UNIVERSITÀ DEGLI STUDI DI
MILANO-BICOCCA

Joint PhD program in Mathematics
Milano Bicocca - Pavia - INdAM
Cycle XXXIV

Hopf-Galois Structures and Skew Braces of order p^2q

Elena Campedel

Supervised by Prof. Ilaria Del Corso

Academic year 2020/2021

Contents

Introduction **5**

1 The gamma function **17**
1.1 Describing the regular subgroups of the holomorph 17
1.2 Invariant subgroups 20
1.3 Isomorphism of Sylow p-subgroups 21
1.4 Tools of the trade 22
1.5 Lifting and restriction 24
1.6 Duality 30
1.7 Gluing 34
1.8 Applications 35
1.8.1 Nilpotent groups 35
1.8.2 Groups of order pq 36

2 Towards enumeration **39**
2.1 The groups of order p^2q and their automorphism groups 39
2.2 The reader's Guide to the next chapters 45
2.2.1 Duality for non-abelian groups of order p^2q 45
2.2.2 Lifting for groups of order p^2q 46
2.2.3 Gluing for groups of order p^2q 47

3 The cyclic Sylow p-subgroups case **48**
3.1 G of type 1 48
3.1.1 Abelian groups 48
3.1.2 The case $p|q-1$ 49
3.1.3 The case $q \mid p-1$ 50
3.2 G of type 2 51
3.2.1 The case $|\ker(\gamma)| = q$ 52
3.2.2 The case $|\ker(\gamma)| = pq$ 53
3.3 G of type 3 54
3.4 G of type 4 55
3.4.1 The case $|\ker(\gamma)| = p^2$ 55
3.4.2 The case $|\ker(\gamma)| = pq$ 56

3.4.3 The case $|\ker(\gamma)| = p$ . . . 56

4 The elementary abelian Sylow p-subgroups case **59**
4.1 Some results on $\mathrm{GL}(2,p)$ . . . 59
4.1.1 Sylow p-subgroups . . . 59
4.1.2 Elements of order p when $p \parallel |\ker(\gamma)|$ . . . 59
4.1.3 Sylow q-subgroups . . . 60
4.1.4 Elements of order q when $|\ker(\gamma)| = p$ . . . 60
4.2 G of type 5 . . . 61
4.2.1 Abelian groups . . . 61
4.2.2 The case $p \mid q-1$ . . . 62
4.2.3 The case $q \mid p-1$ . . . 63
4.2.4 The case $q \mid p+1$ . . . 66
4.3 G of type 6 . . . 68
4.3.1 The case $A \leq \ker(\gamma)$ . . . 69
4.3.2 The case $C \leq \ker(\gamma) \neq A$ . . . 70
4.4 G of type 7, 8 and 9 . . . 72
4.4.1 Outline . . . 73
4.4.2 The case $|\ker(\gamma)| = q$ . . . 78
4.4.3 The case $|\ker(\gamma)| = pq$ . . . 78
4.4.4 The case $|\ker(\gamma)| = p^2$ . . . 80
4.4.5 The case $|\ker(\gamma)| = p$ . . . 84
4.4.6 The case $|\ker(\gamma)| = 1$ . . . 102
4.4.7 Results . . . 105
4.5 G of type 7, $\gamma(A) \not\leq \mathrm{Inn}(G)$ . . . 111
4.5.1 The case $|\ker(\gamma)| = pq$ . . . 111
4.5.2 The case $|\ker(\gamma)| = p$ . . . 112
4.6 G of type 10 . . . 120
4.6.1 The case $|\ker(\gamma)| = p$ . . . 121
4.6.2 The case $|\ker(\gamma)| = p^2$ . . . 121
4.6.3 The case $q \mid |\ker(\gamma)|$ . . . 122
4.6.4 The case $\ker(\gamma) = \{1\}$ . . . 122
4.7 G of type 11 . . . 125
4.7.1 The case $|\ker(\gamma)| = q$ . . . 126
4.7.2 The case $|\ker(\gamma)| = pq$ . . . 127
4.8 Proof of Theorems 2 and 4 . . . 129

5 Groups of order $4q$ **130**
5.1 G of type 1 . . . 132
5.2 G of type 2 . . . 134
5.3 G of type 3 . . . 135
5.4 G of type 5 . . . 136
5.5 G of type 11 . . . 138
5.6 G of type 10 . . . 139

5.7 Proof of Theorem 5.1 140

Appendix A **141**

Appendix B **143**

Bibliography **148**

Introduction

The general problem and the classical approach

Let L/K be a finite Galois field extension, and let $\Gamma = \mathrm{Gal}(L/K)$. Then the group algebra $K[\Gamma]$ is a K-Hopf algebra, and its natural action on L endows L/K with a Hopf-Galois structure. In general this is not the only Hopf-Galois structure on L/K, and the study of Galois module structures different from the classical one is important, for example in the context of algebraic number theory. In fact, when L/K is a wildly ramified extension of local fields, there are cases in which the ring of integers $\mathcal{O}_L$ of L is free as a module over a Hopf order in some K-Hopf algebra H, but not in $K[\Gamma]$ (see Child's book [Chi00] for an overview and for the specific results).

Greither and Pareigis [GP87] showed that the Hopf-Galois structures on L/K correspond to the regular subgroups G of the group $\mathrm{Perm}(\Gamma)$ of permutations on the set Γ, which are normalised by the image $\rho(\Gamma)$ of the right regular representation ρ of Γ (in the relevant literature it is common to use the left regular representation λ instead of the right one ρ we are employing here. We have translated the statements in the literature from left to right).

The groups G and Γ have the same cardinality but they need not be isomorphic. We will say that a Hopf-Galois structure is of *type* G if G is the group associated to it in the Greither-Pareigis correspondence.

As usual we denote by $e(\Gamma, G)$ the number of regular subgroups of $\mathrm{Perm}(\Gamma)$ normalised by $\rho(\Gamma)$, which are isomorphic to G. Equivalently, $e(\Gamma, G)$ is the number of Hopf-Galois structures of type G on a Galois field extension with Galois group isomorphic to Γ.

The direct determination of all regular subgroups of $\mathrm{Perm}(\Gamma)$ normalised by $\rho(\Gamma)$ is in general a difficult task, since the group $\mathrm{Perm}(\Gamma)$ is large. However, Childs [Chi89] and Byott [Byo96] observed that the condition that $\rho(\Gamma)$ normalises G can be reformulated by saying that Γ is contained in the holomorph $\mathrm{Hol}(G)$ of G, regarded as a subgroup of $\mathrm{Perm}(G)$. This translation turns out to be very useful, since $\mathrm{Hol}(G)$ is usually much smaller than $\mathrm{Perm}(\Gamma)$. One obtains the following result.

Theorem 1 ([Byo96, Corollary p. 3320])**.** *Let L/K be a finite Galois field extension with Galois group Γ. For any group G with $|G| = |\Gamma|$, let $e'(\Gamma, G)$ be the number of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ.*

Then the number $e(\Gamma, G)$ of Hopf-Galois structures on L/K of type G is given by

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|}\, e'(\Gamma, G). \tag{1}$$

Moreover $e(\Gamma)$, the total number of Hopf-Galois structures on L/K, is given by $\sum_G e(\Gamma, G)$ where the sum is over all isomorphism types G of groups of order $|\Gamma|$.

There is a rich literature on Hopf-Galois structures on various classes of field extensions (for a survey up to 2000, see the already mentioned book by Childs [Chi00]). For example, if L/K is an almost classically Galois extension of degree a Burnside number, then there is a unique Hopf Galois structure [Byo96, BML22]. For an odd prime p it is known that there are p^{m-1} Hopf-Galois structures on a cyclic extension of degree p^m, and they are all of cyclic type [Koh98]. An elementary abelian extension of degree p^m, with $p > m$, has at least $p^{m(m-1)-1}(p-1)$ Hopf-Galois structures of abelian type (see [Chi05]). An abelian, non cyclic, extension of degree p^m admits also structures of non-abelian type for $m \geq 3$ [BC12].

The exact number of Hopf-Galois structures is known for some families of Galois extensions, such as those of order the square of a prime, [Byo96], the product of two primes [Byo04], the cube of a prime [NZ18, NZ19], for the cyclic extensions of squarefree order [AB18] and for the $\mathcal{S}_n$-extensions [Tsa19].

An interesting issue is also to determine which general properties of either Γ or G force those of the other. For certain Galois groups Γ it is known that every Hopf-Galois structure must have type Γ (see [BC12]). For a Galois extension whose Galois group Γ is abelian, the type G of any Hopf-Galois structure must be soluble [Byo15, Theorem 2], although for a soluble, non-abelian Galois group Γ there can be Hopf-Galois structures whose type is not soluble [Byo15, Corollary 3]; see also [TQ20, CDC21].

The study of Hopf-Galois structures, that is, of regular subgroups of the holomorphs, has also a deep connection with the theory of *skew braces*. In fact, if G is a group with respect to the operation "$\cdot$", classifying the regular subgroups of $\mathrm{Hol}(G)$ is equivalent to determining the operations "$\circ$" on G such that $(G, \cdot, \circ)$ is a (right) skew brace [GV17], that is, $(G, \circ)$ is also a group, and the two group structures on the set G are related by

$$(g \cdot h) \circ k = (g \circ k) \cdot k^{-1} \cdot (h \circ k), \tag{2}$$

where k^{-1} denote the inverse of k with respect to the operation "$\cdot$". This connection was first observed by Bachiller in [Bac16, §2] and it is described in detail in the appendix to [SV18].

The methods

The main goal of this thesis is to classify the Hopf-Galois structures on a Galois extension L/K of order p^2q, where p, q are distinct primes. According to the discussion above we do this by following Byott's approach, that is, by determining the regular subgroups of $\mathrm{Hol}(G)$, for each group $G = (G, \cdot)$ of order p^2q, where p, q are distinct primes. This is in turn equivalent to determining the right skew braces $(G, \cdot, \circ)$ such that $(G, \circ) \cong \Gamma$ (see [Ven19, Problem 16]).

Our method relies on the use of the alternate brace operation $\circ$ on G, mainly indirectly, that is through the use of the function

$$\begin{aligned} \gamma : G &\to \mathrm{Aut}(G) \\ g &\mapsto (x \mapsto (x \circ g) \cdot g^{-1}), \end{aligned}$$

which is characterised by the functional equation

$$\gamma(g^{\gamma(h)} \cdot h) = \gamma(g)\gamma(h). \tag{3}$$

(See Theorem 1.2 and the ensuing discussion for the details.) The functions γ satisfying (3) are in one-to-one correspondence with the regular subgroups of $\mathrm{Hol}(G)$, and occur naturally in the theory of (skew) braces: they are called μ in [Rum07b], and λ in the literature of skew braces [GV17]. They have been exploited, albeit in a somewhat different context, in [CDVS06, CDV17, CDV18, Car18]. It follows that to determine the number $e'(\Gamma, G)$ defined in Theorem 1 we can count the number of functions $\gamma : G \to \mathrm{Aut}(G)$ verifying (3) and such that, for the operation $\circ$ defined on G by

$$g \circ h = g^{\gamma(h)}h,$$

we have $(G, \circ) \cong \Gamma$.

In Chapter 1 we develop methods to deal with these gamma functions, that will make enumerating them easier. As a side effect, our methods allow us also to give alternative proofs of some results in the literature. In Subsection 1.8.1 we give a proof of the results of Byott [Byo13, Theorem 1] about the case of finite nilpotent groups. In Subsection 1.8.2, as a preliminary to our classification, we give a compact treatment of the case of groups of order pq, with p, q distinct primes, dealt with by Byott in [Byo04] (see also [AB20c]).

Hopf-Galois structures of order p^2q

Starting with Chapter 2, we restrict our consideration to the groups of order p^2q, where p and q are distinct primes; they are listed in Table 2.1.

Applying the results of Chapter 1, we show that for $p > 2$ a Galois field extension L/K with group Γ admits Hopf-Galois structures of type G only

for those G such that G and Γ have isomorphic Sylow p-subgroups (see Theorem 2.3 and Corollary 2.4).

In Chapters 3 and 4 we show that if $p > 2$ each G with Sylow p-subgroups isomorphic to the Sylow p-subgroups of Γ defines some Hopf-Galois structure on L/K. We then explicitly determine the number of structures for each type.

We accomplish this by calculating, given a group $G = (G, \cdot)$ of order p^2q, $p > 2$, the following equivalent data (see Theorem 1.2 and the ensuing discussion) for each group Γ of order p^2q:

1. the total number, and the number and lengths of conjugacy classes within $\mathrm{Hol}(G)$, of regular subgroups isomorphic to Γ;

2. the total number, and the number of isomorphism classes, of (right) skew braces $(G, \cdot, \circ)$ such that $\Gamma \cong (G, \circ)$.

Remark. Here and in the following, by the *(total) number of skew braces* we mean, given a group $(G, \cdot)$, the number of distinct operations $\circ$ on the set G such that $(G, \cdot, \circ)$ is a skew brace.

The following theorems summarise our results, where the notation for the groups is that given in Section 2.1. Each of the numbers 1, 2,..., 11 corresponds to an isomorphism class of groups of order p^2q, except for the number 8, which correspond to $\frac{q-3}{2}$ isomorphism classes G_k, where $k \in \mathcal{C}_q$, $k \neq 0, \pm 1$ and $G_k \simeq G_{k^{-1}}$.

Theorem 2. *Let L/K be a Galois field extension of order p^2q, where p and q are two distinct primes with $p > 2$, and let $\Gamma = \mathrm{Gal}(L/K)$.*

Let G be a group of order p^2q.

If the Sylow p-subgroups of G and Γ are not isomorphic, then there are no Hopf-Galois structures of type G on L/K.

If the Sylow p-subgroups of Γ and G are isomorphic, then the numbers $e(\Gamma, G)$ of Hopf-Galois structures of type G on L/K are given in the following tables.

(i) For $q \nmid p - 1$:

Γ \ G	*1*	*2*	*3*
1	p	$2p(p-1)$	$2p(p-1)$
2	pq	$2p(pq-2q+1)$	$2pq(p-1)$
3	pq	$2pq(p-1)$	$2(p^2q-pq-q+1)$

where the upper left sub-tables of sizes 1×1, 2×2 and 3×3 give respectively the cases $p \nmid q-1$, $p \parallel q-1$ and $p^2 \mid q-1$.

Γ \ G	*5*	*11*
5	p^2	$2p(p^2-1)$
11	p^2q	$2p(1+qp^2-2q)$

where the upper left sub-tables of sizes 1×1 *and* 2×2 *give respectively the cases* $p \nmid q-1$ *and* $p \mid q-1$.

(ii) For $q \nmid p-1$ *and* $q \mid p+1$*:*

Γ \ G	*5*	*10*
5	p^2	$p(p-1)(q-1)$
10	p^2	$2+2p^2(q-3)-p^3+p^4$

(iii) For $q \mid p-1$*:*

Γ \ G	*1*	*4*
1	p	$2p(q-1)$
4	p^2	$2(p^2q-2p^2+1)$

If $q=2$,

Γ \ G	*5*	*6*	*7*
5	p^2	$2p(p+1)$	$p(3p+1)$
6	p^2	$2p(p+1)$	$p(3p+1)$
7	p^2	$2p^2(p+1)$	$2+p(p+1)(2p-1)$

If $q=3$,

Γ \ G	*5*	*6*	*7*	*9*
5	p^2	$4p(p+1)$	$2p(3p+1)$	$4p(p+1)$
6	p	$2p(p+3)$	$4p(p+1)$	$p(3p+5)$
7	p^2	$2p^2(p+1)^2$	$2+p^2(2p^2+3p+2)$	$p(p+1)^3$
9	$p^2(2p-1)$	$4p(p^2+1)$	$2(2p^3+3p^2-2p+1)$	$2+2p+p^3(p+3)$

If $q>3$,

Γ \ G	*5*	*6*
5	p^2	$2p(p+1)(q-1)$
6	p	$2p(p+2q-3)$
7	p^2	$2p^2(p+1)(pq-2p+1)$
8, G_2	p^3	$4p(p^2+pq-3p+1)$
8, $G_k \not\simeq G_2$	p^2	$4p(p^2+pq-3p+1)$
9	p^2	$4p(p^2+pq-3p+1)$

Γ \ G	*7*	*9*
5	$p(3p+1)(q-1)$	$2p(p+1)(q-1)$
6	$4(p^2+pq-2p)$	$p(4q+3p-7)$
7	$2+p^2(2p^2+pq+2q-4)$	$p(p+1)(p^2(2q-5)+2p+1)$
8, G_2	$2p(p^2q-4p+pq+2)$	$p(p^3+3p^2-14p+4pq-6)$
8, $G_k \not\simeq G_2$	$4p(2p^2-5p+pq+2)$	$p(p^3+5p^2-18p+4pq+8)$
9	$2(4p^3-9p^2+2p^2q+2p+1)$	$2+4p+p^2(p^2+5p+4q-16)$

Γ \ $G8$	$G \not\simeq G_{\pm 2}$	$G \simeq G_{\pm 2},\ q>5$	$G \simeq G_2,\ q=5$
5	$4p(p+1)(q-1)$	$4p(p+1)(q-1)$	$16p(p+1)$
6	$8p(q+p-2)$	$8p(q+p-2)$	$8p(p+3)$
7	$4p^2(p+1)(pq-3p+2)$	$4p^2(p+1)(pq-3p+2)$	$8p^2(p+1)^2$
8	*Table 1*	*Table 2*	$4(1+p+3p^2(p+1))$
9	$8p(2p^2+pq-5p+2))$	$4p(3p^2+2pq-8p+3)$	$16p(2p^3-2p+p+1)$

Table 1: G and Γ of type 8, $G \simeq G_k \not\simeq G_{\pm 2}$

Γ	if either k or k^{-1} is a solution of $x^2-x-1=0$:
G_k, G_{1-k}	$2(1+5p+4p^2q-17p^2+7p^3)$
G_{1+k}	$4(3p+2p^2q-8p^2+3p^3)$
$G_s \not\simeq G_k, G_{1+k}, G_{1-k}$	$8(2p+p^2q-5p^2+2p^3)$
Γ	if k and k^{-1} are the solutions of $x^2+x+1=0$:
G_k	$2(1+6p+4p^2q-19p^2+8p^3)$
G_{1-k}, $G_{1-k^{-1}}$	$2(7p+4p^2q-18p^2+7p^3)$
G_{1+k}	$2(1+4p+4p^2q-15p^2+6p^3)$
$G_s \not\simeq G_k, G_{1+k}, G_{1-k}, G_{1-k^{-1}}$	$8(2p+p^2q-5p^2+2p^3)$
Γ	if k and k^{-1} are the solutions of $x^2-x+1=0$:
G_{-k}	$2(1+6p+4p^2q-19p^2+8p^3)$
G_{1+k}, $G_{1+k^{-1}}$	$2(7p+4p^2q-18p^2+7p^3)$
G_{1-k}	$2(1+4p+4p^2q-15p^2+6p^3)$
$G_s \not\simeq G_{-k}, G_{1-k}, G_{1+k}, G_{1+k^{-1}}$	$8(2p+p^2q-5p^2+2p^3)$
Γ	if k and k^{-1} are the solutions of $x^2+1=0$:
G_k	$4(1+2p+2p^2q-9p^2+4p^3)$
G_{1+k}, G_{1-k}	$4(3p+2p^2q-8p^2+3p^3)$
$G_s \not\simeq G_k, G_{1+k}, G_{1-k}$	$8(2p+p^2q-5p^2+2p^3)$
Γ	if $k^2 \neq \pm k \pm 1, -1$:
G_k, G_{-k}	$2(1+6p+4p^2q-19p^2+8p^3)$
G_{1+k}, $G_{1+k^{-1}}$, G_{1-k}, $G_{1-k^{-1}}$	$2(7p+4p^2q-18p^2+7p^3)$
$G_s \not\simeq G_{\pm k}, G_{1\pm k}, G_{1\pm k^{-1}}$	$8(2p+p^2q-5p^2+2p^3)$

Table 2: G and Γ of type 8, $G \simeq G_k$ for $k = \pm 2$,

Γ	if $q > 7$:
G_2	$2(1 + 5p + 4p^2q - 17p^2 + 7p^3)$
G_3, $G_{\frac{3}{2}}$	$2(7p + 4p^2q - 18p^2 + 7p^3)$
G_{-2}	$2(1 + 6p + 4p^2q - 19p^2 + 8p^3)$
$G_s \not\simeq G_2, G_3, G_{\frac{3}{2}}, G_{-2}$	$8(2p + p^2q - 5p^2 + 2p^3)$
Γ	if $q = 7$:
G_2	$2(1 + 5p + 11p^2 + 7p^3)$
G_3	$2(1 + 4p + 13p^2 + 6p^3)$

Theorem 3. *Let $G = (G, \cdot)$ be a group of order p^2q, where p, q are distinct primes, with $p > 2$.*

If Γ is a group of order p^2q and the Sylow p-subgroups of G and Γ are not isomorphic, then no regular subgroup of $\mathrm{Hol}(G)$ is isomorphic to Γ.

If G and Γ have isomorphic Sylow p-subgroups, then the following tables give equivalently

1. *the number $e'(\Gamma, G)$ of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ;*
2. *the number of (right) skew braces $(G, \cdot, \circ)$ such that $\Gamma \cong (G, \circ)$.*

(i) For $q \nmid p - 1$:

Γ \ G	*1*	*2*	*3*
1	p	$2pq$	$2q$
2	$p(p-1)$	$2p(pq - 2q + 1)$	$2q(p-1)$
3	$p^2(p-1)$	$2p^2q(p-1)$	$2(p^2q - pq - q + 1)$

where the upper left sub-tables of sizes 1×1, 2×2 and 3×3 give respectively the cases $p \nmid q - 1$, $p \parallel q - 1$ and $p^2 \mid q - 1$.

Γ \ G	*5*	*11*
5	p^2	$2pq$
11	$p^2(p^2-1)$	$2p(1 + qp^2 - 2q)$

where the upper left sub-tables of sizes 1×1 and 2×2 give respectively the cases $p \nmid q - 1$ and $p \mid q - 1$.

(ii) For $q \nmid p - 1$ and $q \mid p + 1$:

Γ \ G	*5*	*10*
5	p^2	$2p^2$
10	$\frac{1}{2}p(p-1)(q-1)$	$2 + 2p^2(q-3) - p^3 + p^4$

(iii) For $q \mid p-1$:

Γ \ G	*1*	*4*
1	p	$2p^3$
4	$q-1$	$2(p^2q-2p^2+1)$

If $q=2$,

Γ \ G	*5*	*6*	*7*
5	p^2	$2p$	$p^3(3p+1)$
6	$p^2(p+1)$	$2p(p+1)$	$p^3(p+1)(3p+1)$
7	1	2	$2+p(p+1)(2p-1)$

If $q=3$,

Γ \ G	*5*	*6*	*7*	*9*
5	p^2	$2p$	$p^3(3p+1)$	$4p^2$
6	$2p(p+1)$	$2p(p+3)$	$4p^3(p+1)^2$	$2p^2(3p+5)$
7	2	$2(p+1)$	$2+p^2(2p^2+3p+2)$	$2p^2+4p+2$
9	$2p^3+p^2-p$	$2(p^2+1)$	$2p^5+5p^4+p^3-p^2+p$	p^4+3p^3+2p+2

If $q>3$,

Γ \ G	*5*	*7*
5	p^2	$p^3(3p+1)$
6	$p(p+1)(q-1)$	$4p^2(p+1)(p^2+pq-2p)$
7	$q-1$	$2+p^2(2p^2+pq+2q-4)$
8, G_2	$p^2(p+1)(q-1)$	$2p^2(p+1)(p^2q-4p+pq+2)$
8, $G_k \not\simeq G_2$	$p(p+1)(q-1)$	$4p^2(p+1)(2p^2-5p+pq+2)$
9	$\frac{1}{2}p(p+1)(q-1)$	$4p^5+p^4(q-2)+p^3(2q-7)+3p^2+p$

Γ \ G	*6*	*9*
5	$2p$	$4p^2$
6	$2p(p+2q-3)$	$2p^2(4q+3p-7)$
7	$2+2p(q-2)$	$2+4p+2p^2(2q-5)$
8, G_2	$4(1+p(p+q-3))$	$2p(p^3+3p^2-14p+4pq-6)$
8, $G_k \not\simeq G_2$	$4(1+p(p+q-3))$	$2p(p^3+5p^2-18p+4pq+8)$
9	$2+2p(p+q-3)$	$2+4p+p^2(p^2+5p+4q-16)$

Γ \ *G8*	$G \not\simeq G_{\pm 2}$	$G \simeq G_{\pm 2},\ q>5$	$G \simeq G_2,\ q=5$
5	$4p^2$	$4p^2$	$4p^2$
6	$8p^2(q+p-2)$	$8p^2(q+p-2)$	$8p^2(p+3)$
7	$8p+4p^2(q-3)$	$8p+4p^2(q-3)$	$8p+8p^2$
8	*Table 1*	*Table 2*	$4(1+p+3p^2(p+1))$
9	$4p(2+p(q+2p-5))$	$2p(3+p(2q+3p-8))$	$8p(1+p+2p(p^2-1))$

The following is also obtained in [AB20a, AB20b] for $q > 2$, and [Cre21] for $q = 2$.

Theorem 4. *Let $G = (G, \cdot)$ be a group of order p^2q, where p, q are distinct primes, with $p > 2$. For each group Γ of order p^2q the following tables give equivalently*

1. *the number of conjugacy classes within $\mathrm{Hol}(G)$ of regular subgroups isomorphic to Γ;*
2. *the number of isomorphism classes of skew braces $(G, \cdot, \circ)$ such that $\Gamma \cong (G, \circ)$.*

(i) For $q \nmid p - 1$:

Γ \ G	*1*	*2*	*3*
1	2	$2p$	2
2	p	$2p(p-1)$	$2(p-1)$
3	p	$2p(p-1)$	$2p(p-1)$

where the upper left sub-tables of sizes 1×1, 2×2 and 3×3 give respectively the cases $p \nmid q - 1$, $p \parallel q - 1$ and $p^2 \mid q - 1$.

Γ \ G	*5*	*11*
5	2	4
11	4	$6p - 4$

where the upper left sub-tables of sizes 1×1 and 2×2 give respectively the cases $p \nmid q - 1$ and $p \mid q - 1$.

(ii) For $q \nmid p - 1$ and $q \mid p + 1$:

Γ \ G	*5*	*10*
5	2	2
10	1	$p + 2q - 4$

(iii) For $q \mid p - 1$:

Γ \ G	*1*	*4*
1	2	4
4	1	$2(q-1)$

If $q = 2$,

Γ \ G	*5*	*6*	*7*
5	2	2	5
6	2	8	$p+10$
7	1	2	5

If $q = 3$,

Γ \ G	*5*	*6*	*7*	*9*
5	2	2	5	3
6	1	12	16	$p+14$
7	1	4	8	4
9	2	6	10	$p+8$

If $q > 3$,

Γ \ G	*5*	*6*	*7*	*8*, G_k	*9*
5	2	2	5	4	3
6	1	$4q$	$4(q+1)$	$8(q+1)$	$4q+p+2$
7	1	$2(q-1)$	$3q-1$	$4(q-1)$	$2(q-1)$
8, $G_s \not\simeq G_2$	1	$4q$	$4(q+1)$	$8(q+1)$	$4q+p+2$
8, G_2	2	$4q$	$6q$	$8(q+1)$	$4q+p+2$
9	1	$2q$	$2(q+1)$	$4(q+1)$	$3q+p-1$

The lengths of the conjugacy classes are spelled out in Propositions 3.1, 3.2, 3.3, 3.4, 4.1, 4.2, 4.8, 4.9, 4.10, 4.12 and 4.13.

The case of groups of order p^2q with $p < q-1$ has been dealt with in [Die18] for braces. Braces have been introduced by Rump in [Rum07a], and correspond to the case when the group $(G, \cdot)$ is abelian.

Corollary 5. *A cyclic extension L/K of degree p^2q, with $p > 2$, admits exactly p cyclic Hopf-Galois structures.*

Moreover, the cyclic structures are the only Hopf-Galois structures on L/K if and only if there is only one isomorphism type of groups of order p^2q with cyclic Sylow p-subgroup, namely if and only if $p \nmid q-1$ and $q \nmid p-1$.

The first statement of the above corollary follows also from [Byo13].

Hopf-Galois structures of order $4q$

In the case $p = 2$ the holomorph of a group G of order $4q$ may have regular subgroups with Sylow 2-subgroups not isomorphic to the Sylow 2-subgroups of

G. In this case, already dealt with in [Koh07] for $q > 3$ and [SV18] for $q = 3$, a Galois extensions L/K with group Γ actually admits Hopf-Galois structures of type G also when the Sylow 2-subgroups of Γ and G are not isomorphic. In Chapter 5 we show an easy criterion to establish when the Sylow 2-subgroups change isomorphism type. Then we enumerate the Hopf Galois structures on Galois extension with group Γ of order $4q$ using gamma functions, and provide moreover the number of isomorphism classes of skew braces of size $4q$.

Related results

After a first part of this work ([CCDC20]) was submitted, two related manuscripts appeared on arXiv.

The first ([AB20a, AB20b]), due to Acri and Bonatto, concerns the enumeration of the isomorphism classes of skew braces of size p^2q for odd primes p and q. Equivalently, they enumerate the conjugacy classes of regular subgroups in the holomorph of groups G of order p^2q, for odd primes p and q.

They employ the methods of [GV17], and according to the algorithm therein, which they already employed in [AB20c], they organise their classification on the basis of the size of what in our context is the image $\gamma(G) \leq \mathrm{Aut}(G)$ of the gamma function.

The second manuscript ([Cre21]), due to Crespo, concerns the enumeration of the Hopf Galois structures on Galois extensions of order $2p^2$, for p odd. This is done by the direct determination of the regular subgroups of the holomorph of G, for every group G of order $2p^2$, p odd. Moreover, employing the methods of [GV17], she obtains the number of the isomorphism classes of skew braces of size $2p^2$, for p odd.

We deal also with the case $q > 2$, and provide in addition the sizes of the conjugacy classes. The common results of [AB20a, AB20b], [Cre21] agree with ours.

Comments

Some parts of this thesis are dealt with explicit computations and should be probably made more conceptual and less intricate. This will certainly be done, but at a later time, since, as often happens to beautiful experiences, my PhD also has come to an end.

> *" Je n'ay fait celle-ey plus longue que parce que je n'ay pas eu le loisir de la faire plus courte. "*
> Blaise Pascal, Les Lettres Provinciales, Seizième Lettre.

Acknowledgments

I would like to thank my supervisor Professor Ilaria Del Corso for her invaluable supervision, for all the support and for guiding me through these years of PhD.

I would also like to thank Professor Andrea Caranti for his fundamental collaboration on this project.

I would like to thank my referee, Nigel Byott and Cindy Tsang, for patiently and carefully reading these pages, and for their comments and suggestions.

My gratitude extends to the University of Milano-Bicocca for the opportunity to undertake my studies.

Last but not least, thanks to my family for being there for me always, and thanks to my friends and colleagues, for making this experience unique.

Chapter 1

The gamma function

1.1 Describing the regular subgroups of the holomorph

There are several equivalent ways to describe the regular subgroups of the holomorph of a group $(G, \cdot)$. As explained in the Introduction, we will appeal to the alternative group operation $\circ$ which occurs in the definition of a skew brace [GV17], but then mainly use the equivalent method of gamma functions, employed in [CDVS06, CDV17, CDV18, Car18].

The *abstract holomorph* of a group G is the natural semidirect product $\mathrm{Aut}(G)G$. We will use a certain concrete realisation of it, namely the *permutational holomorph*, as defined in the following.

Given a group G, denote by $\mathrm{Perm}(G)$ the group of all permutations on the underlying set G. The *right regular representation* of G is the homomorphism

$$\begin{aligned} \rho : G &\to \mathrm{Perm}(G) \\ g &\mapsto (x \mapsto xg). \end{aligned}$$

Similarly, the *left regular representation* of G is the *anti*homomorphism

$$\begin{aligned} \lambda : G &\to \mathrm{Perm}(G) \\ g &\mapsto (x \mapsto gx). \end{aligned}$$

Write $\mathrm{inv} : g \mapsto g^{-1}$ for the inversion map on G. Clearly $\mathrm{inv} \in \mathrm{Perm}(G)$.

The following facts are well known, see for instance [PS18, Lemma 3.8].

Proposition 1.1. *Denoting by* Norm *the normaliser in* $\mathrm{Perm}(G)$*, we have the following.*

1. *The stabiliser of* 1 *in the normaliser* $\mathrm{Norm}(\rho(G))$ *of the image* $\rho(G)$ *of the right regular representation is* $\mathrm{Aut}(G)$*.*

2. *We have*

$$\mathrm{Norm}(\rho(G)) = \mathrm{Aut}(G)\rho(G) = \mathrm{Aut}(G)\lambda(G) = \mathrm{Norm}(\lambda(G)),$$

and this group is isomorphic to the abstract holomorph $\mathrm{Aut}(G)G$ *of* G*.*

3. inv *centralises* $\mathrm{Aut}(G)$*, and conjugates* $\rho(G)$ *to* $\lambda(G) \leq \mathrm{Hol}(G)$*, that is*

$$\rho(G)^{\mathrm{inv}} = \lambda(G).$$

Thus inv *normalises* $\mathrm{Norm}(\rho(G))$*.*

In the following we will refer to $\mathrm{Norm}_{\mathrm{Perm}(G)}(\rho(G))$ as the *(permutational) holomorph* of G, and denote it by $\mathrm{Hol}(G)$.

Let G be a finite group, and let $N \leq \mathrm{Hol}(G)$ be a regular subgroup. Since N is regular, the map $N \to G$ sending $n \in N$ to 1^n is a bijection. Thus for each $g \in G$ there is a unique element $\nu(g) \in N$, such that $1^{\nu(g)} = g$, that is, $\nu : G \to N$ is the inverse of $n \mapsto 1^n$. Now $1^{\nu(g)\rho(g)^{-1}} = 1$, so that $\nu(g)\rho(g)^{-1} \in \mathrm{Aut}(G)$ by Proposition 1.1(1). Therefore for $g \in G$ we can write $\nu(g)$ uniquely in the form

$$\nu(g) = \gamma(g)\rho(g), \tag{1.1}$$

for a suitable map $\gamma : G \to \mathrm{Aut}(G)$. We have

$$\nu(g)\nu(h) = \gamma(g)\rho(g)\gamma(h)\rho(h) = \gamma(g)\gamma(h)\rho(g^{\gamma(h)}h). \tag{1.2}$$

Since N is a subgroup of $\mathrm{Perm}(G)$, $\gamma(g)\gamma(h) \in \mathrm{Aut}(G)$, and the expression (1.1) is unique, we have

$$\gamma(g)\gamma(h)\rho(g^{\gamma(h)}h) = \gamma(g^{\gamma(h)}h)\rho(g^{\gamma(h)}h),$$

from which we obtain

$$\gamma(g^{\gamma(h)}h) = \gamma(g)\gamma(h). \tag{1.3}$$

We obtain

Theorem 1.2. *Let* $(G, \cdot)$ *be a finite group. The following data are equivalent.*

1. *A regular subgroup* $N \leq \mathrm{Hol}(G)$*.*

2. *A map* $\gamma : G \to \mathrm{Aut}(G)$ *such that*

$$\gamma(g^{\gamma(h)}h) = \gamma(g)\gamma(h). \tag{1.4}$$

3. *A group operation* $\circ$ *on* G *such that for* $g, h, k \in G$

$$(gh) \circ k = (g \circ k)k^{-1}(h \circ k), \tag{1.5}$$

that is, such that $(G, \cdot, \circ)$ *is a (right) skew brace.*

The data of (1)-(3) *are related as follows.*

(i) $g \circ h = g^{\gamma(h)}h$ *for* $g, h \in G$.

(ii) Each element of N *can be written uniquely in the form* $\nu(h) = \gamma(h)\rho(h)$, *for some* $h \in G$.

(iii) For $g, h \in G$ *one has* $g^{\nu(h)} = g \circ h$.

(iv) The map

$$\gamma : (G, \circ) \to \mathrm{Aut}(G)$$

is a morphism.

(v) The map

$$\begin{array}{rccc} \nu : & (G, \circ) & \to & N \\ & h & \mapsto & \gamma(h)\rho(h) \end{array}$$

is an isomorphism.

This is basically [Car18, Theorem 1.2]. The equivalence of (3) to the other items of Theorem 1.2 follows from [GV17, Theorem 4.2]; for the convenience of the reader, we provide the table below detailing the relations between the properties of γ and the brace axioms. In this table, $(G, \cdot)$ is a group, $\circ$ is an operation on G, and for each $g \in G$ we define a function $\gamma(g) : G \to G$ by $x \mapsto (x \circ g) \cdot g^{-1}$, so that $x \circ g = x^{\gamma(g)} \cdot g$.

