modular reductions of all m_α ($\alpha \in I$) split over $\mathbb{F}_p$ in linear factors, then $q = p$. Otherwise $q = p^2$. (Whether the p-modular reductions of m_α, $\alpha \in I$, split into linear factors can be read off [10, Table 4.2].) □

12.2 Covering groups of the sporadic simple groups

This section examines the existence of exceptional fat elements in members G of Aschbacher's $\mathscr{S}$-class (see Definition 12.1) satisfying $S \leq G/Z(G) \leq \mathrm{Aut}(S)$ for some sporadic simple group S.

There is, up to isomorphism, a total of 47 covering groups of the sporadic simple groups. (Note that a sporadic simple group is a covering group of itself.) Adopting standard notation from [18], a list of these groups reads as follows.

M_{11}, M_{12}, $2.\mathrm{M}_{12}$, M_{22}, $2.\mathrm{M}_{22}$, $3.\mathrm{M}_{22}$, $4.\mathrm{M}_{22}$, $6.\mathrm{M}_{22}$, $12.\mathrm{M}_{22}$, M_{23}, M_{24}, J_1, J_2, $2.\mathrm{J}_2$, J_3, $3.\mathrm{J}_3$, J_4, HS, 2.HS, McL, 3.McL, He, Ru, 2.Ru, Suz, 2.Suz, 3.Suz, 6.Suz, O′N, 3.O′N, Co_1, $2.\mathrm{Co}_1$, Co_2, Co_3, Fi_{22}, $2.\mathrm{Fi}_{22}$, $3.\mathrm{Fi}_{22}$, $6.\mathrm{Fi}_{22}$, F_{23}, F_3+, $3.\mathrm{F}_3+$, HN, Ly, Th, B, 2.B, M.

The orders of elements in these groups are known and are available for example in GAP [24]. In order to access them we call

```
gap> ct := CharacterTable("name");;
gap> AsSet(OrdersClassRepresentatives(ct));
```

where `name` is the name of the respective group, for example `M11` or `2.Co1`. We use this information throughout this section without further reference.

Recall from Section 2.1 the definition of the Carmichael function $\lambda : \mathbb{N} \to \mathbb{N}$. Recall further (from Definition 5.20) that the term fat$^*(d, q; e)$-*element* is an abbreviation and means an *exceptional* fat$(d, q; e)$-*element*.

Lemma 12.4. *Let H be one of the groups given in Table 12.1, and let $\mathfrak{X}$ be a faithful representation of H over $\mathbb{F}_q$. Let $d = \deg(\mathfrak{X})$ and let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Then* $\mathrm{im}(\mathfrak{X})$ *does not contain any* fat$^*(d, q; e)$*-elements.*

Proof. Let $\lambda_{\max}$ be the maximal value for $\lambda(|h|)$, where h runs over all elements in $H \cong \mathrm{im}(\mathfrak{X})$ such that $|h| \notin \{1, 12, 15, 20, 24, 30, 40, 48, 51, 60, 68\}$ and such that neither $|h|$ nor $|h|/2$ is a prime power. If no such $h \in H$ exists, then we set $\lambda_{\max} = 0$. Let $d_{\min}$ be the minimal value among the degrees of all faithful representations of H over some finite field. According to our assumption, we have $d \geq d_{\min}$. We calculate $\lambda_{\max}$ (see Remark 2.5), read off $d_{\min}$ from [36, Table 1], and collect these values in Table 12.1. Observe that $d_{\min} \geq 2\lambda_{\max}$, whence

$$2\lambda_{\max} \leq d.$$

Seeking a contradiction, suppose that $\mathrm{im}(\mathfrak{X})$ contains a fat$^*(d, q; e)$-element, say g. Since g is fat, from Lemma 5.6 we obtain

$$d < 2\lambda(|g|).$$

H	M_{11}	M_{12}	$2.\mathrm{M}_{12}$	J_1	M_{22}	$2.\mathrm{M}_{22}$	$6.\mathrm{M}_{22}$	$12.\mathrm{M}_{22}$
$\lambda_{\max}$	0	0	0	0	0	0	10	10
$d_{\min}$	5	10	6	7	10	10	36	24
H	J_2	$2.\mathrm{J}_2$	M_{23}	HS	2.HS	J_3	McL	3.McL
$\lambda_{\max}$	0	0	0	0	0	0	0	10
$d_{\min}$	6	6	11	20	28	18	21	45
H	He	Ru	2.Ru	Suz	2.Suz	O′N	Co_3	Co_2
$\lambda_{\max}$	6	0	12	6	6	6	6	6
$d_{\min}$	50	28	28	64	12	154	22	22
H	Fi_{22}	$2.\mathrm{Fi}_{22}$	$3.\mathrm{Fi}_{22}$	$6.\mathrm{Fi}_{22}$	HN	Ly	Th	Fi_{23}
$\lambda_{\max}$	6	6	12	12	12	10	12	12
$d_{\min}$	77	176	27	1728	132	111	248	253
H	Co_1	$2.\mathrm{Co}_1$	J_4	F_{3+}	$3.\mathrm{F}_{3+}$	B	2.B	M
$\lambda_{\max}$	12	12	12	12	28	20	20	48
$d_{\min}$	24	24	112	781	783	4370	96256	196882

Table 12.1: Covering groups of the sporadic simple groups ruled out in Lemma 12.4

Since g is an exceptional fat element, according to Lemma 5.22(a) the order of g is not contained in $\{1, 12, 15, 20, 24, 30, 40, 48, 51, 60, 68\}$, and moreover, neither $|g|$ nor $|g|/2$ are prime powers. Hence, $\lambda(|g|) \le \lambda_{\max}$, which (recalling that $d < 2\lambda(|g|)$ and $2\lambda_{\max} \le d$) yields the contradiction $d < 2\lambda_{\max} \le d$. □

Lemma 12.5. *Let $H \in \{3.\mathrm{M}_{22}, 4.\mathrm{M}_{22}, 3.\mathrm{Suz}, 6.\mathrm{Suz}, 3.\mathrm{O'N}, 3.\mathrm{J}_3\}$ and let $\mathfrak{X}$ be an absolutely irreducible, faithful representation of H over $\mathbb{F}_q$ which is not realisable over a proper subfield. Let $d = \deg(\mathfrak{X})$, and let $e \in \mathbb{N}$ be such that $d/2 < e \le d$. Then $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d, q; e)$-elements.*

Proof. Let I be the set of all irrationalities involved in the Brauer character afforded by $\mathfrak{X}$. Seeking a contradiction, suppose that $g \in \mathrm{im}(\mathfrak{X})$ is a $\mathrm{fat}^*(d, q; e)$-element. By applying Lemma 5.22(a) we narrow down the possibilities for $|g|$. The outcome, along with an upper bound for $\lambda(|g|)$, is listed in Table 12.2. From Lemma 5.6 we get $d < 2\lambda(|g|)$. Using this inequality, we extract from [31, 32] the possibilities for d, p, I, and then determine the size of q by applying Lemma 12.3. We specify d, p, I, and q in Table 12.2.

If $q = p^2$, then we obtain a contradiction, as by Lemma 5.22(b) the order of g is then not contained in $\{21, 28, 33, 39, 42, 44, 57, 66, 78, 84, 93\}$. Hence, $q = p$. Then $H \in \{6.\mathrm{Suz}, 3.\mathrm{O'N}, 3.\mathrm{J}_3\}$ and

$$\mathrm{ord}(q; 3) = 1.$$

H	$3.\mathrm{M}_{22}$	$4.\mathrm{M}_{22}$	$3.\mathrm{Suz}$
$\lvert g\rvert$	$21, 33$	$28, 44$	$21, 33, 39, 42$
$\lambda(\lvert g\rvert)$	≤ 10	≤ 10	≤ 12
d	$6, 15$	16	12
p	2	7	2
I	$\{z_3, b_{11}\}$	$\{i_1, r_{11}\}$	z_3
q	4	49	4

H	$6.\mathrm{Suz}$	$3.\mathrm{O'N}$
$\lvert g\rvert$	$21, 28, 33, 39, 42, 66, 78, 84$	$21, 28, 33, 42, 57, 84, 93$
$\lambda(\lvert g\rvert)$	≤ 12	≤ 30
d	12	45
p	$\neq 2, 3$	7
I	$\{z_3\}$	$\emptyset$
q	$\begin{cases} p, & \text{if } \mathrm{ord}(p;3) = 1, \\ p^2, & \text{else.} \end{cases}$	7

H	$3.\mathrm{J}_3$	$3.\mathrm{J}_3$	$3.\mathrm{J}_3$
$\lvert g\rvert$	57	57	57
$\lambda(\lvert g\rvert)$	18	18	18
d	9	18	18
p	2	5	$\neq 3, 5$
I	$\{z_3, b_{17}, b_{19}\}$	$\{z_3\}$	$\{z_3, b_5\}$
q	4	25	$\begin{cases} p, & \text{if } \mathrm{ord}(p;3) = 1 \\ & \text{and } \mathrm{ord}(p;5) \leq 2, \\ p^2, & \text{else.} \end{cases}$