Property of $\circ$	Property of γ
The brace axiom (1.5) of Theorem 1.2 holds	$\gamma(g)$ is an endomorphism of G, for each $g \in G$
$\circ$ is associative	γ satisfies (1.4) of Theorem 1.2
$\circ$ admits inverses	$\gamma(g)$ is bijective, for each $g \in G$

In the table, the properties on the first line are equivalent. The properties on the second line are equivalent, under the assumption that $\gamma(g)$ is an endomorphism of G, for each $g \in G$. On the third line, the property on the right implies the property on the left, while to prove the left-to-right implication one need to assume (1.4) of Theorem 1.2. The fact that $(G, \circ)$ has an identity follows from the properties in the first line. Moreover the identity of $(G, \circ)$ is the same as the identity of $(G, \cdot)$.

Remark 1.3. In the rest of the paper, every time we discuss a regular subgroup as in (1) of Theorem 1.2, or a γ as in (2), we will employ the rest of the notation of Theorem 1.2 without further mention.

Definition 1.4. Let G be a group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function.

γ is said to satisfy the *gamma functional equation* (or *GFE* for short) if

$$\gamma(g^{\gamma(h)}h) = \gamma(g)\gamma(h), \qquad \text{for all } g, h \in A.$$

γ is said to be a *relative gamma function* (or *RGF* for short) on A if it satisfies the gamma functional equation, and A is $\gamma(A)$-invariant.

If $A = G$, a relative gamma function is simply called a *gamma function* (or *GF* for short) on G.

A RGF $\gamma : A \to \mathrm{Aut}(G)$ defines a group operation $g \circ h = g^{\gamma(h)}h$ on A.

Remark 1.5. Our γ are related to the bijective 1-cocycles of [GV17]. Recall that if the group $(H, \bullet)$ acts (on the right) on the group $(G, \cdot)$ via automorphisms, a map

$$\pi : H \to G$$

is said to be a 1-*cocycle* if

$$\pi(a \bullet b) = \pi(a)^b \cdot \pi(b), \quad \text{for } a, b \in H,$$

where g^h denotes the action of $h \in H$ on $g \in G$.

It is proved in [GV17, Proposition 1.11] that if $(G, \cdot, \circ)$ is a skew brace, then the identity map $\pi : (G, \circ) \to (G, \cdot)$ is a 1-cocycle, where G acts on itself, in our notation, by $g^h = g^{\gamma(h)}$.

In fact

$$\pi(a \circ b) = a \circ b = a^{\gamma(b)} \cdot b = \pi(a)^b \cdot \pi(b).$$

Conversely, a bijective 1-cocycle $\pi : (H, \bullet) \to (G, \cdot)$ induces a skew brace structure $(G, \cdot, \circ)$ on $(G, \cdot)$ via

$$a \circ b = \pi(\pi^{-1}(a) \bullet \pi^{-1}(b)), \quad \text{for } a, b \in G.$$

In our notation, this means that the function

$$\begin{aligned} \gamma : G &\to \mathrm{Aut}(G) \\ b &\mapsto (a \mapsto \pi(\pi^{-1}(a) \bullet \pi^{-1}(b)) \cdot b^{-1}) \end{aligned}$$

is a GF.

1.2 Invariant subgroups

The following proposition is a slightly more general version of [TQ20, Proposition 3.3]

Proposition 1.6. *Let G be a finite group, let $H \subseteq G$ and let γ be a GF on G.*

Any two of the following conditions imply the third one:

1. $H \leq G$;

2. $(H, \circ) \leq (G, \circ)$;

3. H *is* $\gamma(H)$*-invariant.*

If these conditions hold, then $(H, \circ)$ *is isomorphic to a regular subgroup of* $\mathrm{Hol}(H)$.

Proof. The equivalence follows from the fact that for $h_1, h_2 \in H$ we have

$$h_1 \circ h_2 = h_1^{\gamma(h_2)} h_2 \qquad \text{and} \qquad h_1^{\gamma(h_2)^{-1}} \circ h_2 = h_1 h_2.$$

If the conditions hold, the fact that H is $\gamma(H)$-invariant implies that we have a map

$$\begin{aligned} \gamma' : H &\to \mathrm{Aut}(H) \\ h &\mapsto \gamma(h)_{\restriction H} \end{aligned}$$

which satisfies the GFE because γ does, so that γ' is a GF on H. If $\circ'$ is the group operation on H associated to γ', the identity map

$$(H, \circ') \to (G, \circ)$$

is a group morphism, as for $h_1, h_2 \in H$ one has

$$h_1 \circ' h_2 = h_1^{\gamma'(h_2)} h_2 = h_1^{\gamma(h_2)} h_2 = h_1 \circ h_2.$$

It follows that $(H, \circ') = (H, \circ)$ is isomorphic to a regular subgroup of $\mathrm{Hol}(H)$. □

The subgroups H verifying the conditions of Proposition 1.6 in the language of braces are called *sub-skew braces*.

1.3 Isomorphism of Sylow p-subgroups

From Proposition 1.6 we have that if one of the Sylow p-subgroups H of G is invariant under $\gamma(H)$, then the isomorphism type of the Sylow p-subgroups of $(G, \circ)$ is to be found among the isomorphism types of regular subgroups of $\mathrm{Hol}(H)$. If there is no such invariant Sylow p-subgroup, then it is conceivable that the Sylow p-subgroups of regular subgroups of $\mathrm{Hol}(G)$ could take further isomorphism types.

For some classes of p-subgroups the criterion given in Proposition 1.6 can be made more explicit.

Corollary 1.7. *Let G and Γ be finite groups. Suppose $e'(\Gamma, G) \neq 0$. Let $N \leq \mathrm{Hol}(G)$ be a regular subgroup isomorphic to Γ, and γ the GF associated to N.*

If p is an odd prime and H is a $\gamma(H)$-invariant p-subgroup of G, then

1. *if H is cyclic then $H \cong (H, \circ)$;*
2. *if H is abelian and of rank m, with $m < p-1$, or $m = 2$ and $p = 3$, and $(H, \circ)$ is abelian too, then $H \cong (H, \circ)$.*

Proof. If H is a cyclic p-group with $p > 2$, by [Rum07b, Corollary, 680] or by [CS19, Proposition 4], every regular subgroup of $\mathrm{Hol}(H)$ is cyclic (see also [Chi00, (8.6) Proposition]).

In the case when H is abelian of rank m, with $m + 1 < p$, or $m = 2$ and $p = 3$, by [FCC12, Theorem 1 and Proposition 4], all the abelian subgroups of $\mathrm{Hol}(H)$ are isomorphic to H.

Both statements now follow from Proposition 1.6. □

In Theorem 2.3 we will show that in the case of groups of order p^2q with $p > 2$ the conditions of Proposition 1.6 are fulfilled for H a Sylow p-subgroup of G and for each GF. This will simplify our classification since it implies that $e(\Gamma, G) = 0$ whenever the Sylow p-subgroups of Γ and G are not isomorphic (as we will show in Chapter 5 this does not hold for $p = 2$). We will also prove (see Theorem 2) that in that case the condition of having isomorphic Sylow p-subgroups is also sufficient for $e(\Gamma, G) \neq 0$.

1.4 Tools of the trade

We now collect several facts related to the gamma functions, which we are going to exploit for our classification.

We begin by rephrasing conjugacy of regular subgroups within $\mathrm{Hol}(G)$ in terms of gamma functions, and recording a simple property that will be useful in Chapters 3, 4, 5. Conjugacy of regular subgroups of the holomorph of the group $(G, \cdot)$ is equivalent to isomorphism of skew braces $(G, \cdot, \circ)$, and to a certain equivalence of Hopf-Galois structures.

Note that since N is regular, we have $\mathrm{Hol}(G) = \mathrm{Aut}(G)N$, so that the conjugates of N under $\mathrm{Hol}(G)$ coincide with the conjugates under $\mathrm{Aut}(G)$. Now [SV18, Proposition A.3] (see also the last statement of [CDVS06, Theorem 1]) states that, given a group $G = (G, \cdot)$, there is a bijection between isomorphism classes of skew braces $(G, \cdot, \circ)$, and classes of regular subgroups of $\mathrm{Hol}(G)$ under conjugation by elements of $\mathrm{Aut}(G)$. We give the simple translation of the latter in terms of gamma functions.

Lemma 1.8. *Let G be a group, N a regular subgroup of $\mathrm{Hol}(G)$, and γ the associated gamma function.*

Let $\varphi \in \mathrm{Aut}(G)$.

1. *The gamma function γ^φ associated to the regular subgroup N^φ is given by*
$$\gamma^\varphi(g) = \gamma(g^{\varphi^{-1}})^\varphi = \varphi^{-1}\gamma(g^{\varphi^{-1}})\varphi, \tag{1.6}$$
for $g \in G$.

2. *If $H \leq G$ is invariant under $\gamma(H)$, then H^φ is invariant under $\gamma^\varphi(H^\varphi)$.*

We will refer to the action of $\mathrm{Aut}(G)$ on γ of the Lemma as *conjugation.*

Proof. For $x \in G$ we have $\nu(x)^\varphi = \gamma(x)^\varphi\rho(x^\varphi)$. Since $\nu(x)^\varphi$ takes 1 to x^φ, we have $\gamma^\varphi(x^\varphi) = \gamma(x)^\varphi$, which yields (1.6) substituting $g = x^\varphi$.

If $H \leq G$ is invariant under $\gamma(H)$, and $h_1, h_2 \in H$, then

$$(h_1^\varphi)^{\gamma^\varphi(h_2^\varphi)} = h_1^{\varphi\varphi^{-1}\gamma(h_2)\varphi} = (h_1^{\gamma(h_2)})^\varphi \in H^\varphi.$$

□

We now record two simple facts, which we will be using repeatedly, concerning inverses and conjugacy in the group $(G, \circ)$ of Theorem 1.2. We write $a^{\ominus 1}$ for the inverse of $a \in G$ in $(G, \circ)$.

Lemma 1.9. *In the notation of Theorem 1.2, we have, for $a, b \in G$,*

$$a^{\ominus 1} = a^{-\gamma(a)^{-1}},$$

and

$$a^{\ominus 1} \circ b \circ a = a^{-\gamma(a)^{-1}\gamma(b)\gamma(a)} b^{\gamma(a)} a.$$

Proof. If z is the inverse of a in $(G, \circ)$, we have $1 = z \circ a = z^{\gamma(a)}a$, whence $z = a^{-\gamma(a)^{-1}}$.

$$\begin{aligned} a^{\ominus 1} \circ b \circ a &= a^{-\gamma(a)^{-1}} \circ b \circ a \\ &= (a^{-\gamma(a)^{-1}\gamma(b)} b) \circ a \\ &= a^{-\gamma(a)^{-1}\gamma(b)\gamma(a)} b^{\gamma(a)} a. \end{aligned}$$

□

Remark 1.10. Note, for later usage, that (1.4) can be rephrased, setting $k = g^{\gamma(h)}$, as

$$\gamma(kh) = \gamma(k^{\gamma(h)^{-1}})\gamma(h). \tag{1.7}$$

Lemma 1.11. *Let G be a finite group, and γ a GF on G. We have*

1. $\ker(\gamma) \trianglelefteq (G, \circ)$, *and*
2. $\ker(\gamma) \leq G$.

Proof. The first claim is clear as $\gamma : (G, \circ) \to \mathrm{Aut}(G)$ is a morphism (Theorem 1.2(iv)).

Since $\ker(\gamma)$ is invariant under $\gamma(\ker(\gamma)) = \{1\}$, Proposition 1.6 implies $\ker(\gamma) \leq G$. □

In the statement of the next result we write $[g, \alpha] = g^{-1}g^{\alpha}$, for $g \in G$, $\alpha \in \mathrm{Aut}(G)$. This is indeed an ordinary commutator in the abstract holomorph of G. We write

$$[A, \gamma(A)] = \{[x, \gamma(y)] : x, y \in A\}.$$

Lemma 1.12. *Let G be a finite group, $A \leq G$, and $\gamma : A \to \mathrm{Aut}(G)$ a function such that A is invariant under $\gamma(A)$.*

Then any two of the following conditions imply the third one.

1. $\gamma([A, \gamma(A)]) = \{1\}$.
2. $\gamma : A \to \mathrm{Aut}(G)$ *is a morphism of groups.*
3. γ *satisfies the GFE.*

Proof. Suppose $\gamma([A, \gamma(A)]) = \{1\}$. If γ is a morphism, then for $x, y \in A$ we have

$$\gamma(x^{\gamma(y)}y) = \gamma(x[x, \gamma(y)]y) = \gamma(x)\gamma([x, \gamma(y)])\gamma(y) = \gamma(x)\gamma(y),$$

that is, γ satisfies the GFE. Conversely, suppose γ satisfies the GFE, so that $\gamma(A)$ is a subgroup of $\mathrm{Aut}(G)$. Then for $x, y \in A$ we have

$$\begin{aligned}\gamma(xy) &= \gamma(x^{\gamma(y)^{-1}})\gamma(y)\\ &= \gamma(x[x, \gamma(y)^{-1}])\gamma(y)\\ &= \gamma(x^{\gamma([x,\gamma(y)^{-1}])^{-1}})\gamma([x, \gamma(y)^{-1}])\gamma(y)\\ &= \gamma(x)\gamma(y).\end{aligned}$$

Suppose now γ is a morphism and satisfies the GFE. Then for $x, y \in A$ we have

$$\gamma(x)\gamma(y) = \gamma(x^{\gamma(y)}y) = \gamma(x[x, \gamma(y)]y) = \gamma(x)\gamma([x, \gamma(y)])\gamma(y),$$

so that $\gamma([x, \gamma(y)]) = 1$. □

1.5 Lifting and restriction

The next result can be considered as a vestigial form of the First Isomorphism Theorem for gamma functions.

We write

$$\begin{aligned}\iota : &G \to \mathrm{Aut}(G)\\ &g \mapsto (x \mapsto g^{-1}xg).\end{aligned}$$

Proposition 1.13. *Let G be a finite group and let A, B be subgroups of G such that $G = AB$.*

If γ is a GF on G, and $B \leq \ker(\gamma)$, then

$$\gamma(ab) = \gamma(a), \text{ for } a \in A, b \in B, \tag{1.8}$$

so that $\gamma(G) = \gamma(A)$.

Moreover, if A is $\gamma(A)$-invariant, then

$$\gamma' = \gamma_{\restriction A} \colon A \to \mathrm{Aut}(G) \tag{1.9}$$

is a RGF on A and $\ker(\gamma)$ is invariant under the subgroup

$$\{\gamma'(a)\iota(a) : a \in A\}$$

of $\mathrm{Aut}(G)$.

Conversely, let $\gamma' : A \to \mathrm{Aut}(G)$ be a RGF such that

1. *$\gamma'(A \cap B) \equiv 1$,*
2. *B is invariant under $\{\gamma'(a)\iota(a) : a \in A\}$.*

Then the map

$$\gamma(ab) = \gamma'(a), \text{ for } a \in A, b \in B,$$

is a well defined GF on G, and $\ker(\gamma) = \ker(\gamma')B$.

In this situation we will say that γ is a *lifting* of γ'.

Proof. Clearly γ is constant on the cosets of $\ker(\gamma)$, and thus also on the cosets of B, so that (1.8) holds, and thus $\gamma(G) = \gamma(A)$. Assume now that A is $\gamma(A)$-invariant; by Proposition 1.6, A is a subgroup of $(G, \circ)$ and γ' as in (1.9) satisfies the GFE, so that γ' is a RGF.

For $a \in A$ and $k \in \ker(\gamma)$ we have

$$a^{\ominus 1} \circ k \circ a = a^{-\gamma(a)^{-1}\gamma(k)\gamma(a)} k^{\gamma(a)} a = a^{-1} k^{\gamma(a)} a = k^{\gamma(a)\iota(a)},$$

and since $a^{\ominus 1} \circ k \circ a \in \ker(\gamma)$, we get $k^{\gamma(a)\iota(a)} \in \ker(\gamma)$, namely, $\ker(\gamma)$ is invariant under the action of $\{\gamma'(a)\iota(a) : a \in A\}$.

Note that the latter is a subgroup of $\mathrm{Aut}(G)$, as for $a_1, a_2 \in A$ we have

$$\begin{aligned} \gamma(a_1)\iota(a_1)\gamma(a_2)\iota(a_2) &= \gamma(a_1)\gamma(a_2)\iota(a_1^{\gamma(a_2)})\iota(a_2) \\ &= \gamma(a_1^{\gamma(a_2)} a_2)\iota(a_1^{\gamma(a_2)} a_2), \end{aligned}$$

with $a_1^{\gamma(a_2)} a_2 \in A$, as A is $\gamma(A)$-invariant.

Conversely, let $\gamma' : A \to \mathrm{Aut}(G)$ be a RGF such that (1) and (2) hold, and define $\gamma(ab) = \gamma'(a)$ for each $a \in A$, $b \in B$. The map γ is well-defined; in fact

for $i = 1, 2$, let $a_i \in A$ and $b_i \in B$ be such that $a_1 b_1 = a_2 b_2$; then $a_1 = a_2 b_2 b_1^{-1}$, so $b = b_2 b_1^{-1} \in A \cap B$ and

$$\gamma'(a_1) = \gamma'(a_2 b) = \gamma'(a_2^{\gamma'(b)^{-1}})\gamma'(b) = \gamma'(a_2).$$

Moreover

$$\gamma(a_1 b_1)\gamma(a_2 b_2) = \gamma'(a_1)\gamma'(a_2) = \gamma'(a_1^{\gamma(a_2)} a_2)$$

and

$$\begin{aligned}\gamma((a_1 b_1)^{\gamma(a_2 b_2)} a_2 b_2) &= \gamma(a_1^{\gamma(a_2)} b_1^{\gamma(a_2)} a_2 b_2) \\ &= \gamma(a_1^{\gamma(a_2)} a_2 b_1^{\gamma(a_2)\iota(a_2)} b_2) \\ &= \gamma'(a_1^{\gamma(a_2)} a_2),\end{aligned}$$

where the last equality holds because of (2); thus γ is a GF on G. Finally, $\gamma(ab) = \gamma'(a) = 1$ if and only if $a \in \ker(\gamma')$, so $\ker(\gamma) = \ker(\gamma')B$. □

Corollary 1.14. *In the notation of Proposition 1.13, let γ be the lifting of γ' to G. Then γ is a morphism if and only if γ' is a morphism and* $\ker(\gamma)$ *is a normal subgroup of G.*

Proof. Clearly, if γ is a morphism then so is its restriction γ', and $\ker(\gamma)$ is a normal subgroup of G.

Conversely, if γ' is a morphism and $\ker(\gamma)$ is a normal subgroup of G then for $a_i \in A$ and $b_i \in B$, $i = 1, 2$, we have

$$\gamma(a_1 b_1 a_2 b_2) = \gamma(a_1 a_2 b_1^{a_2} b_2) = \gamma'(a_1 a_2) = \gamma'(a_1)\gamma'(a_2) = \gamma(a_1 b_1)\gamma(a_2 b_2).$$

□

We now aim at establishing a criterion (Proposition 1.18) that allows us to define a map $\gamma' : A \to \mathrm{Aut}(G)$ which verifies the GFE, in the case when A is a cyclic p-group.

First, we state separately two elementary arithmetic lemmas which will be useful in the following. The first one is well-known.

Lemma 1.15. *Let $p > 2$ be a prime and let $n > m \geq 0$ be integers. The solutions of the congruence*

$$x^{p^m} \equiv 1 \bmod p^n \tag{1.10}$$

are the integers of type $x = 1 + hp^{n-m}$.

Lemma 1.16. *Let $p > 2$ be a prime and let $s \in \mathbb{Z}$, $s \equiv 1 \bmod p$. Define $e_s(0) = 0$ and for each $k > 0$*

$$e_s(k) = \sum_{i=0}^{k-1} s^i.$$

Then, for each $n \in \mathbb{N}$, the set $\{e_s(0), \ldots, e_s(p^n - 1)\}$ is a set of representatives of the classes modulo p^n.

Proof. We will show that for $k, h \in \mathbb{Z}$

$$e_s(k) \equiv e_s(h) \bmod p^n \iff k \equiv h \bmod p^n$$

and this implies the lemma. Let

$$s = 1 + p^l h \quad \text{with } \gcd(h, p) = 1; \tag{1.11}$$

by hypothesis $l > 0$. If $k > h \geq 0$, taking into account equality (1.11), we have

$$\begin{aligned} e_s(k) \equiv e_s(h) \bmod p^n &\iff s^h \sum_{i=0}^{k-h-1} s^i \equiv 0 \bmod p^n \\ &\iff \sum_{i=0}^{k-h-1} s^i \equiv 0 \bmod p^n \\ &\iff (s-1) \sum_{i=0}^{k-h-1} s^i \equiv 0 \bmod p^{n+l} \\ &\iff s^{k-h} \equiv 1 \bmod p^{n+l}. \end{aligned}$$

By Lemma 1.15, $s = 1 + p^l h$ $(\gcd(h, p) = 1)$ is a solution of the last equation if and only if $k - h \equiv 0 \bmod p^n$. □

Corollary 1.17. *Let G be a finite group, and let $A = \langle\, a \,\rangle$ be a cyclic subgroup of G of order p^n, where p is an odd prime. Let*

$$\gamma : A \to \mathrm{Aut}(G)$$

be a RGF and let $a^{\gamma(a)} = a^s$.

Then, for each k,

$$a^{\circ k} = a^{e_s(k)}, \tag{1.12}$$

so $\mathrm{ord}_{(A,\circ)}(a) = \mathrm{ord}_A(a)$ and $(A, \circ)$ is generated by a.

Proof. The equality in (1.12) can be easily shown by induction; the corollary follows then from Lemma 1.16 since $a^{\circ k} \in A$ for each k. □

Proposition 1.18. *Let G be a finite group, and let $A = \langle a \rangle$ be a cyclic subgroup of G of order p^n, where p is an odd prime.*

Let $\eta \in \mathrm{Aut}(G)$.

The following are equivalent.

1. *There is a RGF*
$$\gamma : A \to \mathrm{Aut}(G)$$
such that $\gamma(a) = \eta$.

2. *(a) A is η-invariant, and*
(b) $\mathrm{ord}(\eta) \mid p^n$.

When these conditions hold, γ is uniquely defined.

Proof. Assume first that the map $\gamma : A \to \mathrm{Aut}(G)$ is a RGF, and let $\gamma(a) = \eta$. Then, $\gamma\colon (A, \circ) \to \mathrm{Aut}(G)$ is a morphism, so

$$\mathrm{ord}(\eta) \ \mid \mathrm{ord}_{(A,\circ)}(a) = \mathrm{ord}_A(a) = p^n$$

where the first equality follows from Corollary 1.17.

As to the converse, assume (2) holds. Then $\eta_{\restriction A} \in \mathrm{Aut}(A) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$ and, if $\eta(a) = a^s$, then $s \in (\mathbb{Z}/p^n\mathbb{Z})^*$ and

$$\mathrm{ord}(s) = \mathrm{ord}(\eta_{\restriction A}) \mid \gcd(p^n, \varphi(p^n)) = p^{n-1},$$

so that, by Lemma 1.15,

$$s \equiv 1 \bmod p. \tag{1.13}$$

In the notation of Lemma 1.16 we have that $\{e_s(0), \ldots, e_s(p^n - 1)\}$ is a set of representatives of the classes modulo p^n, hence $A = \left\{a^{e_s(k)}\right\}_{k=0}^{p^n-1}$. Therefore we can define γ on A letting, for all k,

$$\gamma(a^{e_s(k)}) = \eta^k,$$

and we have only to check that it satisfies the GFE. Now $a_1 = a^{e_s(k_1)}$, $a_2 = a^{e_s(k_2)}$, for some k_1, k_2, so that

$$\begin{aligned}
\gamma(a_1^{\gamma(a_2)} a_2) &= \gamma((a^{e_s(k_1)})^{\gamma(a^{e_s(k_2)})} a^{e_s(k_2)}) \\
&= \gamma((a^{e_s(k_1)})^{\eta^{k_2}} a^{e_s(k_2)}) \\
&= \gamma(a^{s^{k_2} \sum_{i=0}^{k_1-1} s^i} a^{\sum_{i=0}^{k_2-1} s^i}) \\
&= \gamma(a^{\sum_{i=0}^{k_1+k_2-1} s^i}) \\
&= \gamma(a^{e_s(k_1+k_2)}) \\
&= \eta^{k_1+k_2}
\end{aligned}$$

$$= \gamma(a^{e_s(k_1)})\gamma(a^{e_s(k_2)})$$
$$= \gamma(a_1)\gamma(a_2).$$

Finally, if $\gamma' : A \to \mathrm{Aut}(G)$ is a RGF such that $\gamma'(a) = \eta$, denoting by $\circ'$ the operation $a_1 \circ' a_2 = a_1^{\gamma'(a_2)} a_2$, we have that $\gamma'(a^{\circ' k}) = \eta^k$, for each k. On the other hand,

$$a^{\circ' k} = a^{\sum_{i=0}^{k-1} \eta^i} = a^{e_s(k)},$$

so that

$$\gamma'(a^{e_s(k)}) = \gamma'(a^{\circ' k}) = \eta^k = \gamma(a^{e_s(k)}),$$

that is, $\gamma' = \gamma$. □

Corollary 1.19. *Let G be a finite group, and let $A = \langle a \rangle$ be a cyclic subgroup of G of order p^n where p is an odd prime.*

Let $\gamma\colon A \to \mathrm{Aut}(G)$ be a RGF.

Then the following are equivalent:

1. *γ is a morphism, and*
2. *$a^{\gamma(a)} = a^s$, with $s \equiv 1 \bmod \mathrm{ord}(\gamma(a))$.*

Proof. Let $\gamma(a) = \eta$. Then γ is a morphism if and only if, for all k,

$$\gamma(a^{e_s(k)}) = \gamma(a)^{e_s(k)},$$

or equivalently

$$\eta^k = \eta^{e_s(k)},$$

namely, $e_s(k) \equiv k \bmod \mathrm{ord}(\eta)$. The last condition is easily seen to be equivalent to $s \equiv 1 \bmod \mathrm{ord}(\eta)$.

In fact, if $s \equiv 1 \bmod \mathrm{ord}(\eta)$ then clearly $e_s(k) \equiv k \bmod \mathrm{ord}(\eta)$ for all k.

On the the hand, if $e_s(k) \equiv k \bmod \mathrm{ord}(\eta)$ for all k, then, in particular, $e_s(2) = s^0 + s = 2 + (s-1) \equiv 2 \bmod \mathrm{ord}(\eta)$ namely $s \equiv 1 \bmod \mathrm{ord}(\eta)$. □

Corollary 1.20. *In the notation of Corollary 1.19, assume*

$$\mathrm{ord}(\gamma(a)) = p.$$

Then γ is a morphism.

Proof. This follows from Corollary 1.19 and equation (1.13). □

1.6 Duality

The GF associated to the image $\rho(G)$ of the right regular representation is $\gamma(g) = 1$ for every $g \in G$, and the associated circle operation on G is the defining operation on the group G.

The GF associated to the image $\lambda(G) = \rho(G)^{\text{inv}}$ of the left regular representation (see Proposition 1.1(3)) is $\iota(y^{-1})$, and the associated circle operation is the opposite operation, $x \circ y = yx$, as $x^{\iota(y^{-1})}y = yx = x^{\lambda(y)}$. In particular,

$$\begin{aligned} \text{inv} : G &\to (G, \circ) \\ x &\mapsto x^{-1} \end{aligned}$$

is an isomorphism in this case.

Our next result is an extension of the above pairing between the images of the right and the left regular representations to all regular subgroups of $\text{Hol}(G)$. This will be useful, as it allows us to halve the number of GF we have to consider, when G is non-abelian, and also because it allows us in some circumstances to choose a GF with a kernel that is more suitable for calculations (see Proposition 1.23 below).

Proposition 1.21. *Let G be a finite group, $\gamma : G \to \text{Aut}(G)$ a GF, N the associated regular subgroup of $\text{Hol}(G)$, and $\circ$ the associated operation.*

Then

$$\begin{aligned} \tilde{\gamma} : G &\to \text{Aut}(G) \\ x &\mapsto \gamma(x^{-1})\iota(x^{-1}) \end{aligned}$$

is also a GF, which corresponds to the regular subgroup N^{inv}, that is, the conjugate of N under $\text{inv} \in S(G)$. If $\tilde{\circ}$ is the operation associated to $\tilde{\gamma}$, then

$$\text{inv} : (G, \circ) \to (G, \tilde{\circ})$$

is an isomorphism.

Proof. From Proposition 1.1(3) we have that inv normalises $\text{Hol}(G)$.

Consider the conjugate of $N = \{\gamma(y)\rho(y) : y \in G\}$ under inv, which will be another regular subgroup of $\text{Hol}(G)$. We have

$$\begin{aligned} x^{(\gamma(y)\rho(y))^{\text{inv}}} &= (x^{-\gamma(y)}y)^{-1} \\ &= y^{-1}x^{\gamma(y)} \\ &= x^{\gamma(y)\iota(y)\rho(y^{-1})}. \end{aligned}$$

In particular, $1^{(\gamma(y)\rho(y))^{\text{inv}}} = y^{-1}$, that is, $(\gamma(y)\rho(y))^{\text{inv}}$ is the element of N^{inv} taking 1 to y^{-1}. Therefore the GF associated to N^{inv} is

$$\begin{aligned} \tilde{\gamma} : G &\to \text{Aut}(G) \\ y &\mapsto \gamma(y^{-1})\iota(y^{-1}). \end{aligned}$$

The operation associated to $\tilde{\gamma}$ is

$$\begin{aligned} x \,\tilde{\circ}\, y &= x^{\tilde{\gamma}(y)} y \\ &= x^{\gamma(y^{-1})\iota(y^{-1})} y \\ &= y x^{\gamma(y^{-1})} \\ &= (x^{-\gamma(y^{-1})} y^{-1})^{-1} \\ &= (x^{-1} \circ y^{-1})^{-1}, \end{aligned}$$

so that, as in the case of G and its opposite group, $\mathrm{inv} : (G, \circ) \to (G, \tilde{\circ})$ is an isomorphism. (See also [CDV18, Lemma 1.4].) □

Lemma 1.22. *Let G be a finite non-abelian group. Let C be a non-trivial subgroup of G such that:*

1. *C is abelian;*
2. *C is characteristic in G;*
3. *$C \cap Z(G) = \{1\}$.*

Let $\gamma : G \to \mathrm{Aut}(G)$ be a GF, and suppose that for every $c \in C$ we have $\gamma(c) = \iota(c^{-\sigma})$ for some function $\sigma : C \to C$.

Then $\sigma \in \mathrm{End}(C)$, and for every $g \in G$ the following relation holds in $\mathrm{End}(C)$:

$$\sigma\, \gamma(g)_{\restriction C}\, (\sigma - 1) = (\sigma - 1)\, \gamma(g)_{\restriction C}\, \iota(g)_{\restriction C}\, \sigma. \tag{1.14}$$

Proof. For $c_1, c_2 \in C$ we have

$$\begin{aligned} \iota((c_1 c_2)^{-\sigma}) &= \gamma(c_1 c_2) \\ &= \gamma(c_1^{\gamma(c_2)^{-1}})\gamma(c_2) \\ &= \gamma(c_1^{\iota((c_2^{-\sigma})^{-1})})\gamma(c_2) \\ &= \iota(c_1^{-\sigma})\iota(c_2^{-\sigma}) \\ &= \iota(c_1^{-\sigma} c_2^{-\sigma}). \end{aligned}$$

Since C is abelian, and $C \cap Z(G) = \{1\}$, we obtain that σ is an endomorphism of C.

For $g \in G$ and $c \in C$ we have

$$\begin{aligned} g^{\ominus 1} \circ c \circ g &= g^{-\gamma(g)^{-1}\gamma(c)\gamma(g)} c^{\gamma(g)} g \\ &= g^{-\iota(c^{-\sigma\gamma(g)})} g c^{\gamma(g)\iota(g)} \\ &= c^{\sigma\gamma(g)} g^{-1} c^{-\sigma\gamma(g)} g c^{\gamma(g)\iota(g)} \\ &= c^{\sigma\gamma(g) - \sigma\gamma(g)\iota(g) + \gamma(g)\iota(g)}. \end{aligned} \tag{1.15}$$

On the other hand

$$\gamma(g^{\ominus 1} \circ c \circ g) = \gamma(g)^{-1}\gamma(c)\gamma(g) = \iota(c^{-\sigma\gamma(g)}),$$

so that, writing τ for the exponent $\sigma\gamma(g) - \sigma\gamma(g)\iota(g) + \gamma(g)\iota(g)$ of c in the last term of (1.15), we get

$$\gamma(c^{\tau}) = \iota(c^{-\tau\sigma}).$$

Since $C \cap Z(G) = \{1\}$, we obtain $\sigma\gamma(g) = \tau\sigma$, and thus (1.14). □

Proposition 1.23. *Let G be a finite non-abelian group. Let C be a subgroup of G such that:*

1. *$C = \langle\, c \,\rangle$ is cyclic, of order a power of the prime r,*
2. *C is characteristic in G,*
3. *$C \cap Z(G) = \{1\}$, and*
4. *there is $g \in G$ which induces by conjugation on C an automorphism whose order is not a power of r.*

Let $\gamma : G \to \mathrm{Aut}(G)$ be a GF, and suppose that for every $c \in C$ we have $\gamma(c) = \iota(c^{-\sigma})$, for some function $\sigma : C \to C$.

Then

1. *either $\sigma = 0$, that is, $C \leq \ker(\gamma)$,*
2. *or $\sigma = 1$, that is, $\gamma(c) = \iota(c^{-1})$, so that $C \leq \ker(\tilde{\gamma})$.*

Note that the hypotheses of Proposition 1.23 contain those of Lemma 1.22.

Proof. It is immediate that $\sigma \in \mathrm{End}(C)$, so that we can identify σ with an integer modulo the order of C.

Since $\mathrm{End}(C)$ is abelian, and $\gamma(g)_{\restriction C} \in \mathrm{Aut}(C)$, we obtain from (1.14) the equality

$$\sigma(\sigma - 1)(\iota(g)_{\restriction C} - 1) = 0$$

in $\mathrm{End}(C)$, for all $g \in G$. Choose now $g \in G$ which induces on C an automorphism $\iota(g)$ whose order is not a power of r. Then $\iota(g)_{\restriction C} - 1$ is not a zero divisor in $\mathrm{End}(C)$, so that

$$\sigma(\sigma - 1) = 0.$$

Since $\mathrm{End}(C)$ is a local ring, we obtain that either $\sigma = 0$, or $\sigma = 1$.

If the latter holds we have then

$$\tilde{\gamma}(c) = \gamma(c^{-1})\iota(c^{-1}) = \iota(c)\iota(c^{-1}) = 1.$$

□

Remark 1.24. In Proposition 1.23, once γ has been chosen, we can replace the hypothesis (2) with the slightly more general hypothesis that C is normal and $\gamma(G)$-invariant. In fact, in that case $\gamma(g)_{|C} \in \mathrm{Aut}(C)$. Moreover, the proof of Lemma 1.22 still works, as $c^{\iota(g)}, c^{\gamma(g)} \in C$, so that equation (1.14) is satisfied.

Corollary 1.25. *Let G be a finite non-abelian group. Suppose that G contains a subgroup C which satisfies the hypotheses of Proposition 1.23, and that every GF γ on G satisfies $\gamma(C) \leq \iota(C)$.*

For each group $\mathcal{G}$ of the same order as G, let

$$n_C(\mathcal{G}) = |\{\gamma \text{ GF on } G : (G,\circ) \cong \mathcal{G} \text{ and } C \leq \ker(\gamma)\}|\,.$$

Then

$$e'(\mathcal{G},G) = |\{\gamma \text{ GF on } G : (G,\circ) \cong \mathcal{G}\}| = 2n_C(\mathcal{G}).$$

Proof. Denote by X the set of the GF's on G for which the corresponding operation $\circ$ is such that $(G,\circ) \cong \mathcal{G}$. Write

$$X_1 = \{\gamma \text{ GF on } G : (G,\circ) \cong \mathcal{G} \text{ and } C \leq \ker(\gamma)\}\,,$$
$$X_2 = \{\gamma \text{ GF on } G : (G,\circ) \cong \mathcal{G} \text{ and } C \not\leq \ker(\gamma)\}\,.$$

We have

$$e'(\mathcal{G},G) = |X| = |X_1| + |X_2| = n_C(\mathcal{G}) + |X_2|.$$

Now we show that there is a bijection between X_1 and X_2, so that $e'(\mathcal{G},G) = 2n_C(\mathcal{G})$. Consider

$$\psi : X \to X$$
$$\gamma \mapsto \tilde{\gamma},$$

where $\tilde{\gamma}$ is as in Proposition 1.21. The map ψ is well defined, indeed $\tilde{\gamma}$ is a GF on G and $(G,\tilde{\circ}) \cong (G,\circ) \cong \mathcal{G}$ (see the proof of Proposition 1.21); moreover

$$\psi^2(\gamma) = \psi(\tilde{\gamma}) = \tilde{\tilde{\gamma}}.$$

By Theorem 1.2 each GF on G corresponds to a unique regular subgroup of $\mathrm{Hol}(G)$, so let N be the regular subgroup corresponding to γ; then, by Proposition 1.21, the regular subgroup corresponding to $\tilde{\tilde{\gamma}}$ is $(N^{\mathrm{inv}})^{\mathrm{inv}} = N$, so that $\psi^2 = 1$ and ψ is bijective. Now, using Proposition 1.23, we obtain $\psi(X_2) = X_1$, and so $|X_2| = |X_1|$. □

Note that this duality is equivalent to the notion of an *opposite skew brace* as introduced by Koch and Truman in [KT20]. In fact, given a brace $(G,\cdot,\circ)$, Koch and Truman define the opposite brace to be $(G,\cdot',\circ)$, where $x \cdot' y = yx$ gives the opposite group $(G,\cdot')$ of $(G,\cdot)$. With our construction, the circle operation associated to the regular subgroup N^{inv} is given by $x\,\tilde{\circ}\,y = x^{\tilde{\gamma}(y)} \cdot y = x^{\gamma(y^{-1})\iota(y^{-1})} \cdot y = y \cdot x^{\gamma(y^{-1})}$.

Now $\mathrm{inv} : (G,\cdot',\circ) \to (G,\cdot,\tilde{\circ})$ is an isomorphism of skew braces, as for $x,y \in G$ we have $(x \cdot' y)^{\mathrm{inv}} = (y \cdot x)^{-1} = x^{-1} \cdot y^{-1} = x^{\mathrm{inv}} \cdot y^{\mathrm{inv}}$, and, $(x \circ y)^{\mathrm{inv}} = (x^{\gamma(y)} \cdot y)^{-1} = y^{-1} \cdot x^{-\gamma(y)} = x^{-\gamma(y)\iota(y)} \cdot y^{-1} = x^{\mathrm{inv}}\,\tilde{\circ}\,y^{\mathrm{inv}}$.

1.7 Gluing

The next result acts as a converse for Lemma 1.22, and partly extends Proposition 1.13, describing a way to construct GF on $G = AB$ by gluing together a RGF on A defined as $\gamma(a) = \iota(a^{-\sigma})$, where $\sigma \in \mathrm{End}(A)$, and a RGF on B once equation (1.14) is satisfied.

Note that, in equation (1.14), $\gamma(g)\iota(g) = \iota(g^{\gamma(g)^{-1}})\gamma(g)$. Setting $g' = g^{\ominus 1} = g^{-\gamma(g)^{-1}}$, we see that $\gamma(g)\iota(g) = \iota(g')^{-1}\gamma(g')^{-1}$ (recall that $\gamma(g^{\ominus 1}) = \gamma(g)^{-1}$). Therefore (1.14) can be rewritten as

$$\sigma\,\gamma(g)^{-1}_{\restriction C}\,(\sigma - 1) = (\sigma - 1)\,\iota(g)^{-1}_{\restriction C}\,\gamma(g)^{-1}_{\restriction C}\,\sigma, \quad \text{for } g \in G. \tag{1.16}$$

Proposition 1.26. *Let $G = AB$ be a finite group, where A, B are subgroups of G, such that*

1. *$A \cap B = \{1\}$,*
2. *A is abelian,*
3. *A is characteristic in G,*
4. *$A \cap Z(G) = \{1\}$.*

If moreover there exists a RGF $\gamma : B \to \mathrm{Aut}(G)$ and $\sigma \in \mathrm{End}(A)$ which satisfy (1.14)*, then the extension of γ to the function $\gamma : G \to \mathrm{Aut}(G)$ defined by, for $a \in A$ and $b \in B$,*

$$\gamma(ab) = \iota(a^{-\gamma(b)^{-1}\sigma})\gamma(b) \tag{1.17}$$

is a GF on G.

Conversely, every GF γ on G such that $\gamma(a) = \iota(a^{-\sigma})$, where $\sigma \in \mathrm{End}(A)$, and for which B is $\gamma(B)$-invariant, is obtained as the extension of a RGF on B as in (1.17)*.*

In this situation we will say that γ is a *gluing* of a RGF on A defined by σ, and a RGF on a $\gamma(B)$-invariant subgroup B.

Proof. Assume first that γ is a GF on G and B is invariant, then $\gamma_{|B}$ is RGF on B, and for $a \in A$ and $b \in B$, $\gamma(ab) = \gamma(a^{\gamma(b)^{-1}})\gamma(b)$. If for each $a \in A$, $\gamma(a) = \iota(a^{-\sigma})$, where $\sigma \in \mathrm{End}(A)$, we obtain (1.17).

Conversely, let γ be a RGF on B and $\sigma \in \mathrm{End}(A)$ such that (1.14) is satisfied. We now show that the function defined in (1.17) satisfies the GFE. Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$.

We have

$$\begin{aligned}\gamma(a_1b_1)\gamma(a_2b_2) &= \iota(a_1^{-\gamma(b_1)^{-1}\sigma})\gamma(b_1)\iota(a_2^{-\gamma(b_2)^{-1}\sigma})\gamma(b_2)\\ &= \iota(a_1^{-\gamma(b_1)^{-1}\sigma}a_2^{-\gamma(b_2)^{-1}\sigma\gamma(b_1)^{-1}})\gamma(b_1)\gamma(b_2).\end{aligned}$$

On the other hand

$$\begin{aligned}
&\gamma((a_1b_1)^{\gamma(a_2b_2)}a_2b_2) = \\
=&\gamma(a_1^{\gamma(b_2)}b_1^{\iota(a_2^{-\gamma(b_2)^{-1}\sigma})\gamma(b_2)}a_2b_2) \\
=&\gamma(a_1^{\gamma(b_2)}(a_2^{\gamma(b_2)^{-1}\sigma}b_1a_2^{-\gamma(b_2)^{-1}\sigma})^{\gamma(b_2)}a_2b_2) \\
=&\gamma(a_1^{\gamma(b_2)}a_2^{\gamma(b_2)^{-1}\sigma\gamma(b_2)}b_1^{\gamma(b_2)}a_2^{-\gamma(b_2)^{-1}\sigma\gamma(b_2)}a_2b_2) \\
=&\gamma(a_1^{\gamma(b_2)}a_2^{\gamma(b_2)^{-1}\sigma\gamma(b_2)}a_2^{-\gamma(b_2)^{-1}\sigma\iota(b_1)^{-1}\gamma(b_2)}a_2^{\gamma(b_2)^{-1}\iota(b_1)^{-1}\gamma(b_2)}b_1^{\gamma(b_2)}b_2) \\
=&\iota((a_1^{\gamma(b_2)}a_2^{\gamma(b_2)^{-1}\sigma\gamma(b_2)}a_2^{-\gamma(b_2)^{-1}\sigma\iota(b_1)^{-1}\gamma(b_2)}a_2^{\gamma(b_2)^{-1}\iota(b_1)^{-1}\gamma(b_2)})^{-\gamma(b_2)^{-1}\gamma(b_1)^{-1}\sigma}) \\
&\gamma(b_1)\gamma(b_2) \\
=&\iota(a_1^{-\gamma(b_1)^{-1}\sigma}a_2^{-\gamma(b_2)^{-1}\sigma\gamma(b_1)^{-1}\sigma+\gamma(b_2)^{-1}\sigma\iota(b_1)^{-1}\gamma(b_1)^{-1}\sigma-\gamma(b_2)^{-1}\iota(b_1)^{-1}\gamma(b_1)^{-1}\sigma}) \\
&\gamma(b_1)\gamma(b_2).
\end{aligned}$$

Now (1.16) shows that the two expressions

$$-\sigma\gamma(b_1)_{\restriction A}^{-1}$$

and

$$-\sigma\gamma(b_1)_{\restriction A}^{-1}\sigma + \sigma\iota(b_1)_{\restriction A}^{-1}\gamma(b_1)_{\restriction A}^{-1}\sigma - \iota(b_1)_{\restriction A}^{-1}\gamma(b_1)_{\restriction A}^{-1}\sigma$$

coincide. □

1.8 Applications

1.8.1 Nilpotent groups

The following result is due to N. P. Byott.

Theorem 1.27 ([Byo13, Theorem 1])**.** *Let Γ be a finite nilpotent group of order n.*

Then for each nilpotent group G of order n we have

$$e(\Gamma, G) = \prod_p e(\Gamma_p, G_p),$$

where p ranges over the primes dividing n, and Γ_p resp. G_p denote the Sylow p-subgroups of Γ resp. G.

We now give an alternate proof of Byott's result, using gamma functions.

Proof. Let $p_1, \ldots, p_k$ be the distinct primes dividing n. The finite nilpotent group G is the direct product of its distinct Sylow subgroups, each of which is characteristic in G, so we have

$$\mathrm{Aut}(G) = \prod_{i=1}^{k} \mathrm{Aut}(G_{p_i}). \tag{1.18}$$

and the same holds for Γ. Therefore, in view of (1) of Theorem 1, we can rephrase Byott's result as

$$e'(\Gamma, G) = \prod_{i=1}^{k} e'(\Gamma_{p_i}, G_{p_i}), \tag{1.19}$$

As we already noted in the Introduction

$$e'(\Gamma, G) = |\{\gamma \text{ GF on } G : (G, \circ) \cong \Gamma\}|.$$

Let now γ be a gamma function on G such that $(G, \circ) \cong \Gamma$. Proposition 1.6 implies that the Sylow p_i-subgroup $(G, \circ)_{p_i}$ of $(G, \circ)$ is $(G_{p_i}, \circ)$ (which is then isomorphic to Γ_{p_i}). So, let p, q be distinct primes dividing n, and let a be a p-element, and b a q-element of G and $(G, \circ)$. Since G and $(G, \circ)$ are nilpotent, a and b commute in both groups. We thus have

$$a^{\gamma(b)}b = a \circ b = b \circ a = b^{\gamma(a)}a = ab^{\gamma(a)},$$

which implies $b^{\gamma(a)} = b$ (and $a^{\gamma(b)} = a$).

This shows that the image $\gamma(G_p)$ of the Sylow p-subgroup of G under γ acts trivially on the Sylow q-subgroups of G, for $q \neq p$. The composition of the restriction of γ to G_p, followed by the projection of $\mathrm{Aut}(G)$ onto $\mathrm{Aut}(G_p)$, is clearly a gamma function on G_p.

It follows that every gamma function γ on G is obtained as

$$\gamma(x) = \gamma_1(x_1) \dots \gamma_k(x_k),$$

where x is uniquely written as $x_1 \cdots x_k$, with $x_i \in G_{p_i}$, and $\gamma_i : G_{p_i} \to \mathrm{Aut}(G_{p_i}) \leq \mathrm{Aut}(G)$ is a gamma function on G_{p_i}. This proves equality (1.19). □

1.8.2 Groups of order pq

To exemplify our methods, we first apply them to the case, dealt with by Byott in [Byo04], of groups of order pq, where p and q are distinct primes. We also recover the classification of skew braces of order pq of Acri and Bonatto [AB20c].

So let $p > q$ be two primes. We will write $\mathcal{C}_{pq}$ for the cyclic group of order pq, and $\mathcal{C}_p \rtimes \mathcal{C}_q$ for the non-abelian one, which occurs when $q \mid p - 1$.

Byott has proved the following.

Theorem 1.28 ([Byo04, Section 6])**.** *Let L/K be a Galois field extension of order pq, and let $\Gamma = \mathrm{Gal}(L/K)$.*

Then the following table gives the numbers $e(\Gamma, G)$ of Hopf-Galois structures on L/K of type G for each group G of order pq.

Γ \ G	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2(q-1)$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	p	$2(pq-2p+1)$

We now compute with our methods the number $e'(\Gamma, G)$ of the regular subgroups of $\mathrm{Hol}(G)$ which are isomorphic to Γ, in the form

Γ \ G	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	1	$2p$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	$q-1$	$2(pq-2p+1)$

from which the previous theorem can be obtained using formula (1) of Theorem 1.

In terms of conjugacy classes of regular subgroups, we have

Theorem 1.29. *Let $G = (G, \cdot)$ be a group of order pq, where p, q are primes, with $p > q$.*

For each group Γ of order pq, the following table gives equivalently

1. *the number (and lengths) of conjugacy classes within $\mathrm{Hol}(G)$ of regular subgroups isomorphic to Γ;*

2. *the number of isomorphism classes of braces $(G, \cdot, \circ)$ such that $\Gamma \cong (G, \circ)$.*

Γ \ G	$\mathcal{C}_{pq}$	$\mathcal{C}_p \rtimes \mathcal{C}_q$
$\mathcal{C}_{pq}$	$(1,1)$	$(2,p)$
$\mathcal{C}_p \rtimes \mathcal{C}_q$	$(1,q-1)$	$(2,1),(2(q-2),p)$

Here (c, l) denotes c conjugacy classes of length l; the full table refers to the case when $q \mid p-1$, and the 1×1 upper left sub-table refers to the case $q \nmid p-1$.

We obtain that when $q \mid p-1$ there are $2q+2$ isomorphism classes of braces of order pq, which coincides with the results of [AB20c].

Let γ be a GF on G, let A be the Sylow p-subgroup of G and B a Sylow q-subgroup.

If $G = \mathcal{C}_{pq}$, then $A \leq \ker(\gamma)$, since in $\mathrm{Aut}(G) \cong \mathcal{C}_{p-1} \times \mathcal{C}_{q-1}$ there are no elements of order p.

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, we may take $r = p$ and $C = A$ in the hypotheses of Corollary 1.25 here, so that we need only to consider the case $A \leq \ker(\gamma)$.

If $\ker(\gamma) = G$, we get the right regular representation, whose image forms a conjugacy class in itself.

Suppose thus $\ker(\gamma) = A$, so that $|\gamma(G)| = q$. We claim that there is a unique $\gamma(G)$-invariant Sylow q-subgroup B of G. This is clearly true for

$G = \mathcal{C}_{pq}$. When $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, the q-elements of $\mathrm{Aut}(G) \cong \mathcal{C}_p \rtimes \mathcal{C}_{p-1}$ are inner automorphisms, so that $\gamma(G) = \langle\, \iota(b) \,\rangle$ for some $b \in G$ of order q. It follows that $B = \langle\, b \,\rangle$ is the unique $\gamma(G)$-invariant Sylow q-subgroup.

Now $B\gamma(G)$ is a subgroup of order q^2 of $\mathrm{Hol}(G)$, so that $[B, \gamma(G)] = 1$, and thus

$$[G, \gamma(G)] = [AB, \gamma(G)] = [A, \gamma(G)] = [A, \langle\, \iota(b) \,\rangle] = A = \ker(\gamma).$$

By Lemma 1.12, all such GF's are precisely the morphisms $\gamma : G \to \mathrm{Aut}(G)$ of groups with kernel A.

If $G = \mathcal{C}_{pq}$, and $q \nmid p - 1$, there are no such morphisms, as in this case $q \nmid |\mathrm{Aut}(G)|$. If $q \mid p - 1$, there are exactly $q - 1$ such morphisms with kernel of order p, as they correspond to sending a fixed element of order q of G to one of the $q - 1$ elements of order q of $\mathrm{Aut}(G)$. The corresponding regular subgroups are non-abelian by Lemma 1.9, as for $a \in A$ we have

$$b^{\ominus 1} \circ a \circ b = a^{\gamma(b)} \neq a.$$

Let $\beta \in \mathrm{Aut}(G)$ send b to b^t, for some t. Then, according to Lemma 1.8, and since $\mathrm{Aut}(G)$ is abelian, we have $\gamma^\beta(b) = \gamma(b^{\beta^{-1}}) = \gamma(b)^{t^{-1}}$. It follows that all these $q - 1$ GF's are conjugate.

If $G = \mathcal{C}_p \rtimes \mathcal{C}_q$, one has first to choose a $\langle\, \iota(b) \,\rangle$ among the p subgroups of order q of the Sylow q-subgroups of $\mathrm{Aut}(G)$. Since for $a \in A$ Lemma 1.9 yields

$$b^{\ominus 1} \circ a \circ b = b^{-1} a^{\gamma(b)} b = a^{\gamma(b)\iota(b)},$$

the choice $\gamma(b) = \iota(b)^{-1}$ yields p instances of $(G, \circ) = \mathcal{C}_{pq}$. According to Lemma 1.8.(2), all these γ are conjugate under $\iota(A)$, which conjugates transitively the Sylow q-subgroups.

The other non-trivial choices of $\gamma(b) = \iota(b)^s$, with $s \neq 0, -1$ yield $p(q - 2)$ instances of $(G, \circ) = \mathcal{C}_p \rtimes \mathcal{C}_q$. Once more, the action of $\iota(A)$, which conjugates transitively the Sylow q-subgroups, shows that the conjugacy classes are of length at least p. The cyclic complement of order $p - 1$ of $\iota(A)$ in $\mathrm{Aut}(G)$ which contains $\gamma(b) = \iota(b^s)$ then centralises b and $\gamma(b)$, so that it centralises γ by Lemma 1.8, and the conjugacy classes have length precisely p.

Chapter 2

Towards enumeration

In this chapter we prepare the field for the proof of Theorem 2, which will take place in the next chapters.

In Section 2.1 we will first recall the classification of the groups of order p^2q, where p and q are distinct primes, and of their automorphism groups. We will then show how to apply some results of Chapter 1 to the groups of order p^2q. In particular we will show that for odd p, if G is a group of order p^2q, a Sylow p-subgroup of a regular subgroup of $\mathrm{Hol}(G)$ is isomorphic to a Sylow p-subgroup of G.

In Section 2.2 we will give an overview of how the tools of Chapter 1 will actually be used in Chapters 3, 4 and 5 to enumerate the gamma functions.

2.1 The groups of order p^2q and their automorphism groups

The classification of groups of order p^2q, where p, q are distinct primes, goes back to O. Hölder [Höl93]. In particular, Hölder showed that in such a group there is always a normal Sylow subgroup. As a handy reference, we have recorded the classification of these groups and of their automorphism groups in [CCDC21]. We briefly describe the groups of order p^2q, and list them and their automorphisms in the table below, referring to [CCDC21] for the details.

We will say that two groups have the same *type* if they have isomorphic automorphism groups. For groups of order p^2q each type corresponds to an isomorphism class, except for the type 8, which corresponds to $\frac{q-3}{2}$ isomorphism classes.

We use the notation $\mathcal{C}_n$ for a cyclic group of order n.

Groups with cyclic Sylow p-subgroups

Type 1 Cyclic group.

Type 2 This is the non-abelian group with centre of order p for $p \mid q-1$, which we denote by $\mathcal{C}_q \rtimes_p \mathcal{C}_{p^2}$. It can be described as

$$\left\langle a, b : a^{p^2} = b^q = 1,\ b^{\iota(a)} = b^u \right\rangle,$$

where u is an element of order p in $\mathcal{C}_q^*$.

Type 3 This is the non-abelian group with trivial centre for $p^2 \mid q-1$, which we denote by $\mathcal{C}_q \rtimes_1 \mathcal{C}_{p^2}$. It can be described as

$$\left\langle a, b : a^{p^2} = b^q = 1,\ b^{\iota(a)} = b^v \right\rangle,$$

where v is an element of order p^2 in $\mathcal{C}_q^*$.

Type 4 This is the non-abelian group for $q \mid p-1$, which we denote by $\mathcal{C}_{p^2} \rtimes \mathcal{C}_q$. It can be described as

$$\left\langle a, b : a^{p^2} = b^q = 1,\ a^{\iota(b)} = a^w \right\rangle,$$

where w is an element of order q in $\mathcal{C}_{p^2}^*$.

Groups with elementary abelian Sylow p-subgroups

Type 5 Abelian group.

Type 6 This is the non-abelian group with centre of order p for $q \mid p-1$, which we denote by $\mathcal{C}_p \times (\mathcal{C}_p \rtimes \mathcal{C}_q)$. It can be described as

$$\left\langle a_1, a_2, b : a_1^p = a_2^p = b^q = 1,\ a_2^{\iota(b)} = a_2^\lambda \right\rangle,$$

where λ is an element of order q in $\mathcal{C}_p^*$, $\lambda \neq 1$.

Type 7 This is the non-abelian group for $q \mid p-1$ in which a generator of $\mathcal{C}_q$ acts on $\mathcal{C}_p \times \mathcal{C}_p$ as a non-identity scalar matrix. We denote it by $(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_S \mathcal{C}_q$, and it can be described as

$$\left\langle a_1, a_2, b : a_1^p = a_2^p = b^q = 1,\ a_1^{\iota(b)} = a_1^\lambda,\ a_2^{\iota(b)} = a_2^\lambda \right\rangle,$$

where λ is an element of order q in $\mathcal{C}_p^*$, $\lambda \neq 1$.

Type 8 These are the non-abelian groups for $q \mid p-1$, $q > 3$, in which a generator of $\mathcal{C}_q$ acts on $\mathcal{C}_p \times \mathcal{C}_p$ as a diagonal, non-scalar matrix with no eigenvalue 1, and determinant different from 1. We denote this type by $(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D1} \mathcal{C}_q$, and it consists of the groups G_k which can be described as

$$G_k = \left\langle a_1, a_2, b : a_1^p = a_2^p = b^q = 1,\ a_1^{\iota(b)} = a_1^\lambda,\ a_2^{\iota(b)} = a_2^{\lambda^k} \right\rangle,$$

where λ is an element of order q, $\lambda \neq 1$, and $k \neq 0, \pm 1$.

Since for each $k \neq 0, \pm 1$ we have that $G_k \simeq G_{k^{-1}}$, the type 8 includes $\frac{q-3}{2}$ isomorphism classes of groups.

We will denote by $\mathcal{K}$ the set of the elements $k \neq 0, \pm 1$ for which $\{G_k : k \in \mathcal{K}\}$ is a set of representatives of the isomorphism classes of groups of type 8.

Type 9 This is the non-abelian group for $q \mid p-1$, $q > 2$, in which a generator of $\mathcal{C}_q$ acts on $\mathcal{C}_p \times \mathcal{C}_p$ as a diagonal, non-scalar matrix with no eigenvalue 1, and determinant 1. We denote it by $(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D1} \mathcal{C}_q$, and it can be described as

$$\left\langle a_1, a_2, b : a_1^p = a_2^p = b^q = 1,\ a_1^{\iota(b)} = a_1^{\lambda},\ a_2^{\iota(b)} = a_2^{\lambda^{-1}} \right\rangle,$$

where λ is an element of order q in $\mathcal{C}_p^*$, $\lambda \neq 1$.

Type 10 This is the non-abelian group group for $q \mid p+1$, $q > 2$, in which a generator of $\mathcal{C}_q$ acts on $\mathcal{C}_p \times \mathcal{C}_p$ as a matrix C with $\det(C) = 1$ and $\mathrm{tr}(C) = \lambda + \lambda^{-1}$, where $\lambda \neq 1$ is a q-th root of unity in a quadratic extension of $\mathbb{F}_p$. We denote it by $(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_C \mathcal{C}_q$, and it can be described as

$$\left\langle a_1, a_2, b : a_1^p = a_2^p = b^q = 1,\ a_1^{\iota(b)} = a_1^{\lambda+\lambda^{-1}} a_2,\ a_2^{\iota(b)} = a_1^{-1} \right\rangle.$$

Type 11 This is the non-abelian group with centre of order p for $p \mid q-1$, which we denote by $(\mathcal{C}_q \rtimes \mathcal{C}_p) \times \mathcal{C}_p$. It can be described as

$$\left\langle a_1, a_2, b : a_1^p = a_2^p = b^q = 1,\ b^{\iota(a_1)} = b^u \right\rangle,$$

where u is an element of order p in $\mathcal{C}_q^*$.

Table 2.1: Groups of order p^2q and their automorphisms

Type	Conditions	G	$\mathrm{Aut}(G)$
1		$\mathcal{C}_{p^2} \times \mathcal{C}_q$	$\mathcal{C}_{p(p-1)} \times \mathcal{C}_{q-1}$
2	$p \mid q-1$	$\mathcal{C}_q \rtimes_p \mathcal{C}_{p^2}$	$\mathcal{C}_p \times \mathrm{Hol}(\mathcal{C}_q)$
3	$p^2 \mid q-1$	$\mathcal{C}_q \rtimes_1 \mathcal{C}_{p^2}$	$\mathrm{Hol}(\mathcal{C}_q)$
4	$q \mid p-1$	$\mathcal{C}_{p^2} \rtimes \mathcal{C}_q$	$\mathrm{Hol}(\mathcal{C}_{p^2})$
5		$\mathcal{C}_p \times \mathcal{C}_p \times \mathcal{C}_q$	$\mathrm{GL}(2,p) \times \mathcal{C}_{q-1}$
6	$q \mid p-1$	$\mathcal{C}_p \times (\mathcal{C}_p \rtimes \mathcal{C}_q)$	$\mathcal{C}_{p-1} \times \mathrm{Hol}(\mathcal{C}_p)$
7	$q \mid p-1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_S \mathcal{C}_q$	$\mathrm{Hol}(\mathcal{C}_p \times \mathcal{C}_p)$
8	$3 < q \mid p-1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D0} \mathcal{C}_q$	$\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_p)$
9	$2 < q \mid p-1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D1} \mathcal{C}_q$	$(\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_p)) \rtimes \mathcal{C}_2$
10	$2 < q \mid p+1$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_C \mathcal{C}_q$	$(\mathcal{C}_p \times \mathcal{C}_p) \rtimes (\mathcal{C}_{p^2-1} \rtimes \mathcal{C}_2)$
11	$p \mid q-1$	$(\mathcal{C}_q \rtimes \mathcal{C}_p) \times \mathcal{C}_p$	$\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_q)$

For (some types of) groups of order p^2q, some results of Chapter 1 can be made more explicit.

Proposition 2.1. *Let G be a non-abelian group of order p^2q, and let γ be a GF on G.*

1. *Let H be the normal Sylow r-subgroup of G ($r \in \{p, q\}$);*
2. *if $r = p$, assume H cyclic;*
3. *denote by C the unique subgroup of H of order r.*

Then

$$C \leq \ker(\gamma) \text{ if and only if } C \not\leq \ker(\tilde{\gamma}).$$

Moreover, for each group $\mathcal{G}$ of order p^2q, let

$$n_r(\mathcal{G}) = |\{\gamma \text{ GF on } G : (G, \circ) \cong \mathcal{G} \text{ and } r \mid |\ker(\gamma)|\}|.$$

Then

$$e'(\mathcal{G}, G) = |\{\gamma \text{ GF on } G : (G, \circ) \cong \mathcal{G}\}| = 2n_r(\mathcal{G}).$$

Proof. We show that G, H, C fulfil the assumptions of Proposition 1.23 and Corollary 1.25, from which the result will follow.

The subgroup H is cyclic and characteristic in G, so C is the only subgroup of order r of G, and (1) and (2) of Proposition 1.23 hold. Let now $r = q$; in this case $H = B$, where B is the Sylow q-subgroup, and $C = B$. G can be of type 2, 3 or 11 and we always have $B \cap Z(G) = \{1\}$. Moreover, $\mathrm{ord}(\gamma(b)) \mid \mathrm{ord}_{(G,\circ)}(b) \mid q$, since $(B, \circ) \leq (G, \circ)$ (by Proposition 1.6) and $\gamma : (G, \circ) \to \mathrm{Aut}(G)$ is a morphism. For G of type 2, 3 or 11, $|\mathrm{Aut}(G)/\mathrm{Inn}(G)|$ is coprime to q, thus all the elements of order q in $\mathrm{Aut}(G)$ belong to $\mathrm{Inn}(G)$ and so $\gamma(b) = \iota(b^{-\sigma})$ for some σ.

On the other hand, for $r = p$ we have $H = A = \langle a \rangle$, where A is the Sylow p-subgroup, and G is of type 4, so that $p > 2$. Here $Z(G) = \{1\}$, so that we have only to show that for all $c \in C = \langle a^p \rangle$ we have $\gamma(c) = \iota(c^{-\sigma})$. According to Theorem 3.4 and Remark 3.5 of [CCDC21], the Sylow p-subgroup of $\mathrm{Aut}(G) = \mathrm{Hol}(\mathcal{C}_{p^2})$ is a non-abelian group $X = \mathcal{C}_{p^2} \rtimes \mathcal{C}_p$ of order p^3, spanned by $\iota(a)$, of order p^2, and another element ψ of order p which maps $a \mapsto a^{1+p}$, and fixes elementwise a Sylow q-subgroup B of G of one's choice. The derived subgroup $\langle \iota(a^p) \rangle$ of X is central, of order p. We now quote the following elementary result.

Remark 2.2. For $x, y \in X$ we have

$$(xy)^p = x^p y^p [y, x]^{\binom{p}{2}} = x^p y^p,$$

as p is odd.

We have once more $(A,\circ) \leq (G,\circ)$ and since $p > 2$, by Corollary 1.17, $\mathrm{ord}_{(A,\circ)}(a^{\circ k}) = \mathrm{ord}_A(a^k)$ for all k, thus $\mathrm{ord}(\gamma(a^p)) \mid p$. If $\gamma(a^p) = 1$ we are done, otherwise $\mathrm{ord}(\gamma(a^p)) = p$. Let $\gamma(a) = \iota(a^{-\sigma})\psi^t$; then

$$a^{\circ p} = a^{\sum_{i=0}^{p-1}\gamma(a)^i} = a^{\sum_{i=0}^{p-1}(1+ipt)} = a^p,$$

so that

$$\gamma(a^p) = \gamma(a^{\circ p}) = \gamma(a)^p = (\iota(a^{-\sigma})\psi^t)^p = \iota(a^{-\sigma p}),$$

where we have used Remark 2.2.

Finally, since G is not abelian, then $\mathrm{Inn}(G)$ contains elements of order both p and q, so there exists $g \in G$ whose order is not a power of r and Proposition 1.23 and Corollary 1.25 can be applied. □

Theorem 2.3. *Let G be a group of order p^2q and γ a GF on G.*
Then there exists a Sylow p-subgroup A of G which is $\gamma(A)$-invariant.
In particular, for $p > 2$, G and $(G,\circ)$ have isomorphic Sylow p-subgroups.

Proof. We show that there is always a Sylow p-subgroup A of G which is $\gamma(A)$-invariant; then the result will follow from Corollary 1.7, since the groups of order p^2 are abelian. Clearly, this is always the case when A is characteristic; otherwise the set $\mathcal{P}$ of the Sylow p-subgroups of G has q elements. For each γ, the group $\gamma(G)$ acts on $\mathcal{P}$, partitioning it into orbits whose length divides $|\gamma(G)|$. So, denoting by N_l the number of orbits of length l, we have

$$\sum_{l||\gamma(G)|} N_l l = |\mathcal{P}| = q \equiv 1 \bmod p.$$

If $q \mid |\ker(\gamma)|$, then $|\gamma(G)| = 1, p$ or p^2 and necessarily $N_1 \geq 1$, namely there exist $A \in \mathcal{P}$ which is $\gamma(G)$-invariant.

This argument covers the cases when G is of type 1, 4, 5, 6, 7, 8, 9, 10 (that is, the Sylow p-subgroup is characteristic) and when G is of type 2, 3 or 11, and the Sylow q-subgroup B is contained in $\ker(\gamma)$. So suppose G of type 2, 3 or 11 and $B \not\leq \ker(\gamma)$; here B is characteristic and by Proposition 2.1 we get that $B \leq \ker(\tilde{\gamma})$. The previous argument ensures that there exists a Sylow p-subgroup A of G which is $\tilde{\gamma}(G)$-invariant and, by Proposition 1.6, it is also a Sylow p-subgroup of $(G,\tilde{\circ})$.

Now, $(G,\tilde{\circ})$ is isomorphic to $(G,\circ)$ via the map $\mathrm{inv}\colon x \mapsto x^{-1}$ (see the proof of Proposition 1.21), thus $A^{\mathrm{inv}} = A$ is also a Sylow p-subgroup of $(G,\circ)$. Using Proposition 1.6 again we get that A is $\gamma(A)$-invariant.

We can conclude that, for each G and for each GF γ, there exists a Sylow p-subgroup of G which is also a Sylow p-subgroup of $(G,\circ)$. Corollary 1.7 allows us to conclude that A and $(A,\circ)$ are isomorphic. □

We immediately get

Corollary 2.4. *Let $p > 2$ and q be distinct primes. Let Γ and G be groups of order p^2q with non isomorphic Sylow p-subgroups. Then $e'(\Gamma, G) = e(\Gamma, G) = 0$.*

Remark 2.5. If G is a group of order p^2q, then either G has a unique Sylow q-subgroup or it has p^f Sylow q-subgroups, where $f = 1, 2$.

In the first case, since the unique Sylow q-subgroup B is characteristic, it is $\gamma(B)$-invariant.

In the second case, there are p Sylow q-subgroups when G is of type 6, and p^2 when G is of type 4, 7, 8, 9, 10. Reasoning as in the proof of Theorem 2.3, let γ be a GF in G, and consider the action of $\gamma(G)$ on the set $\mathcal{Q}$ of the Sylow q-subgroups of G. If $p^2 \mid |\ker(\gamma)|$, then $|\gamma(G)| = 1$ or q, so that there exists at least one orbit of length 1, namely there exists $B \in \mathcal{Q}$ which is $\gamma(G)$-invariant.

Moreover, if $q \mid |\ker(\gamma)|$, then there exists a Sylow q-subgroup B contained in $\ker(\gamma)$, therefore it is $\gamma(B)$-invariant.

In the remaining cases, namely when $|\ker(\gamma)| = 1$ or p, we will prove for some specific type of group G that we can find such a Sylow q-subgroup (see Subsections 3.4.3, 4.4.5, 4.4.6, 4.5.2, and 4.6.4), but we do not have a general argument to prove it.

As a corollary of Proposition 1.6 and Theorem 2.3 we have the following.

Lemma 2.6. *Let G be a group of order p^2q, $p > 2$, and assume that the Sylow p-subgroup A of G is normal. Let $b \in G$ an element of order q.*

1. *If $A = \langle a \rangle$ is cyclic, then $\{a, b\}$ is a set of generators for both G and $(G, \circ)$, for each possible operation $\circ$ on G.*
2. *If $A = \langle a_1, a_2 \rangle$ is elementary abelian and γ is a GF on G such that $\langle a_1 \rangle$ is $\gamma(\langle a_1 \rangle)$-invariant, then $\{a_1, a_2, b\}$ is a set of generators for both G and $(G, \circ)$.*

Proof. Clearly the generator(s) of A together with the element b generate G.

Let γ be a GF on G and let $\circ$ be the corresponding operation on G. By Proposition 1.6, A is a subgroup of $(G, \circ)$, and since $p > 2$, by Theorem 2.3 $A \simeq (A, \circ)$.

If $A = \langle a \rangle$ is cyclic then $\mathrm{ord}_A(a) = \mathrm{ord}_{(A,\circ)}(a)$ (take $\gamma_{|A}$ in Corollary 1.17), therefore a generates $(A, \circ)$ too.

If A is elementary abelian then every non-trivial element of $(A, \circ)$ has order p. Moreover if $A_1 := \langle a_1 \rangle$ is $\gamma(A_1)$-invariant then $a_2 \notin A_1 = (A_1, \circ)$, so that a_1, a_2 generate $(A, \circ)$ too.

Now, since $b \in G \setminus A$ and $[G : A] = q$, the generator(s) of A together with the element b generate also $(G, \circ)$. □

2.2 The reader's Guide to the next chapters

To prove our main Theorem 2, we will mostly rely on the general results established in Chapter 1, appealing occasionally to ad hoc arguments.

According to Theorem 2.3, if G is a group of order p^2q, with p, q distinct primes and $p > 2$, then G and $(G, \circ)$ have isomorphic Sylow p-subgroups. Thus to prove Theorem 2 we only need to consider groups G whose Sylow p-subgroups are in the same isomorphism class of the Sylow p-subgroups of the group under consideration. In Chapters 3 and 4 we deal with the case of groups with cyclic, respectively elementary abelian, Sylow p-subgroups. In Chapter 5 we consider the case of groups of order $4q$.

In the next chapters we will proceed to the enumeration of the regular subgroups of $\mathrm{Hol}(G)$ by analysing the possible types for G one by one, and for each type we will distinguish by the size of the kernel of γ. We will usually tacitly ignore the case $\gamma(G) = \{1\}$, that is, $\ker(\gamma) = G$, as it corresponds to the (trivial) case of the right regular representation.

This will prove Theorem 3. Then Theorem 2 will be obtained via Theorem 1.

With a view to the next chapters we now describe how some of the tools from Chapter 1 will be applied in the specific case of groups of order p^2q.

2.2.1 Duality for non-abelian groups of order p^2q

For non-abelian groups we will make full use of duality. Certainly we can apply Proposition 2.1 to the groups G of type 2, 3, 4 and 11. Therefore, for these types, we consider only the case $r \mid |\ker(\gamma)|$, where $r = q$ for the types 2, 3, and 11, and $r = p$ for the type 4, and then we double the number of regular subgroups we find.

If G is of type 6 then the normal subgroup C of order p in $\mathcal{C}_p \rtimes \mathcal{C}_q$ satisfies the hypotheses of Proposition 1.23. Therefore, we can apply Corollary 1.25 and consider only the case $C \leq \ker(\gamma)$, doubling the numbers obtained.