Table 12.2: Covering groups of the sporadic simple groups ruled out in Lemma 12.5

Since g is a $\mathrm{fat}(d, q; e)$-element, by Lemma 5.6 we have $\lambda(|g|) > d/2$, and thus

$$|g| \in \{33, 39, 57, 66, 78, 93\}.$$

By Lemma 5.4 the order of g is divisible by a primitive divisor of $q^e - 1$. If some primitive divisor of $q^e - 1$ which divides $|g|$ is a prime power, then g is a $\mathrm{pppd}(d, q; e)$-element, which is assumed not the case. Hence, each primitive divisor of $q^e - 1$ dividing $|g|$ is divisible by at least two distinct primes. Take r to be a minimal such divisor (see Definition 2.25.) From Lemma 2.28(a) we know that r is either odd or divisible by 4. It follows that $r \in \{33, 39, 57, 93\}$ and, in particular, $3 \mid r$ and $\gcd(3, r/3) = 1$. Since $\mathrm{ord}(q; 3) = 1$ divides $\mathrm{ord}(q; r/3)$, by Lemma 2.27 (applied to $a = q$, $m = e$, r and $r' = 3$) r is not a minimal primitive divisor of $q^e - 1$, which is not true. □

Theorem 12.6. *Let H be a covering group of a sporadic simple group. Let $\mathfrak{X}$ be an absolutely irreducible, faithful representation of H over $\mathbb{F}_q$ which is not realisable over a proper subfield. Let $d = \deg(\mathfrak{X})$, and let e be an integer satisfying $d/2 < e \leq d$.*

(*a*) *If $H \neq \mathrm{M}_{24}$ or $d \neq 11$, then $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d, q; e)$-elements.*

(*b*) *If $H = \mathrm{M}_{24}$ and $d = 11$, then the following hold.*

(*i*) *We have $q = 2$.*

(*ii*) *The group $\mathrm{im}(\mathfrak{X})$ contains $\mathrm{fat}^*(11, 2; e)$-elements if and only if $e = 6$.*

(*iii*) *An element $g \in \mathrm{im}(\mathfrak{X})$ is a $\mathrm{fat}^*(11, 2; 6)$-element if and only if $|g| = 21$.*

Proof. If $H \neq \mathrm{M}_{24}$, then H is one of the 46 groups listed in Tables 12.1, 12.2, and by Lemmas 12.4, 12.5 the group $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d, q; e)$-elements.

Hence, assume that $H = \mathrm{M}_{24}$. Consider $g \in \mathrm{im}(\mathfrak{X})$ and suppose that g is a $\mathrm{fat}^*(d, q; e)$-element. Then by Lemma 5.22(*a*) we get $|g| = 21$. Using [31, 32] and the inequality $d < 2\lambda(|g|) = 12$ given in Lemma 5.6 we see that $d = 11$, $p = 2$, and that the Brauer character afforded by $\mathfrak{X}$ involves the irrationalities b_7, i_{15} and b_{23}. Then by Lemma 12.3(*c*) we have $q = 2$. Since g is a $\mathrm{fat}(11, 2; e)$-element of order 21, by Lemma 5.4 there exists a divisor r of 21 satisfying $\mathrm{ord}(2; r) = e$. Since $e > 11/5$ and $\mathrm{ord}(2; 3) = 2$, $\mathrm{ord}(2; 7) = 3$, we conclude that $e = \mathrm{ord}(2; 21) = 6$.

In order to complete the proof it remains to show that any element of order 21 in $\mathrm{im}(\mathfrak{X})$ is a $\mathrm{fat}^*(11, 2; 6)$-element. Let $h \in \mathrm{im}(\mathfrak{X})$ with $|h| = 21$. The characteristic polynomial of h can be recovered from the Brauer character. We do this in GAP [24]. Let `chi` be the Brauer character (in GAP) afforded by $\mathfrak{X}$ and let `class` be a positive integer such that (in GAP) h is contained in the `class`-th conjugacy class. Then by calling

```
gap> ct := CharacterTable("M24") mod 2;;
gap> ev := EigenvaluesChar(chi,class);;
gap> x := X(GF(2));;
gap> pol := 1;;
gap> for i in [1..21] do
> pol := pol*(x-FrobeniusCharacterValue(E(21)^i,2))^ev[i];
> od;
gap> pol;
```

we obtain the characteristic polynomial of h, which is one of the following.

(The right hand-side specifies the respective irreducible factors over $\mathbb{F}_2$.)

$$x^{11}+x^8+x^7+x^2+1=(x^2+x+1)(x^3+x+1)(x^6+x^5+x^4+x^2+1),$$
$$x^{11}+x^9+x^4+x^3+1=(x^2+x+1)(x^3+x^2+1)(x^6+x^4+x^2+x+1).$$

Thus, by Lemma 5.2, h is a $\mathrm{fat}(11,2;6)$-element. Since $\mathrm{ord}(2;7),\mathrm{ord}(2;3)<6$, h is not a $\mathrm{pppd}(11,2;6)$-element, and hence a $\mathrm{fat}^*(11,2;6)$-element. □

12.3 Some quasi-simple Lie type groups in non-defining characteristic

Let $n,m,s\in\mathbb{N}$ be such that $n\geq 2$ and s is a prime power. Following the notation used in [18], we write $\mathrm{L}_n(s),\mathrm{U}_n(s)$, and $\mathrm{S}_{2m}(s)$ for the quotient of the special linear group $\mathrm{SL}(n,s)$, the special unitary group $\mathrm{SU}(n,s)$, and respectively the symplectic group $\mathrm{Sp}(2m,s)$, by its centre, that is by the scalar matrices contained in the respective group. With the exceptions of

$$\mathrm{L}_2(2)\cong\mathrm{U}_2(2)\cong\mathrm{S}_2(2),\quad \mathrm{L}_2(3)\cong\mathrm{U}(2,3)\cong\mathrm{S}_2(3),\quad \mathrm{U}(3,2),\quad \mathrm{S}_4(2)$$

the groups $\mathrm{L}_n(s),\mathrm{U}_n(s)$, and $\mathrm{S}_{2m}(s)$ are simple. This section is concerned with exceptional fat elements in covering groups of these simple groups.

12.3.1 Element orders

Our approach requires information on element orders in the special linear group, the special unitary group, and the symplectic group. To this end we apply and modify results from [12,13] such that they meet our needs.

Lemma 12.7. *Let $n\geq 2$ be an integer and let s be a power of the prime t. Let $g\in\mathrm{SL}(n,s)$.*

(a) If $n=2$, then $|g|$ divides $s+1$, or $s-1$, or $2t$.

(b) If $n\geq 3$, then $|g|\leq(s^n-1)/(s-1)$.

Proof. For $n=2$ the assertion follows directly from [12, Corollary 1]. The case $n\geq 3$ holds by [19, Theorem 1] (or can be alternatively also derived from [12, Corollary 1]). □

Our bounds on element orders in $\mathrm{SU}(n,s)$, and $\mathrm{Sp}(2m,s)$ require two preliminary results.

Lemma 12.8. *Let a, b, s be positive integers. If $s \geq 2$, then*

$$\frac{\left(s^a - (-1)^a\right)\left(s^b - (-1)^b\right)}{s+1} \leq s^{a+b-1} - (-1)^{a+b-1}.$$

Proof. We may assume that $a \geq b$. Let

$$\alpha = \frac{\left(s^a - (-1)^a\right)\left(s^b - (-1)^b\right)}{s+1}.$$

If $b = 1$, then $\alpha = s^a - (-1)^a = s^{a+b-1} - (-1)^{a+b-1}$, as asserted. So, suppose that $b \geq 2$. Note that $s^b - (-1)^b$ is divisible by $s+1$. More precisely, we have

$$\frac{s^b - (-1)^b}{s+1} = \sum_{i=0}^{b-1} (-1)^{b-1-i} s^i.$$

Hence,

$$\begin{aligned}
\alpha &= \sum_{i=0}^{b-1} (-1)^{b-1-i} s^{a+i} - \sum_{i=0}^{b-1} (-1)^{a+b-1-i} s^i \\
&= \left(\sum_{i=0}^{b-3} (-1)^{b-1-i} s^{a+i} - s^{a+b-2} + s^{a+b-1} \right) - \left(\sum_{i=1}^{b-1} (-1)^{a+b-1-i} s^i + (-1)^{a+b-1} \right) \\
&\leq \sum_{i=0}^{b-3} s^{a+i} + \sum_{i=1}^{b-1} s^i + s^{a+b-1} - s^{a+b-2} - (-1)^{a+b-1} \\
&= \underbrace{\sum_{i=a}^{a+b-3} s^i + \sum_{i=1}^{b-1} s^i}_{=\beta} + s^{a+b-1} - s^{a+b-2} - (-1)^{a+b-1}. \qquad (12.1)
\end{aligned}$$