For G of the remaining types, namely 7, 8, 9 and 10, denote by A the elementary abelian Sylow p-subgroup of G. As we will show in Sections 4.4 and 4.6, the equation

$$\forall a \in A,\ \gamma(a) = \iota(a^{-\sigma}), \tag{2.1}$$

where $\sigma \in \mathrm{End}(A)$, is always satisfied for the types 8, 9 and 10 (when $p > 2$). If G is of type 7 then $\gamma(A)$ is not necessarily contained in $\mathrm{Inn}(G)$, and it has to be assumed (the case $\gamma(A) \not\leq \mathrm{Inn}(G)$ will be treated separately in Section 4.5). Therefore, for G as above, we can apply Lemma 1.22 with $C = A$, and this yields equation (1.14).

We have the following case distinction.

2.2.1.1 $\sigma, 1-\sigma$ are not both invertibile

This means that σ has an eigenvalue 0 or 1. If it is 0, then $p \mid |\ker(\gamma)|$. If it is 1 then Proposition 1.21 yields $\tilde{\gamma}(a) = \gamma(a^{-1})\iota(a^{-1}) = \iota(a^{\sigma-1})$, so that $p \mid |\ker(\tilde{\gamma})|$. Therefore, up to switch γ with $\tilde{\gamma}$, we can assume the eigenvalue is 0, so that p divides the order of the kernel of γ.

2.2.1.2 $\sigma, 1-\sigma$ are both invertibile

This means that σ has no eigenvalues $0, 1$. Then equation (1.14) yields

$$(\sigma^{-1}-1)^{-1}\gamma(b)_{|A}(\sigma^{-1}-1) = \gamma(b)_{|A}\iota(b)_{|A}, \tag{2.2}$$

where $b \neq 1$ is a q-element. Thus $\gamma(b)_{|A}$ and $\gamma(b)_{|A}\iota(b)_{|A}$ are conjugate, and this yields some information about the eigenvalues of $\gamma(b)_{|A}$. We will show in Section 4.4 that for G of type 7 (with the additional hypothesis $\gamma(A) \leq \mathrm{Inn}(G)$ and $q > 2$) and 8, equation (2.2) is impossible. Therefore in these cases we can always switch a gamma function γ with $p \nmid |\ker(\gamma)|$, with a gamma function $\tilde{\gamma}$ with $p \mid |\ker(\tilde{\gamma})|$.

We cannot do this for G of type 9, 10, and 7 when $q = 2$, as in these cases there may be gamma functions γ which satisfy (2.2). As we will see in Sections 4.4 and 4.6, that will be the case. Therefore here, except for the case when both γ and $\tilde{\gamma}$ have kernel not divisible by p, we can use duality to swich to a more convenient kernel.

Lastly, if G is of type 7 and $\gamma(A) \not\leq \mathrm{Inn}(G)$, then we will show in Section 4.5 that there exists a subgroup C of G of order p for which Remark 1.24 applies, so that the same conclusion of Proposition 1.23 holds, namely $C \leq \ker(\gamma)$ or $C \leq \ker(\tilde{\gamma})$. By Corollary 1.25 we can suppose $C \leq \ker(\gamma)$, and then double the number of regular subgroups we find.

2.2.2 Lifting for groups of order p^2q

Proposition 1.13 establishes a connection between the gamma functions on G and the gamma functions defined on a subgroup of G.

We discuss here a recurring pattern which occurs in the application of Proposition 1.13. Let $\{r, s\} = \{p, q\}$ and let K be a Sylow r-subgroup, and H be a Sylow s-subgroup of G. Clearly $G = KH$ and we know that at least one of K and H is characteristic. In the following we restrict our attention to the GF's $\gamma : G \to \mathrm{Aut}(G)$ such that $H \leq \ker(\gamma)$.

Suppose first K is characteristic. Then γ is the lifting of $\gamma' = \gamma_{\restriction K} : K \to \mathrm{Aut}(G)$. On the other hand, by Proposition 1.13, in this case the RGF's $\gamma' : K \to \mathrm{Aut}(G)$ which can be lifted to G are exactly those for which H is invariant under $\{\gamma'(x)\iota(x) : x \in K\}$.

If K is not characteristic in G, and thus H is, the situation is slightly more involved.

Consider the action of $\gamma(G)$ on the set $\mathcal{R}$ of the Sylow r-subgroups of G. Since by assumption $\gamma(G)$ has order a power of r, Sylow's theorems imply that $\gamma(G)$ has $N_1 > 0$ fixed points in this action. Let $\bar{K} \in \mathcal{R}$ be one of these Sylow r-subgroups of G invariant under $\gamma(G)$. Then $\gamma_{\restriction \bar{K}} : \bar{K} \to \mathrm{Aut}(G)$ is a RGF. On the other hand, since H is characteristic, it is invariant under $\{\gamma'(x)\iota(x) : x \in K\} \leq \mathrm{Aut}(G)$, and thus each RGF $\gamma' : \bar{K} \to \mathrm{Aut}(G)$ can be lifted to a GF on G. It follows that when K is not characteristic, each γ with $H \leq \ker(\gamma)$ can be obtained as a lifting of a γ' defined on a Sylow r-subgroup in N_1 ways, one for each Sylow r-subgroup $\bar{K}$ which is invariant under $\gamma(G)$.

2.2.3 Gluing for groups of order p^2q

Proposition 1.26 describes a way to construct gamma functions on $G = AB$ by gluing together a RGF on A defined as in (2.1) and a RGF on B once equation (1.14) is satisfied.

The main application will be to the kernels of size 1 and p for G of type 8, 9 and 7 when $\gamma(A) \leq \mathrm{Inn}(G)$, and to the kernel of size 1 for G of type 10 (in this case $|\ker(\gamma)| \neq p$, as explained in Subsection 4.6.1).

As said in Subsection 2.2.1, we will show that for G as above, denoting by A the Sylow p-subgroup of G, equation (2.1) is always satisfied.

Moreover, we will show in Subsections 4.4.5, 4.4.6 and 4.6.4 that for a group G as above each γ on G with kernel of size p or 1, as well as for the γ's with kernel of size p^2q, pq, q and p^2 (see Remark 2.5), always admits at least one *invariant* Sylow q-subgroup B, namely a Sylow q-subgroup B such that $B^{\gamma(B)} = B$.

Therefore, in these cases, every GF γ can be obtained as a gluing of a RGF on A determined by σ, and a RGF on B, and the knowledge of the exact number of the invariant Sylow q-subgroups will permit to count all the GF's exactly once.

Chapter 3

The cyclic Sylow p-subgroups case

We are now ready to prove our main Theorem 2. In this chapter we deal with the case of groups with cyclic Sylow p-subgroups. The elementary abelian Sylow p-subgroups case will be dealt with in the next chapter.

We fix the following notation: q and $p > 2$ are distinct primes, G is a group of order p^2q with cyclic Sylow p-subgroups, and $\gamma : G \to \mathrm{Aut}(G)$ is a GF on G.

3.1 G of type 1

In this case $G = \mathcal{C}_{p^2} \times \mathcal{C}_q$; the Sylow p-subgroup $A = \langle a \rangle$ and the Sylow q-subgroup $B = \langle b \rangle$ are both cyclic and characteristic. By Proposition 1.6 A and B are also subgroups of $(G, \circ)$, for each operation $\circ$ induced on G by γ. Moreover, $\mathrm{Aut}(G) = \mathrm{Aut}(A) \times \mathrm{Aut}(B) \cong \mathcal{C}_{p(p-1)} \times \mathcal{C}_{q-1}$ is abelian.

3.1.1 Abelian groups

Assume $(G, \circ)$ abelian, namely it is of type 1. These are in particular the only cases when there are no divisibilities. Let $b \in B$. Then $\gamma(b)$ will be an element of $\mathrm{Aut}(G)$ of order dividing q, so it is an element of $\mathrm{Aut}(A)$ of order dividing q. For $a \in A$, according to Lemma 1.9,

$$a = b^{\ominus 1} \circ a \circ b = b^{-\gamma(b)^{-1}\gamma(a)\gamma(b)} a^{\gamma(b)} b = b^{-\gamma(a)} b a^{\gamma(b)},$$

where the first and the last equality are due to the facts that $G, (G, \circ)$ and $\mathrm{Aut}(G)$ are abelian groups here. Therefore, $\gamma(b) = 1$ and $\gamma(a)_{|B} = 1$, so that $B \leq \ker(\gamma)$. Since A and B are both characteristic in G, Subsection 2.2.2 ensures that the GF's on G are in one-to-one correspondence with the RGF's

$$\gamma' : A \to \mathrm{Aut}(G).$$

On the other hand, since A is cyclic, by Proposition 1.18 each γ' is uniquely defined by assigning the image of the generator a as $\gamma'(a) = \eta \in \mathrm{Aut}(G)$ where $\mathrm{ord}(\eta) \mid p^2$ and $\eta = (\eta_{\restriction A}, \eta_{\restriction B})$.

There are p choices of $\gamma'(a) \in \mathrm{Aut}(G)$ as above, namely

$$\gamma'(a) : \begin{cases} a \mapsto a^{1+ph} \\ b \mapsto b \end{cases},$$

where $1 \leq h \leq p$, and they correspond to p groups $(G, \circ)$ of type 1.

As to the conjugacy classes, let $\varphi \in \mathrm{Aut}(G)$. By Lemma 2.6, we can look at the action of φ on a GF defined on the generators.

Since $B \leq \ker(\gamma)$ is characteristic, for $b \in B$ we have $b^{\varphi^{-1}} \in B$, so that, according to Lemma 1.8,

$$\gamma^{\varphi}(b) = \varphi^{-1}\gamma(b^{\varphi^{-1}})\varphi = 1 = \gamma(b).$$

For $\gcd(u, p) = \gcd(v, q) = 1$, let

$$\varphi : \begin{cases} a \mapsto a^u \\ b \mapsto b^v \end{cases}. \tag{3.1}$$

If f_s is the inverse of the function e_s of Lemma 1.16, we have

$$\gamma(a^{\varphi^{-1}}) = \gamma(a^{u^{-1}}) = \gamma(a^{\circ f_s(u^{-1})}) = \gamma(a)^{f_s(u^{-1})} : \begin{cases} a \mapsto a^{1+phf_s(u^{-1})} \\ b \mapsto b\ . \end{cases}$$

Then,

$$\gamma^{\varphi}(a) = \varphi^{-1}\gamma(a^{\varphi^{-1}})\varphi = \gamma(a)^{f_s(u^{-1})},$$

so that if $h = 0$ we have the conjugacy class of length 1 of $\rho(G)$, whereas if $h \neq 0$, the stabiliser is given by $f_s(u^{-1}) \equiv 1 \bmod p$ and any v, so the stabiliser has order $p(q-1)$, and there is a conjugacy class of length $p - 1$.

In the following we exclude the abelian cases just dealt with.

3.1.2 The case $p|q-1$

If $p \mid q - 1$, necessarily $B \leq \ker(\gamma)$. As in the previous case, Subsection 2.2.2 yields that the GF's on G are in one-to-one correspondence with the RGF's on A, and by Proposition 1.18 each γ' is uniquely defined by the assignment $\gamma'(a) = \eta \in \mathrm{Aut}(G)$, where $A = \langle\, a \,\rangle$, $\mathrm{ord}(\eta) \mid p^2$ and $\eta = (\eta_{\restriction A}, \eta_{\restriction B})$.

Therefore in this case we can also choose $\mathrm{ord}(\eta_{\restriction B}) = p$. There are $p - 1$ choices for such an $\eta_{\restriction B}$, which paired with the p choices for $\eta_{\restriction A} \in \mathrm{Aut}(A)$ of order dividing p yield $p(p-1)$ choices for $\eta \in \mathrm{Aut}(G)$. Thus

$$\gamma'(a) : \begin{cases} a \mapsto a^{1+ph} \\ b \mapsto b^r, \end{cases} \tag{3.2}$$

where r has order p.

For such a γ', the unique γ induced on G defines an operation $\circ$ for which

$$a^{\ominus 1} \circ b \circ a = a^{-\gamma(a)^{-1}\gamma(b)\gamma(a)} b^{\gamma(a)} a = b^{\eta}. \tag{3.3}$$

Since $b^{\circ k} = b^k$, the latter shows that $(G, \circ)$ is of type 2.

As to the conjugacy classes, if φ is as in (3.1), then

$$\gamma^{\varphi}(a) = \begin{cases} a \mapsto a^{1+phf_s(u^{-1})} \\ b \mapsto b^{r^{f_s(u^{-1})}} \end{cases},$$

so the stabiliser is the same as in the previous case, and we get p classes of length $p-1$.

If $p^2 \mid q-1$, we can also choose $\mathrm{ord}(\eta_{|B}) = p^2$. As above, in this case there are $p^2(p-1)$ choices of $\eta \in \mathrm{Aut}(G)$ with this property, and (3.3) shows that $(G, \circ)$ is of type 3.

As to the conjugacy classes, this time r in (3.2) has period p^2, so for the stabiliser we need $f_s(u^{-1}) \equiv 1 \bmod p^2$, that is, $u = 1$. Therefore the stabiliser has order $q-1$, and we get p classes of length $p(p-1)$.

3.1.3 The case $q \mid p-1$

Here $q \mid p-1$, so that $(G, \circ)$ can only be of type 4, beside the type 1 already considered. Moreover, $p \parallel |\mathrm{Aut}(G)|$, so that necessarily $p \mid |\ker(\gamma)|$.

If $A \leq \ker(\gamma)$, since B is the unique Sylow q-subgroup of G, Subsection 2.2.2 yields that the GF's on G are in one-to-one correspondence with the RGF's $\gamma' : B \to \mathrm{Aut}(G)$. In turn, the latter are uniquely determined by the assignment $b \mapsto \gamma'(b)$, where $\mathrm{ord}(\gamma'(b)) \mid q$. Note that all such γ' are morphisms: this follows either from Corollary 1.20, or from Lemma 1.12, as $\gamma(G)$, of order q, acts trivially on the group G/A of order q, so that $[G, \gamma(G)] \leq A \leq \ker(\gamma)$.

For each such γ', the unique γ induced on G defines an operation $\circ$ such that

$$b^{\ominus 1} \circ a \circ b = b^{-1} a^{\gamma(b)} b = a^{\gamma(b)}.$$

Since $(G, \circ)$ is non-abelian, $\mathrm{ord}(\gamma'(b)) = q$. Therefore there are $q-1$ choices for such a $\gamma'(b) \in \mathrm{Aut}(G)$, namely

$$\gamma'(b) : \begin{cases} a \mapsto a^t \\ b \mapsto b \end{cases}$$

with t of order q modulo p^2, and they correspond to $q-1$ groups $(G, \circ)$ of type 4.

As to the conjugacy classes, here $A \leq \ker(\gamma)$ is characteristic, so that the action of any automorphism φ on $\gamma_{|A}$ is trivial.

With φ as in (3.1), we have

$$\gamma^{\varphi}(b) = \gamma(b^{\varphi^{-1}}) = \gamma(b^{v^{-1}}) = \gamma(b)^{v^{-1}} : \begin{cases} a \mapsto a^{t^{v^{-1}}} \\ b \mapsto b \end{cases},$$

which coincides with γ if $v = 1$. Therefore the stabiliser has order $p(p-1)$, and we get a single conjugacy class of length $q-1$.

If $A \not\leq \ker(\gamma)$, then $|\ker(\gamma)| = pq$ or p. Since a group of type 4 has no normal subgroups of order pq, we have $|\ker(\gamma)| = p$. Therefore, $\gamma(G)$ is an abelian group of order pq, and it is isomorphic to the quotient of $(G, \circ)$ by $\ker(\gamma)$. But the latter is a non-abelian group, so we obtain a contradiction.

We summarise, including the right regular representation.

Proposition 3.1. *Let G be a group of order p^2q, $p > 2$, of type 1. Then in* $\mathrm{Hol}(G)$ *there are:*

1. *p regular subgroups of type 1, which split in one conjugacy class of length* 1*, and one conjugacy class of length $p-1$.*
2. *if $p \mid q-1$,*
   (a) *$p(p-1)$ regular subgroups of type 2, which split in p conjugacy classes of length $p-1$;*
   (b) *$p^2(p-1)$ further regular subgroups of type 3, if $p^2 \mid q-1$, which split in p conjugacy classes of length $p(p-1)$.*
3. *if $q \mid p-1$,*
   (a) *$q-1$ regular subgroups of type 4, which form a single conjugacy class.*

3.2 G of type 2

In this case $p \mid q-1$, and $G = \mathcal{C}_q \rtimes_p \mathcal{C}_{p^2}$. The Sylow q-subgroup $B = \langle\, b \,\rangle$ is characteristic in G. Here an element of order p^2 of G induces an automorphism of order p of B.

We have

$$\mathrm{Aut}(G) \cong \mathrm{Hol}(\mathcal{C}_q) \times \mathcal{C}_p.$$

According to Subsection 4.5 of [CCDC21], the second direct factor is generated by the automorphism ψ of G which fixes b, and maps every element of order p^2 to its $(1+p)$-th power. It follows that ψ fixes every element of the unique subgroup of G of order pq.

Since G is non-abelian, as explained in Subsection 2.2.1 in counting the GF's we consider only the case $B \leq \ker(\gamma)$, and then double the number of regular subgroups we find.

Setting aside as always the case of the right regular representation, $\gamma(G)$ will thus be a subgroup of $\mathrm{Aut}(G)$ of order p or p^2.

A Sylow p-subgroup of $\mathrm{Aut}(G)$ is abelian, isomorphic to the direct product of one of the Sylow p-subgroups of $\mathrm{Hol}(\mathcal{C}_q)$ (which is cyclic of order p^e where $p^e \parallel q-1$), and the group $\langle\, \psi \,\rangle$. Moreover, the elements of $\mathrm{Hol}(\mathcal{C}_q)$ of order dividing p are of the form $\iota(x)$ where x is a p-element of G.

3.2.1 The case $|\ker(\gamma)| = q$

This case can only occur when $p^2 \mid q-1$, as by Theorem 1.2(iv) we have $\gamma(G) \cong (G,\circ)/\ker(\gamma)$, and this is a cyclic group by Theorem 2.3. Therefore $\gamma(G)$ is generated by an element (η, ψ^t), where $\eta \in \mathrm{Hol}(\mathcal{C}_q)$ has order p^2 and $0 \le t < p$. Since η^p is an element of order p of $\mathrm{Hol}(\mathcal{C}_q)$, we have $\eta^p = \iota(a)$ for an element $a \in G$ of order p^2. Since every Sylow p-subgroup of G is self-normalising, $A = \langle\, a \,\rangle$ is the only $\gamma(G)$-invariant Sylow p-subgroup.

Once one of the q Sylow p-subgroups A has been chosen, by Subsection 2.2.2 to count the GF's on G we can count the RGF's $\gamma' : A \to \mathrm{Aut}(G)$. By Proposition 1.18, these are as many as the possible images

$$\gamma'(a) = (\eta, \psi^t), \tag{3.4}$$

with $\mathrm{ord}(\eta) = p^2$, $0 \le t < p$, such that A is invariant under $\gamma'(a)$. Since $\langle\, \psi \,\rangle$ fixes all the Sylow p-subgroups of G, it follows as above that $A = \langle\, a \,\rangle$, where $\eta^p = \iota(a)$.

Therefore, once A is chosen, we have $p(p-1)$ choices for η, and p choices for t. So we have $qp^2(p-1)$ GF's on G with $\gamma(G)$ of order p^2.

In this case $(G,\circ)$ is always of type 3. In fact, if $b^\eta = b^j$, then j has order p^2 modulo q and

$$a^{\ominus 1} \circ b \circ a = a^{-1} b^{\gamma(a)} a = a^{-1} b^\eta a = a^{-1} b^j a = b^{j\iota(a)}.$$

Since $\iota(a)$ is an automorphism of B of order p, conjugation by a in $(G,\circ)$ is an automorphism of B of order p^2.

As to the conjugacy classes, since each γ has a unique Sylow p-subgroup A which is $\gamma(A)$-invariant, by Lemma 1.8(2), for $b \in B$, $\gamma^{\iota(b)}$ has $\bar{A} = A^{\iota(b)}$ as $\gamma(\bar{A})$-invariant Sylow p-subgroup. Since $\iota(B)$ conjugates transitively the Sylow p-subgroups of G, all classes have order a multiple of q.

Since the Sylow p-subgroups of $\mathrm{Aut}(G)$ are abelian, we then have for the action of ψ on one of our γ

$$\gamma^\psi(a) = \psi^{-1}\gamma(a^{\psi^{-1}})\psi = \gamma(a^{1-p}),$$

so that all classes have also order a multiple of p. Finally, if ϑ is an element of order $q-1$ of $\mathrm{Aut}(G)$ which fixes a, then $\langle\, \vartheta \,\rangle$ is in the stabiliser of each γ. It follows that we have $p(p-1)$ classes of length qp here.

3.2.2 The case $|\ker(\gamma)| = pq$

Here $\ker(\gamma)$ is the unique subgroup of G of index p. Since $\gamma(G)$ acts trivially on $G/\ker(\gamma)$, we have $[G, \gamma(G)] \leq \ker(\gamma)$, and thus by Lemma 1.12 all the GF's are morphisms $G \to \mathrm{Aut}(G)$ here.

In the case when $\gamma(G) = \langle \psi \rangle$, each Sylow p-subgroup of G is $\gamma(G)$-invariant, thus the lifts of the RGF on any Sylow subgroup all give the same set of GF on G. If $\langle a \rangle$ is any of the Sylow p-subgroups, there are $p-1$ choices for $\gamma(a)$, and such a choice determines γ uniquely. It is immediate to check that $a^{\ominus 1} \circ b \circ a = a^{-1}ba$, so that the corresponding groups $(G, \circ)$ are all of type 2.

As to the conjugacy classes, ψ is central in $\mathrm{Aut}(G)$ and [CCDC21, Remark 3.3] implies that $\mathrm{Aut}(G)$ acts trivially on $G/\ker(\gamma)$ so that for $\varphi \in \mathrm{Aut}(G)$ we have $\gamma^{\varphi}(a) = \gamma(a^{\varphi^{-1}}) = \gamma(a)$, and we end up with $p-1$ conjugacy classes of length 1.

If $\gamma(G) \neq \langle \psi \rangle$, as above there is a unique Sylow p-subgroup $A = \langle a \rangle$ fixed by $\gamma(G)$, and

$$\gamma(a) = (\iota(a)^{-s}, \psi^t), \quad \text{for some } 0 < s < p,\ 0 \leq t < p.$$

Since there are q choices for the Sylow p-subgroup A, this gives a total of $q(p-1)p$ GF's. For the operation $\circ$ we have

$$a^{\ominus 1} \circ b \circ a = a^{-1}b^{\gamma(a)}a = a^{-1}b^{\iota(a)^{-s}}a = b^{\iota(a^{-s+1})}.$$

If $s \equiv 1 \bmod p$, then $(G, \circ)$ is of type 1 for each of the qp choices of A and t.

If $s \not\equiv 1 \bmod p$, $(G, \circ)$ is of type 2; here there are q choices for A, $p-2$ choices for s, and p choices for t.

As to the conjugacy classes, with the above arguments we see that they have all length a multiple of q, and that the subgroup $\langle \psi, \vartheta \rangle$ of order $p(q-1)$ is in the stabiliser, so that each class has indeed length q.

We summarise, including the right and left regular representations.

Proposition 3.2. *Let G be a group of order p^2q, $p > 2$, of type 2. Then in $\mathrm{Hol}(G)$ there are:*

1. *$2pq$ regular subgroups of type 1, which split into $2p$ conjugacy classes of length q;*
2. *$2qp(p-2) + 2p$ of type 2, which split into $2p(p-2)$ conjugacy classes of length q, and $2p$ conjugacy classes of length 1;*
3. *$2qp^2(p-1)$ further regular subgroups of type 3, if $p^2 \mid q-1$, which split into $2p(p-1)$ conjugacy classes of length qp.*

3.3 G of type 3

In this case $G = \mathcal{C}_q \rtimes_1 \mathcal{C}_{p^2}$, with $p^2 \mid q-1$. The Sylow q-subgroup $B = \langle b \rangle$ is characteristic in G, and an element of order p^2 of G induces an automorphism of order p^2 on B. Here $\mathrm{Aut}(G) \cong \mathrm{Hol}(\mathcal{C}_q)$, and since G has trivial centre we have $\mathrm{Inn}(G) \cong G$.

Since

$$\left|\frac{\mathrm{Aut}(G)}{\mathrm{Inn}(G)}\right| = \frac{q-1}{p^2}$$

is coprime to q, and the Sylow p-subgroups of $\mathrm{Aut}(G)$ are cyclic, we get $\gamma(G) \leq \mathrm{Inn}(G)$.

By Proposition 1.6, B is also a Sylow q-subgroup of $(G, \circ)$, so that $|\gamma(B)|$ divides q, and

$$\gamma(B) \leq \iota(B) = \{\iota(b^x) : 0 \leq x < q\}.$$

By Subsection 2.2.1 we consider only the case $B \leq \ker(\gamma)$, and then double the number of regular subgroups we find.

Now Theorem 1 of [Cur08] (as recorded in Theorem 3.2 and Remark 3.3 of [CCDC21]) yields that $\mathrm{Aut}(G)$ acts trivially on G/B, so that $[G, \gamma(G)] \leq [G, \mathrm{Aut}(G)] \leq B \leq \ker(\gamma)$, and then by Lemma 1.12 all the GF's are morphisms $\gamma : G \to \mathrm{Aut}(G)$ in this case.

If $\gamma(G) \neq \{1\}$, we claim that there is exactly one Sylow p-subgroup of G which is $\gamma(G)$-invariant. In fact, $|\gamma(G)| = p$ or p^2, and $\gamma(G)$ is a cyclic subgroup of $\langle\, \iota(a) \,\rangle$ for some $a \in G$ with $\mathrm{ord}(a) = p^2$. Since every Sylow p-subgroup of G is self-normalising, $A = \langle\, a \,\rangle$ is the only $\gamma(G)$-invariant Sylow p-subgroup.

Let $\gamma(a) = \iota(a^{-s})$, for some $0 < s < p^2$.

In G we have $a^{-1}ba = b^t$, for some t of order p^2 modulo q. We get

$$a^{\ominus 1} \circ b \circ a = a^{-1} b^{\gamma(a)} a = a^{-1} b^{\iota(a)^{-s}} a = a^{-(1-s)} b a^{1-s} = b^{t^{1-s}}, \tag{3.5}$$

and since b is $\gamma(b)$-invariant, $a^{\ominus 1} \circ b \circ a = b^{\circ t^{1-s}}$. We obtain the following.

- If $s \equiv 1 \bmod p^2$, then $(G, \circ)$ is of type 1, and for each of the q Sylow p-subgroups A of G there is exactly one GF with this property.
- If $s \equiv 1 \bmod p$ but $s \not\equiv 1 \bmod p^2$, then conjugation by a in $(G, \circ)$ has order p, so $(G, \circ)$ is of type 2. For each of the q Sylow p-subgroups A there are $p-1$ such GF's, so that we get $q(p-1)$ GF's in this case.
- If $s \not\equiv 1 \bmod p$, conjugation by a in $(G, \circ)$ has order p^2, hence $(G, \circ)$ is of type 3. For each of the q Sylow p-subgroups A of G there are $p^2 - p - 1$ such choices of s with $0 < s < p^2$, so that we get $q(p^2 - p - 1)$ groups in this case.

As to the conjugacy classes, $\iota(B)$ conjugates transitively the Sylow p-subgroups of G, so that by Lemma 1.8.(2) each conjugacy class for $s \neq 0$ has length

a multiple of q. The cyclic complement of order $q-1$ of $\iota(B)$ in $\mathrm{Aut}(G)$ which contains $\gamma(a) = \iota(a^{-s})$ centralises a and $\gamma(a)$, so that, by Lemma 1.8, it centralises γ. It follows that the conjugacy classes have length precisely q.

We summarise, including the right and left regular representations.

Proposition 3.3. *Let G be a group of order p^2q, $p > 2$, of type 3. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $2q$ *regular subgroups of type 1, which split into* 2 *conjugacy classes of length q;*
2. $2q(p-1)$ *regular subgroups of type 2, which split into* $2(p-1)$ *conjugacy classes of length q;*
3. $2(1+q(p^2-p-1))$ *regular subgroups of type 3, which split into* 2 *conjugacy classes of length* 1*, and* $2(p^2-p-1)$ *conjugacy classes of length q.*

3.4 G of type 4

Here $q \mid p-1$, and $G = \mathcal{C}_{p^2} \rtimes \mathcal{C}_q$, where an element of order q acts non-trivially on the unique Sylow p-subgroup $A = \langle\, a \,\rangle$. We have $\mathrm{Aut}(G) \cong \mathrm{Hol}(\mathcal{C}_{p^2})$, and $\mathrm{Inn}(G) \cong G$, as $Z(G) = 1$. The groups $(G, \circ)$ can be of type 1 or 4.

As discussed in the proof of Proposition 2.1, $\mathrm{Aut}(G)$ has a unique Sylow p-subgroup, which is isomorphic to $\mathcal{C}_{p^2} \rtimes \mathcal{C}_p$ where the normal factor is $\langle\, \iota(a) \,\rangle$. For the second factor we have p choices. In fact, according to Theorem 3.4 and Remark 3.5 of [CCDC21], for each of the p^2 Sylow q-subgroups B we can choose a generator ψ of the second factor such that $\psi : a \mapsto a^{1+p}$, and ψ restricts to the identity on B: we will make a convenient choice of B, and thus ψ, later. Note that if ψ is the identity on the Sylow q-subgroup $B = \langle\, b \,\rangle$, then it is also the identity on the p Sylow q-subgroups $\langle\, a^{p^i} b \,\rangle$, for $0 \le i < p$.

Since the Sylow q-subgroups of $\mathrm{Aut}(G)$ are cyclic, the elements of $\mathrm{Aut}(G)$ of order q are inner automorphisms, given by conjugation by an element of G of order q.

By Subsection 2.2.1, in counting the GF's we consider only the case in which p divides $|\ker(\gamma)|$.

3.4.1 The case $|\ker(\gamma)| = p^2$

Here $\ker(\gamma) = A$ and $|\gamma(G)| = q$. Hence $\gamma(G) = \langle\, \iota(b) \,\rangle$ for some $b \in G$ of order q, so that $B = \langle\, b \,\rangle$ is the unique $\gamma(G)$-invariant subgroup. Since $[G, \gamma(G)] \le A = \ker(\gamma)$, each such γ is a morphism. For the operation $\circ$ we have

$$b^{\ominus 1} \circ a \circ b = b^{-1} a^{\gamma(b)} b = a^{\gamma(b)\iota(b)}.$$

Since a is $\gamma(a)$-invariant, once we have made one of the p^2 choices for B, the value $\gamma(b) = \iota(b)^{-1}$ will give an abelian group $(G, \circ)$ of type 1, while all other $q-2$ choices for $\gamma(b)$ will give groups of type 4.

As to the conjugacy classes, $\iota(A)$ conjugates transitively the Sylow q-subgroups, so that all classes have length a multiple of p^2. The cyclic complement of order $p(p-1)$ of $\iota(A)$ in $\mathrm{Aut}(G)$ which contains $\gamma(G) = \langle\, \iota(b) \,\rangle$ centralises b and $\gamma(b)$ so that, by Lemma 1.8, it fixes γ. Hence the conjugacy classes have length precisely p^2.

3.4.2 The case $|\ker(\gamma)| = pq$

This case does not occur. In fact, since $\ker(\gamma) \trianglelefteq (G, \circ)$, we have that $(G, \circ)$ is abelian here. Thus if $b \in \ker(\gamma)$ is an element of order q, we have

$$b = a^{\ominus 1} \circ b \circ a = a^{-\gamma(a)^{-1}\gamma(b)\gamma(a)} b^{\gamma(a)} a = b^{\gamma(a)\iota(a)}.$$

Now $\gamma(a)$ is an element of order p in $\mathrm{Aut}(G)$. Therefore, by Remark 2.2, we have

$$(\gamma(a)\iota(a))^p = \iota(a^p).$$

This implies that b and a^p commute, a contradiction.

3.4.3 The case $|\ker(\gamma)| = p$

Here $\ker(\gamma) = A^p$, and $|\gamma(G)| = pq$. Clearly $\gamma(A)$ has order p, as $A \leq (G, \circ)$. An element of order q of $\gamma(G)$ will thus be of the form $\gamma(b)$, for some $b \in G$, which will be of order q, as all elements of G outside of A have order q.

Therefore

$$\gamma(b) = \iota(a^m b^{-l})$$

for some $0 < l < q$ and m, so that $a^m b^{-l}$ has also order q. Now choose a ψ as above that fixes $a^m b^{-l}$.

$\gamma(a)$ will be an element of order p of $\mathrm{Aut}(G)$, that is, an element of $\langle\, \iota(a^p), \psi \,\rangle$, an elementary abelian group of order p^2. Since $\gamma(G)$ is a subgroup of $\mathrm{Aut}(G)$ of order pq, and $p > q$, we will have that $\langle\, \gamma(a) \,\rangle$ is normalised by $\iota(a^m b^{-l})$, an element of order q. Now $\iota(a^m b^{-l})$ centralises ψ by the choice of the latter, and normalises but does not centralise $\langle\, \iota(a^p) \,\rangle$. In other words, $\iota(a^m b^{-l})$ has two distinct eigenvalues in its action on $\langle\, \iota(a^p), \psi \,\rangle$, so that there are two possibilities for $\gamma(a)$ to be normalised by $\iota(a^m b^{-l})$.

If $\gamma(a) = \iota(a^{ps}) \neq 1$, for some s, Proposition 1.23 yields that $ps \equiv -1 \bmod p^2$, a contradiction.

Therefore $\gamma(a) = \psi^t$ for some $t \neq 0$. It follows that $\gamma(G) = \left\langle\, \psi, \iota(a^m b^{-l}) \,\right\rangle$ is abelian, and thus $(G, \circ)$ is of type 1, as a group of type 4 does not have an abelian quotient of order pq.

Comparing $b \circ a^p = ba^p$ with

$$a^p \circ b = a^{p\gamma(b)}b = a^{p\iota(b^{-l})}b = ba^{p\iota(b^{-l+1})}$$

in the abelian group $(G, \circ)$, we get $l = 1$.

Now

$$(b^{-1})^\psi = (a^{-m}a^m b^{-1})^\psi = (a^{-m})^\psi a^m b^{-1} = a^{-m(1+p)}a^m b^{-1} = a^{-pm}b^{-1},$$

so that, taking the inverse, we get

$$b^\psi = ba^{pm}.$$

Comparing

$$a \circ b = a^{\gamma(b)}b = a^{\iota(b^{-1})}b = ba,$$

with

$$b \circ a = b^{\gamma(a)}a = ba^{pmt}a$$

we obtain $p \mid m$. Write $m = pn$ for some n. We have thus

$$\gamma(ba^{-pn}) = \gamma(b) = \iota(a^{pn}b^{-1}) = \iota(ba^{-pn})^{-1},$$

so that all the GF's with kernel of order p can be constructed as follows.

Choose first one of the p^2 Sylow q-subgroups $B = \langle\, b \,\rangle$. Then define ψ as the automorphism of G that is the power $1+p$ on A, and fixes b. Finally define γ as

$$\begin{cases} \gamma(a) = \psi^t \\ \gamma(b) = \iota(b^{-1}). \end{cases} \tag{3.6}$$

It is immediate to see that $\gamma(b^i a^j) = \iota(b^{-i})\psi^{tj}$ defines indeed a GF satisfying the GFE. Note that (3.1) determines $\langle\, b \,\rangle$ uniquely as the only Sylow q-subgroup B of G which is $\gamma(B)$-invariant. In fact, if $B = \langle ba^k \rangle$ is $\gamma(B)$-invariant, we have, writing $a^{\iota(b^{-1})} = a^\lambda$,

$$(ba^k)^{\gamma(ba^k)} = ba^{k\lambda(1+ptk)},$$

and since $(ba^k)^{\gamma(ba^k)} \in B$, the latter equals ba^k and we have

$$k(\lambda(1 + ptk) - 1) \equiv 0 \bmod p^2.$$

Since λ has order q modulo p^2, we have that $\lambda \not\equiv 1 \bmod p$, so that $k \equiv 0 \bmod p^2$ and $B = \langle\, b \,\rangle$.

Therefore the p^2 choices for B and the $p - 1$ choices for t yield $p^2(p - 1)$ choices for γ.

As to the conjugacy classes, take γ defined as in (3.6). By Lemma 1.8(2), $\langle\, \iota(a) \,\rangle$ acts regularly on the γ's, so that all conjugacy classes have order a multiple of p^2.

Consider now the group R of automorphisms of G, of order $p(p-1)$, of the form

$$\varphi : \begin{cases} a \mapsto a^r \\ b \mapsto b \end{cases} .$$

We claim that the stabiliser in R of any γ is $\langle \psi \rangle$, of order p. It follows that all conjugacy classes have order a multiple of $p-1$, and thus all conjugacy classes have order $p^2(p-1)$.

In fact one sees immediately, using the fact that $\psi \in R$, and that the latter is cyclic, that

$$\begin{cases} \gamma^\varphi(a) = \psi^{tr^{-1}} \\ \gamma^\varphi(b) = \iota(b^{-1}) \end{cases}$$

Thus $\gamma^\varphi = \gamma$ if and only if $r \equiv 1 \bmod p$, as claimed.

We summarise, including the right and left regular representations.

Proposition 3.4. *Let G be a group of order p^2q, $p > 2$, of type 4. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $2p^3$ *regular groups of type 1, which split into* 2 *conjugacy classes of length* p^2*, and* 2 *conjugacy classes of length* $p^2(p-1)$*;*
2. $2(1 + p^2(q-2))$ *regular groups of type 4, which split into* 2 *conjugacy classes of length* 1*, and* $2(q-2)$ *conjugacy classes of length* p^2*.*

Chapter 4

The elementary abelian Sylow p-subgroups case

In this chapter we deal with the case of groups with elementary abelian Sylow p-subgroups.

We fix the following notation: q and $p > 2$ are distinct primes, G is a group of order p^2q with elementary abelian Sylow p-subgroups, and $\gamma : G \to \mathrm{Aut}(G)$ is a GF on G.

Before starting with the enumeration of the regular subgroup of $\mathrm{Hol}(G)$, we report some result on $\mathrm{GL}(2,p)$ which will be useful throughout this chapter.

4.1 Some results on $\mathrm{GL}(2,p)$

We collect here some information about $\mathrm{GL}(2,p)$, which will be useful for dealing with the groups G of type 5 or 7.

We write A for the Sylow p-subgroup of G (which is unique in both cases), and B for a Sylow q-subgroup of G.

4.1.1 Sylow p-subgroups

$\mathrm{GL}(2,p)$ has $p+1$ Sylow p-subgroups and each of them fixes a p subgroup of $\mathcal{C}_p \times \mathcal{C}_p$. In the following we will denote by α an element of order p of $\mathrm{GL}(2,p)$.

4.1.2 Elements of order p when $p \parallel |\ker(\gamma)|$

Suppose that G is of type 5 or 7, and let γ be a GF on G such that $\langle\, a_1 \,\rangle \leq \ker(\gamma) \neq A$, where $a_1 \in A$, $a_1 \neq 1$. Let $a_2 \in A \setminus \langle\, a_1 \,\rangle$, then $\gamma(a_2) = \alpha$ (possibly modulo $\iota(A)$), where $\alpha \in \mathrm{GL}(2,p)$ has order p. Then

$$a_1^{\alpha} a_2 = a_1 \circ a_2 = a_2 \circ a_1 = a_2 a_1, \tag{4.1}$$

so that a_1 is fixed by α. This means that $\ker(\gamma)$ determines $\langle\, \alpha \,\rangle$, which is the Sylow p-subgroup of $\mathrm{GL}(2,p)$ fixing $\ker(\gamma)$.

4.1.3 Sylow q-subgroups

Suppose that $q \mid p-1$ and recall that $|\mathrm{GL}(2,p)| = (p-1)^2 p(p+1)$.

If $q > 2$ a Sylow q-subgroup of $\mathrm{GL}(2,p)$ has order q^{2e}, where $q^e \parallel p-1$. Every Sylow q-subgroup of $\mathrm{GL}(2,p)$ is of the form

$$\begin{aligned} Q_{A_1,A_2} &= \{\beta \in \mathrm{GL}(2,p) \colon A_1, A_2 \text{ are eigenspaces of } \beta \text{ with respect} \\ &\qquad\qquad \text{to eigenvalues of order dividing } q^e\} \\ &\cong \mathcal{C}_{q^e} \times \mathcal{C}_{q^e}, \end{aligned}$$

for any choice of a pair $\{A_1, A_2\}$ of distinct one-dimensional subspaces of A. Thus there are $\frac{p(p+1)}{2}$ Sylow q-subgroups.

Moreover, each Sylow q-subgroup of $\mathrm{GL}(2,p)$ has q^2-1 elements of order q. However, the scalar elements are common to all the Sylow q-subgroups. Hence $\mathrm{GL}(2,p)$ has

$$(q^2-q) \cdot \frac{(p+1)p}{2} + q - 1$$

elements of order q.

If $q = 2$, the Sylow 2-subgroups of $\mathrm{GL}(2,p)$ are described in [CF64]. Note that in this case if ϑ has order 2, then its minimal polynomial divides x^2-1, and therefore its egeinvalues belong to $\{\pm 1\}$. Moreover all the elements with eigenvalues $1, -1$ are conjugate, and such an element, say ϑ, is stabilised by the diagonal matrices, therefore $|\mathrm{Orb}(\vartheta)| = p(p+1)$. Thus there are $p(p+1)$ non-scalar elements of order 2, plus the scalar matrix $\mathrm{diag}(-1,-1)$.

4.1.4 Elements of order q when $|\ker(\gamma)| = p$

Suppose that $q \mid p-1$ and G is of type 5 or 7. Let γ be a GF on G with kernel $\langle\, a_1 \,\rangle$, where $a_1 \in A$. Let $b \in G$ be such that $\gamma(b) = \beta$ (possibly modulo $\iota(A)$), where β is an element of order q in the normaliser of α. Then $\alpha^\beta = \alpha^t$ for a certain t, and Subsection 4.1.2 yields that $\langle\, a_1 \,\rangle$ is fixed by α, so that

$$a_1^{\beta\alpha} = a_1^{\alpha^{t^{-1}}\beta} = a_1^\beta,$$

namely a_1^β is fixed by α as well. Therefore $a_1^\beta \in \langle\, a_1 \,\rangle$, so that $\langle\, a_1 \,\rangle$ is an eigenspace for β too.

Let $\langle\, a_3 \,\rangle$ be another eigenspace for β. Then, since $\det(\alpha)^p = 1$, up to change a_3 with a suitable element in $\langle\, a_3 \,\rangle$ we can write, with respect to the basis $\langle\, a_1, a_3 \,\rangle$,

$$\alpha = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ \beta = \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{x_2} \end{pmatrix},$$

where λ has order q, and x_1, x_2 are not both 0.

Note that if β is a scalar matrix, there are $q-1$ elements β as above. If β is non-scalar, taking into account the choice of $\langle\, a_3 \,\rangle$, there are $q(q-1)p$ possibilities for β.

4.2 G of type 5

In this case $G = (\mathcal{C}_p \times \mathcal{C}_p) \times \mathcal{C}_q$; the Sylow p-subgroup A and the Sylow q-subgroup $B = \langle\, b \,\rangle$ are both characteristic. Moreover, $\mathrm{Aut}(G) = \mathrm{GL}(2,p) \times \mathcal{C}_{q-1}$.

In the following we will denote by α an element of order p of $\mathrm{GL}(2,p)$. If $p \mid q-1$, η will be a fixed element of order p of $\mathcal{C}_{q-1}$; clearly η fixes A point-wise. If $q \mid p-1$ we will denote by β an element of order q of $\mathrm{GL}(2,p)$.

4.2.1 Abelian groups

Assume here $(G, \circ)$ abelian. These are in particular the only cases when there are no divisibilities.

Let $b \in B$. Then $\gamma(b)$ will have order dividing q, so it is an element in $\mathrm{GL}(2,p)$ of order dividing q. Therefore, for $a \in A$, we have

$$a = b^{\ominus 1} \circ a \circ b = b^{-\gamma(b)^{-1}\gamma(a)\gamma(b)} b a^{\gamma(b)} = b^{-\gamma(a)} b a^{\gamma(b)},$$

from which we get that $\gamma(b) = 1$, thus $B \leq \ker(\gamma)$, and also that $\gamma(a)_{|B} = 1$, namely $\gamma(a) \in \mathrm{Aut}(A) = \mathrm{GL}(2,p)$.

If $\gamma(G) = \{1\}$, then we obtain the right regular representation, so suppose $\gamma(G) \neq \{1\}$. Since $p \parallel |\mathrm{GL}(2,p)|$, we can only have $\gamma(G) = \gamma(A) = \langle\, \alpha \,\rangle$, where $\alpha \in \mathrm{GL}(2,p)$ has order p. Therefore γ is the lifting of a RGF on A (which will still denote by γ) with $|\gamma(A)| = p$.

Let $1 \neq a_1 \in A$ and let $\ker(\gamma) = \langle\, a_1 \,\rangle$; there are $p+1$ choices for such a subgroup. Subsection 4.1.2 shows that $\langle\, a_1 \,\rangle$ is fixed by α, so that $\ker(\gamma)$ determines $\gamma(A)$. So, if $a_2 \in A \setminus \langle\, a_1 \,\rangle$, then $\gamma(a_2) = \alpha^i$, for $1 \leq i \leq p-1$.

Now for each i the unique morphism defined as $\gamma(a_1) = 1$ and $\gamma(a_2) = \alpha^i$ satisfies $[A, \gamma(A)] = \ker(\gamma)$, so that Lemma 1.12 yields that these morphisms coincide with the RGF's. Therefore there are $(p+1)(p-1) = p^2 - 1$ different GF's on G, corresponding to groups $(G, \circ)$ of type 5.

As to the conjugacy classes, since $B \leq \ker(\gamma)$ is characteristic, every automorphism φ of G stabilises $\gamma_{|B}$. Moreover, if $\mu \in \mathrm{Aut}(B) \cong \mathcal{C}_{q-1}$, then $\langle\, \mu \,\rangle$ centralises a and $\gamma(a)$, so that it centralises γ.

Now, let $\delta \in \mathrm{Aut}(A) \cong \mathrm{GL}(2,p)$. If δ stabilises γ, then $\gamma^\delta(a_1) = 1$, namely $\gamma(a_1^{\delta^{-1}}) = 1$. Therefore δ^{-1} fixes $\langle\, a_1 \,\rangle$, and writing $\delta = (\delta_{ij})_{i,j}$ with respect to the basis $\{a_1, a_2\}$, this implies that $\delta_{12} = 0$.

As for a_2, we have

$$\gamma^\delta(a_2) = \delta^{-1}\gamma(a_2^{\delta^{-1}})\delta = \delta^{-1}\alpha^{\delta_{22}^{-1}}\delta,$$

and it coincides with $\gamma(a_2)$ precisely when $\delta^{-1}\alpha^{\delta_{22}^{-1}}\delta = \alpha$. An explicit computation shows that the latter yields $\delta_{11} = \delta_{22}^2$. Therefore, the stabiliser of γ has order $(q-1)p(p-1)$, and there is one orbit of length $p^2 - 1$.

In the following we exclude the abelian cases just dealt with.

4.2.2 The case $p \mid q-1$

Here $B \leq \ker(\gamma)$, and the only type of groups $(G, \circ)$ we can have is the type 11, beside the type 5 already considered.

The case $|\ker(\gamma)| = pq$. Suppose first $\ker(\gamma) = \langle a_1 \rangle B$ has order pq. Then $\gamma(G)$ has order p, and let a_2 be such that $\gamma(a_2) = \alpha^i \eta^j$, where $0 \leq i, j < p$, $j \neq 0$ (since we are assuming $(G, \circ)$ non abelian). The argument in 4.1.2 shows that $a_1^\alpha = a_1$, and by Lemma A.2 in the Appendix, γ is a RGF if and only if it is a morphism. Therefore the GF's are as many as the choices of $(\langle a_1 \rangle, i, j)$, namely $(p+1)p(p-1) = p(p^2-1)$, and each of them corresponds to a group $(G, \circ)$ of type 11.

As to the conjugacy classes, again $\mathcal{C}_{q-1}$ stabilises every γ. Moreover, if $\delta \in \mathrm{GL}(2,p)$ stabilises γ, then δ^{-1} fixes $\langle a_1 \rangle$, so that $\delta_{12} = 0$. This time

$$\gamma^\delta(a_2) = \delta^{-1}\gamma(a_2^{\delta_{22}^{-1}})\delta = \delta^{-1}\alpha^{i\delta_{22}^{-1}}\delta\eta^{j\delta_{22}^{-1}},$$

where $j \neq 0$. Therefore δ stabilises γ precisely when $\delta_{12} = 0$, $\delta_{22} = 1$, and δ centralises α^i. If $i = 0$, the latter yields no condition, while corresponds to take $\delta_{11} = 1$ if $i \neq 0$. So the δ's in the stabiliser are those of the form

$$\delta = \begin{pmatrix} \delta_{11} & 0 \\ \delta_{21} & 1 \end{pmatrix} \text{ if } i = 0, \text{ and } \delta = \begin{pmatrix} 1 & 0 \\ \delta_{21} & 1 \end{pmatrix} \text{ if } i \neq 0.$$

Therefore, if $i = 0$ the stabiliser has order $(q-1)p(p-1)$, and there is one orbit of length p^2-1. If $i \neq 0$, the stabiliser has order $(q-1)p$, and there is one orbit of length $(p^2-1)(p-1)$.

The case $|\ker(\gamma)| = q$. Now suppose $\ker(\gamma) = B$ has order q. Then $\gamma(G) = \gamma(A) = \langle \alpha, \eta \rangle$. Let $a_1, a_2 \in A$ be such that

$$\begin{cases} \gamma(a_1) = \eta \\ \gamma(a_2) = \alpha \end{cases}. \tag{4.2}$$

Since

$$a_1^\alpha a_2 = a_1 \circ a_2 = a_2 \circ a_1 = a_2 a_1,$$

a_1 is a fixed point of α, and since α has determinant equal to 1, we can suppose

$$\alpha = \begin{pmatrix} 1 & 0 \\ d & 1 \end{pmatrix},$$

with respect to $\{a_1, a_2\}$, where $1 \leq d \leq p-1$. By Lemma 2.6 and Lemma A.1 in the Appendix, each assignment (4.2) defines exactly one GF. Therefore, in this case, we have $p+1$ choices for $\gamma(G)$, and once $\gamma(G)$ has been chosen, there

are $p-1$ ways to choose a_1 among the fixed points of α, and p^2-p choices for a_2, which is any element of $A \setminus \langle a_1 \rangle$. So there are $(p^2-1)p(p-1)$ groups of type 11.

As to the conjugacy classes, every automorphism in $\mathcal{C}_{q-1}$ stabilises γ. Since $B = \ker(\gamma)$ is characteristic, by Lemma 2.6, we just consider the action of $\mathrm{GL}(2,p)$ on γ defined on the generators of A.

Let $\delta \in \mathrm{GL}(2,p)$. Then, $\gamma^\delta(a_1) = \gamma(a_1)$ if and only if $\gamma(a_1^{\delta^{-1}}) = \gamma(a_1)$, as δ^{-1} centralises η. The latter yields $\gamma(a_1^{\delta^{-1}})_{|A} = 1$, so that $a_1^{\delta^{-1}} \in \langle a_1 \rangle$, namely $\delta_{12} = 0$. Moreover, since $\gamma_{|\langle a_1 \rangle}$ is a morphism, $\gamma(a_1^{\delta^{-1}}) = \eta$ if and only if $\delta_{11} = 1$. Now, since

$$\gamma(a_2^k) = \gamma(a_1)^{-d(\frac{k(k-1)}{2})}\gamma(a_2)^k = \eta^{-d(\frac{k(k-1)}{2})}\alpha^k,$$

we have

$$\gamma^\delta(a_2) = \delta^{-1}\gamma(a_2^{\delta^{-1}})\delta = \delta^{-1}\gamma(a_1^{-\delta_{21}\delta_{22}^{-1}}a_2^{\delta_{22}^{-1}})\delta = \eta^{-\delta_{22}^{-1}(\delta_{21}+\frac{d}{2}(\delta_{22}^{-1}-1))}\delta^{-1}\alpha^{\delta_{22}^{-1}}\delta,$$

and the latter coincides with $\gamma(a_2)$ precisely when

$$\begin{cases} \delta^{-1}\alpha^{\delta_{22}^{-1}}\delta = \alpha \\ \delta_{21} = -\frac{d}{2}(\delta_{22}^{-1}-1). \end{cases}$$

The first condition yields $\delta_{22}^2 = 1$, namely $\delta_{22} = \pm 1$, so that the second yields $\delta_{21} = 0, d$ respectively when $\delta_{22} = 1, -1$. Therefore the stabiliser has order $2(q-1)$ and we get 2 orbits of length $\frac{1}{2}(p^2-1)p(p-1)$.

4.2.3 The case $q \mid p-1$

Here $\gamma(G) \subseteq \mathrm{GL}_2(p)$, so $p \mid |\ker(\gamma)|$ and $\gamma(G)$ acts trivially on B, so that

$$b^{\ominus 1} \circ a \circ b = b^{-\gamma(b)^{-1}\gamma(a)\gamma(b)}a^{\gamma(b)}b = b^{-1}ba^{\gamma(b)} = a^{\gamma(b)}. \tag{4.3}$$

If $pq \mid |\ker(\gamma)|$, then equation (4.3) becomes

$$b^{\ominus 1} \circ a \circ b = a,$$

so $(G, \circ)$ is of type 5 and has already been considered. Thus we just deal with the cases of kernel p^2 and p.

The case $|\ker(\gamma)| = p^2$. If $\ker(\gamma) = A$ the GF's are exactly the morphisms. Let $\lambda \in \mathcal{C}_p^*$ be an element of order q. By Subsection 4.1.3, with respect to a suitable basis $\{a_1, a_2\}$ of A, we have

$$T = [\gamma(b)] = \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{x_2} \end{pmatrix}.$$

Now, since $a^k = a^{\circ k}$, equation (4.3) yields that the action of $\iota(b)$ on A in $(G, \circ)$ is precisely $\gamma(b)$. Thus, according to the choices of $\gamma(b)$ we easily obtain, besides the abelian cases,

1. $q-1$ groups of type 7, corresponding to the choices $x_1 = x_2 \neq 0$.

2. $\frac{p(p+1)}{2} \cdot 2(q-1)$ groups of type 6: choose the eigenspaces, and then the eigenvalue different from 1.

3. if $q > 2$ we get $\frac{p(p+1)}{2}(q-1)$ groups of type 9.

4. if $q > 3$ we get $\frac{p(p+1)}{2}(q-1)(q-3)$ groups of type 8. More precisely, denoting by $Z_\circ$ the action of b on A in $(G, \circ)$, since $Z_\circ \sim \mathrm{diag}(\mu^{x_1 x_2^{-1}}, \mu)$, where $\mu = \lambda^{x_2}$, they split in $p(p+1)(q-1)$ groups isomorphic to G_s for every $s \in \mathcal{K}$.

As to the conjugacy classes, since $A = \ker(\gamma)$ is characteristic, $\gamma_{|A}$ is stabilised by every automorphism φ of G.

As for $\gamma_{|B}$, let $\mu \in \mathcal{C}_{q-1}$, so that $b^{\mu^{-1}} = b^k$ for some k, and let $\delta \in \mathrm{GL}(2,p)$. Then

$$\gamma^{\mu\delta}(b) = \delta^{-1}\gamma(b)^k\delta.$$

Therefore $\mu\delta$ stabilises γ precisely when T and T^k are conjugate, and in that case they need to have the same eigenvalues, namely $kx_1 = x_1$ and $kx_2 = x_2$ or $kx_1 = x_2$ and $kx_2 = x_1$. Note that if $k = 1$, then δ stabilises γ if and only if it is in the centraliser of T: if T is scalar, then every $\delta \in \mathrm{GL}(2,p)$ stabilises γ, while for a non-scalar matrix T the condition is equivalent to have δ a diagonal matrix with no diagonal elements equal to zero.

Referring to the cases above, we have the following.

1. T is scalar and $T \sim T^k$ if and only if $k = 1$, so that the stabiliser has order $|\mathrm{GL}(2,p)|$, and there is one orbit of length $q-1$.

2. T is non-scalar and $k = 1$. In this case the centraliser of T consists of the elements $\delta = \mathrm{diag}(\delta_{11}, \delta_{22})$, with $\delta_{ii} \neq 0$, therefore it has $(p-1)^2$ elements. Thus $|\mathrm{Stab}(\gamma)| = (p-1)^2$, and there is one orbit of length $p(p+1)(q-1)$.

3. T is non-scalar and $k = \pm 1$. If $k = 1$ then the elements in the stabiliser are the diagonal matrices as above. If $k = -1$ the stabiliser consists of the elements $\mu\delta$, where $b^{\mu^{-1}} = b^{-1}$, and

$$\delta = \begin{pmatrix} 0 & \delta_{12} \\ \delta_{21} & 0 \end{pmatrix},$$

   where $\delta_{12} \neq 0 \neq \delta_{21}$. Therefore $|\mathrm{Stab}\,\gamma| = 2(p-1)^2$, and there is one orbit of length $\frac{1}{2}p(p+1)(q-1)$.

4. T is non-scalar and $k = 1$, indeed if $kx_1 = x_2$ and $kx_2 = x_1$, then $x_2^{-1}x_1 = k = x_1^{-1}x_2$, namely $x_1 = \pm x_2$ (contradiction). Therefore $|\mathrm{Stab}\,\gamma| = (p-1)^2$, and for each G_k there is one orbit of length $p(p+1)(q-1)$.

The case $|\ker(\gamma)| = p$**.** If $\ker(\gamma) = \langle\, a_1 \,\rangle$ has order p, then $\gamma(G)$ is a subgroup of $\mathrm{GL}(2,p)$ of order pq, so $\gamma(G) = \langle\, \alpha, \beta \,\rangle$, where α has order p, $a_1^\alpha = a_1$, and β is an element of order q in the normaliser of α in $\mathrm{GL}(2,p)$. By Subsection 4.1.4, we can choose $a_2 \in A$ such that together with a_1 generates A, and with respect to the basis $\{a_1, a_2\}$ we can write

$$[\alpha] = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ [\beta] = \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{x_2} \end{pmatrix},$$

where $\lambda \in \mathcal{C}_p^*$ has order q, and $(x_1, x_2) \neq (0,0)$.

Let γ be a GF such that $\gamma(G) = \langle\, \alpha, \beta \,\rangle$. Then $\gamma(a_1) = 1$ and $\gamma(a_2) = \alpha^d$, where $1 \leq d \leq p-1$. Morever, let $b \in B$ be such that $\gamma(b) = \beta$.

By applying γ to (4.3), we get

$$\gamma(b)^{-1}\gamma(a)\gamma(b) = \gamma(a^{\gamma(b)})$$

which for $a = a_2$, in terms of our notation, can be rewritten as

$$\beta^{-1}\alpha^d\beta = \alpha^{d\lambda^{x_2}},$$

namely

$$\alpha^{d\lambda^{x_1} - x_2} = \alpha^{d\lambda^{x_2}},$$

which corresponds to the condition

$$x_1 \equiv 2x_2 \bmod q. \tag{4.4}$$

The latter restricts the choices of β to a set of $(q-1)p$ maps, namely the elements of order q in the normaliser of α with diagonal $\lambda^{2x_2}, \lambda^{x_2}$. Thus for each choice of $\langle\, \alpha \,\rangle$ only one group of order pq can be the image of a GF.

Note that the maps β satisfying (4.4) normalise but do not centralise $\langle\, \alpha \,\rangle$, so that $\langle\, \alpha, \beta \,\rangle$ is non-abelian.

The condition (4.4) is also sufficient to have that the map γ, defined as

$$\gamma(a_1^e a_2^f b^g) = \beta^g \alpha^f,$$

is a gamma function, indeed we have

$$\begin{aligned}
\gamma((a_1^e a_2^f b^g)^{\gamma(a_1^u a_2^v b^z)} a_1^u a_2^v b^z) &= \gamma((a_1^e a_2^f b^g)^{\beta^z \alpha^v} a_1^u a_2^v b^z) \\
&= \gamma((a_1^* a_2^{f\lambda^{x_2 z}} b^g) a_1^u a_2^v b^z) \\
&= \gamma(a_1^* a_2^{f\lambda^{x_2 z} + v} b^{g+z}) \\
&= \beta^{g+z} \alpha^{f\lambda^{x_2 z} + v}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}\gamma(a_1^e a_2^f b^g)\gamma(a_1^u a_2^v b^z) &= \beta^g \alpha^f \beta^z \alpha^v \\ &= \beta^{g+z} \alpha^{f\lambda^{(x_1-x_2)z}+v},\end{aligned}$$

so that γ defined as above satisfies the GFE precisely when $x_1 \equiv 2x_2 \bmod q$.

Now, since we have $p+1$ choices for $\langle\, \alpha \,\rangle$, $p-1$ for d, and $p(q-1)$ for β, we obtain $p(p^2-1)(q-1)$ groups $(G, \circ)$.

As for the type of $(G, \circ)$, with respect to the basis $\{a_1, a_2\}$ we have

$$T = [\beta] = \begin{pmatrix} \lambda^{2x_2} & 0 \\ 0 & \lambda^{x_2} \end{pmatrix};$$

Since $a_1^k = a_1^{\circ k}$ and $a_2^k = a_2^{\circ k}$ modulo $\langle\, a_1 \,\rangle$, denoting by $Z_\circ$ the action of b on A in $(G, \circ)$, we have $Z_\circ \sim T$. Therefore,

- if $q > 3$ all groups $(G, \circ)$ are of type 8, and they are all isomorphic to G_2;
- if $q = 3$ all groups $(G, \circ)$ are of type 9;
- if $q = 2$ we have $x_1 = 0$, $x_2 = 1$, so all groups $(G, \circ)$ are of type 6.

As to the conjugacy classes, let $\varphi \in \mathrm{Aut}(G)$, and write $\varphi = \mu\delta$ as above. If φ is in the stabiliser of γ then φ, and hence δ, stabilises $\langle\, a_1 \,\rangle$, so $\delta_{12} = 0$. Moreover,

$$\gamma^\varphi(a_2) = \varphi^{-1}\gamma(a_2^{\delta^{-1}})\varphi = \varphi^{-1}\gamma(a_2^{\delta_{22}^{-1}})\varphi = \delta^{-1}\alpha^{\delta_{22}^{-1}}\delta,$$

and $\gamma^\varphi(a_2) = \gamma(a_2)$ if and only if $\delta_{11} = \delta_{22}^2$. Now,

$$\gamma^\varphi(b) = \varphi^{-1}\gamma(b^{\mu^{-1}})\varphi = \varphi^{-1}\gamma(b^k)\varphi = \delta^{-1}T^k\delta,$$

so that, if φ stabilises γ, then T and T^k are conjugate, and they have the same eigenvalues. This implies that either $k = 1$ or $k = 2$ and $q = 3$. If $k = 1$, then every diagonal matrix δ commutes with T. If $q = 3$ and $k = 2$, then the condition $\delta^{-1}T^{-1}\delta = T$ yields $\lambda^{x_2} = \lambda^{-x_2}$, and since $x_2 \neq 0$ this case does not arise. Therefore the stabiliser has order $p-1$, and there is one orbit of length $p(p^2-1)(q-1)$.

4.2.4 The case $q \mid p+1$

We have to exclude the cases already considered, so we restrict to $q > 2$ (otherwise q also divides $p-1$) and $(G, \circ)$ non-abelian. Therefore $(G, \circ)$ can only have type 10.

As in the previous case $p \mid |\ker(\gamma)|$, and the only possibility is $|\ker(\gamma)| = p^2$ since a group of type 10 has no normal subgroups of order p or pq.

Lemma 1.12 guarantees that in this case all the GF's are morphisms, so to count them we can just count the possibilities for the image of b.

An element $\vartheta \in \mathrm{GL}(2,p)$ of order q has determinant equal to 1, as $q \nmid p-1$, and its eigenvalues λ, λ^{-1}, belongs to a quadratic extension of $\mathcal{C}_p$. Therefore, every subgroup of $\mathrm{GL}(2,p)$ of order q is conjugate to $\langle\, \vartheta \,\rangle$, and in $\mathrm{GL}(2,p)$ there are

$$\frac{|\mathrm{GL}(2,p)|}{|\mathrm{Stab}(\langle\, \vartheta \,\rangle)|}$$

subgroups of order q. Now, if ϑ and ϑ^k are conjugate, they have the same eigenvalues, and this yields $k = \pm 1$. For each of these two choices we obtain p^2-1 elements in the stabiliser, therefore there are

$$\frac{(p^2-1)(p^2-p)}{2(p^2-1)} = \binom{p}{2}$$

subgroups of order q in $\mathrm{GL}(2,p)$. So we can choose the image of b in such a subgroup in $q-1$ ways, and we get

1. $\binom{p}{2}(q-1)$ groups of type 10.

As to the conjugacy classes, $A = \ker(\gamma)$ is characteristic, therefore every automorphism φ of G stabilises $\gamma_{|A}$.

Let $b \in B$ such that $\gamma(b) = \vartheta$, and let $\varphi = \mu\delta \in \mathrm{Aut}(G)$. Then

$$\gamma^{\varphi}(b) = \delta^{-1}\gamma(b^k)\delta,$$

so that φ stabilises γ if and only if ϑ and ϑ^k are conjugate via δ. As above, in this case $k = \pm 1$, and for each of these values of k there are p^2-1 possibilities for δ. Therefore, we get one orbit of length $\frac{1}{2}(q-1)p(p-1)$.

We summarise, including the right regular representation.

Proposition 4.1. *Let G be a group of order p^2q, $p > 2$, of type 5. Then in* $\mathrm{Hol}(G)$ *there are:*

1. *p^2 groups of type 5, which split in one conjugacy class of length one, and one conjugacy class of length p^2-1;*
2. *if $p|(q-1)$,*
   (a) *$p^2(p^2-1)$ groups of type 11, which split in one conjugacy class of length p^2-1, one conjugacy class of length $(p-1)(p^2-1)$, and two conjugacy classes of length $\frac{1}{2}p(p-1)(p^2-1)$;*
3. *if $q|(p-1)$,*
   (a) *$p(p+1)(q-1)$ groups of type 6, which form one conjugacy class of length $p(p+1)(q-1)$;*

(b) $q-1$ *groups of type 7, which form one conjugacy class of length* $q-1$*;*

(c) *if* $q=2$*, further* $p(p^2-1)$ *groups of type 6, which form one conjugacy class of length* $p(p^2-1)$*;*

(d) *if* $q>2$*,* $\frac{1}{2}p(p+1)(q-1)$ *groups of type 9, which form one conjugacy class of length* $\frac{1}{2}p(p+1)(q-1)$*;*

(e) *if* $q=3$*, further* $p(p^2-1)(q-1)$ *groups of type 9, which form one conjugacy class of length* $p(p^2-1)(q-1)$*;*

(f) *if* $q>3$*,*

- $p^2(p+1)(q-1)$ *groups of type 8 isomorphic to* G_2*, which split in one conjugacy class of length* $p(p+1)(q-1)$ *and one conjugacy class of length* $p(p^2-1)(q-1)$*;*
- *for every* $s\neq 2$*,* $s\in\mathcal{K}$*,* $p(p+1)(q-1)$ *groups of type 8 isomorphic to* G_s*, which form one conjugacy class of length* $p(p+1)(q-1)$*;*

4. *if* $q|(p+1)$ *and* $q>2$*,*

(a) $\frac{p(p-1)}{2}(q-1)$ *groups of type 10, which form one conjugacy class of length* $\frac{p(p-1)}{2}(q-1)$*.*

4.3 G of type 6

In this case $q \mid p-1$, and $G=\mathcal{C}_p\times(\mathcal{C}_p\rtimes\mathcal{C}_q)$. The Sylow p-subgroup A is characteristic in G. Write $C=\langle\, c\,\rangle$ for the normal subgroup of order p in $\mathcal{C}_p\rtimes\mathcal{C}_q$, and $Z=\langle\, z\,\rangle$ for the central factor of order p, so that $A=CZ=\langle\, c,z\,\rangle$.

We have

$$\mathrm{Aut}(G)=\mathcal{C}_{p-1}\times\mathrm{Hol}(\mathcal{C}_p).$$

Write $\langle\,\psi\,\rangle=\mathcal{C}_{p-1}$ for the central factor in $\mathrm{Aut}(G)$, and let $\mathrm{Hol}(\mathcal{C}_p)=\iota(C)\rtimes\langle\,\mu\,\rangle$, where, according to [CCDC21],

$$\psi:\begin{cases} z\mapsto z^k\\ c\mapsto c\\ b\mapsto b\end{cases},\quad \mu:\begin{cases} z\mapsto z\\ c\mapsto c^h\\ b\mapsto b\end{cases}, \tag{4.5}$$

with $1\leq k,h\leq p-1$.

By Subsection 2.2.1, we can assume that $C\leq\ker(\gamma)$. In the following, it is useful to keep in mind that

$$\begin{cases} b^{\ominus 1}\circ c\circ b=c^{\gamma(b)\iota(b)}\\ b^{\ominus 1}\circ z\circ b=(b^{-\gamma(b)^{-1}\gamma(z)\gamma(b)}b)z^{\gamma(b)}.\end{cases}$$

4.3.1 The case $A \leq \ker(\gamma)$

Suppose $\ker(\gamma) = A$, as the case $\ker(\gamma) = G$ yields the right regular representation. So $\gamma(G)$ has order q.

By Remark 2.5 there is at least one $\gamma(G)$-invariant Sylow q-subgroup B of G. Therefore, by Subsection 2.2.2, the GF's on G are induced by the RGF's on B, and each γ is obtained s times, where s is the number of $\gamma(G)$-invariant Sylow q-subgroups of G.

Note moreover that $[B, \gamma(B)] = 1$, as B and $\gamma(B)$ have order q, so that by Lemma 1.12 the RGF's on B are precisely the morphisms $B \to \mathrm{Aut}(G)$.

Let β be the element of order q in the central factor $\mathcal{C}_{p-1}$ of $\mathrm{Aut}(G)$, such that $z^\beta = z^\lambda$, where λ is the eigenvalue of C under the action of $\iota(b)$, namely $c^b = c^\lambda$.

Here $c^{\circ k} = c^k$ and $z^{\circ k} = z^k$. Let $Z_\circ$ be the action of b on A in $(G, \circ)$. We will write $Z_\circ$ with respect to the basis $\langle\, c, z \,\rangle$ of $(A, \circ)$.

1. If $\gamma(b) = \beta^i$, for some $0 < i < q$, then $Z_\circ = \mathrm{diag}(\lambda, \lambda^i)$. Here the choice of B is immaterial, and we get
   (a) 1 group of type 7 when $i = 1$;
   (b) 1 group of type 9 when $i = q - 1$ and $q > 2$;
   (c) $q-3$ groups of type 8, when $q > 3$. They split in 2 groups isomorphic to G_s for every $s \in \mathcal{K}$.
2. If $\gamma(b) = \iota(b)^j$, for some $0 < j < q$, then $Z_\circ = \mathrm{diag}(\lambda^{j+1}, 1)$ and we get
   (a) p groups of type 5 when $j = -1$, for the possible choices of B;
   (b) $p(q-2)$ groups of type 6, for the possible choices of B.
3. If $\gamma(b) = \beta^i \iota(b)^j$, for some $0 < i, j < q$, then $Z_\circ = \mathrm{diag}(\lambda^{1+j}, \lambda^i)$ and we get
   (a) $p(q-1)$ groups of type 6, when $j = -1$;
   (b) $p(q-2)$ of type 7, when $i = j + 1 \neq 0$;
   (c) $p(q-2)$ of type 9, when $-i = j + 1 \neq 0$ and $q > 2$;
   (d) $p((q-1)^2 - 3q + 5) = p(q-2)(q-3)$ groups of type 8 in the remaining cases; they occur only for $q > 3$. They split in $2p(q-2)$ groups isomorphic to G_s, for every $s \in \mathcal{K}$.

As to the conjugacy classes, since $A = \ker(\gamma)$ is characteristic, to find the automorphisms which stabilise γ, we can look at the action of $\mathrm{Aut}(G)$ on $\gamma_{|B}$.

The central factor $\langle\, \psi \,\rangle$ of $\mathrm{Aut}(G)$ and $\langle\, \mu \,\rangle$ are in the stabiliser of γ, as they centralise b and $\gamma(b)$. As for $\iota(C)$ we have

$$\gamma^{\iota(c^m)}(b) = \iota(c^{-m})\gamma(b)\iota(c^m) = \beta^i \iota(b^j c^{m(1-\lambda^j)}),$$

so that it stabilises γ if and only if $m = 0$ or $j = 0$.

Therefore, if γ is a GF defined by $\gamma(b) = \beta^i \iota(b)^j$, $j \neq 0$, the stabiliser has order $(p-1)^2$, and the orbits have length p. Otherwise $\gamma(b) = \beta^i$ and every automorphism stabilises γ, so that the orbits have length 1. More precisely we obtain

1. p groups of type 5 which form one class of length p;
2. $p(q-2) + p(q-1) = p(2q-3)$ groups of type 6 which split in $2q-3$ classes of length p;
3. $p(q-2)+1$ groups of type 7, which split in $q-2$ classes of length p and one class of length one (the last one is for $j = 0$).
4. if $q > 3$, $2p(q-2)+2$ groups for each isomorphism class G_s of groups of type 8, which split in $2(q-2)$ classes of length p, and 1 classes of length one (these are for $j = 0$).
5. if $q > 2$, $p(q-2)+1$ groups of type 9, which split in $q-2$ classes of length p, and one class of length one (this is for $j = 0$).

4.3.2 The case $C \leq \ker(\gamma) \neq A$

Suppose now $C \leq \ker(\gamma) \neq A$, so that we will have $\gamma(z) = \iota(c)^s$, for some $s \neq 0$. If $\gamma(b)$ is a (possibly trivial) q-element in $\gamma(G)$, then b is a q-element in G, and we will have

$$\gamma(b) \in \langle\, \beta, \iota(bc^m) \,\rangle$$

for some m.