Let $\beta = \sum_{i=a}^{a+b-3} s^i + \sum_{i=1}^{b-1} s^i$. Since $b \leq a$, we get

$$\beta \leq \sum_{i=1}^{a+b-3} s^i = s^{a+b-3} \sum_{i=1}^{a+b-3} s^{i-a-b+3} = s^{a+b-3} \sum_{i=0}^{a+b-4} s^{-1},$$

and thus

$$\beta < s^{a+b-3} \sum_{i=0}^{\infty} s^{-i} = s^{a+b-3} \frac{1}{1 - s^{-1}} = \frac{s^{a+b-2}}{s-1} \leq s^{a+b-2}.$$

Combining this upper bound on β with (12.1) shows that

$$\alpha < s^{a+b-2} + s^{a+b-1} - s^{a+b-2} - (-1)^{a+b-1} = s^{a+b-1} - (-1)^{a+b-1},$$

as required. □

Lemma 12.9. *Let $n, s, k, n_1, \dots, n_k \in \mathbb{N}$ be such that $n, s, k \geq 2$, $\sum_{i=1}^{k} n_i = n$.*

(*a*) *We have* $\operatorname{lcm}\{s^{n_1} - (-1)^{n_1}, \dots, s^{n_k} - (-1)^{n_k}\} \leq s^{n-k+1} - (-1)^{n-k+1}$.

(*b*) [29, Lemma 2.9] *Suppose that s is a prime power. Then*

$$\operatorname{lcm}\{s^{n_1} \pm 1, \dots, s^{n_k} \pm 1\} \leq \begin{cases} \dfrac{s^{n+1}}{s-1}, & \text{if } s \text{ is even,} \\ \dfrac{s^{n+1}}{2(s-1)}, & \text{if } s \text{ is odd.} \end{cases}$$

Proof. Assertion (*b*) is shown in [29, Lemma 2.9]. We only prove assertion (*a*) (which is a refinement of [29, Lemma 2.13]). Note that $s+1$ divides $s^{n_i} - (-1)^{n_i}$ for all $i \in \{1, \dots, k\}$. We argue by induction on k. If $k = 2$, then

$$\operatorname{lcm}\{s^{n_1} - (-1)^{n_1}, s^{n_2} - (-1)^{n_2}\} \mid \frac{(s^{n_1} - (-1)^{n_1})\,(s^{n_2} - (-1)^{n_2})}{s+1},$$

and the assertion holds by Lemma 12.8. Next, assuming that the assertion holds for $k-1$, we consider $\operatorname{lcm}_{i=1}^{k}\{s^{n_i} - (-1)^{n_i}\}$. Since $\operatorname{lcm}_{i=1}^{k-1}\{s^{n_i} - (-1)^{n_i}\}$ and $s^{n_k} - (-1)^{n_k}$ are both divisible by $s+1$, and since $\operatorname{lcm}_{i=1}^{k}\{s^{n_i} - (-1)^{n_i}\} = \operatorname{lcm}\{\operatorname{lcm}_{i=1}^{k-1}\{s^{n_i} - (-1)^{n_i}\}, s^{n_k} - (-1)^{n_k}\}$ we have

$$\operatorname{lcm}_{i=1}^{k}\{s^{n_i} - (-1)^{n_i}\} \mid \frac{\operatorname{lcm}_{i=1}^{k-1}\{s^{n_i} - (-1)^{n_i}\}\,(s^{n_k} - (-1)^{n_k})}{s+1}.$$

Now, by induction, $\operatorname{lcm}_{i=1}^{k-1}\{s^{n_i} - (-1)^{n_i}\} \leq s^{n_1+\cdots+n_{k-1}-k+2} - (-1)^{n_1+\cdots+n_{k-1}-k+2}$, and hence

$$\operatorname{lcm}_{i=1}^{k}\{s^{n_i} - (-1)^{n_i}\} \leq \frac{(s^{n_1+\cdots+n_{k-1}-k+2} - (-1)^{n_1+\cdots+n_{k-1}-k+2})(s^{n_k} - (-1)^{n_k})}{s+1}.$$

Then Lemma 12.8 yields $\operatorname{lcm}_{i=1}^{k}\{s^{n_i} - (-1)^{n_i}\} \leq s^{n-k+1} - (-1)^{n-k+1}$. □

Lemma 12.10. *Let $n \geq 3$ be an integer and let s be a power of the prime t. Suppose that $(n, s) \notin \{(3, 2), (4, 3)\}$ and let $g \in \mathrm{SU}(n, s)$.*

(*a*) *If $t \nmid |g|$, then either there exist $n_1, n_2 \in \mathbb{N}$ such that $n_1 + n_2 = n$ and $|g|$ divides $\operatorname{lcm}\{s^{n_1} - (-1)^{n_1}, s^{n_2} - (-1)^{n_2}\}$, or $|g| \leq (s^n - (-1)^n)/(s+1)$.*

(*b*) *If t divides $|g|$, then* $|g| \leq \begin{cases} t(s^{n-2}+2), & \text{if } s = t = 2 \text{ and } n \text{ is even,} \\ t(s^{n-2}+1), & \text{else.} \end{cases}$

Proof. By [12, Corollary 1], one of the following cases holds.

(*i*) The order of g divides $(s^n-(-1)^n)/(s+1)$.

(*ii*) The order of g divides $\operatorname{lcm}\{s^{n_1}-(-1)^{n_1},\dots,s^{n_k}-(-1)^{n_k}\}$, where $k\geq 2$ and $n_1\dots,n_k\in\mathbb{N}$ satisfy $\sum_{i=1}^k n_i=n$.

(*iii*) The order of g divides $t^\ell(s^{n'}-(-1)^{n'})/\gcd(n,s+1,n')$ for some $\ell,n'\in\mathbb{N}$ satisfying $t^{\ell-1}+1+n'=n$.

(*iv*) The order of g divides $t^\ell\operatorname{lcm}\{s^{n_1}-(-1)^{n_1},\dots,s^{n_k}-(-1)^{n_k}\}$, where $k\geq 2$ and $\ell,n_1,\dots,n_k\in\mathbb{N}$ satisfy $t^{\ell-1}+1+\sum_{i=1}^k n_i=n$.

(*v*) The order of g divides $t^\ell\gcd(n,s+1)$ for some $\ell\in\mathbb{N}$ such that $t^{\ell-1}+1=n$.

(*vi*) The order of g divides $t(s-1)\gcd(2,s-1)$ and $n=4$.

We first prove assertion (*a*). So, assume that t does not divide $|g|$. In case (*i*), and in case (*ii*) with $k=2$, there is nothing to show. In the remaining cases, (using Lemma 12.9(*a*) in case (*ii*) with $k\geq 3$, as well as in case (*iv*)) we obtain

$$|g|\leq s^{n-2}-(-1)^{n-2}=\frac{s^{n-1}+s^{n-2}-(-1)^n s-(-1)^n}{s+1}.$$

Recalling that $s\geq 2$ and $n\geq 3$, it follows that

$$|g|\leq\left(\frac{s^n}{2}+\frac{s^n}{4}+\frac{s^n}{2^{n-1}}-(-1)^n\right)(s+1)^{-1}\leq\frac{s^n-(-1)^n}{s+1}.$$

In order to prove assertion (*b*), assume that t divides $|g|$. Cases (*i*) and (*ii*) do not occur. Suppose that case (*iii*) holds. Then, for some $\ell\in\mathbb{N}$, we have

$$|g|\leq t^\ell\left(s^{n-1-t^{\ell-1}}-(-1)^{n-1-t^{\ell-1}}\right).$$

Observe that $t^{\ell-1}\geq\ell+1$ for $\ell\geq 3$. Hence,

$$\begin{aligned}|g|&\leq\begin{cases}t(s^{n-2}+1), & \text{if } \ell=1,\\ t^2(s^{n-3}+1)=t(s^{n-2}+2), & \text{if } \ell=2,\ s=t=2,\ n \text{ even},\\ t^2(s^{n-3}+1)=t(2s^{n-3}+2)<ts^{n-2}, & \text{if } \ell=2,\ s>t=2,\ n \text{ even},\\ t^2(s^{n-3}-1)\leq t(s^{n-2}-2), & \text{if } \ell=t=2,\ n \text{ odd},\\ t^2(s^{n-4}+1)<t^2s^{n-3}\leq ts^{n-2}, & \text{if } \ell=2,\ t\geq 3,\\ t^\ell s^{n-t^{\ell-1}}\leq t^\ell s^{n-\ell-1}\leq ts^{n-2}, & \text{if } \ell\geq 3,\end{cases}\\ &\leq\begin{cases}t(s^{n-2}+2), & \text{if } s=t=2,\ n \text{ even},\\ t(s^{n-2}+1), & \text{else},\end{cases}\end{aligned}$$

as needed. Next, suppose that case (*iv*) holds. Note that $t^{\ell-1}\geq\ell$. Since $k\geq 2$ (and hence $-k+1\leq -1$), using Lemma 12.9(*a*) it follows that

$$|g|\leq t^\ell\left(s^{n_1+\cdots+n_k-1}+1\right)<t^\ell s^{n_1+\cdots+n_k}=t^\ell s^{n-1-t^{\ell-1}}\leq t^\ell s^{n-1-\ell}\leq ts^{n-2}.$$