If $\gamma(b) = \beta^t$, for some t, then $\gamma(G)$ is abelian, so that $(G, \circ)$ is of type 5 or 6. However,

$$b^{\ominus 1} \circ c \circ b = c^{\gamma(b)\iota(b)} = c^{\lambda} = c^{\circ\lambda} \neq c,$$

so that $(G, \circ)$ is not abelian, and thus of type 6.

We also have

$$b^{\ominus 1} \circ z \circ b = b^{-\gamma(b)^{-1}\gamma(z)\gamma(b)} z^{\gamma(b)} b \equiv_{\mathrm{mod}\, C} z^{\lambda^t} = z^{\circ\lambda^t},$$

so that $t = 0$, as $(G, \circ)$ has to be of type 6. Therefore the kernel has order pq, $\gamma(G) = \gamma(Z)$ and $[Z, \gamma(Z)] = 1$, so that by Proposition 1.13 and Lemma 1.12 the GF's on G are precisely the morphisms $Z \to \mathrm{Aut}(G)$, which are as many as the choices for s, namely $p-1$.

If $\gamma(b) = \beta^t \iota(bc^m)^l$ for some $l \neq 0$ and t, replacing b with bc^m we see that we can take $m = 0$.

We have

$$b^{\ominus 1} \circ c \circ b = c^{\gamma(b)\iota(b)} = c^{\lambda^{l+1}} = c^{\circ\lambda^{l+1}}.$$

Then

$$b^{\ominus 1} \circ z \circ b = b^{-\gamma(b)^{-1}\gamma(z)\gamma(b)} z^{\gamma(b)} b \equiv_{\mathrm{mod}\ C} z^{\lambda^t} = z^{\circ \lambda^t}.$$

However

$$\gamma(b^{\ominus 1} \circ z \circ b) = \gamma(b)^{-1}\gamma(z)\gamma(b) = \iota(c)^{s\lambda^l} = \gamma(z)^{\lambda^l}.$$

It follows that $t = l$.

The latter is also a sufficient condition in order to have that the map γ defined by

$$\gamma(b^m c^k z^n) = \beta^{mt} \iota(b^{ml} c^{ns})$$

satisfies the GFE. Indeed

$$\begin{aligned} \gamma(b^m c^k z^n)\gamma(b^u c^v z^w) &= \beta^{mt}\iota(b^{ml}c^{ns})\beta^{ut}\iota(b^{ul}c^{ws}) \\ &= \beta^{(m+u)t}\iota(b^{(m+u)l}c^{(n\lambda^{ul}+w)s}), \end{aligned}$$

$$\begin{aligned} \gamma((b^m c^k z^n)^{\gamma(b^u c^v z^w)} b^u c^v z^w) &= \gamma((b^m c^k z^n)^{\beta^{ut}\iota(b^{ul}c^{ws})} b^u c^v z^w) \\ &= \gamma((b^m c^* z^{n\lambda^{ut}}) b^u c^v z^w) \\ &= \gamma((b^{m+u} c^* z^{n\lambda^{ut}+w}) \\ &= \beta^{(m+u)t}\iota(b^{(m+u)l}c^{(n\lambda^{ut}+w)s}), \end{aligned}$$

and they are equal if and only if $l = t$.

As for $(G, \circ)$ we have that $Z_\circ \sim \mathrm{diag}(\lambda^{t+1}, \lambda^t)$.

1. For $t = -1$ we get groups of type 6, with p choices for B and $p-1$ choices for s.

2. For $q > 2$ and $t = (q-1)/2$ we have $\lambda^{t+1}\lambda^t = \lambda^{2t+1} = 1$, so $p(p-1)$ groups of type 9.

3. For $q > 3$ for each of the remaining $q-3$ values of t, we get $p(p-1)$ groups of type 8, so $(q-3)p(p-1)$ in total. They split in $2p(p-1)$ groups isomorphic to G_s, for every $s \in \mathcal{K}$.

As to the conjugacy classes, write $\varphi = \psi\iota(c^m)\mu$ for an automorphism of G, with ψ and μ as in (4.5). Here $C = \ker(\gamma)$ is characteristic, so that by Lemma 2.6, we can look at the action of φ on γ defined on the generators z, b.

Write $\mu^{-1}\iota(c^m)\mu = \iota(c^m)^r$ for the commutation rule in $\mathrm{Hol}(\mathcal{C}_p)$, where $1 \le r \le p-1$. Then

$$\gamma^\varphi(z) = \varphi^{-1}\gamma(z^{\psi^{-1}})\varphi = \mu^{-1}\iota(c^{sk^{-1}})\mu = \iota(c^{sk^{-1}})^r,$$

so that $\gamma^\varphi(z) = \gamma(z)$ if and only if $k = r$. Moreover

$$\begin{aligned}\gamma^\varphi(b) &= \varphi^{-1}\gamma(c^{m(1-\lambda^{-1})}b)\varphi \\ &= \mu^{-1}\iota(c^{-m})\gamma(b)\iota(c^m)\mu \\ &= \beta^t\mu^{-1}\iota(c^{-m})\iota(b^t)\iota(c^m)\mu \\ &= \beta^t\mu^{-1}\iota(b^t c^{m(1-\lambda^t)})\mu \\ &= \beta^t\iota(b^t)\iota(c^{m(1-\lambda^t)})^r,\end{aligned}$$

so that $\gamma^\varphi(b) = \gamma(b)$ if and only if $t = 0$ or $m = 0$.

Therefore, if $t = 0$, namely when $\ker(\gamma)$ has size pq, the stabiliser has order $p(p-1)$, and there is one orbit of length $p-1$. Otherwise, if $t \neq 0$, namely $\ker(\gamma)$ has size p, then the stabiliser has order $p-1$, and there are $q-1$ orbits of length $p(p-1)$.

We summarise, including the right and left regular representations.

Proposition 4.2. *Let G be a group of order p^2q, $p > 2$, of type 6. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $2p$ *groups of type 5, which split in two conjugacy classes of length p;*
2. $2p(p+2q-3)$ *groups of type 6, which split in two conjugacy classes of length* 1, $2(2q-3)$ *conjugacy classes of length p, two conjugacy classes of length $p-1$, and two conjugacy classes of length $p(p-1)$;*
3. $2(p(q-2)+1)$ *groups of type 7, which split in two conjugacy classes of length* 1, *and* $2(q-2)$ *conjugacy classes of length p;*
4. *if $q > 3$, for every $s \in \mathcal{K}$ there are $4(1+p(p+q-3))$ groups of type 8 isomorphic to G_s which split in* 4 *conjugacy classes of length* 1, $4(q-2)$ *conjugacy classes of length p, and* 4 *conjugacy classes of length $p(p-1)$;*
5. *if $q > 2$, $2(1+p(p+q-3))$ groups of type 9, which split in two conjugacy classes of length* 1, $2(q-2)$ *conjugacy classes of length p, and two conjugacy classes of length $p(p-1)$.*

4.4 G of type 7, 8 and 9

In this section we deal with the types 8, 9 and a part of the type 7. Indeed, the study of these cases presents many similarities, so we handle them all together. We will conclude the study of the type 7 in the next section, since, as better explained below, part of this case requires a separate treatment.

Here $q \mid p-1$, and the Sylow p-subgroup A of G is characteristic.

If G is of type 7, then G is isomorphic to a group $(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_S \mathcal{C}_q$, for which a Sylow q-subgroup B acts by scalars on $A = \mathcal{C}_p \times \mathcal{C}_p$.

If G is of type 8 or 9, then G is isomorphic to a group $(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_{D_i} \mathcal{C}_q$, where for $q > 3$, $i = 0$ yields the type 8, and for $q > 2$, $i = 1$ yields the type 9. If $a_1, a_2 \in A$ are in the eigenspaces of the action of a generator b of a Sylow q-subgroup B on A, then this action can be represented by a non-scalar diagonal matrix Z, with no eigenvalues 1. The group G is of type 9 if moreover $\det(Z) = 1$, and of type 8 otherwise.

For all the section, we consider $A = \langle\, a_1, a_2 \,\rangle$, where a_1, a_2 are eigenvectors for $\iota(b)$. With respect to that basis, we have

$$Z = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^k \end{pmatrix},$$

where $\lambda \neq 1$ has order q, and k accounts for the type of G, namely if $k = 1$ the type is 7, if $k = -1$ the type is 9, and if $k \neq 0, 1, -1$ the type is 8.

Recall that the type 8 includes $\frac{q-3}{2}$ different isomorphism classes of groups (see [CCDC21] for details).

The divisibility condition on p and q implies that $(G, \circ)$ can be of type 5, 6, 7, 8 and 9.

According to Subsections 4.1, 4.2 and 4.3 of [CCDC21], we have

$$\mathrm{Aut}(G) = \begin{cases} \mathrm{Hol}(\mathcal{C}_p \times \mathcal{C}_p), & \text{if } G \text{ is of type 7,} \\ \mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_p), & \text{if } G \text{ is of type 8,} \\ (\mathrm{Hol}(\mathcal{C}_p) \times \mathrm{Hol}(\mathcal{C}_p)) \rtimes \mathcal{C}_2, & \text{if } G \text{ is of type 9.} \end{cases}$$

If G is of type 8 or 9, the Sylow p-subgroup of $\mathrm{Aut}(G)$ has order p^2 and is characteristic, so, since G has trivial center, all its elements are conjugation by elements of A.

If γ is a GF on G, then $\gamma_{|A} : A \to \mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ is a RGF, as A is characteristic in G. Moreover, Lemma 1.12 yields that $\gamma_{|A}$ is a morphism, as $\iota(A)$ acts trivially on the abelian group A. Therefore, for each gamma function γ there exists $\sigma \in \mathrm{End}(A)$ such that

$$\gamma(a) = \iota(a^{-\sigma}) \tag{4.6}$$

for each $a \in A$.

If G is of type 7, then $\gamma(A)$ is not necessarily contained in $\mathrm{Inn}(G)$, as here a Sylow p-subgroup of $\mathrm{Aut}(G)$ is of the form $\iota(A) \rtimes \mathcal{P}$, where $\mathcal{P}$ is a Sylow p-subgroup of $\mathrm{GL}(2, p)$.

Hereafter, for all the section, we will assume that $\gamma(A) \leq \mathrm{Inn}(G)$, so that we can write equation (4.6) for the type 7 too. The case $\gamma(A) \not\leq \mathrm{Inn}(G)$ (which only happens for the type 7) will be discussed in Section 4.5.

4.4.1 Outline

As usual, we use the tools of Subsection 2.2 to enumerate the GF's. This will be done, as usual distinguishing by the size of the kernel of γ, in Subsections 4.4.2, 4.4.3, 4.4.4, 4.4.5, and 4.4.6, but we need some preparation first.

In Subsubsection 4.4.1.1 we show that if G is of type 7 (and $q > 2$) or 8 then either $p \mid |\ker(\gamma)|$ or $p \mid |\ker(\tilde{\gamma})|$. On the contrary, for G of type 9 (and G of type 7 when $q = 2$) there will be gamma functions γ such that both $p \nmid |\ker(\gamma)|$ and $p \nmid |\ker(\tilde{\gamma})|$. Therefore, except for the case when both γ and $\tilde{\gamma}$ have kernel of size not divisble by p, we will use duality to swich to a more convenient kernel.

We will use Proposition 1.13 to deal with the kernels of size q, pq, and p^2. As for the kernels of size p and 1, we will appeal to Proposition 1.26. To do this, we will show that for G as above each γ on G with kernel of size p or 1 always admits at least one invariant Sylow q-subgroup B.

In order to do that, in Subsubsection 4.4.1.2 we describe the elements of $\mathrm{Aut}(G)$ of order q, and in Subsubsection 4.4.1.3 we give a characterization of the invariant Sylow q-subgroups of G.

Lastly, in Subsubsection 4.4.1.4 we give a short description of the automorphisms of G and fix some notation; this will be useful to calculate the conjugacy classes.

4.4.1.1 Duality

Here we show that for the types 8, and 7 when $q > 2$, either $p \mid |\ker(\gamma)|$ or $p \mid |\ker(\tilde{\gamma})|$, and this is not true for the type 9 and for the type 7 when $q = 2$.

For the groups G under consideration, we have that every γ on G satisfies equation (4.6). By the discussion in Subsection 2.2.1, if σ and $1 - \sigma$ are not both invertible, then $p \mid |\ker(\gamma)|$ or $p \mid |\ker(\tilde{\gamma})|$, namely σ has 0 or 1 as an eigenvalue.

Otherwise σ and $1 - \sigma$ are both invertible, and we have (2.2):

$$(\sigma^{-1} - 1)^{-1}\gamma(b)_{|A}(\sigma^{-1} - 1) = \gamma(b)_{|A}\iota(b)_{|A},$$

for $b \neq 1$ a q-element. Therefore $\gamma(b)_{|A}$ and $\gamma(b)_{|A}\iota(b)_{|A}$ are conjugate.

For type 7, if $q > 2$ (2.2) is plainly impossible, as

$$\iota(b)_{|A} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix},$$

for some $\lambda \neq 1$, λ of order q.

For type 8, the two normal subgroups of order p are characteristic, so $\gamma(b)_{|A}$ and $\iota(b)_{|A}$ commute, as they are simultaneously diagonal. Let

$$\iota(b)_{|A} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \qquad \gamma(b)_{|A} = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix},$$

with $\lambda_i \neq 1$. This implies $\alpha_1 = \lambda_2\alpha_2$ and $\alpha_2 = \lambda_1\alpha_1$, so that $\alpha_1 = \lambda_1\lambda_2\alpha_1$ and $\lambda_1\lambda_2 = 1$, against the assumption of type 8.

For type 9, however, this is well possible. This time there is an automorphism of order two exchanging the two eigenspaces, but since $\gamma(b)_{|A}$ has odd order q, it leaves them invariant, so that once more $\gamma(b)_{|A}$ and $\iota(b)_{|A}$ commute, as they are simultaneously diagonal.

In the same notation as for type 8, here we get $\lambda_1 = \lambda$, $\lambda_2 = \lambda^{-1}$, $\alpha_1 = \alpha$ and $\alpha_2 = \lambda\alpha$. We get

$$\sigma^{-1} - 1 = \begin{pmatrix} 0 & s_1 \\ s_2 & 0 \end{pmatrix}$$

(with $s_1 s_2 \neq 1$), or

$$\sigma = (1 - s_1 s_2)^{-1} \begin{pmatrix} 1 & -s_1 \\ -s_2 & 1 \end{pmatrix}.$$

For the type 7 when $q = 2$, in the same notation as above we get $\lambda_1 = \lambda_2 = \lambda$, and $\alpha_1 = \lambda^2 \alpha_1$, therefore also in this case (2.2) is possible.

Therefore for the type 9 and for the type 7 when $q = 2$ there are actually σ with no eigenvalues 0 and 1, and this corresponds to the existence of γ such that $p \nmid |\ker(\gamma)|, |\ker(\tilde{\gamma})|$.

4.4.1.2 Description of the elements of order q of $\mathrm{Aut}(G)$

Type 7. Suppose first G of type 7. An element of order q in $\mathrm{Aut}(G)$ is of the form $\iota(a_*)\beta$, where $a_* \in A$, and $\beta \in \mathrm{GL}(2,p)$ of order q.

As we now show, the Sylow q-subgroups of $\mathrm{Aut}(G)$ are as many as the Sylow q-subgroups of $\mathrm{GL}(2,p)$ (see Subsection 4.1.3) multiplied by p^2. In fact, the number of the Sylow q-subgroups is equal to the index of $\mathrm{Norm}_{\mathrm{Aut}(G)}(Q)$ in $\mathrm{Aut}(G)$, where Q is any Sylow q-subgroup of $\mathrm{Aut}(G)$. Since $\mathrm{Aut}(G) = A \rtimes \mathrm{GL}(2,p)$, necessarily a Sylow q-subgroup of $\mathrm{GL}(2,p)$ is a Sylow q-subgroup of $\mathrm{Aut}(G)$ as well, therefore we can suppose that Q is contained in $\mathrm{GL}(2,p)$.

We use the following lemma to show that the normaliser of Q in $\mathrm{Aut}(G)$ is equal to the normaliser of Q in $\mathrm{GL}(2,p)$, obtaining the claim above.

Lemma 4.3. *Let H be a permutation group containing a regular subgroup. Let $Q \leq H$ be such that Q is contained in a unique stabiliser T_a. Then $\mathrm{Norm}_H(Q) \leq T_a$.*

Proof. Let $R \leq H$ be a regular subgroup, and let $h \in H$. Then, given a and a^h, there exists $r \in R$ such that $a^{hr} = a$. Therefore $hr \in T_a$ and $h = hr \cdot r^{-1} \in T_a R$.

Now, let $h = sr \in \mathrm{Norm}_H(Q)$, with $s \in T_a$, and $r \in R$. Then $Q = Q^{sr} = Q^r \leq T_a^r = T_{a^r}$. It follows that $r = 1$. □

Now we identify $\mathrm{Aut}(G)$ with $H := \mathrm{Hol}(A) = \rho(A)\,\mathrm{Aut}(A)$, in particular $\iota(A)$ with $R := \rho(A)$ and H is acting on A. If the Sylow q-subgroup Q is such that $Q \subseteq \mathrm{Stab}(a)$ for a certain $a \in A$, then a is fixed by every matrix with eigenvalues of order a power of q, and this yields $a = 1$. Therefore Q is contained in a unique stabiliser, $T_1 \simeq \mathrm{GL}(2,p)$, and by the lemma above $\mathrm{Norm}_{\mathrm{Aut}(G)}(Q) \leq \mathrm{GL}(2,p)$, namely $\mathrm{Norm}_{\mathrm{Aut}(G)}(Q) = \mathrm{Norm}_{\mathrm{GL}(2,p)}(Q)$.

Types 8 and 9. Suppose now that G is of type 8 or type 9. Here the Sylow q-subgroups of $\mathrm{Aut}(G)$ are of the form $\mathcal{C}_{q^e} \times \mathcal{C}_{q^e}$, for $q^e || p-1$, and they can be described as the Sylow q-subgroups of $C_{\mathrm{Aut}(G)}(\langle\, \iota(b)\,\rangle)$, where $\langle\, b\,\rangle$ varies among the Sylow q-subgroups of G.

Since they are abelian, each of them contains exactly one subgroup of type $\iota(\langle\, b\,\rangle)$, and this establishes a one-to-one correspondence between the Sylow q-subgroups of G and the Sylow q-subgroups of $\mathrm{Aut}(G)$.

We note also that for $a \in A$ one has

$$C_{\mathrm{Aut}(G)}(\langle\, \iota(b)\,\rangle)^{\iota(a)} = C_{\mathrm{Aut}(G)}(\langle\, \iota(b^a)\,\rangle).$$

For $b \in G \setminus A$, recalling that $\iota(b)$ acts on A as $\mathrm{diag}(\lambda, \lambda^k)$, we write

$$\begin{array}{cc} \beta_1 : a_1 \mapsto a_1^{\lambda} & \beta_2 : a_1 \mapsto a_1 \\ a_2 \mapsto a_2 & a_2 \mapsto a_2^{\lambda^k} \\ b \mapsto b & b \mapsto b \end{array} \tag{4.7}$$

so that $\iota(b) = \beta_1\beta_2$, and $\langle\, \beta_1, \beta_2\,\rangle$ is the q-part of a Sylow q-subgroup of $C_{\mathrm{Aut}(G)}(\langle\, \iota(b)\,\rangle)$.

Now, if $\beta \in \mathrm{Aut}(G)$ is an element of order q, then it belongs to the centraliser of $\langle\, \iota(b)\,\rangle$, where $\langle\, b\,\rangle$ is a Sylow q-subgroup of G. Therefore, if β_1, β_2 are as above, then $\beta \in \langle\, \beta_1, \beta_2\,\rangle$, namely $\beta = \beta_1^{x_1}\beta_2^{x_2}$, where $0 \le x_1, x_2 < q$ not both zero.

4.4.1.3 Invariant Sylow q-subgroups of G

Here we give a characterization of the invariant Sylow q-subgroups of G, and we make some considerations on those cases in which the condition we find is not satisfied.

If $q \mid |\ker(\gamma)|$ then there is a Sylow q-subgroup B contained in $\ker(\gamma)$, so that B is invariant, and therefore, in this case, there always exists an invariant Sylow q-subgroup.

Suppose $q \nmid |\ker(\gamma)|$. Then $q \mid |\gamma(G)|$, and let $\iota(a_*)\beta$ be an element of order q in $\gamma(G)$, where $a_* \in A$ and, if G is of type 7 then $\beta \in \mathrm{GL}(2,p)$ has order q, and if G is of type 8 or 9 then $\beta = \beta_1^{x_1}\beta_2^{x_2}$, where β_1, β_2 are as in (4.7) with $0 \le x_1, x_2 < q$ not both zero. Moreover, let $b \in G$ such that $\gamma(b) = \iota(a_*)\beta$. The Sylow q-subgroup $\langle\, b^x\,\rangle$ is invariant if and only if $(b^x)^{\gamma(b^x)} \in \langle\, b^x\,\rangle$. Denoting by T the matrix of $\gamma(b)_{|A}$ with respect to the basis $\{a_1, a_2\}$, since

$$\gamma(b^x) = \gamma(x^{-1+Z^{-1}}b) = \iota(x^{(1-Z^{-1})T^{-1}\sigma}a_*)\beta,$$

we have

$$\begin{aligned} (b^x)^{\gamma(b^x)} &= (x^{-1+Z^{-1}}b)^{\iota(x^{(1-Z^{-1})T^{-1}\sigma}a_*)\beta} \\ &= (x^{-(1-Z^{-1})(1+T^{-1}\sigma(1-Z^{-1}))}a_*^{-(1-Z^{-1})}b)^{\beta} \\ &= x^{-(1-Z^{-1})(1+T^{-1}\sigma(1-Z^{-1}))T}a_*^{-(1-Z^{-1})T}b. \end{aligned}$$

Now, $\langle\, b^x \,\rangle = \left\{(b^x)^j = x^{-1+Z^{-j}}b^j : j = 0, \ldots, q-1\right\}$, so that the Sylow q-subgroup $\langle\, b^x \,\rangle$ is invariant if and only if

$$x^{-(1-Z^{-1})(1+T^{-1}\sigma(1-Z^{-1}))T}a_*^{-(1-Z^{-1})T}b = x^{-(1-Z^{-1})}b,$$

which, denoting by M the matrix $1-(1+T^{-1}\sigma(1-Z^{-1}))T$, is equivalent to

$$x^{(1-Z^{-1})M} = a_*^{(1-Z^{-1})T}. \tag{4.8}$$

If the system (4.8) admits at least a solution x, then the Sylow q-subgroup $B = \langle\, b^x \,\rangle$ is invariant, and, taking into account (4.6), we can build every GF on G as a gluing of a RGF on B and a RGF on A as in Proposition 1.26. This will be always the case for the kernels of size p^2, as we will show in Subsection 4.4.4.

On the contrary, as explained in Subsections 4.4.5 and 4.4.6, for the kernels of size p and 1, there are some elements a_* which make the system (4.8) unsolvable. We will show that for these a_*, there are no gamma functions extending the assignment $\gamma(b) = \iota(a_*)\beta$. In fact, if γ is such a GF, then the gamma functional equation yields $\gamma(b^m) = \gamma((b^{m-1})^{\gamma(b)^{-1}})\gamma(b)$, and proceeding by induction we obtain that

$$\gamma(b^m) = \iota(a_*^{-A_m\sigma+1+T^{-1}+\cdots+T^{-(m-1)}})\beta^m, \tag{4.9}$$

where

$$A_m = \sum_{i=1}^{m-1}(1-Z^{-i})T^{-i}.$$

Since $\gamma(b^q) = 1$ and G has trivial centre, (4.9) yields

$$a_*^{A_m\sigma} = a_*^{1+T^{-1}+\cdots+T^{-(m-1)}}. \tag{4.10}$$

We will show in Subsections 4.4.5 and 4.4.6 that the elements a_* which satisfy (4.10) are precisely the elements for which the system (4.8) admits solutions. Therefore, in these cases too, every GF on G can be built as a gluing of a RGF on B and a RGF on A.

4.4.1.4 Description of the automorphisms of G

We fix some notation, which will be useful to deal with the calculation of the conjugacy classes for all the types 7, 8 and 9 together.

Let $\varphi \in \mathrm{Aut}(G)$. According to [CCDC21], if G is of type 7, then φ has the form $\iota(x)\delta$, where $x \in A$, $\delta_{|B} = 1$ and, with respect to the fixed basis, $\delta_{|A} = (\delta_{ij}) \in \mathrm{GL}(2,p)$.

If G is of type 8, then $\varphi = \iota(x)\delta$, where, with respect to the basis $\{a_1, a_2\}$ given by the eigenspaces of $\iota(b)$, δ acts on A as a diagonal matrix with non-zero elements on its diagonal, so that $\delta_{|A} = \mathrm{diag}(\delta_{11}, \delta_{22})$, where $\delta_{ii} \neq 0$.

If G is of type 9, then $\varphi = \iota(x)\delta\psi$, where δ is as for the type 8, and ψ is defined as $b^\psi = b^r$ and $a^\psi = a^S$, where either $r = 1$ and $S = 1$, or $r = -1$ and

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In the following we will write $\varphi = \iota(x)\delta\psi$ for an automorphism of G, with the convention that δ is diagonal for the types 8 and 9, and $\psi = 1$ for the types 7 and 8.

Let us start with the enumeration of the GF's on G. We proceed case by case, according to the size of the kernel.

As usual, if $|\ker(\gamma)| = p^2q$, then γ corresponds to the right regular representation, so that we will assume $\gamma \neq 1$.

4.4.2 The case $|\ker(\gamma)| = q$

Let $B = \ker(\gamma)$. Here $(G, \circ)$ is necessarily of type 5, as it is the only type having a normal subgroup of order q.

By Proposition 1.13, since A is characteristic, each GF on G is the lifting of a RGF on A, and, conversely, a RGF on A lifts to G if and only if B is invariant under $\{\gamma(a)\iota(a) \mid a \in A\}$.

For each $a \in A$, $\gamma(a) = \iota(a^{-\sigma})$, where $\sigma \in \mathrm{GL}(2, p)$, so that $\gamma(a)\iota(a) = \iota(a^{1-\sigma})$. Taking into account that each Sylow q-subgroup of G is self-normalising, we obtain that γ lifts to G if and only if $\sigma = 1$, namely when

$$\gamma(a) = \iota(a^{-1}).$$

Since this map is a morphism and $[A, \gamma(A)] = \{1\}$, by Lemma 1.12 γ is actually a RGF. Therefore, for each of the p^2 choices for a Sylow q-subgroup, there is a unique RGF on A which lifts to G, and we obtain p^2 groups.

Note that for all the γ's in this case $p \mid |\ker(\tilde{\gamma})|$.

As to the conjugacy classes, if γ has kernel B, then, for $x \in A$, $\gamma^{\iota(x)}$ has kernel $B^{\iota(x)}$, as for $b \in \ker(\gamma)$,

$$\gamma^{\iota(x)}(b^{\iota(x)}) = \iota(x^{-1})\gamma(b)\iota(x) = 1.$$

Since $\iota(A)$ conjugates transitively the p^2 Sylow q-subgroups of G, the orbits contain at least p^2 elements. Since there are p^2 GF, there is a unique orbit of length p^2.

4.4.3 The case $|\ker(\gamma)| = pq$

Here $K = \ker(\gamma)$ is a subgroup of G isomorphic to $\mathcal{C}_p \rtimes \mathcal{C}_q$, therefore we will obtain $(G, \circ)$ of type 6, as it is the only type having a non abelian normal subgroup of order pq.

We can choose K in $2p$ ways if G is of type 8 or 9, and in $(p+1)p$ ways if G is of type 7, indeed for each of the p^2 choices for a Sylow q-subgroup B, the subgroups of order p that are B-invariant are the 1-dimensional invariant subspaces of the action of B. Therefore, there are 2 of such subgroups when G is of type 8 or 9, and $p+1$ when G is of type 7, since in this case the action is scalar, so that every subgroup of G of order p is invariant. Moreover, since $\mathcal{C}_p \rtimes \mathcal{C}_q$ has p subgroups of order q, exactly p choices for B give the same group.

Let $K = \langle\, a_1, b \,\rangle$, and let $a_2 \in A$ be such that $A = \langle\, a_1, a_2 \,\rangle$. The cyclic complement $\langle\, a_2 \,\rangle$ of K in G can be chosen in p ways, and since $\gamma(G) \leq \iota(A)$, each of these choices yields a $\gamma(G)$-invariant subgroup.

Therefore, by Proposition 1.13, each γ is the lifting of a RGF defined on any of the complements of order p. So, we fix $\langle\, a_2 \,\rangle$ and we consider the RGF's $\gamma' : \langle\, a_2 \,\rangle \to \mathrm{Aut}(G)$, taking into account that the choice of the complement is immaterial. Again appealing to Proposition 1.13, the RGF's γ' which can be lifted to G are those for which K is invariant under $\{\gamma'(x)\iota(x) : x \in \langle\, a_2 \,\rangle\}$, namely the maps defined as

$$\gamma'(a_2) = \iota(a_1^j a_2^{-1}),$$

for some j, $0 \leq j \leq p-1$. Moreover, since $[\langle\, a_2 \,\rangle, \gamma(\langle\, a_2 \,\rangle)] = \{1\}$, by Lemma 1.12 the RGF's correspond to the morphisms. Therefore, since there are p choices for j, and either $2p$ or $(p+1)p$ for K, the number of distinct gamma functions is

1. $2p^2$ if G is of type 8 or 9, and
2. $p^2(p+1)$ if G is of type 7.

Notice that, for every γ as above, $p \mid |\ker(\tilde{\gamma})|$.

As to the conjugacy classes, in the notation of Subsubsection 4.4.1.4 let $\varphi = \iota(x)\delta\psi$ an automorphism of G.

We have that $\gamma(a_1^{\varphi^{-1}}) = \gamma(a_1^{\psi\delta^{-1}})$, and $\gamma^\varphi(a_1) = 1$ if and only if $a_1^{\varphi^{-1}} \in \ker(\gamma) \cap A = \langle\, a_1 \,\rangle$. Therefore $\delta_{12} = 0$ if G is of type 7, and $\psi = 1$ if G is of type 9. Moreover,

$$\gamma^\varphi(b) = \varphi^{-1}\gamma(b^{\iota(x^{-1})})\varphi = \varphi^{-1}\gamma(x^{1-Z^{-1}})\varphi,$$

so it is equal to $\gamma(b) = 1$ when $x \in \langle\, a_1 \,\rangle$. Now, writing $a = a_1^j a_2^{-1}$, we have

$$\gamma^\varphi(a_2) = \varphi^{-1}\gamma(a_2^{\delta^{-1}})\varphi = \varphi^{-1}\gamma(a_2^{\delta_{22}^{-1}})\varphi = \iota(a^{\delta_{22}^{-1}})^\delta,$$

so that φ stabilises γ if and only if $\iota(a^{\delta_{22}^{-1}})^\delta = \iota(a)$, and this yields the condition $j(\delta_{11} - \delta_{22}) = \delta_{21}$.

If G is of type 7, the latter yields δ_{21} as a function of the diagonal elements, so that the stabiliser has order $p(p-1)^2$, and we obtain one orbit of length $p^2(p+1)$.

If G is of type 8 or 9, then δ is diagonal, so that, if $j = 0$ the last condition is always satisfied, and if $j \neq 0$ the δ's in the stabiliser are the scalar matrices. Therefore, if G is of type 9 we get one orbit of length $2p$ and one orbit of length $2p(p-1)$, and if G is of type 8 we get two orbits of length p and two orbits of length $p(p-1)$.

4.4.4 The case $|\ker(\gamma)| = p^2$

By Remark 2.5, the action of $\gamma(G)$ of order q on G fixes at least one of the p^2 Sylow q-subgroups of G, say $B = \langle\, b \,\rangle$. Therefore, by Proposition 1.13, each γ on G is the lifting of at least one RGF defined on a such Sylow q-subgroup B. Moreover, since $[B, \gamma(B)] = \{1\}$, by Lemma 1.12 the RGF's on B are precisely the morphisms.

Now, as B is $\gamma(G)$-invariant, $\gamma(b)_{|B} = 1$, and let $\gamma(b)_{|A} = \beta$.

If G is of type 7, then β is an element of order q in $\mathrm{GL}(2, p)$, and, with respect to a suitable basis of A, we have $[\beta] = \mathrm{diag}(\lambda^{x_1}, \lambda^{x_2})$, where $\lambda \neq 1$ has order q, and $0 \leq x_1, x_2 < q$ not both trivial (see Subsection 4.1.3). We assume that $[\beta]$ is diagonal with respect to $\{a_1, a_2\}$, taking into account that if $[\beta]$ is non-scalar, then there are $\frac{p(p+1)}{2}$ choices for a pair $\{A_1, A_2\}$ of distinct one-dimensional subspaces of A.

If G is of type 8 or 9, the discussion in Subsubsection 4.4.1.2 yields that $\beta = \beta_1^{x_1}\beta_2^{x_2}$, where x_1, x_2 not both zero, so that, with respect to the basis $\{a_1, a_2\}$, $[\beta] = \mathrm{diag}(\lambda^{x_1}, \lambda^{kx_2})$.

Therefore, for all the types of group here, we can represent β as the matrix

$$T = \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{kx_2} \end{pmatrix},$$

where λ, x_1, x_2 are as above, and k accounts for the type of G.

To count each GF exactly once, we need to know the number of the invariant Sylow q-subgroups. Equation (4.8) yields

$$x^{(1-Z^{-1})M} = 1,$$

where

$$M = 1 - T = \begin{pmatrix} 1 - \lambda^{x_1} & 0 \\ 0 & 1 - \lambda^{kx_2} \end{pmatrix}.$$

Since $\det(1 - Z^{-1}) \neq 0$, we obtain that

1. there is a unique solution, namely a unique invariant Sylow q-subgroup, when both $x_1, x_2 \neq 0$;

2. there are p solutions, that is, p invariant Sylow q-subgroups, when either $x_1 = 0$ or $x_2 = 0$.

The action of b on A with respect to the operation $\circ$ is given by

$$b^{\ominus 1} \circ a \circ b = b^{-\gamma(b)^{-1}\gamma(a)\gamma(b)} a^{\gamma(b)} b = a^{\gamma(b)\iota(b)},$$

thus denoting by $Z_\circ$ its associated matrix, since $a^{\circ j} = a^j$, with respect to the basis $\{a_1, a_2\}$ of $(A, \circ)$ we have

$$Z_\circ \sim \begin{pmatrix} \lambda^{x_1+1} & 0 \\ 0 & \lambda^{kx_2+k} \end{pmatrix}.$$

We obtain the followings groups $(G, \circ)$.

Type 5 if $x_1 = x_2 = -1$, therefore p^2 groups.

Type 6 if either $x_1 = -1$ and $x_2 \neq -1$, or $x_1 \neq -1$ and $x_2 = -1$. In both cases there is a unique invariant Sylow q-subgroup, except if either $x_2 = 0$ or $x_1 = 0$, when there are p invariant Sylow q-subgroups. Therefore, if G is of type 8 or 9 there are $2p^2(q-2)$ groups when the invariant Sylow q-subgroup is unique, plus other $2p$ groups when there are p invariant Sylow q-subgroups. If G is of type 7 there are $p^3(p+1)(q-2)+p^2(p+1)$ groups.

Type 7 if $x_1+1 = k(x_2+1) \neq 0$. If G is of type 7, the condition is equivalent to have $x_1 = x_2 \neq -1$, therefore we are in case (1) and we obtain $p^2(q-2)$ groups. Otherwise, G is of type 8 or 9, and there are $p^2(q-3)$ groups for the case (1), plus $2p$ groups for the case (2).

Type 8 if $Z_\circ$ is a non scalar matrix with no eigenvalues 1, and determinant different from 1.

In case (1) this corresponds to the conditions $x_2 \neq 0, -1$ and the four conditions $x_1 \neq 0, -1, -kx_2 - k - 1, kx_2 + k - 1$, which are independent if and only if in addition $x_2 \neq k^{-1} - 1, -k^{-1} - 1$. When these four conditions are dependent, they reduce to three independent condition on x_1.

If G is of type 7 or 9, then $k = \pm 1$. For $x_2 \neq 0, -1, -2$ we have 4 independent conditions on x_1, and therefore we obtain $\frac{1}{2}p^3(p+1)(q-4)(q-3)$, respectively $p^2(q-4)(q-3)$, groups. For $x_2 = -2$ the conditions are three, and we obtain further $\frac{1}{2}p^3(p+1)(q-3)$, respectively $p^2(q-3)$, groups.

If G is of type 8, we obtain $p^2(q-4)^2$ groups if $x_2 \neq -k^{-1} - 1$, $k^{-1} - 1$, plus further $p^2(q-3)$ groups if $x_2 = -k^{-1} - 1, k^{-1} - 1$.

In case (2), suppose $x_1 = 0$. Then, there are three independent conditions on x_2 when G is of type 7 or 9, and four when G is of type 8. Doubling for the case $x_2 = 0$, we obtain $p^2(p+1)(q-3)$, $2p(q-3)$, and $2p(q-4)$ groups respectively for G of type 7, 9 and 8.