Suppose that case (v) holds. If $n = 3$, then $t^{\ell-1} = 2$, that is $t = \ell = 2$, and (recalling that $s \neq 2$, whence $s \geq 4$) we get

$$|g| \leq t^2 \gcd(3, s+1) \leq \left\{ \begin{array}{ll} t^2, & \text{if } s = t^2 \\ 3t^2, & \text{if } s \geq t^3 \end{array} \right\} \leq s < ts^{n-2}.$$

If $n = 4$, then $t^{\ell-1} = 3$, that is $t = 3$ and $\ell = 2$, and (recalling that $s \neq 3$, whence $s \geq 9$) we obtain

$$|g| \leq t^2 \gcd(4, s+1) \leq \left\{ \begin{array}{ll} 2t^2, & \text{if } s = t^2 \\ 4t^2, & \text{if } s \geq t^3 \end{array} \right\} < ts = ts^{n-3}.$$

If $n = 5$, then $t^{\ell-1} = 4$, that is $t = 2$ and $\ell = 3$, and we have

$$|g| \leq t^3 \gcd(5, s+1) \leq \left\{ \begin{array}{ll} t^3, & \text{if } s = t \\ 5t^3, & \text{if } s \geq t^2 \end{array} \right\} \leq s^3 < ts^{n-2}.$$

If $n = 6$, then $t^{\ell-1} = 5$, that is $t = 5$ and $\ell = 2$, and we get

$$|g| \leq t^2(s+1) < ts^3 = ts^{n-3}.$$

If $n = 7$, then $t^{\ell-1} = 6$ is not a prime power, so this case does not occur. Suppose that $n \geq 8$. Note that $n(n-1) < 2^{n-2}$. Now, since (by assumption) $t^{\ell-1} + 1 = n$ we have $t^\ell = t(n-1)$, and it follows that

$$|g| \leq t^\ell \gcd(n, s+1) \leq t(n-1)n < t2^{n-2} \leq ts^{n-2}.$$

Finally, suppose that case (vi) holds. Then $|g| \leq t(s-1)^2 < ts^2 = ts^{n-2}$. □

Lemma 12.11. *Let $m \geq 2$ be an integer and let s be a power of the prime t. Let $g \in \mathrm{Sp}(2m, s)$.*

(a) If $t = 2$, then $|g| \leq s^{m+1}/(s-1)$.

(b) If $t \neq 2$, then one of the following hold.

- *(i) The order of g divides $2t^\ell$, where $\ell \in \mathbb{N}$ such that $\ell \geq 2$, $t^{\ell-1}+1 = 2m$.*
- *(ii) The order of g divides $t^m + t$, and $s = t$.*
- *(iii) The order of g divides $t^m + t^2$, and $s = t = 3$.*
- *(iv) The order of g divides an even integer less than or equal to $s^m + 1$.*

Proof. (a) Assume that $t = 2$. According to [13, Corollary 3], one of the following holds.

(1) The order of g divides $2^\ell \operatorname{lcm}\{s^{m_1} \pm 1, \dots, s^{m_k} \pm 1\}$, where ℓ is a non-negative integer, $k \geq 1$, and $m_1, \dots, m_k \in \mathbb{N}$ satisfy

$$m = \sum_{i=1}^{k} m_i + \begin{cases} \ell, & \text{if } \ell \in \{0, 1\}, \\ 2^{\ell-2} + 1, & \text{if } \ell \geq 2. \end{cases}$$

(2) The order of g divides 2^ℓ where $\ell \geq 2$ and $2^{\ell-2} + 1 = m$.

Suppose that we are in case (1). Then by Lemma 12.9(b) we have

$$|g| \leq \frac{2^\ell s^\alpha}{s-1} \leq \frac{s^{\ell+\alpha}}{s-1}, \quad \alpha = \begin{cases} m - \ell + 1, & \text{if } \ell \in \{0, 1\}, \\ m - 2^{\ell-2}, & \text{if } \ell \geq 2. \end{cases}$$

For $\ell \in \{0, 1\}$ the assertion follows immediately. In order to see that our assertion also holds for $\ell \geq 2$, observe that $\ell \leq 2^{\ell-2} + 1$.

Suppose that we are in case (2). Then $|g|$ divides $4(m-1)$. If $m = 2$, then $|g| \leq 4(m-1) = 4 \leq s^2 < s^3/(s-1)$, as needed. If $m \geq 3$, then $|g| \leq 4(m-1) \leq s^m < s^{m+1}/(s-1)$.

(b) Assume that t is an odd prime. Then by [13, Corollary 1] the order of g either satisfies condition (i) in the assertion above (in which case there is nothing to prove), or $|g|$ divides

$$\beta = t^\ell \operatorname{lcm}\{s^{m_1} \pm 1, \dots, s^{m_k} \pm 1\},$$

where ℓ is a non-negative integer, $k, m_1, \dots, m_k$ are positive integers, and

$$m = \sum_{i=1}^{k} m_i + \begin{cases} 0, & \text{if } \ell = 0, \\ (t^{\ell-1} + 1)/2, & \text{if } \ell \geq 1. \end{cases}$$

Note that β is even. We distinguish between four cases

Case $k \geq 2$: One can quickly verify that $\sum_{i=1}^{k} m_i \leq m - \ell$. Then by Lemma 12.9($b$) we get

$$\beta \leq \frac{t^\ell s^{m-\ell+1}}{2(s-1)} \leq \frac{s^{m+1}}{2(s-1)},$$

which (using $s/(2(s-1)) < 1$) shows that $\beta < s^m$. Hence, $|g|$ satisfies condition (iv) in the assertion.

Case $k = 1$ and $\ell = 0$: We have $\beta = s^m \pm 1$, whence $|g|$ satisfies condition (iv) in the assertion.

Case $k = 1$ and $\ell \in \{1, 2\}$: We have $\beta = t^\ell(s^{m-(t^{\ell-1}+1)/2} + \epsilon)$ for some $\epsilon \in \{-1, 1\}$. Then

$$\beta = \begin{cases} t^m + t, & \text{if } \epsilon = 1, \ell = 1, s = t, \\ t^m + t^2, & \text{if } \epsilon = 1, \ell = 2, s = t = 3, \end{cases}$$

and in these cases $|g|$ satisfies condition (ii), and respectively condition (iii), in the assertion. Further, (noting that $m \geq 4$, if $\ell = 2$ and $t \geq 5$) we have

$$\begin{aligned} \beta &\leq \begin{cases} t(s^{m-1} + 1) \leq s(s^{m-1} + 1)/3, & \text{if } \epsilon = 1, \ell = 1, s \neq t, \\ t^2(s^{m-2} + 1) \leq s^2(s^{m-2} + 1)/9, & \text{if } \epsilon = 1, \ell = 2, s > t = 3, \\ t^2(s^{m-3} + 1) \leq s^{m-1} + s^2 & \\ \quad \leq s^{m-1} + s^{m-2}, & \text{if } \epsilon = 1, \ell = 2, t \geq 5, \\ t(s^{m-1} - 1) \leq s^m - s, & \text{if } \epsilon = -1, \ell = 1, \\ t^2(s^{m-2} - 1) \leq s^m - s^2, & \text{if } \epsilon = -1, \ell = 2, \end{cases} \\ &< s^m, \end{aligned}$$

and in these cases $|g|$ satisfies condition (iv).

Case $k = 1$ and $\ell \geq 3$: Observe that

$$m_1 = m - \frac{t^{\ell-1} + 1}{2} \leq m - \frac{3^{\ell-1} + 1}{2}.$$

Since $\ell \geq 3$ one can check that $(3^{\ell-1} + 1)/2 \geq \ell + 2$, which is why $m_1 \leq m - \ell - 2$. (This implies that $\ell \leq m - 3$.) Recalling that $\beta = t^\ell(s^{m_1} \pm 1)$ it follows that

$$\beta \leq t^\ell(s^{m-\ell-2} + 1) \leq s^{m-2} + s^\ell \leq s^{m-2} + s^{m-3} < s^m.$$

Hence, $|g|$ satisfies condition (iv) in the assertion, and the proof is complete. □

12.3.2 Ruling out exceptional fat elements

In small dimensions two finite Lie type groups may be isomorphic, yet have different defining characteristics. This happens for example for $\mathrm{L}_2(4) \cong \mathrm{L}_2(5)$ or $\mathrm{L}_3(2) \cong \mathrm{L}_2(7)$. (A complete list of such exceptional isomorphisms is given in [38, Proposition 2.9.1].) In what follows, the defining characteristic of a given Lie type group always means the defining characteristic of the group as written down in the text.

Recall that q is a power of the prime p.

H	$\mathrm{L}_2(4)$	$2.\mathrm{L}_2(4)$	$\mathrm{L}_2(9)$	$2.\mathrm{L}_2(9)$	$3.\mathrm{L}_2(9)$	$6.\mathrm{L}_2(9)$
$\lambda_{\max}$	0	0	0	0	0	0
$d_{\min}$	3	2	4	4	3	6
H	$\mathrm{L}_3(2)$	$2.\mathrm{L}_3(2)$	$\mathrm{L}_3(4)$	$2.\mathrm{L}_3(4)$	$3.\mathrm{L}_3(4)$	$12_1.\mathrm{L}_3(4)$
$\lambda_{\max}$	0	0	0	0	6	6
$d_{\min}$	3	2	15	6	15	24
H	$12_2.\mathrm{L}_3(4)$	$\mathrm{L}_4(2)$	$2.\mathrm{L}_4(2)$	$\mathrm{L}_4(3)$	$2.\mathrm{L}_4(3)$	$\mathrm{U}_4(2)$
$\lambda_{\max}$	6	0	0	0	0	0
$d_{\min}$	12	7	8	26	40	5
H	$2.\mathrm{U}_4(2)$	$\mathrm{U}_4(3)$	$2.\mathrm{U}_4(3)$	$3_2.\mathrm{U}_4(3)$	$4.\mathrm{U}_4(3)$	$6_2.\mathrm{U}_4(3)$
$\lambda_{\max}$	0	0	0	6	6	6
$d_{\min}$	4	20	20	36	20	90
H	$12_1.\mathrm{U}_4(3)$	$12_2.\mathrm{U}_4(3)$	$\mathrm{U}_6(2)$	$2.\mathrm{U}_6(2)$	$3.\mathrm{U}_6(2)$	$6.\mathrm{U}_6(2)$
$\lambda_{\max}$	6	6	0	0	10	10
$d_{\min}$	84	36	21	56	21	120
H	$\mathrm{S}_6(2)$	$2.\mathrm{S}_6(2)$				
$\lambda_{\max}$	0	0				
$d_{\min}$	7	8				

Table 12.3: Covering groups of simple groups of Lie type ruled out in Lemma 12.12

Lemma 12.12. *Let H be one of the groups in Table 12.3. Assume that p is not the defining characteristic of H, and let $\mathfrak{X}$ be a faithful, absolutely irreducible representation of H over $\mathbb{F}_q$. Let $d = \deg(\mathfrak{X})$. Then, for all integers e satisfying $d/2 < e \leq d$, the group $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d, q; e)$-elements.*

Proof. (The proof is analogous to the proof of Lemma 12.4.) Let $\lambda_{\max}$ be the maximal value for $\lambda(|h|)$, where h runs over all elements in $H \cong \mathrm{im}(\mathfrak{X})$ such that $|h| \neq \{1, 12, 15, 20, 24, 30, 40, 60\}$ and such that neither $|h|$ nor $|h|/2$ is a prime power. If no such $h \in H$ exists, then let $\lambda_{\max} = 0$. Let $d_{\min}$ be minimal among the degrees of all faithful, absolutely irreducible representations of H over a finite field of characteristic other than the defining characteristic of H. Then

$$d \geq d_{\min}.$$

We calculate $\lambda_{\max}$ (in GAP [24], see also Remark 2.5), read off $d_{\min}$ from [31,32], and record these values in Table 12.3. Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Seeking a contradiction, assume that $\mathrm{im}(\mathfrak{X})$ contains a $\mathrm{fat}^*(d, q; e)$-element g. Since g is fat, Lemma 5.6 yields

$$d < 2\lambda(|g|).$$

H	$4_1.\mathrm{L}_3(4)$	$4_2.\mathrm{L}_3(4)$	$3_1.\mathrm{U}_4(3)$
$\lvert g\rvert$	28	28	21
$\lambda(\lvert g\rvert)$	6	6	6
d	8	4	6
p	5	3	2
I	$\{i_1\}$	$\{i_1, r_7\}$	$\{z_3\}$
q	5	9	4

H	$4_1.\mathrm{L}_3(4)$	$6.\mathrm{L}_3(4)$, $6_1.\mathrm{U}_4(3)$
$\lvert g\rvert$	28	$21, 42$
$\lambda(\lvert g\rvert)$	6	6
d	8	6
p	$\neq 2, 5$	$\neq 2, 3$
I	$\{i_1, b_5\}$	$\{z_3\}$
q	$\begin{cases} p, & \text{if } \mathrm{ord}(p;4) = 1 \\ & \text{and } \mathrm{ord}(p;5) \leq 2, \\ p^2, & \text{else} \end{cases}$	$\begin{cases} p, & \text{if } \mathrm{ord}(p;3) = 1, \\ p^2, & \text{else} \end{cases}$

Table 12.4: Covering groups of simple groups of Lie type ruled out in Lemma 12.13

Since g is a $\mathrm{fat}^*(d, q; e)$-element, according to Lemma 5.22(a) we have $|g| \notin \{1, 12, 15, 20, 24, 30, 40, 60\}$. Moreover, neither $|g|$ nor $|g|/2$ are prime powers. Hence, $\lambda(|g|) \leq \lambda_{\max}$. It follows that $d_{\min} \leq d < 2\lambda(|g|) \leq 2\lambda_{\max}$. This, however, yields a contradiction, as by Table 12.3 we have $d_{\min} \geq 2\lambda_{\max}$. □

Lemma 12.13. *Let $S \in \{\mathrm{L}_2(4), \mathrm{L}_2(9), \mathrm{L}_3(2), \mathrm{L}_3(4), \mathrm{L}_4(2), \mathrm{L}_4(3), \mathrm{U}_4(2), \mathrm{U}_4(3), \mathrm{U}_6(2), \mathrm{S}_6(2)\}$ and let H be a covering group of S. Assume that p is not the defining characteristic of S, and let $\mathfrak{X}$ be a non-trivial, absolutely irreducible representation of H over $\mathbb{F}_q$ which is not realisable over a proper subfield. Let $d = \deg(\mathfrak{X})$. Then, for all integers e satisfying $d/2 < e \leq d$, $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d, q; e)$-elements.*

Proof. The group H is among the following.

$\mathrm{L}_2(4)$, $2.\mathrm{L}_2(4)$, $\mathrm{L}_2(9)$, $2.\mathrm{L}_2(9)$, $3.\mathrm{L}_2(9)$, $6.\mathrm{L}_2(9)$, $\mathrm{L}_3(2)$, $2.\mathrm{L}_3(2)$, $\mathrm{L}_3(4)$, $2.\mathrm{L}_3(4)$, $3.\mathrm{L}_3(4)$, $4_1.\mathrm{L}_3(4)$, $4_2.\mathrm{L}_3(4)$, $6.\mathrm{L}_3(4)$, $12_1.\mathrm{L}_3(4)$, $12_2.\mathrm{L}_3(4)$, $\mathrm{L}_4(2)$, $2.\mathrm{L}_4(2)$, $\mathrm{L}_4(3)$, $2.\mathrm{L}_4(3)$, $\mathrm{U}_4(2)$, $2.\mathrm{U}_4(2)$, $\mathrm{U}_4(3)$, $2.\mathrm{U}_4(3)$, $3_1.\mathrm{U}_4(3)$, $3_2.\mathrm{U}_4(3)$, $4.\mathrm{U}_4(3)$, $6_1.\mathrm{U}_4(3)$, $6_2.\mathrm{U}_4(3)$, $12_1.\mathrm{U}_4(3)$, $12_2.\mathrm{U}_4(3)$, $\mathrm{U}_6(2)$, $2.\mathrm{U}_6(2)$, $3.\mathrm{U}_6(2)$, $6.\mathrm{U}_6(2)$, $\mathrm{S}_6(2)$, $2.\mathrm{S}_6(2)$

We may assume that $\mathfrak{X}$ is faithful. (This is because $\mathrm{im}(\mathfrak{X})$ is isomorphic to a quotient of H by a central subgroup of H and that quotient is also a covering group of S.) If H is one of the groups in Table 12.3, then the assertion holds by Lemma 12.12. Hence,

$$G \in \big\{4_1.\mathrm{L}_3(4), 4_2.\mathrm{L}_3(4), 6.\mathrm{L}_3(4), 3_1.\mathrm{U}_4(3), 6_1.\mathrm{U}_4(3)\big\}.$$

Let I be the set of irrationalities involved in the Brauer character afforded by $\mathfrak{X}$. Seeking a contradiction, suppose that $g \in \mathrm{im}(\mathfrak{X})$ is a $\mathrm{fat}^*(d,q;e)$-element, where $e \in \mathbb{N}$ is such that $d/2 < e \leq d$. We proceed as in the proof of Lemma 12.5. We first apply Lemma 5.22(a) in order to restrict the possibilities for $|g|$. Then we use [31, 32] together with the inequality $d < 2\lambda(|g|)$ given in Lemma 5.6 in order to limit the possibilities for d and gain information on p and I. Finally, we determine the possible values for q using Lemma 12.3. The possibilities for $|g|$, $\lambda(|g|)$, d, p, I and q can be found in Table 12.4.