Summing up, we have just obtained

- if G is of type 7, $\frac{1}{2}p^3(p+1)(q-3)^2 + p^2(p+1)(q-3)$ groups of type 8; looking at the eigenvalues of $Z_\circ$, we easily obtain that they are $2p^2(p+1) + p^3(p+1)(q-3)$ groups isomorphic to G_s, for every $s \in \mathcal{K}$;
- if G is of type 9, $p^2(q-3)^2 + 2p(q-3)$ groups of type 8, which split in $2p^2(q-3) + 4p$ groups isomorphic to G_s, for every $s \in \mathcal{K}$;
- if G is of type 8, $G \simeq G_k$, there are $p^2((q-4)^2 + 2(q-3)) + 2p(q-4)$ groups of type 8. Looking at the eigenvalues of $Z_\circ$ as x_1 and x_2 vary, and taking into account the conditions on x_1 and x_2, one can see that the $2p^2(q-3)$ groups split in $4p^2$ groups isomorphic to G_s for every $s \in \mathcal{K}$, and the $p^2(q-4)^2 + 2p(q-4)$ groups split in $2p^2(q-5) + 4p$ groups isomorphic to G_s for every $s \neq k$, and $2p^2(q-5) + p^2 + 2p$ groups isomorphic to G_k. Therefore in total they split in
  - $2p^2(q-3) + 4p$ groups isomorphic to G_s for every $s \neq k$;
  - $p^2(2q-5) + 2p$ groups isomorphic to G_k.

Type 9 if $Z_\circ$ is a non-scalar matrix with no eigenvalue 1 and determinant 1, namely $x_1 \neq -1, kx_2 + k - 1$, $x_2 \neq -1$, and $x_1 + 1 + kx_2 + k = 0$.

In case (1) $x_2 \neq 0, -1$ and also $x_2 \neq -k^{-1} - 1$, otherwise we would have $x_1 = 0$; note that this is a new condition only when G is of type 7 or 8, since if $k = -1$ then $-k^{-1} - 1 = 0$. Therefore there are $p^2(q-2)$ groups if G is of type 9, $\frac{1}{2}p^3(p+1)(q-3)$ if G is of type 7, and $p^2(q-3)$ if G is of type 8.

The case (2) occurs only for G of type 7 or 8, and yields respectively $p^2(p+1)$ and $2p$ groups.

Summing up, there are $p^2(q-2)$ groups if G is of type 9, $p^2(p+1) + \frac{1}{2}p^3(p+1)(q-3)$ groups if G is of type 7 and $2p + p^2(q-3)$ groups if G is of type 8.

As to the conjugacy classes, since the kernel A is characteristic, we have that $\gamma^\varphi(a) = \gamma(a)$, for every $\varphi \in \mathrm{Aut}(G)$.

In the notation of Subsubsection 4.4.1.4, write $\varphi = \iota(x)\delta\psi$. Since $b^{\varphi^{-1}} = b^{\psi\iota(x^{-1})} \equiv b^r \bmod \ker(\gamma)$, we have

$$\gamma^\varphi(b) = \varphi^{-1}\gamma(b^r)\varphi = \psi\delta^{-1}T^r\iota(x^{1-T^r})\delta\psi = \psi\delta^{-1}T^r\delta\iota(x^{(1-T^r)\delta})\psi.$$

Therefore, φ stabilises γ if and only if

$$\begin{cases} x^{(1-T^r)\delta} = 1 \\ \delta^{-1}T^r\delta = \psi T\psi. \end{cases}$$

The first condition yields $x = 1$ or, if $x = a_1^u a_2^v$, either $x_1 = 0$ and $v = 0$, or $x_2 = 0$ and $u = 0$. If $\psi = 1$, from the second condition we obtain that δ is

any matrix when T is scalar, and δ is diagonal when T is non-scalar. If $\psi \neq 1$, then G is of type 9, so that δ is diagonal. Since $\delta^{-1}T^{-1}\delta = T^{-1}$, and ψ acts on T by conjugation exchanging the eigenvalues, the second condition yields $x_1 = x_2$.

We obtain the following.

1. For $(G, \circ)$ of type 5 , $x_1 = x_2 = -1$, so that the stabiliser has order $|\mathrm{GL}(2, p)|$ if G is of type 7, $(p-1)^2$ if G is of type 8, and $2(p-1)^2$ if G is of type 9. In all the cases there is one orbit of length p^2.

2. For $(G, \circ)$ of type 6, $x_1 \neq x_2$. For all the types of G, the stabiliser has order $p(p-1)^2$ when either $x_1 = 0$ or $x_2 = 0$, and $(p-1)^2$ when $x_1 \neq 0 \neq x_2$. Therefore,

   - if G is of type 7 we obtain one orbit of length $p^2(p+1)$ and $q-2$ orbits of length $p^3(p+1)$;
   - if G is of type 8 we obtain 2 orbits of length p and $2(q-2)$ orbits of length p^2;
   - if G is of type 9, one orbit of length $2p$ together with $q-2$ orbits of length $2p^2$.

3. For $(G, \circ)$ of type 7, $x_1 + 1 = k(x_2 + 1)$.

   - If G is of type 7 then $x_1 = x_2 \neq 0$, so that the stabiliser has order $|\mathrm{GL}(2, p)|$ and there are $q-2$ orbits of length p^2.

   For both the types 8 and 9, the stabiliser has order $(p-1)^2$ when $x_1 \neq 0 \neq x_2$, and $p(p-1)^2$ otherwise. Therefore,

   - if G is of type 8 there are $q-3$ orbits of length p^2 and 2 orbits of length p;
   - if G is of type 9 there are $\frac{q-3}{2}$ orbits of length $2p^2$, and one orbit of length $2p$.

4. For $(G, \circ)$ of type 8, $x_1 \neq x_2$ for both the types 7 and 9, so that if $x_1, x_2 \neq 0$, for all the types the stabiliser has order $(p-1)^2$. Otherwise either $x_1 = 0$ or $x_2 = 0$, and the stabiliser has order $p(p-1)^2$. Therefore,

   - if G is of type 7 and $(G, \circ) \simeq G_s$, for every $s \in \mathcal{K}$ we obtain $q-3$ orbits of length $p^3(p+1)$ and two orbits of length $p^2(p+1)$;
   - if G is of type 9 and $(G, \circ) \simeq G_s$, for every $s \in \mathcal{K}$ we obtain $q-3$ orbits of length $2p^2$ and two orbits of length $2p$;
   - if G is of type 8 (so $G \simeq G_k$) and $(G, \circ) \simeq G_s$, then for every $s \neq k$, $s \in \mathcal{K}$, we obtain $2(q-3)$ orbits of length p^2 and 4 orbits of length p, otherwise $s = k$, and we get $2q-5$ orbits of length p^2 and 2 orbits of length p.

5. For $(G, \circ)$ of type 9, $x_1 = x_2$ only for the type 9. When $x_1, x_2 \neq 0$, for all the types of groups G the stabiliser has order $(p-1)^2$. Otherwise G can not be of type 9, and for the type 7 and 8 the stabiliser has order $p(p-1)^2$. Therefore,
   - if G is of type 7 there are $\frac{q-3}{2}$ orbits of length $p^3(p+1)$ and one of length $p^2(p+1)$;
   - if G is of type 8 there are $q-3$ orbits of length p^2 and 2 orbits of length p;
   - if G is of type 9 there are $q-2$ orbits of length p^2.

4.4.5 The case $|\ker(\gamma)| = p$

To enumerate the GF's in this case we will use Proposition 1.26.

Here $|\gamma(G)| = pq$. If G is of type 8 or 9, the discussion in Subsubsection 4.4.1.2 yields that $\gamma(G) = \langle\, \iota(a_0), \beta \,\rangle$, for some $1 \neq a_0 \in A$ with $A^\sigma = \langle\, \iota(a_0) \,\rangle$, and $\beta \neq 1$. We can assume $\gamma(b) = \iota(a_0^j)\beta$ for some j, where $\beta = \beta_1^{x_1}\beta_2^{x_2}$. With respect to the basis $\langle\, a_1, a_2 \,\rangle$, where $\langle\, a_1 \,\rangle$ and $\langle\, a_2 \,\rangle$ are the eigenspaces of $\iota(b)$, the matrix associated to β is $\mathrm{diag}(\lambda^{x_1}, \lambda^{kx_2})$, where x_1 and x_2 are not both zero.

If G is of type 7, since here $\gamma(G)$ intersects $\iota(A)$ non-trivially, $\gamma(G) = \langle\, \iota(c), \iota(d)\beta \,\rangle$ for some $c, d \in A$, with $A^\sigma = \langle\, \iota(c) \,\rangle$, and $\beta \in \mathrm{GL}(2,p)$, $\beta \neq 1$. Let $b \in G$ (of order q) such that $\gamma(b) = \iota(d)\beta$. With respect to a suitable basis of A, the matrix associated to $\gamma(b)_{|A}$ is $\mathrm{diag}(\lambda^{x_1}, \lambda^{x_2})$, where $(x_1, x_2) \neq (0,0)$. Denote by $\{a_1, a_2\}$ such a basis, and keep in mind that when $[\gamma(b)_{|A}]$ is not scalar there are $\frac{1}{2}p(p+1)$ choices for a pair $\{A_1, A_2\}$ of distinct one-dimensional subspaces of A.

Therefore, in all the cases above, we write $\gamma(b) = \iota(a_*)\beta$, and with respect to the fixed basis of A we can represent $\beta_{|A}$ as

$$T = \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{kx_2} \end{pmatrix},$$

where k accounts for the type of the group G, and x_1, x_2 are not both zero. Equation (1.14) yields

$$\sigma T(\sigma - 1) = (\sigma - 1)TZ\sigma. \tag{4.11}$$

The condition $|\ker(\gamma)| = p$ means that $|\ker(\sigma)| = p$, so let $\ker(\sigma) = \langle\, v \,\rangle$. Using (4.11) we obtain $v^{-TZ\sigma} = 1$, that is, $v^{-TZ} \in \langle\, v \,\rangle$, so that v is an eigenvector for TZ. Note that if G is of type 7 then Z is scalar and v is an eigenvector for T.

If TZ is non-scalar, then its eigenspaces are $\langle\, a_1 \,\rangle$ and $\langle\, a_2 \,\rangle$, and since v is an eigenvector for TZ, then either $v \in \langle\, a_1 \,\rangle$ or $v \in \langle\, a_2 \,\rangle$. Otherwise TZ is scalar, and v is any element in A, so that $v = a_1^x a_2^y$.

We proceed by distinguishing three cases, namely when $\ker(\sigma) = \langle a_1 \rangle$, when $\ker(\sigma) = \langle a_2 \rangle$, and lastly when $\ker(\sigma)$ is generated by $v = a_1^x a_2^y$, where $x, y \neq 0$.

Suppose first that $v \in \langle a_1 \rangle$, namely $\ker(\sigma) = \langle a_1 \rangle$. Therefore $a_1^\sigma = 1$, and we write $a_2^\sigma = a_1^\mu a_2^\nu$ for some μ, ν not both 0. Evaluating equation (4.11) on a_2 we get

$$\begin{cases} \mu(\nu - \lambda^{x_1 - x_2 k}) = \mu(\nu - 1)\lambda^k \\ (\nu - 1)\nu = (\nu - 1)\nu\lambda^k. \end{cases} \tag{4.12}$$

Since $\lambda^k \neq 1$, it must be either $\nu = 0$ or $\nu = 1$. If $\nu = 0$, then $\mu \neq 0$ and $x_1 - x_2 k = k$. Otherwise $\nu = 1$ and then either $\mu = 0$ or $\mu \neq 0$ and $x_1 = x_2 k$.

Suppose that $v \in \langle a_2 \rangle$, namely $\ker(\sigma) = \langle a_2 \rangle$. This case can be reduced to the previous case by swapping a_1 and a_2. In the new basis $\langle a_2, a_1 \rangle$ the matrix $[\sigma]$ is as in the previous case, while the diagonal elements in the matrices Z and T are swapped, so that evaluating equation (4.11) on a_1 we obtain the system (4.12) in which λ^{x_1} and λ^{kx_2}, resp. λ and λ^k, are swapped.

Suppose now that $v = a_1^x a_2^y$, where $x, y \neq 0$. Here TZ is scalar, so that $x_1 = x_2 k + k - 1$. Moreover, up to change a_i, $i = 1, 2$, with another non trivial element in $\langle a_i \rangle$ ($p - 1$ possibilities), we can suppose that $v = a_1 a_2$. Therefore, here σ is defined as

$$(a_1^z)^\sigma = a_1^{-z\mu} a_2^{-z\nu}, \ (a_2^z)^\sigma = a_1^{z\mu} a_2^{z\nu},$$

for some μ, ν not both 0. Evaluating equation (4.11) on a_2 we get

$$\begin{cases} \mu(-\mu\lambda^{-1} - \lambda^{-1} + \nu\lambda^{-k}) = \mu(-\mu + \nu - 1) \\ \nu(-\mu\lambda^{-1} - \lambda^{-k} + \nu\lambda^{-k}) = \nu(-\mu + \nu - 1). \end{cases}$$

If $\nu = 0$ then $\mu \neq 0$ and we get $-(\mu + 1)\lambda^{-1} = -(\mu + 1)$, that is, $\mu = -1$, so $A^\sigma = \langle a_1 \rangle$. If $\nu \neq 0$ and $\mu = 0$, we get $(\nu - 1)\lambda^{-k} = \nu - 1$, that is, $\nu = 1$ and $A^\sigma = \langle a_2 \rangle$. Lastly, if $\nu, \mu \neq 0$, then if $k = 1$ we get $\mu + 1 - \nu = 0$, and if $k \neq 1$ the system has no solution. Therefore this last case can happen only when G is of type 7, and in this case the condition $\mu + 1 - \nu = 0$ includes also the cases above in which $\mu = -1$ and $\nu = 0$, or $\mu = 0$ and $\nu = 1$.

If G is of type 8 or 9, we carry the case $(\mu, \nu) = (0, -1)$ into the case $(\mu, \nu) = (1, 0)$ by swapping a_1 and a_2 in the matrix σ.

For convenience we schematise our analysis as follows:

- Case A: $\ker(\sigma) = \langle a_1 \rangle$.

  (A1) $\nu = 0$, $\mu \neq 0$, $x_1 - x_2 k = k$;
  (A2) $\nu = 1$, $\mu \neq 0$, $x_1 = x_2 k$;
  (A3) $\nu = 1$, $\mu = 0$.

- Case A*: $\ker(\sigma) = \langle a_2 \rangle$.

(A1*) $\nu = 0$, $\mu \neq 0$, $x_2k - x_1 = 1$;

(A2*) $\nu = 1$, $\mu \neq 0$, $x_2k = x_1$;

(A3*) $\nu = 1$, $\mu = 0$.

- Case B: $\ker(\sigma) = \langle\, a_1a_2 \,\rangle$.

  1. If G is of type 8 or 9:

  (B1) $\nu = 0$, $\mu = -1$, $x_1 = x_2k + k - 1$;

  (B1*) $\nu = 1$, $\mu = 0$, $x_1 = x_2k + k - 1$.

  2. If G is of type 7:

  (B2) $\mu + 1 - \nu = 0$, $x_1 = x_2$.

Notice that p divides both $|\ker(\gamma)|$ and $|\ker(\tilde{\gamma})|$ if and only if σ has both 0 and 1 as eigenvalues, that is, in all the cases above except A1 and A1*, where, since σ has only 0 as eigenvalue, $p \mid |\ker(\gamma)|$ but $p \nmid |\ker(\tilde{\gamma})|$.

4.4.5.1 Invariant Sylow q-subgroups

Now we will show that there always exists at least one invariant Sylow q-subgroup.

Subsubsection 4.4.1.3 yields that, for a fixed b such that $\gamma(b) = \iota(a_*)\beta$, the Sylow q-subgroup $\langle\, b^x \,\rangle$ is invariant if and only if x is a solution of (4.8):

$$x^{(1-Z^{-1})M} = a_*^{(1-Z^{-1})T},$$

where $M = 1 - (1 + T^{-1}\sigma(1 - Z^{-1}))T$, and $\det(1 - Z^{-1}) \neq 0$.

If $\det(M) \neq 0$, then M has rank 2, so that the system (4.8) admits a unique solution. Therefore, a GF on G extending the assignment $\gamma(b) = \iota(a_*)\beta$ has a unique invariant Sylow q-subgroup B. By Proposition 1.26, every GF on G can be obtained as a gluing of a RGF on B and a RGF on A determined by σ.

Otherwise $\det(M) = 0$, and there are two cases, namely a_* is such that the system (4.8) admits solutions, or there are no solutions.

In the first case there are r solutions, where $r = p, p^2$, so that every GF γ on G extending the assignment $\gamma(b) = \iota(a_*)\beta$ has r invariant Sylow q-subgroups. Moreover, Proposition 1.26 yields that such a γ is the gluing of a RGF defined on any of the r invariant Sylow q-subgroups, and a RGF on A determined by σ.

In the second case, there are no invariant Sylow q-subgroups. We show that this case does not arise. More precisely, if γ is a GF on G extending the assignment $\gamma(b) = \iota(a_*)\beta$, then γ satisfies (4.9), and (4.10). We will show, case by case, that if a_* is such that the system (4.8) has no solution, then a_* does not satisfy the condition (4.10). Therefore in this case the assignment $\gamma(b) = \iota(a_*)\beta$ cannot be extended to a GF.

Write $a_* = a_1^x a_2^y$. We proceed by cases.

Case A Here $\ker(\sigma) = \langle\, a_1 \,\rangle$, and

$$M = \begin{pmatrix} 1-\lambda^{x_1} & 0 \\ -\mu\lambda^{x_1-x_2k}(1-\lambda^{-1}) & 1-\lambda^{x_2k}-\nu(1-\lambda^{-k}) \end{pmatrix}.$$

According to the division into subcases, we have

A1 $\det(M) = (1-\lambda^{x_1})(1-\lambda^{x_1-k})$, so that there is a unique invariant Sylow q-subgroup when $x_1 \neq 0, k$.

If $x_1 = 0$, then the system (4.8) admits (p) solutions if and only if $a_* = a_1^{-\mu y} a_2^y$. In this case there are p invariant Sylow q-subgroups. Moreover, if $a_* = a_1^x a_2^y$, the condition (4.10) yields that $x = -\mu y$. Therefore, by the discussion above, the case in which there are no invariant Sylow q-subgroups does not arise.

If $x_1 = k$, then (4.8) admits (p) solutions if and only if $a_* = a_1^x$, and in this case there are p invariant Sylow q-subgroups. (4.10) yields that $y = 0$, therefore the case in which there are no invariant Sylow q-subgroups does not arise.

A2 $\det(M) = (1-\lambda^{x_1})(\lambda^{-k}(1-\lambda^{x_1+k}))$, so that there is a unique invariant Sylow q-subgroup when $x_1 \neq 0, -k$. Note that here necessarily $x_1 \neq 0$, otherwise we would also have $x_2 = 0$, namely $\beta = 1$.

If $x_1 = -k$, then the system (4.8) admits (p) solutions if and only if $a_* = a_1^x$, and in this case there are p invariant Sylow q-subgroups. Also here the a_*'s for which (4.8) has no solutions are precisely those for which (4.10) is not satisfied, in fact here (4.10) yields $y = 0$.

A3 $\det(M) = (1-\lambda^{x_1})(\lambda^{-k}(1-\lambda^{x_2k+k}))$, so that there is a unique solution when $x_1 \neq 0$ and $x_2 \neq -1$.

If either $x_1 = 0$ and $x_2 \neq -1$, or $x_1 \neq 0$ and $x_2 = -1$, then $(1-Z^{-1})M$ has rank 1, and the system (4.8) admits p solutions if and only if $a_* = a_2^y$ in the first case, and $a_* = a_1^x$ in the second case. Once again, the a_*'s for which (4.8) has no solutions are precisely those for which (4.10) is not satisfied, in fact here (4.10) yields $x = 0$ in the case $x_1 = 0$ and $x_2 \neq -1$, and $y = 0$ in the case $x_1 \neq 0$ and $x_2 = -1$.

If $x_1 = 0$ and $x_2 = -1$, then $(1-Z^{-1})M$ has rank 0, and the system (4.8) admits p^2 solutions if and only if $a_*^{(1-Z^{-1})T} = 1$, namely when $a_* = 1$. Moreover, the condition (4.10) yields $x, y = 0$, so that the case in which the system has no solution does not arise.

Case A* Here $\ker(\sigma) = \langle\, a_2 \,\rangle$ and equation (4.8) gives a system whose matrix of coefficients, C^*, can be obtain by the matrix $(1-Z^{-1})M$ computed in case A swapping respectively λ^{x_1} and λ^{kx_2}, λ and λ^k. In this way we get C^* in the basis $\langle\, a_2, a_1 \,\rangle$, so that swapping a_1 and a_2 we get the matrix C^* in the basis $\langle\, a_1, a_2 \,\rangle$.

Case B Here $\ker(\sigma) = \langle\, a_1a_2 \,\rangle$ and (4.8) yields

$$M = \begin{pmatrix} 1-\lambda^{x_1}+\mu(1-\lambda^{-1}) & \lambda^{-x_1+kx_2}\nu(1-\lambda^{-k}) \\ -\lambda^{x_1-kx_2}\mu(1-\lambda^{-1}) & 1-\lambda^{kx_2}-\nu(1-\lambda^{-k}) \end{pmatrix}.$$

According to the division into subcases, we have

B1 $\det(M) = \lambda^{-1}(1-\lambda^{x_1+1})(1-\lambda^{x_1+1-k})$, and there exists a unique invariant Sylow q-subgroup when $x_1 \neq -1, k-1$.

If $x_1 = -1, k-1$, then there are p invariant Sylow q-subgroups when $a_* = a_1^x a_2^x$ in the case $x_1 = -1$, and $a_* = a_1^x$ in the case $x_1 = k-1$. The other cases, namely those for which there are no invariant Sylow q-subgroups, do not arise, in fact the condition (4.10) yields precisely $x = y$ in the case $x_1 = -1$, and $y = 0$ in the case $x_1 = k-1$.

B1* $\det(M) = (1-\lambda^{kx_2+k-1})(\lambda^{-k}(1-\lambda^{kx_2-k}))$, and there is one invariant Sylow q-subgroup when $x_2 \neq -1, k^{-1}-1$.

If $x_2 = -1, k^{-1}-1$, then there are p invariant Sylow q-subgroups when $a_* = a_1^x a_2^x$ in the case $x_2 = -1$, and $a_* = a_2^y$ in the case $x_2 = k^{-1}-1$. The other cases, namely those for which there are no invariant Sylow q-subgroups, do not arise, in fact the condition (4.10) yields precisely $x = y$ in the case $x_2 = -1$, and $x = 0$ in the case $x_2 = k^{-1}-1$.

Note that here the matrix of the coefficients of (4.8), C^*, can also be obtained by the matrix $(1-Z^{-1})M$ of the case B1 swapping λ^{x_1} and λ^{kx_2}, respectively λ and λ^k. This yields C^* in the basis $\langle\, a_2, a_1 \,\rangle$, so that swapping a_1 and a_2 we get C^* in the basis $\langle\, a_1, a_2 \,\rangle$.

B2 $\det(M) = (\lambda^{x_1}-1)\lambda^{-1}(\lambda^{x_1+1}-1)$, and there exists a unique invariant Sylow q-subgroup when $x_1 \neq 0, -1$. Note that here necessarily $x_1 \neq 0$, otherwise we would also have $x_2 = 0$.

If $x_1 = -1$, then there are p invariant Sylow q-subgroups when $a_* = a_1^x a_2^x$. Also here the other cases do not arise, in fact the condition (4.10) yields precisely $x = y$.

By the discussion above we get the following.

Proposition 4.4. *The number of invariant Sylow q-subgroups is*

(A1) 1 *when* $x_1 \neq 0, k$ *and* p *otherwise.*

(A2) 1 *when* $x_1 \neq -k$ *and* p *otherwise.*

(A3) 1 *when* $x_1 \neq 0$ *and* $x_2 \neq -1$, p^2 *when* $x_1 = 0$ *and* $x_2 = -1$, *and* p *otherwise.*

(A1*) 1 *when* $x_2 \neq 0, k^{-1}$ *and* p *otherwise.*

(A2*) 1 *when* $x_2 \neq -k^{-1}$ *and* p *otherwise.*

(A3*) 1 *when* $x_2 \neq 0$ *and* $x_1 \neq -1$, p^2 *when* $x_2 = 0$ *and* $x_1 = -1$, *and* p *otherwise.*

(B1) 1 *when* $x_1 \neq -1, k-1$ *and* p *otherwise.*

(B1*) 1 *when* $x_2 \neq -1, -1+k^{-1}$ *and* p *otherwise.*

(B2) 1 *when* $x_1 \neq -1$ *and* p *otherwise.*

Proof. All the cases except A1*, A2* and A3* are discussed above.

In the case A1*, $\det(C^*) = \det(1-Z^{-1})(1-\lambda^{kx_2})(1-\lambda^{kx_2-1})$, where $\det(1-Z^{-1}) \neq 0$. Therefore, if $x_2 \neq 0, k^{-1}$, the system (4.8) has a unique solution. If $x_2 = 0, k^{-1}$, then there are p solutions when $a_* = a_1^x a_2^{-\mu x}$ in the case $x_2 = 0$, and $a_* = a_2^y$ in the case $x_2 = k^{-1}$. Moreover the condition (4.10) yields precisely $y = -x\mu$ in the case $x_2 = 0$, and $x = 0$ in the case $x_2 = k^{-1}$.

In the case A2*, $\det(C^*) = \det(1-Z^{-1})(1-\lambda^{kx_2})\lambda^{-1}(1-\lambda^{kx_2+1})$, therefore there is a unique solution if $x_2 = 0$ or $x_2 = -k^{-1}$. Here necessarily $x_2 \neq 0$. If $x_2 = -k^{-1}$, then there are p solutions when $a_* = a_2^y$, and the case in which there are no solutions does not arise, since condition (4.10) yields $x = 0$.

In the case A3*, $\det(C^*) = \det(1-Z^{-1})(1-\lambda^{kx_2})\lambda^{-1}(1-\lambda^{x_1+1})$, and there is a unique solution when both $x_2 \neq 0$ and $x_1 \neq -1$. If either $x_2 = 0$ and $x_1 \neq -1$, or $x_2 \neq 0$ and $x_1 = -1$, there are p solutions when $a_* = a_1^x$ in the case $x_2 = 0$ and $x_1 \neq -1$, and $a_* = a_2^y$ in the case $x_2 \neq 0$ and $x_1 = -1$. Moreover the condition (4.10) yields $y = 0$ when $x_2 = 0$ and $x_1 \neq -1$, and $x = 0$ when $x_2 \neq 0$ and $x_1 = -1$, therefore the case in which there are no solutions does not arise.

Lastly, if $x_2 = 0$ and $x_1 = -1$ there are p^2 solutions when $a_* = 1$, and (4.10) yields $x, y = 0$. □

4.4.5.2 Computations

In the previous Subsubsection we show that there always exists a Sylow q-subgroup B which is invariant under $\gamma(B)$, and Proposition 4.4 yields the exact number of invariant Sylow q-subgroups. Moreover, every $a \in A$ satisfies equation (4.6). Therefore by Proposition 1.26, all the GF's of this case can be obtained as a gluing of a function γ_A on A defined as in (4.6) and a RGF γ_B on B, where B is an invariant Sylow q-subgroup, whenever γ_A and γ_B satisfy (4.11).

To enumerate the GF's we can count the possible couples (γ_A, γ_B) with the properties above, taking into account that every such choice defines a unique γ and a given γ built in this way is obtained s times, where s is the number of invariant Sylow q-subgroups of G. Thus to obtain the number of distinct GF's on G we count the choices for (γ_A, γ_B) as above, and then divide this number by s.

Let $Z_\circ$ be the action of b on A in $(G,\circ)$. We have

$$\begin{aligned} b^{\ominus 1}\circ a\circ b &= (b^{\gamma(b)^{-1}\gamma(a)\gamma(b)})^{-1}a^{\gamma(b)}b \\ &= (b^{\iota(a^{-\sigma})\beta})^{-1}a^{\gamma(b)}b \\ &= ((a^{-\sigma(-1+Z^{-1})}b)^{\beta})^{-1}a^{\gamma(b)}b \\ &= (a^{-\sigma(-1+Z^{-1})T}b)^{-1}a^{T}b \\ &= b^{-1}a^{\sigma(-1+Z^{-1})T+T}b \\ &= a^{(\sigma(1-Z)+Z)T}, \end{aligned}$$

and since $a^{\circ k}=a^k$, with respect to the basis $\{a_1,a_2\}$ of $(A,\circ)$ we have

$$Z_\circ = (\sigma(1-Z)+Z)T. \tag{4.13}$$

Case A. Here $\ker(\sigma)=\langle\, a_1\,\rangle$ and equality (4.13) yields

$$Z_\circ = \begin{pmatrix} \lambda^{x_1+1} & 0 \\ \mu(1-\lambda)\lambda^{x_1} & \lambda^{x_2 k}(\nu(1-\lambda^k)+\lambda^k) \end{pmatrix}.$$

(A1) We have $p-1$ choices for σ, and

$$Z_\circ \sim \begin{pmatrix} \lambda^{x_1+1} & 0 \\ 0 & \lambda^{x_1} \end{pmatrix}.$$

We obtain the following groups $(G,\circ)$.

Type 5 does not arise.

Type 6 if $x_1=0$ or $x_1=-1$. If $x_1=0$ for each of the $(p-1)$ choices for σ we have p^2/p choices for B giving different GF's, so $p(p-1)$ groups if G is of type 8 or 9, and $\frac{1}{2}p^2(p^2-1)$ groups if G is of type 7. If $x_1=-1$, then $x_1=k$ if and only if either G is of type 9 or G is of type 7 and $q=2$. If $q>2$ there are respectively $\frac{1}{2}p^3(p^2-1)$, $p^2(p-1)$ and $p(p-1)$ groups for G of type 7, 8 and 9, otherwise if $q=2$ (and G is of type 7) there are $\frac{1}{2}p^2(p^2-1)$ groups.

Type 7 does not arise.

Type 8 if $x_1\neq 0,\,-1,\,(q-1)/2$, and these are always three independent conditions.

- If G is of type 9, then $x_1\neq k$ and we get $p^2(p-1)(q-3)$ groups. They split in $2p^2(p-1)$ groups isomorphic to G_s for every $s\in\mathcal{K}$.

If G is of type 7 or 8, x_1 can be equal to k.

- If G is of type 7, we have $\frac{1}{2}p^2(p^2-1)$ groups when $x_1=1$ and $\frac{1}{2}p^3(p^2-1)(q-4)$ groups when $x_1\neq 1$. They split in $\frac{1}{2}p^2(p^2-1)+\frac{1}{2}p^3(p^2-1)$ groups isomorphic to G_2, and $p^3(p^2-1)$ groups isomorphic to G_s, for every $s\neq 2, s\in\mathcal{K}$.

– If G is of type 8, then $G \simeq G_k$. Suppose first that $k = (q-1)/2$; then $x_1 \neq k$ and there are $p^2(p-1)(q-3)$ groups. Otherwise $k \neq (q-1)/2$ and there are $p(p-1) + p^2(p-1)(q-4)$ groups. Therefore, if $k = \frac{q-1}{2}$, there are $2p^2(p-1)$ groups isomorphic to G_s for every $s \in \mathcal{K}$, and if $k \neq \frac{q-1}{2}$, then there are $p(p-1) + p^2(p-1)$ groups isomorphic to $G_{1+k^{-1}}$ (obtained for $x_1 = k, -(k+1)$) and $2p^2(p-1)$ groups isomorphic to G_s for every $s \neq 1 + k^{-1}, s \in \mathcal{K}$.

Type 9 if $x_1 = (q-1)/2$. If G is of type 7, since $(q-1)/2 = 1$ if and only if $q = 3$, we have $\frac{1}{2}p^2(p^2-1)$ groups when $q = 3$ and $\frac{1}{2}p^3(p^2-1)$ groups when $q > 3$. If G is of type 9, then $x_1 \neq k$ and we get $p^2(p-1)$ groups. If G is of type 8, then $G \simeq G_k$. When $k = (q-1)/2$ then $x_1 = k$ and there are $p(p-1)$ groups. Otherwise $k \neq (q-1)/2$ so that $x_1 \neq k$ and there are $p^2(p-1)$ groups.

(A2) We have $p-1$ choices for σ, and

$$Z_\circ \sim \begin{pmatrix} \lambda^{x_1+1} & 0 \\ 0 & \lambda^{x_1} \end{pmatrix}.$$

We obtain the following groups $(G, \circ)$.

Type 5 does not arise.

Type 6 when $x_1 = -1$. If G is of type 7 then $x_1 = -k$ and there are $p(p-1)$ groups. If G is of type 8 or 9 $x_1 \neq -k$ and there are $p^2(p-1)$ groups.

Type 7 does not arise.

Type 8 if $x_1 \neq 0, -1, (q-1)/2$, and these are always three independent conditions.

– If G is of type 7 then $x_1 \neq -k$ and there are $p^2(p-1)(q-3)$ groups. They split in $2p^2(p-1)$ groups isomotphic to G_s for every $s \in \mathcal{K}$.

– If G is of type 9 then x_1 can be equal to $-k$ and so there are $p(p-1)+p^2(p-1)(q-4)$ groups. They split in $p(p-1)+p^2(p-1)$ groups isomorphic to G_2 and $2p^2(p-1)$ groups isomorphic to G_s for every $s \neq 2, s \in \mathcal{K}$.

– If G is of type 8, then $G \simeq G_k$. When $k = 1/2$ then $x_1 \neq -k$ and there are $(p-1)(q-3)p^2$ groups, which split $2p^2(p-1)$ groups isomorphic to G_s for every $s \in \mathcal{K}$. If $k \neq 1/2$ then there are $(p-1)p+p^2(p-1)(q-4)$ groups, which split in $p^2(p-1)+p(p-1)$ groups isomorphic to $G_{1-k^{-1}}$, and $2p^2(p-1)$ groups isomorphic to G_s for every $s \neq 1 - k^{-1}, s \in \mathcal{K}$.

Type 9 if $x_1 = (q-1)/2$. If G is of type 7 then $x_1 \neq -k$ and there are $p^2(p-1)$ groups. If G is of type 9 then $x_1 = -k$ if and only if $q = 3$, and there are $p^2(p-1)$ groups if $q > 3$ and $p(p-1)$ if $q = 3$. If G is of type 8, $G \simeq G_k$. If $k = 1/2$ then $x_1 = -k$ and there are $p(p-1)$ groups. Otherwise $k \neq 1/2$, so $x_1 \neq -k$ and there are $p^2(p-1)$ groups.

(A3) We have 1 choice for σ, and

$$Z_\circ \sim \begin{pmatrix} \lambda^{x_1+1} & 0 \\ 0 & \lambda^{x_2 k} \end{pmatrix}.$$

We obtain the following groups $(G, \circ)$.

Type 5 if $1 + x_1 = x_2 k = 0$. Since $x_1 \neq 0$ and $x_2 \neq -1$, there are p^2 groups if G is of type 8 or 9 and $\frac{1}{2}p^3(p+1)$ if G is of type 7.

Type 6 if either $x_1 = -1$ and $x_2 \neq 0$ or $x_1 \neq -1$ and $x_2 = 0$. In the first case, there are p groups when $x_2 = -1$, otherwise, for $x_2 \neq -1$, there are $p^2(q-2)$ groups if G is of type 8 or 9 and $\frac{1}{2}p^3(p+1)(q-2)$ groups if G is of type 7. In the second case, since $x_2 = 0$, we have to take $x_1 \neq 0$ and there there $p^2(q-2)$ groups if G is of type 8 or 9, and $\frac{1}{2}p^3(p+1)(q-2)$ if G is of type 7.

Type 7 when $x_2 k = 1 + x_1 \neq 0$. If $x_1 = 0$ and $x_2 = -1$, then either $k = -1$ and G is of type 9, or $q = 2$ and G is of type 7; in the first case there is one group, and in the second case there are $\frac{1}{2}p(p+1)$ groups. In both the cases $x_1 \neq 0$, $x_2 = -1$, and $x_1 = 0$, $x_2 \neq -1$ we have $k \neq -1$ so G is of type 7 or 8 and there are respectively $p^2(p+1)$ and $2p$ groups. If $x_1 \neq 0$ and $x_2 \neq -1$ there are $\frac{1}{2}p^3(p+1)(q-3)$ groups if G is of type 7, $p^2(q-2)$ groups if G is of type 9 and $p^2(q-3)$ groups when G is of type 8.

Type 8 when $x_1 \neq -1, x_2 k - 1, -x_2 k - 1$, $x_2 \neq 0$. If $x_1 = 0$ and $x_2 = -1$, then $k \neq -1, 1$ and so this happens only when G is of type 8 and there is one group. If $x_1 \neq 0$ and $x_2 = -1$, the four conditions on x_1 are independent when G is of type 8, and so there are $p(q-4)$ groups, while they are actually three conditions when G is of type 7 or 9, and there are respectively $\frac{1}{2}p^2(p+1)(q-3)$ and $p(q-3)$ groups. If $x_1 = 0$ and $x_2 \neq -1$ we get further $\frac{1}{2}p^2(p+1)(q-3)$, $p(q-4)$ and $p(q-3)$ groups, respectively when G is of type 7, 8, and 9.