If $q = p^2$, then we obtain a contradiction, as by Lemma 5.22(b), $|g| \notin \{21, 28, 42\}$.

Hence, $q = p$. By Lemma 5.4, $|g|$ is divisible by a primitive divisor r of q^e-1. We may assume that r is a minimal primitive divisor of $q^e - 1$ as introduced in Definition 2.25. Since g is an exceptional $\mathrm{fat}(d,q;e)$-element, the integer r is divisible by at least two distinct primes. (Or else g is a $\mathrm{pppd}(d,q;e)$-element.) Further, from Lemma 2.28(a) we know that r is either odd or divisible by 4. Hence, either $r = 28$ and $\mathrm{ord}(q;4) = 1$, or $r = 21$ and $\mathrm{ord}(q;3) = 1$. In both cases, r has a divisor r' (namely $r' = 3$ if $r = 21$, and $r' = 4$ if $r = 28$) such that $r' \geq 2$, $\gcd(r', r/r') = 1$ and $\mathrm{ord}(q;r') \mid \mathrm{ord}(q;r/r')$. Thus, by Lemma 2.27, r is not a minimal primitive divisor of $q^e - 1$. Contradiction. □

We are now ready to prove the main results of this section.

Proposition 12.14. *Let $n, s \in \mathbb{N}$ be such that $n \geq 2$ and s is a power of a prime other than p. Let $\mathfrak{X}$ be a non-trivial, absolutely irreducible representation of $\mathrm{SL}(n,s)$ over $\mathbb{F}_q$ which is not realisable over a proper subfield, and let $d = \deg(\mathfrak{X})$. Then, for all integers e satisfying $d/2 < e \leq d$, the group $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d,q;e)$-elements.*

Proof. Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Seeking a contradiction, assume that $g \in \mathrm{im}(\mathfrak{X})$ is an $\mathrm{fat}^*(d,q;e)$-element. If $(n,s) \in \{(2,4), (2,9), (3,2), (3,4), (4,2), (4,3)\}$, then $\mathrm{SL}(n,s)$ is a covering group of $\mathrm{L}_2(4), \mathrm{L}_2(9), \mathrm{L}_3(2), \mathrm{L}_3(4), \mathrm{L}_4(2)$, and $\mathrm{L}_4(3)$, respectively, and the assertion holds by Lemma 12.13. (We note that in these cases, except for $(n,s) = (4,3)$, the group $\mathrm{SL}(n,s)$ is not the full covering group of $\mathrm{L}_n(s)$. However, we do not use this information here.) If $(n,s) \in \{(2,2), (2,3)\}$, then by Lemma 12.7($a$) we get $|g| \leq 6$, which contradicts Lemma 5.22(a). Hence, we may assume that

$$(n,s) \notin \big\{(2,2), (2,3), (2,4), (2,9), (3,2), (3,4), (4,2), (4,3)\big\}.$$

First, suppose that $n = 2$. By [39, Theorem on p. 419] we have

$$d \geq \frac{s-1}{\gcd(2, s-1)}. \tag{12.2}$$

Further, from Lemmas 5.22(a), 12.7(a) it follows that $|g|$ divides $s+1$ or $s-1$. In particular, $|g| \leq s+1$. If s is even, then Lemma 5.23(a) combined with (12.2) yields the contradiction

$$s - 1 \leq d < |g| - 8 \leq s - 7.$$

If s is odd (and hence $s-1$, $s+1$ are even) then, again by combining (12.2) with Lemma 5.23(a), we obtain a contradiction, namely

$$\frac{s-1}{2} \leq d < \begin{cases} \dfrac{|g|-2}{2} \leq \dfrac{s-1}{2}, & \text{if } |g| \in \{s+1, s-1\}, \\ |g| - 8 \leq \dfrac{s-15}{2}, & \text{if } |g| \leq \dfrac{s+1}{2}. \end{cases}$$

Now, let $n \geq 3$. According to [53, Table II] we have $d \geq (s^n-1)/(s-1)-2$. Combining this lower bound (originally proven in [30]) with Lemmas 5.23(a), 12.7(b), we obtain

$$\frac{s^n-1}{s-1} - 2 \leq d < |g| - 8 \leq \frac{s^n-1}{s-1} - 8,$$

which is not true. This completes the proof. □

Proposition 12.15. *Let $n, s \in \mathbb{N}$ be such that $n \geq 2$ and s is a power of a prime other than p. Let $\mathfrak{X}$ be a non-trivial, absolutely irreducible representation of $\mathrm{SU}(n, s)$ over $\mathbb{F}_q$ which is not realisable over a proper subfield, and let $d = \deg(\mathfrak{X})$. Then, for all integers e satisfying $d/2 < e \leq d$, the group $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d, q; e)$-elements.*

Proof. Let $e \in \mathbb{N}$ be such that $d/2 < e \leq d$. Seeking a contradiction, we assume that $\mathrm{im}(\mathfrak{X})$ contains a $\mathrm{fat}^*(d, q; e)$-element, say g. By [38, Proposition 2.9.1(i)] we have $\mathrm{SU}(2, s) \cong \mathrm{SL}(2, s)$, whence for $n = 2$ the assertion holds by Proposition 12.14. If (n, s) is contained in $\{(4, 2), (4, 3), (6, 2)\}$, then $\mathrm{SU}(n, s)$ is a covering group of the simple group $\mathrm{U}_4(2), \mathrm{U}_4(3)$, and $\mathrm{U}_6(2)$, respectively, and we have already treated these cases in Lemma 12.13. If $(n, s) = (3, 2)$, then $|g| \leq 12$ (which can be quickly verified in GAP [24]), whence g is not an exceptional fat element by Lemma 5.22(a). We may thus assume that

$$n \geq 3 \quad \text{and} \quad (n, s) \notin \big\{(3, 2), (4, 2), (4, 3), (6, 2)\big\}.$$

Then by [39, Theorem on p. 419] we have $d \geq (s^n+1)/(s+1) - 1$, or more specifically

$$d \geq \begin{cases} \dfrac{s^n-1}{s+1}, & \text{if } n \text{ is even,} \\ \dfrac{s^n-s}{s+1}, & \text{if } n \text{ is odd.} \end{cases} \tag{12.3}$$

Suppose that t is the defining characteristic of $\mathrm{SU}(n,s)$. (That is t is a prime and s is a power of t.) We distinguish two cases according as t divides $|g|$ or not.

(a) First, suppose that $t \nmid |g|$. Then by Lemma 12.10(a), there either exist two positive integers n_1, n_2 such that $n_1+n_2 = n$ and the order of g divides $\operatorname{lcm}\{s^{n_1}-(-1)^{n_1}, s^{n_2}-(-1)^{n_2}\}$, or $|g| \leq (s^n+1)/(s+1)$. In the latter case, by Lemma 5.23(a) we have $d < |g| - 8 \leq (s^n+1)/(s+1) - 8$, which combined with (12.3) yields the contradiction

$$\frac{s^n+1}{s+1} - 1 \leq d < \frac{s^n+1}{s+1} - 8.$$

Hence, suppose that there exist integers $n_1, n_2 \in \mathbb{N}$ such that $n_1+n_2 = n$ and

$$|g| \quad \text{divides} \quad \underbrace{\operatorname{lcm}\big\{s^{n_1}-(-1)^{n_1}, s^{n_2}-(-1)^{n_2}\big\}}_{=\alpha}.$$

Let $\alpha = \operatorname{lcm}\{s^{n_1}-(-1)^{n_1}, s^{n_2}-(-1)^{n_2}\}$. Note that, $|g|$ either equals α or $|g| \leq \alpha/2$. Note also that, by Lemma 12.9(a) we have

$$\alpha \leq s^{n-1} - (-1)^{n-1}.$$

If $|g| \leq \alpha/2$, then

$$|g| \leq \frac{s^{n-1}+1}{2} = \frac{s^n+s^{n-1}+s+1}{2(s+1)} < \frac{2s^n}{2(s+1)} = \frac{s^n}{s+1},$$

which combined with (12.3) and Lemma 5.23(a) reveals that

$$\frac{s^n+1}{s+1} - 1 \leq d < |g| - 8 < \frac{s^n}{s+1} - 8,$$

and this is not true. Thus, suppose that $|g| = \alpha$. Then $|g|$ is divisible by $s+1$, and hence also by some prime $\ell \leq s+1$. Using Lemma 5.23(a), we get

$$d < \frac{\ell-1}{\ell}(|g|-\ell) = \underbrace{\frac{\ell-1}{\ell}}_{<s/(s+1)} |g| - \underbrace{(\ell-1)}_{\geq 1} \leq \frac{s}{s+1}|g| - 1,$$

and thus, recalling that $|g| = \alpha \leq s^{n-1} - (-1)^{n-1}$,

$$d < \frac{s}{s+1}\big(s^{n-1} - (-1)^{n-1}\big) - 1, \tag{12.4}$$

Then (12.3) and (12.4) yield a contradiction as follows. If n is even, then

$$\frac{s^n - 1}{s+1} \leq d < \frac{s(s^{n-1}+1)}{s+1} - 1,$$

and consequently $s^n - 1 < s(s^{n-1}+1) - s - 1 = s^n - 1$ (which is not true). If n is odd, then

$$\frac{s^n - s}{s+1} \leq d < \frac{s(s^{n-1}-1)}{s+1} - 1,$$

and thus $s^n - s < s(s^{n-1} - 1) - s - 1 = s^n - 2s - 1$ (which is not true).

(b) It remains to consider the situation where t divides $|g|$. In that case, by Lemma 5.23(a) we get

$$d < \frac{(t-1)(|g| - t)}{t} \leq (s-1)\left(\frac{|g|}{t} - 1\right).$$

Thus, using Lemma 12.10(b), according to which the order of g satisfies

$$|g| \leq \begin{cases} t(s^{n-2}+2), & \text{if } n \text{ is even,} \\ t(s^{n-2}+1), & \text{if } n \text{ is odd,} \end{cases}$$

we obtain

$$d < \begin{cases} (s-1)(s^{n-2}+1), & \text{if } n \text{ is even,} \\ (s-1)s^{n-2}, & \text{if } n \text{ is odd.} \end{cases}$$

Combining this with the lower bound for d given in (12.3), we see that

$$\begin{cases} \dfrac{s^n - 1}{s+1} \leq d < (s-1)(s^{n-2}+1), & \text{if } n \text{ is even,} \\ \dfrac{s^n - s}{s+1} \leq d < (s-1)s^{n-2}, & \text{if } n \text{ is odd,} \end{cases}$$

whence

$$\begin{cases} s^n - 1 \leq d < (s^2-1)(s^{n-2}+1), & \text{if } n \text{ is even,} \\ s^n - s \leq d < (s^2-1)s^{n-2}, & \text{if } n \text{ is odd.} \end{cases}$$

This is a contradiction, since (recalling that $n \geq 3$, and hence $n \geq 4$ if n is even) we have

$$\begin{cases} s^n - 1 \geq s^n + s^2 - s^{n-2} - 1 = (s^2-1)(s^{n-2}+1), & \text{if } n \text{ is even,} \\ s^n - s \geq s^n - s^{n-2} = (s^2-1)s^{n-2}, & \text{if } n \text{ is odd.} \end{cases}$$ □

Proposition 12.16. *Let m be a positive integer and let s be a power of a prime other than p. Let $\mathfrak{X}$ be a non-trivial, absolutely irreducible representation of $\mathrm{Sp}(2m,s)$ over $\mathbb{F}_q$ which is not realisable over a proper subfield, and let $d=\deg(\mathfrak{X})$. Then, for all integers e satisfying $d/2<e\leq d$, the group $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d,q;e)$-elements.*

Proof. Let $e\in\mathbb{N}$ be such that $d/2<e\leq d$. Seeking a contradiction, assume that $\mathrm{im}(\mathfrak{X})$ contains a $\mathrm{fat}^*(d,q;e)$-element g. According to [38, Proposition 2.9.1(i)] we have $\mathrm{Sp}(2,s)\cong\mathrm{SL}(2,s)$. Hence, by Proposition 12.14 the assertion holds for $m=1$, and we may assume that

$$m\geq 2.$$

Let t be the defining characteristic of $\mathrm{Sp}(2m,s)$. (That is, let t be a prime such that s is a power of the prime t.) We distinguish between the cases where $t=2$ and $t\neq 2$.

(a) Assume that $t=2$. The group $\mathrm{Sp}(6,2)=\mathrm{S}_6(2)$ is covered in Lemma 12.13, whence suppose that $(m,s)\neq(3,2)$. By [38, Proposition 2.9.1(xvi)]), $\mathrm{Sp}(4,2)$ is isomorphic to the symmetric group S_6. Since the maximal element order in S_6 is 6, by Lemma 5.22(a) we may assume that $(m,s)\neq(2,2)$. Then by [52, Proposition on p. 235] we have

$$d\geq\frac{(s^m-1)(s^m-s)}{2(s+1)}.$$

Recall from Lemma 12.11 that $|g|\leq s^{m+1}/(s-1)$. which, (recalling that g is a $\mathrm{fat}^*(d,q;e)$-element and) using Lemma 5.23(a) reveals that $d<s^{m+1}/(s-1)-8$. It follows that

$$\frac{(s^m-1)(s^m-s)}{2(s+1)}<\frac{s^{m+1}}{s-1}-8.$$

Then (multiplying the inequality above by $2(s^2-1)$) we get

$$(s-1)(s^{2m}-s^{m+1}-s^m+s)\leq 2(s+1)s^{m+1}-16(s^2+1),$$

which is equivalent to

$$\underbrace{s^{2m+1}-s^{2m}-3s^{m+2}-2s^{m+1}+s^m+17s^2-s+16}_{=\alpha}\leq 0. \tag{12.5}$$

Let α be the left hand-side of (12.5). If $s\geq 8$, then $\alpha\geq 8s^{2m}-s^{2m}-3s^{m+2}-2s^{m+1}+s^m+17s^2-s+16>0$, which contradicts (12.5). So assume that $s\in\{2,4\}$. If $(m,s)=(2,4)$ or $(m,s)=(3,4)$, then (a

direct calculation verifies that) $\alpha > 0$. This contradict (12.5). Since, by assumption, $(m,s) \notin \{(2,2),(3,2)\}$ it remains to consider the situation where $s \in \{2,4\}$ and $m \geq 4$. In that case we have

$$\begin{aligned}\alpha &= \underbrace{s^{2m+1} - s^{2m}}_{\geq s^{2m} \geq 4s^{m+2}} - 3s^{m+2} - 2s^{m+1} + s^m + 17s^2 - s + 16 \\ &\geq \underbrace{s^{m+2} - 2s^{m+1}}_{\geq 0} + s^m + 17s^2 - s + 16 \\ &> 0.\end{aligned}$$

This also contradicts (12.5), and completes the proof (for $t = 2$).

(b) Assume that t is an odd prime. By [39, Theorem on p. 419] we have the following lower bound for d.

$$d \geq \frac{s^m - 1}{2} \tag{12.6}$$

Now, as we show in Lemma 12.11, one of the following holds.

(i) The order of g divides $2t^\ell$, and $\ell \geq 2$.

(ii) The order of g divides $t^m + t$, and $s = t$.

(iii) The order of g divides $t^m + t^2$, and $s = t = 3$.

(iv) The order of g divides an even integer which is less or equal to $s^m + 1$.

If we are in case (i), then by Lemma 5.22(a), g is not a fat$^*(d,q;e)$-element. If case (ii) holds, or if we are in case (iii) with $m \geq 4$, then Lemmas 2.6, 5.6 yield $d < 2\lambda(|g|) \leq (s^m - 1)/2$, and this contradicts (12.6). If we are in case (iii) with $m = 2$, then $|g| \leq 18$, whence g is not a fat$^*(d,q;e)$-element by Lemma 5.22(a). If case (iii) holds and $m = 3$ then, using Lemma 2.4, we have $\lambda(|g|) \mid \lambda(36)$. Hence, in this case, by combining (12.6) with Lemma 5.6, we obtain the contradiction $13 \leq d < 2\lambda(36) = 12$. Finally, assume that case (iv) holds. Then by Lemma 5.23(a) we have

$$\frac{s^m - 1}{2} \leq d < \begin{cases} \dfrac{|g| - 2}{2} \leq \dfrac{s^m - 1}{2}, & \text{if } |g| \text{ is even,} \\ |g| - 8 \leq \dfrac{s^m + 1}{2} - 8, & \text{if } |g| \text{ is odd,} \end{cases}$$

which is not true. □

Theorem 12.17. *Let $n \in \mathbb{N}$ and let s be a power of a prime other than p. Let S be one of the following finite simple classical groups.*

$$\begin{aligned} &\mathrm{L}_n(s), && n \geq 2,\ (n,s) \notin \{(2,2),(2,3)\} \\ &\mathrm{U}_n(s), && n \geq 2,\ (n,s) \notin \{(2,2),(2,3),(3,2)\} \\ &\mathrm{S}_n(s), && n \text{ even},\ (n,s) \notin \{(2,2),(2,3),(4,2)\} \end{aligned}$$

Let H be a covering group of S, and let $\mathfrak{X}$ be a non-trivial, absolutely irreducible representation of H over $\mathbb{F}_q$ which is not realisable over a proper subfield. Let $d = \deg(\mathfrak{X})$. Then, for all integers e satisfying $d/2 < e \leq d$, the group $\mathrm{im}(\mathfrak{X})$ does not contain any $\mathrm{fat}^*(d,q;e)$-elements.

Proof. We have already treated several individual cases in Lemma 12.13, and can thus assume that

$$(n,s) \notin \begin{cases} \{(2,4),(2,9),(3,2),(3,4),(4,2)\}, & \text{if } S = \mathrm{L}_n(s), \\ \{(4,2),(4,3),(6,2)\}, & \text{if } S = \mathrm{U}_n(s), \\ \{(6,2)\}, & \text{if } S = \mathrm{S}_n(s). \end{cases}$$

Then by [38, Theorem 5.1.4(*ii*)] and [18, p. *xii*, Table 2], the group

$$F = \begin{cases} \mathrm{SL}(n,s), & \text{if } S = \mathrm{L}_n(s), \\ \mathrm{SU}(n,s), & \text{if } S = \mathrm{U}_n(s), \\ \mathrm{Sp}(n,s), & \text{if } S = \mathrm{S}_n(s) \end{cases}$$

is the full covering group of S. The group $\mathrm{im}(\mathfrak{X})$ is the image of a non-trivial absolutely irreducible representation $\mathfrak{Y}$ of F over $\mathbb{F}_q$ which is not realisable over a proper subfield. Hence, the assertion holds by Propositions 12.14, 12.15, 12.16. □

List of Tables

Bibliography

[1] S. S. Abhyankar. Again nice equations for nice groups. *Proc. Amer. Math. Soc.*, 124(10):2967–2976, 1996.

[2] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[3] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2000.

[4] J. Bamberg, S. P. Glasby, T. Popiel, and C. E. Praeger. Generalized quadrangles and transitive pseudo-hyperovals. *J. Combin. Des.*, 24(4):151–164, 2016.

[5] J. Bamberg and T. Penttila. Overgroups of cyclic Sylow subgroups of linear groups. *Comm. Algebra*, 36(7):2503–2543, 2008.

[6] A. Bang. Taltheoretiske Undersøgelser. *Tidsskrifft Math.*, 4(5):70–80 and 130–137, 1886.

[7] B. Baumeister. Primitive permutation groups with a regular subgroup. *J. Algebra*, 310(2):569–618, 2007.

[8] G. D. Birkhoff and H. S. Vandiver. On the integral divisors of $a^n - b^n$. *Ann. of Math. (2)*, 5(4):173–180, 1904.

[9] J. V. Brawley and L. Carlitz. Irreducibles and the composed product for polynomials over a finite field. *Discrete Math.*, 65(2):115–139, 1987.

[10] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013. With a foreword by Martin Liebeck.

[11] T. C. Burness and H. P. Tong-Viet. Derangements in primitive permutation groups, with an application to character theory. *Q. J. Math.*, 66(1):63–96, 2015.

[12] A. A. Buturlakin. Spectra of finite linear and unitary groups. *Algebra Logika*, 47(2):157–173, 264, 2008.

[13] A. A. Buturlakin. Spectra of finite symplectic and orthogonal groups. *Siberian Advances in Mathematics*, 21:176–210, 2011.

[14] P. J. Cameron. *Combinatorics: topics, techniques, algorithms*. Cambridge University Press, Cambridge, 1994.

[15] P. J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[16] R. D. Carmichael. Note on a new number theory function. *Bull. Amer. Math. Soc.*, 16(5):232–238, 1910.

[17] S. K. Chebolu and J. Mináč. Counting irreducible polynomials over finite fields using the inclusion-exclusion principle. *Mathematics Magazine*, 84(5):369–371, 2011.

[18] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray.

[19] M. R. Darafsheh. Order of elements in the groups related to the general linear group. *Finite Fields Appl.*, 11(4):738–747, 2005.

[20] U. Dempwolff. On irreducible semilinear transformations. *Forum Math.*, 22(6):1193–1206, 2010.

[21] J. DiMuro. *On prime power elements of $GL_d(q)$ acting irreducibly on large subspaces*. ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–University of Southern California.

[22] J. DiMuro. On prime power order elements of general linear groups. *J. Algebra*, 367:222–236, 2012.

[23] W. Feit. On large Zsigmondy primes. *Proc. Amer. Math. Soc.*, 102(1):29–36, 1988.

[24] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.9.1*, 2018.

[25] M. Garcia-Planas and M. D. Magret. Eigenvalues and eigenvectors of monomial matrices. In *Congreso de Ecuaciones Diferenciales y Aplicaciones / Congreso de Matemática Aplicada*, pages 963–966. Universidad de Cádiz, Jun 2015.

[26] C. F. Gauss. *Untersuchungen über höhere Arithmetik*. Deutsch herausgegeben von H. Maser. Chelsea Publishing Co., New York, 1965.

[27] S. P. Glasby, F. Lübeck, A. C. Niemeyer, and C. E. Praeger. Primitive prime divisors and the nth cyclotomic polynomial. *J. Aust. Math. Soc.*, 102(1):122–135, 2017.

[28] A. Grytczuk and M. Wójtowicz. An application of the Minkowski inequality. *Int. J. Pure Appl. Math.*, 11(3):311–314, 2004.

[29] S. Guest, J. Morris, C. E. Praeger, and P. Spiga. On the maximum orders of elements of finite almost simple groups and primitive permutation groups. *Trans. Amer. Math. Soc.*, 367(11):7665–7694, 2015.

[30] R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl. Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc. (3)*, 78(1):167–214, 1999.

[31] G. Hiss and G. Malle. Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math.*, 4:22–63 (electronic), 2001.

[32] G. Hiss and G. Malle. Corrigenda: "Low-dimensional representations of quasi-simple groups". *LMS J. Comput. Math.*, 5:95–126 (electronic), 2002.

[33] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

[34] B. Huppert and W. Willems. *Lineare Algebra: Mit zahlreichen Anwendungen in Kryptographie, Codierungstheorie, Mathematischer Physik und Stochastischen Prozessen*. Vieweg Studium. Vieweg+Teubner Verlag, 2010.

[35] I. M. Isaacs. *Character theory of finite groups*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976. Pure and Applied Mathematics, No. 69.

[36] C. Jansen. The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comput. Math.*, 8:122–144 (electronic), 2005.

[37] N. L. Johnson and A. Montinaro. The transitive t-parallelisms of a finite projective space. *Adv. Geom.*, 12(3):401–429, 2012.

[38] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[39] V. Landazuri and G. M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.

[40] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order*, volume 27 of *London Mathematical Society Monographs. New Series*. Oxford University Press, Oxford, 2002. Oxford Science Publications.

[41] W. J. LeVeque. *Elementary theory of numbers*. Dover Books on Advanced Mathematics. Dover Publications, Inc., New York, second edition, 1990.

[42] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[43] M. W. Liebeck, C. E. Praeger, and J. Saxl. Transitive subgroups of primitive permutation groups. *J. Algebra*, 234(2):291–361, 2000. Special issue in honor of Helmut Wielandt.

[44] S. Ligh and L. Neal. A note on Mersenne numbers. *Math. Mag.*, 47:231–233, 1974.

[45] P. M. Neumann and C. E. Praeger. A recognition algorithm for special linear groups. *Proc. London Math. Soc. (3)*, 65(3):555–603, 1992.

[46] P. M. Neumann and C. E. Praeger. Cyclic matrices over finite fields. *J. London Math. Soc. (2)*, 52(2):263–284, 1995.

[47] A. C. Niemeyer, S. B. Pannek, and C. E. Praeger. Irreducible linear subgroups generated by pairs of matrices with large irreducible submodules. *Arch. Math. (Basel)*, 98(2):105–114, 2012.

[48] A. C. Niemeyer and C. E. Praeger. A recognition algorithm for classical groups over finite fields. *Proc. London Math. Soc. (3)*, 77(1):117–169, 1998.

[49] P. Ribenboim. *The little book of bigger primes*. Springer-Verlag, New York, second edition, 2004.

[50] M. Roitman. On Zsigmondy primes. *Proc. Amer. Math. Soc.*, 125(7):1913–1919, 1997.

[51] J. Schur. Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. *J. Reine Angew. Math.*, 132:85–137, 1907.

[52] G. M. Seitz and A. E. Zalesskii. On the minimal degrees of projective representations of the finite Chevalley groups. II. *J. Algebra*, 158(1):233–243, 1993.

[53] P. H. Tiep. Low dimensional representations of finite quasisimple groups. In *Groups, combinatorics & geometry (Durham, 2001)*, pages 277–294. World Sci. Publ., River Edge, NJ, 2003.

[54] R. A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London Ltd., London, 2009.

[55] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.