Suppose now $x_1 \neq 0$, $x_2 \neq -1$. If G is of type 8 there are always four independent conditions on x_1, except when $x_2 = \pm k^{-1}$, where the conditions become three. Thus there are $p^2(q-4)^2 + 2p^2(q-3)$ groups.

If G is of type 7 or 9 there are always four independent conditions on x_1 except when $x_2 = 1$, where the conditions become three. If G is of type 9 there are $p^2((q-4)(q-3)+(q-3)) = p^2(q-3)^2$ groups. If G is of type 7, if $x_2 = 1$ then there is one invariant Sylow q-subgroup and β is scalar if and only if $x_1 = 1 = x_2$, so there are $p^2 + \frac{1}{2}p^3(p+1)(q-4)$ groups. If $x_2 \neq 1$, there is one invariant Sylow q-subgroup and β can always be scalar except when $x_2 = (q-1)/2$, thus there are $\frac{1}{2}p^3(p+1)(q-4)$ groups when $x_2 = (q-1)/2$ and $p^2(q-4) + \frac{1}{2}p^3(p+1)(q-5)(q-4)$ when $x_2 \neq (q-1)/2$.
Therefore we have just obtained

- if G is of type 7, $p^2(p+1)(q-3)+p^2(q-3)+\frac{1}{2}p^3(p+1)(q-4)(q-3)$ groups. They split in $2p^2(p+1)+2p^2+p^3(p+1)(q-4)$ groups isomorphic to G_s for every $s \in \mathcal{K}$.
- If G is of type 9, $2p(q-3)+p^2(q-3)^2$ groups. They split in $4p+2p^2(q-3)$ groups isomorphic to G_s for every $s \in \mathcal{K}$.
- If G is of type 8, so $G \simeq G_k$, $1+2p(q-4)+p^2(q-4)^2+2p^2(q-3)$ groups. Looking at the eigenvalues of $Z_\circ$ as x_1 and x_2 vary, and taking into account the conditions on x_1 and x_2, one can see that the $2p^2(q-3)$ groups split in $4p^2$ groups isomorphic to G_s for every $s \in \mathcal{K}$, and the $1+2p(q-4)+p^2(q-4)^2$ groups split in $4p+2p^2(q-5)$ groups isomorphic to G_s for every $s \neq -k$, and $1+2p+p^2+2p^2(q-5)$ groups isomorphic to G_{-k}. Therefore in total they split in $1+2p+p^2(2q-5)$ groups isomorphic to G_{-k}, and $4p+2p^2(q-3)$ groups isomorphic to G_s for every $s \neq -k, s \in \mathcal{K}$.

Type 9 if $x_1 \neq -1$, $x_2 \neq 0$ and $1+x_1+x_2k = 0$. Suppose first that G is of type 7. Here $x_1 = x_2$ if and only if $x_2 = (q-1)/2$. If $x_2 = -1$ then $x_1 = 0$ and there are $\frac{1}{2}p(p+1)$ groups. If $x_2 = (q-1)/2 = x_1$ there are p^2 groups. Otherwise $x_2 \neq 0, -1, (q-1)/2$ and there are $\frac{1}{2}p^3(p+1)(q-3)$ groups.
If G is of type 8 or 9, it can not be $x_1 = 0$ and $x_2 = -1$, since otherwise $k = 1$. For $x_2 = -1$ and $x_1 = k-1 \neq 0$ there are p groups. Similarly, for $x_2 \neq -1$ and $x_1 = 0$ and there are p groups. For $x_2 \neq -1$ and $x_1 = -x_2k - 1 \neq 0$, namely $x_2 \neq 0, -1, k^{-1}$, we get $p^2(q-3)$ groups.

Case A*. This case can be recovered by the previous one, since the matrix $Z_\circ^*$ here can be obtained by swapping λ^{x_1} and λ^{kx_2}, λ and λ^k in the matrix $Z_\circ$ of the case A. The swapped matrices $Z_\circ^*$ in the subcases A1*, A2* and A3* are similar to $\mathrm{diag}(\lambda^{kx_2+k}, \lambda^{kx_2})$, $\mathrm{diag}(\lambda^{kx_2+k}, \lambda^{kx_2})$ and $\mathrm{diag}(\lambda^{kx_2+k}, \lambda^{x_1})$ respectively. The subcase distinction can therefore be obtained by the previous one, since any given $(G, \circ)$ obtained for a certain value of x_1 in one of the subcases A1 and A2, is also obtained in the corresponding subcase A1* or A2*,

considering the same value for x_2. Moreover, in the case A1 and A2, when G is of type 8 and $(G,\circ)$ is of type 8 or 9, the number of the groups depends on the value of k. By Proposition 4.4, when we swap to the cases A1* and A2*, this number depends on the value of k^{-1}.

In the case A3*, proceeding as in the case A3, for each type we obtain as many groups as in A3.

Case B. Here $\ker(\sigma) = \langle\, a_1a_2 \,\rangle$, $x_1 = x_2k+k-1$, and equality (4.13) yields

$$Z_\circ = \begin{pmatrix} \lambda^{x_1+1} - \lambda^{x_1}\mu(1-\lambda) & -\lambda^{kx_2}\nu(1-\lambda^k) \\ \lambda^{x_1}\mu(1-\lambda) & \lambda^{kx_2+k} + \lambda^{kx_2}\nu(1-\lambda^k) \end{pmatrix}.$$

(B1) Here G is of type 8 or 9. We have $p-1$ choices for σ, and

$$Z_\circ = \begin{pmatrix} \lambda^{x_1} & 0 \\ -\lambda^{x_1}(1-\lambda) & \lambda^{x_2k+k} \end{pmatrix} \sim \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{x_1+1} \end{pmatrix}.$$

We obtain the following groups $(G,\circ)$.

Type 5 does not arise.

Type 6 when $x_1 = 0$ or $x_1 = -1$. In the first case $x_1 \neq k-1, -1$ and there are $p^2(p-1)$ groups, while in the second case there are $p(p-1)$ groups.

Type 7 does not arise.

Type 8 when $x_1 \neq 0, -1, -1/2$. If $x_1 = k-1$ (and thus $k \neq 1/2$) there are $p(p-1)$ groups. Suppose now $x_1 \neq k-1$; when $k \neq 1/2$ (in particular when G is of type 9) the four conditions on x_1 are independent and there are $(p-1)(q-4)p^2$ groups. Otherwise $k = 1/2$ (and this happens only for G of type 8) and the four conditions are actually three, thus there are $p^2(p-1)(q-3)$ groups. Therefore there are $p^2(p-1)(q-3)$ groups if $k = 1/2$, and they split in $2p^2(p-1)$ groups isomorphic to G_s for every $s \in \mathcal{K}$. If $k \neq 1/2$ and G is of type 8, there are $p^2(p-1)(q-4) + p(p-1)$ groups, which split in $p(p-1) + p^2(p-1)$ groups isomorphic to $G_{1-k^{-1}}$, and $2p^2(p-1)$ groups isomorphic to G_s for every $s \neq 1-k^{-1}, s \in \mathcal{K}$. If G is of type 9 we obtain the same number, with $k = -1$.

Type 9 if $x_1 = (q-1)/2$ ($x_1 \neq 0$ and $x_1 \neq -1$). We have that $x_1 = k-1$ when $k = 1/2$ and in this case there are $(p-1)p$ groups. Otherwise $k \neq 1/2$ (in particular when G is of type 9) and there are $(p-1)p^2$ groups.

(B1*) This case can be recovered by the previous one, since the matrix $Z_\circ^*$ here can be obtained by swapping λ^{x_1} and λ^{kx_2}, λ and λ^k in the matrix $Z_\circ$ of the case B. The swapped matrix $Z_\circ^*$ is similar to $\mathrm{diag}(\lambda^{kx_2+k}, \lambda^{kx_2})$, therefore also here any given $(G,\circ)$ obtained for a certain value of x_1 in

the case B1, is obtained in the case B1* too, considering the same value for x_2. When, in the case B1, the number of the groups depends on the value of k, here, by Proposition 4.4, this number depends on the value of k^{-1}.

(B2) Here G is of type 7, $x_1 = x_2$, $\mu + 1 = \nu$, and we have $p(p-1)$ choices for

$$\sigma = \begin{pmatrix} -\mu & -\mu - 1 \\ \mu & \mu + 1 \end{pmatrix}.$$

We have

$$Z_\circ = \begin{pmatrix} \lambda^{x_1+1} - \lambda^{x_1}\mu(1-\lambda) & -\lambda^{x_1}(\mu+1)(1-\lambda) \\ \lambda^{x_1}\mu(1-\lambda) & \lambda^{x_1+1} + \lambda^{x_1}(\mu+1)(1-\lambda) \end{pmatrix},$$

and

$$Z_\circ \sim \begin{pmatrix} \lambda^{x_1+1} & 0 \\ 0 & \lambda^{x_1} \end{pmatrix}.$$

We obtain the following groups $(G, \circ)$.

Type 5 does not arise.

Type 6 if $x_1 = -1$, and there are $p^2(p-1)$ groups.

Type 7 does not arise.

Type 8 when $x_1 \neq -1, 0, (q-1)/2$. These are three independent conditions and there are $p^3(p-1)(q-3)$ groups.

Type 9 if $x_1 \neq -1, 0$, $x_1 = (q-1)/2$, and there are $p^3(p-1)$ groups, which split in $2p^3(p-1)$ groups isomorphic to G_s for every s.

The results of this subsection are collected in tables B.1, B.2, and B.3 of the Appendix.

As to the conjugacy classes, let $\varphi = \iota(x)\delta$, where $x \in A$ and $\delta \in \mathrm{GL}(2,p)$. We have

$$\begin{aligned} \gamma^\varphi(a) &= \varphi^{-1}\gamma(a^{\delta^{-1}})\varphi \\ &= \delta^{-1}\iota(a^{-\delta^{-1}\sigma})\delta \\ &= \iota(a^{-\delta^{-1}\sigma\delta}), \end{aligned}$$

and

$$\begin{aligned} \gamma^\varphi(b) &= \varphi^{-1}\gamma(x^{1-Z^{-1}}b)\varphi \\ &= \varphi^{-1}\iota(x^{-(1-Z^{-1})T^{-1}\sigma})\beta\varphi \\ &= \delta^{-1}\iota(x^{-1+T^{-1}-(1-Z^{-1})T^{-1}\sigma})\beta\delta \end{aligned}$$

$$= \iota(x^{(-1+T^{-1}-(1-Z^{-1})T^{-1}\sigma)\delta})\delta^{-1}\beta\delta.$$

We denote by H the matrix $-1+T^{-1}-(1-Z^{-1})T^{-1}\sigma$. Imposing $\gamma^{\varphi}(a) = \iota(a^{-\sigma})$ and $\gamma^{\varphi}(b) = \beta$, we obtain that φ stabilises γ if and only if the conditions

$$[\sigma, \delta] = 1, \tag{4.14}$$

$$[\beta, \delta] = 1, \tag{4.15}$$

$$x^{H\delta} = 1, \tag{4.16}$$

are satisfied.

Conjugacy classes for G of type 8. Suppose first that G is of type 8. In this case $\delta = \mathrm{diag}(\delta_{11}, \delta_{22})$, so that (4.15) is satisfied for every δ. In both the case (A) and (B1), the condition (4.14) yields $\mu\delta_{22}^{-1}\delta_{11} = \mu$, so that $\mu = 0$ or δ is scalar. Note that $\mu = 0$ only in the case (A3), thus we consider any δ in this case, and δ scalar in the cases (A1), (A2) and (B1).

In the case (A1) we have

$$H = \begin{pmatrix} -1+\lambda^{-x_1} & 0 \\ -\mu(1-\lambda^{-k})\lambda^{k+x_1} & -1+\lambda^{k+x_1} \end{pmatrix},$$

so that (4.14) has one solution if $x_1 \neq 0, k$, and p solutions if $x_1 = 0, k$. Therefore the orbits have length $p(p-1)$ if $x_1 = 0, k$, and $p^2(p-1)$ when $x_1 \neq 0, k$.

In the case (A2),

$$H = \begin{pmatrix} -1+\lambda^{-x_1} & 0 \\ -\mu(1-\lambda^{-k})\lambda^{-x_1} & -1+\lambda^{-k-x_1} \end{pmatrix},$$

and (4.14) has one solution if $x_1 \neq -k$, and p solutions if $x_1 = -k$. Therefore the orbits have length $p(p-1)$ when $x_1 = -k$, and $p^2(p-1)$ when $x_1 \neq -k$.

In the case (A3),

$$H = \begin{pmatrix} -1+\lambda^{-x_1} & 0 \\ 0 & -1+\lambda^{-k-kx_2} \end{pmatrix},$$

and (4.14) has one solution if $x_1 \neq 0$ and $x_2 \neq -1$, p^2 solutions if $x_1 = 0$ and $x_2 = -1$, and p solutions otherwise. Therefore the orbits have length p^2 if $x_1 \neq 0$ and $x_2 \neq -1$, 1 if $x_1 = 0$ and $x_2 = -1$, and p otherwise.

In the case (B1),

$$H = \begin{pmatrix} -1+\lambda^{-x_1-1} & 0 \\ (1-\lambda^{-k})\lambda^{k-1-x_1} & -1+\lambda^{k-1-x_1} \end{pmatrix},$$

and (4.14) has one solution if $x_1 \neq -1, k-1$, and p solutions otherwise. Therefore the orbits have length $p^2(p-1)$ if $x_1 \neq -1, k-1$, and $p(p-1)$ otherwise.

In the case (A*) and (B1*), proceeding as above we obtain as many conjugacy classes, with the same lengths, as in the case A and B1.

Conjugacy classes for G of type 9. If G is of type 9, consider $\varphi = \iota(x)\delta\psi$, where δ is diagonal, and $\psi \in \mathcal{C}_2$. Suppose $\psi \neq 1$. Then

$$\gamma^{\varphi}(a_1) = \varphi^{-1}\gamma(a_1^{S\delta^{-1}})\varphi = \varphi^{-1}\iota(a_2^{\delta_{22}^{-1}\sigma})\varphi = \varphi^{-1}\iota(a_1^{-\mu\delta_{22}^{-1}}a_2^{-\nu\delta_{22}^{-1}})\varphi.$$

In the case (A) we have that $\gamma(a_1) = 1$, and since $\iota(a_1^{-\mu\delta_{22}^{-1}}a_2^{-\nu\delta_{22}^{-1}}) \neq 1$, then $\gamma^{\varphi}(a_1) \neq \gamma(a_1)$. In the case (B1), $\gamma(a_1) = \iota(a_1^{-\sigma}) = \iota(a_1)$, and since here $\nu = 0$ and $\mu = -1$,

$$\gamma^{\varphi}(a_1) = \psi^{-1}\delta^{-1}\iota(a_1^{\delta_{22}^{-1}})\delta\psi = \psi^{-1}\iota(a_1^{\delta_{22}^{-1}\delta_{11}})\psi = \iota(a_2^{\delta_{22}^{-1}\delta_{11}}) \neq \gamma(a_1).$$

Therefore $\psi = 1$, and with the same computations made for the type 8, we obtain that in each case the order of the stabiliser is the same as for the type 8. Thus here the orbits have length:

1. in the cases (A1), (A1*), $2p(p-1)$ if $x_1 = 0, -1$, and $2p^2(p-1)$ otherwise;
2. in the cases (A2), (A2*), $2p(p-1)$ if $x_1 = -1$, and $2p^2(p-1)$ otherwise;
3. in the cases (A3), (A3*), $2p^2$ if $x_1 \neq 0$ and $x_2 \neq -1$, 2 if $x_1 = 0$ and $x_2 = -1$, and $2p$ otherwise;
4. in the cases (B1), (B1*), $2p(p-1)$ if $x_1 = -1, -2$, and $2p^2(p-1)$ otherwise.

Conjugacy classes for G of type 7. Suppose now G of type 7, and let $\varphi = \iota(x)\delta$ an automorphism of G, where $x \in A$, and $\delta \in \mathrm{GL}(2,p)$.

If we are in the case (A1), then (4.14) yields $\delta_{12} = 0$ and $\delta_{11} = \delta_{22}$, and (4.15) yields $\delta_{21} = 0$. Therefore δ is scalar, and with the same computations made for the type 8 we obtain that H has rank 2 if $x_1 \neq 0, 1$, and 1 otherwise. Therefore the orbits have length $p^3(p^2-1)$ if $x_1 \neq 0, 1$ and $p^2(p^2-1)$ otherwise.

If we are in the case (A2), then (4.14) yields $\delta_{12} = 0$ and $\delta_{21} = \mu(\delta_{22} - \delta_{11})$. Here T is scalar, so that (4.15) is satisfied for every δ. Moreover H has rank 2 if $x_1 \neq -1$, and 1 otherwise. Therefore, the orbits have length $p^3(p+1)$ if $x_1 \neq -1$ and $p^2(p+1)$ otherwise.

If we are in the case (A3), then (4.14) yields $\delta_{12}, \delta_{21} = 0$, namely δ is diagonal. In particular (4.15) is satisfied. H has rank 2 if $x_1 \neq 0$ and $x_2 \neq -1$, 0 if $x_1 = 0$ and $x_2 = -1$, and 1 otherwise. Therefore, the orbits have length $p^3(p+1)$ if $x_1 \neq 0$ and $x_2 \neq -1$, $p(p+1)$ if $x_1 = 0$ and $x_2 = -1$, and $p^2(p+1)$ otherwise.

If we are in the case (B2), then (4.14) yields

$$\begin{cases} \mu\delta_{12} = -(\mu+1)\delta_{21} \\ \mu(\delta_{12} - \delta_{11}) = \mu(\delta_{21} - \delta_{22}) \\ (\mu+1)(\delta_{12} - \delta_{11}) = (\mu+1)(\delta_{21} - \delta_{22}). \end{cases}$$

If $\mu = 0$ then $\delta_{21} = 0$ and $\delta_{12} = \delta_{11} - \delta_{22}$; if $\mu = -1$, then $\delta_{12} = 0$ and $\delta_{21} = \delta_{22} - \delta_{21}$; if $\mu \neq 0, -1$, then $\delta_{12} = -\frac{\mu+1}{\mu}\delta_{21}$ and $\frac{2\mu+1}{\mu}\delta_{21} = \delta_{22} - \delta_{11}$. Therefore, in all the cases, we have one choice for the elements δ_{12}, δ_{21}, and $(p-1)^2$ choices for δ_{11}, δ_{22}. Since T is scalar here, (4.15) is always satisfied. Moreover

$$H = \begin{pmatrix} -1 + \lambda^{-x_1} + \mu(1-\lambda^{-1})\lambda^{-x_1} & (\mu+1)(1-\lambda^{-1})\lambda^{-x_1} \\ -\mu(1-\lambda^{-1})\lambda^{-x_1} & -1 + \lambda^{-x_1} + (\mu+1)(1-\lambda^{-1})\lambda^{-x_1} \end{pmatrix}$$

has determinant $(1-\lambda^{-x_1})(1-\lambda^{-x_1-1})$, so that, since $x_1 \neq 0$, H has rank 2 if $x_1 \neq -1$, and 1 otherwise. Therefore the orbits have length $p^3(p+1)$ if $x_1 \neq -1$, and $p^2(p+1)$ if $x_1 = -1$.

In the case A*, proceeding as above we obtain as many conjugacy classes, with the same lengths, as in the case A.

Recap 4.5. *For G of type 7 and γ a GF on G with kernel of size p and such that $\gamma(A) \leq \mathrm{Inn}(G)$, we obtain the following.*

1. *$p^3(p+1)$ groups $(G, \circ)$ of type 5 form one class of length $p^3(p+1)$.*
2. *the groups $(G, \circ)$ of type 6 split in this way:*
   - *$p^2(p^2-1)$ groups form one class of length $p^2(p^2-1)$;*
   - *$p^3(p^2-1)$ groups form one class of length $p^3(p^2-1)$;*
   - *$p^2(p+1)$ groups form one class of length $p^2(p+1)$;*
   - *$2p^3(p+1)(q-2)$ groups split in $2(q-2)$ classes of length $p^3(p+1)$;*

   In total they split in $2q-1$ classes.
3. *the $2p^2(p+1) + p^3(p+1)(q-3)$ groups $(G, \circ)$ of type 7 split in*
   - *2 classes of length $p^2(p+1)$;*
   - *$q-3$ classes of length $p^3(p+1)$;*

   In total they split in $q-1$ classes.
4. *the groups $(G, \circ)$ of type 8 split in this way:*
   - *$p^2(p^2-1)$ groups isomorphic to G_2, which form one class of length $p^2(p^2-1)$.*
   - *$p^3(p^2-1)$ groups isomorphic to G_2, which form one class of length $p^3(p^2-1)$, and $2p^3(p^2-1)$ groups isomorphic to G_s, which split in two classes of length $p^3(p^2-1)$, for every $s \neq 2, s \in \mathcal{K}$.*
   - *$4p^2(p+1)$ groups isomorphic to G_s, which split in 4 classes of length $p^2(p+1)$, for every $s \in \mathcal{K}$.*

– $2p^3(p+1)(q-3)$ *groups isomorphic to* G_s*, which split in* $2(q-3)$ *classes of length* $p^3(p+1)$*, for every* $s \in \mathcal{K}$*.*

In total they split in $2q$ *classes for every* G_s*.*

5. *the groups* $(G, \circ)$ *of type 9 split in this way:*

   – $p(p+1)$ *groups form one class of length* $p(p+1)$*;*
   – $p^3(p+1)(q-2)$ *groups split in* $(q-2)$ *classes of length* $p^3(p+1)$*;*
   – *if* $q = 3$*,* $p^2(p^2-1)$ *groups form one class of length* $p^2(p^2-1)$*;*
   – *if* $q > 3$*,* $p^3(p^2-1)$ *groups form one class of length* $p^3(p^2-1)$*;*

   In total they split in q *classes.*

Recap 4.6. *For* G *of type 8,* $G \simeq G_k$*, and* γ *a GF on* G *with kernel of size* p*, we obtain the following.*

1. $2p^2$ *groups* $(G, \circ)$ *of type 5 which split in two classes of length* p^2*.*

2. *The groups* $(G, \circ)$ *of type 6 split in this way:*

   – $2p$ *groups split in two classes of length* p*;*
   – $4p^2(q-2)$ *groups split in* $4(q-2)$ *classes of length* p^2*;*
   – $4p(p-1)$ *groups split in* 4 *classes of length* $p(p-1)$*;*
   – $6p^2(p-1)$ *groups split in* 6 *classes of length* $p^2(p-1)$*.*

   Therefore in total $4(q+1)$ *classes.*

3. *The* $4p + 2p^2(q-3)$ *groups* $(G, \circ)$ *of type 7 split in*

   – 4 *classes of length* p*;*
   – $2(q-3)$ *classes of length* p^2*.*

   In total $2(q-1)$ *classes.*

4. *The groups* $(G, \circ)$ *of type 8 split in this way:*

   – *the cases (A3),(A3*) yield* $1 + 2p + p^2(2q-5)$ *groups isomorphic to* G_{-k}*,* $4p + 2p^2(q-3)$ *groups isomorphic to* G_s *for every* $s \neq -k, s \in \mathcal{K}$*,* $1+2p+p^2(2q-5)$ *groups isomorphic to* $G_{-k^{-1}}$ *and* $4p+2p^2(q-3)$ *groups isomorphic to* G_s *for every* $s \neq -k^{-1}, s \in \mathcal{K}$*.*
   Therefore there are $2 + 4p + 2p^2(2q-5)$ *groups isomorphic to* G_{-k}*, which split in two classes of length* 1*,* 4 *classes of length* p*, and* $2(2q-5)$ *classes of length* p^2*, and* $8p+4p^2(q-3)$ *groups isomorphic to* G_s*, for every* $s \neq -k, s \in \mathcal{K}$*, which split in* 8 *classes of length* p*, and* $4(q-3)$ *classes of length* p^2*.*
   In total there are $4(q-1)$ *conjugacy classes of groups isomorphic to* G_s *for every* $s \in \mathcal{K}$*.*

- *The cases (A1),(A1*) yield the following. If one among* k, k^{-1} *is equal to* $q-2$*, then there are* $p(p-1)+3p^2(p-1)$ *groups isomorphic to* G_2 *and* $4p^2(p-1)$ *groups isomorphic to* G_s*, for every* $s \neq q-2, s \in \mathcal{K}$*. Otherwise both* $k, k^{-1} \neq q-2$*, and there are* $2p(p-1)+2p^2(p-1)$ *groups isomorphic to* G_{1+k} *if* $G_{1+k} \simeq G_{1+k^{-1}}$*,* $p(p-1)+3p^2(p-1)$ *groups isomorphic to* G_s *for* $s = 1+k, 1+k^{-1}$ *if* $G_{1+k} \not\simeq G_{1+k^{-1}}$*, and* $4p^2(p-1)$ *groups isomorphic to* G_s*, for every* $s \neq 1+k$*,* $1+k^{-1}$*,* $s \in \mathcal{K}$*.*

  We obtain two classes of length $p(p-1)$ *and two classes of length* $p^2(p-1)$ *in the first case, one class of length* $p(p-1)$ *and* 3 *classes of length* $p^2(p-1)$ *in the second case, and* 4 *classes of length* $p^2(p-1)$ *in the last case.*

  In total there are 4 *conjugacy classes of groups isomorphic to* G_s *for every* $s \in \mathcal{K}$*.*

- *The cases (A2),(A2*),(B1),(B1*) yield the following. If one among* k, k^{-1} *is equal to* 2*, then there are* $2p(p-1)+6p^2(p-1)$ *groups isomorphic to* G_2*, and* $8p^2(p-1)$ *groups isomorphic to* G_s *for every* $s \neq 2, s \in \mathcal{K}$*. Otherwise both* $k, k^{-1} \neq 2$*, and there are* $4p(p-1)+4p^2(p-1)$ *groups isomorphic to* G_{1-k} *if* $G_{1-k} \simeq G_{1-k^{-1}}$*,* $2p(p-1)+6p^2(p-1)$ *groups isomorphic to* G_s *for* $s = 1-k, 1-k^{-1}$ *if* $G_{1-k} \not\simeq G_{1-k^{-1}}$*, and* $8p^2(p-1)$ *groups isomorphic to* G_s*, for every* $s \neq 1-k, 1-k^{-1}, s \in \mathcal{K}$ *.*

  We obtain 4 *classes of length* $p(p-1)$ *and* 4 *classes of length* $p^2(p-1)$ *in the first case, two classes of length* $p(p-1)$ *and* 6 *classes of length* $p^2(p-1)$ *in the second case, and* 8 *classes of length* $p^2(p-1)$ *in the last case.*

  In total there are 8 *conjugacy classes of groups isomorphic to* G_s *for every* $s \in \mathcal{K}$*.*

In total there are $4(q+2)$ *classes for every* G_s*.*

5. *the groups* $(G, \circ)$ *of type 9 split in this way:*

   - *the cases (A3),(A3*) yield* $4p+2p^2(q-3)$ *groups, which split in* 4 *classes of length* p*, and* $2(q-3)$ *classes of length* p^2*;*
   - *the cases (A1),(A1*) yield* $p(p^2-1)+p^2(p^2-1)$ *groups if one among* k, k^{-1} *is equal to* $q-2$ *(namely if* $G \simeq G_{-2}$*) and* $2p^2(p-1)$ *groups if both* $k, k^{-1} \neq q-2$ *(so* $G \not\simeq G_{-2}$*). We obtain one class of length* $p(p-1)$ *plus one class of length* $p^2(p-1)$ *in the first case, and two classes of length* $p^2(p-1)$ *in the second case.*
   - *the cases (A2),(A2*),(B1),(B1*) yield* $2p(p^2-1)+2p^2(p^2-1)$ *groups if* $G \simeq G_2$*, and* $4p^2(p-1)$ *groups if* $G \not\simeq G_2$*. We obtain two classes of length* $p(p-1)$ *plus two classes of length* $p^2(p-1)$ *in the first case, and* 4 *classes of length* $p^2(p-1)$ *in the second case.*

In all the cases in total there are $2(q+2)$ classes.

Recap 4.7. *For G of type 9 and γ a GF on G with kernel of size p, we obtain the following.*

1. *the $2p^2$ groups $(G,\circ)$ of type 5 form one class of length $2p^2$.*
2. *the groups $(G,\circ)$ of type 6 split in this way:*
   - *$2p$ groups form one class of length $2p$;*
   - *$4p^2(q-2)$ groups split in $2(q-2)$ classes of length $2p^2$;*
   - *$6p(p-1)$ groups split in 3 classes of length $2p(p-1)$;*
   - *$4p^2(p-1)$ groups split in 2 classes of length $2p^2(p-1)$;*

   In total there are $2(q+1)$ classes.
3. *the $2+2p^2(q-2)$ groups $(G,\circ)$ of type 7 split in*
   - *1 class of length 2;*
   - *$q-2$ classes of length $2p^2$;*

   In total there are $q-1$ classes.
4. *the groups $(G,\circ)$ of type 8 split in this way:*
   - *$8p$ groups isomorphic to G_k, which split in 4 classes of length $2p$, for every $k \in \mathcal{K}$.*
   - *$4p^2(q-3)$ groups isomorphic to G_k, which split in $2(q-3)$ classes of length $2p^2$, for every $k \in \mathcal{K}$.*
   - *$4p(p-1)$ groups isomorphic to G_2, which split in two classes of length $2p(p-1)$.*
   - *$12p^2(p-1)$ groups isomorphic to G_k, which split in 6 classes of length $2p^2(p-1)$, for every $k \neq 2$, $k \in \mathcal{K}$, and $8p^2(p-1)$ groups isomorphic to G_2 which split in 4 classes of length $2p^2(p-1)$.*

   In total there are $2(q+2)$ classes for every G_k.
5. *the groups $(G,\circ)$ of type 9 split in this way:*
   - *$4p$ groups split in two classes of length $2p$;*
   - *$2p^2(q-3)$ groups split in $q-3$ classes of length $2p^2$;*
   - *if $q=3$ there are further $2p(p-1)+4p^2(p-1)$ groups, which split in one class of length $2p(p-1)$ and two classes of length $2p^2(p-1)$;*
   - *if $q>3$, there are further $6p^2(p-1)$ groups, which split in 3 classes of length $2p^2(p-1)$.*

   In total there are $q+2$ classes.

4.4.6 The case $|\ker(\gamma)| = 1$

The GF's of this case can be divided into subclasses according to the size of $\ker(\tilde{\gamma})$. Those for which $|\ker(\tilde{\gamma})| \neq 1$ can be recovered via duality from the previous computations applied to $\tilde{\gamma}$. For the others, for which $|\ker(\tilde{\gamma})| = 1$, we will use Proposition 1.26.

We recall that $\tilde{\gamma}(x) = \gamma(x^{-1})\iota(x^{-1})$ for all $x \in G$, so $|\ker(\tilde{\gamma})| \neq 1$ means that there exists $x_0 \in G$, $x_0 \neq 1$, such that

$$\gamma(x_0) = \iota(x_0^{-1}) \tag{4.17}$$

whereas the condition $|\ker(\gamma)| = 1$ corresponds to

$$\tilde{\gamma}(x) \neq \iota(x^{-1}), \text{ for each } x \in G, x \neq 1. \tag{4.18}$$

Clearly, when $|\ker(\tilde{\gamma})| = p^2q$, $\gamma = \tilde{\tilde{\gamma}}$ corresponds to the left regular representation, and this gives one group of the same type as G.

In the remaining cases for which $q \mid |\ker(\tilde{\gamma})|$, the condition (4.18) is not fulfilled, so none of the corresponding γ's has trivial kernel.

Consider now the GF's γ for which $p \mid |\ker(\tilde{\gamma})|$ (and $q \nmid |\ker(\tilde{\gamma})|$). Here $\gamma(a) = \iota(a^{-\sigma})$, where σ has 1, but not 0, as eigenvalue (because $p \mid |\ker(\tilde{\gamma})|$ and γ is injective). Therefore, for each $a \in A$, we have that $\tilde{\gamma}(a) = \gamma(a^{-1})\iota(a^{-1}) = \iota(a^{\sigma-1})$.

Suppose first $\sigma = 1$. Then $|\ker(\tilde{\gamma})| = p^2$ and $\gamma(a) = \iota(a^{-1})$. Therefore $p^2 \mid |\gamma(G)|$, and $\ker(\gamma)$ can have size 1 or q. We have $|\ker(\gamma)| = 1$ if and only if (4.18) is satisfied, and by Subsection 4.4.4, $\tilde{\gamma}(b) = \iota(b^{-1})$ if and only if $x_1 = x_2 = -1$. Therefore, the p^2 GF's $\tilde{\gamma}$ corresponding to $(G, \circ)$ of type 5 are such that the corresponding γ have kernel of size q, and all the others $\tilde{\gamma}$ correspond to γ with kernel of size 1.

Suppose now that $\sigma \neq 1$. Since σ has 1 as eigenvalue, then $|\ker(\tilde{\gamma})| = p$, and if $a_0 \in A$ generates $\ker(\tilde{\gamma})$, then $\gamma(a_0) = \iota(a_0^{-1})$, namely $p \mid \gamma(G)$. Moreover, since 0 is not an eigenvalue for σ, $p \nmid |\ker(\gamma)|$. Therefore, again, $\ker(\gamma)$ can have size 1 or q. By Subsection 4.4.5, the $\tilde{\gamma}$'s such that $p \mid |\ker(\tilde{\gamma})|$ and $p \nmid |\ker(\gamma)|$ are those of the cases A1 and A1*. Moreover, for every $\tilde{\gamma}$ belonging to these cases the condition (4.18) is satisfied, namely the corresponding γ are injective.

We are left with the case where $|\ker(\gamma)| = |\ker(\tilde{\gamma})| = 1$, which can happen only for G of type 9 and, if $q = 2$, for G of type 7 (see the discussion in Subsubsection 4.4.1.1). In the following we suppose that G is of type 9 and σ has no eigenvalues 0 or 1.

Here $\gamma(G) = \langle\, \iota(a_1), \iota(a_2), \beta \,\rangle$, where $\beta \neq 1$. As in Subsubsection 4.4.1.3, if b is an element of order q fixed by β, we can assume $\gamma(b) = \iota(a_*)\beta$ for some $a_* \in A^\sigma$, and $\beta = \beta_1^{x_1}\beta_2^{x_2}$. As usual, denote by T the matrix of $\gamma(b)_{|A}$ with respect to the basis $\{a_1, a_2\}$. The discussion in Subsection 4.4.1 yields equation (2.2), which in our notation here is

$$(\sigma^{-1} - 1)^{-1}T(\sigma^{-1} - 1) = TZ. \tag{4.19}$$

Now T and TZ, being conjugate, have the same eigenvalues, so that $\lambda^{-x_2} = \lambda^{x_1+1}$. Therefore $T = \mathrm{diag}(\lambda^{x_1}, \lambda^{1+x_1})$, and $\sigma^{-1}-1$ exchanges the two eigenspaces, so

$$\sigma^{-1} - 1 = \begin{pmatrix} 0 & s_1 \\ s_2 & 0 \end{pmatrix} \tag{4.20}$$

with the conditions $s_1, s_2 \neq 0$ (due to our assumptions on the eigenvalues of σ) and $s_1 s_2 \neq 1$.

4.4.6.1 Invariant Sylow q-subgroups

We will show that also in this case there always exists at least one invariant Sylow q-subgroup. By the discussion above $\gamma(b) = \iota(a_*)\beta_1^{x_1}\beta_2^{-(x_1+1)}$, for some $a_* \in A^\sigma$ and $0 \leq x_1 < q$.

By Subsubsection 4.4.1.3 there exists an invariant Sylow q-subgroup, $\langle\, b^x \,\rangle$ where $x \in A$, if and only if the equation (4.8), namely

$$x^{(1-Z^{-1})M} = a_*^{(1-Z^{-1})T}$$

where $M = 1 - (1 + T^{-1}\sigma(1 - Z^{-1}))T$, has a solution in x.

Here

$$M = \begin{pmatrix} 1 - \lambda^{x_1} - \frac{(1-\lambda^{-1})}{1-s_1s_2} & \frac{s_1\lambda(1-\lambda)}{1-s_1s_2} \\ \frac{s_2\lambda^{-1}(1-\lambda^{-1})}{1-s_1s_2} & 1 - \lambda^{x_1+1} - \frac{(1-\lambda)}{1-s_1s_2} \end{pmatrix},$$

and since $\det(1 - Z^{-1}) \neq 0$ and $\det(M) = (1 - \lambda^{x_1})(1 - \lambda^{x_1+1})$, we have the following.

1. If $x_1 \neq 0, -1$, then M has rank 2 and the system (4.8) admits a unique solution.

2. If $x_1 = 0$, then, writing $a_* = a_1^x a_2^y$, the system (4.8) admits solutions if and only if $y = -s_1 x$. Moreover, in that case there are p solutions.

   If $y \neq -s_1 x$, then there are no GF on G extending the assignment $\gamma(b) = \iota(a_*)\beta$, as the condition (4.10) is not satisfied.

3. If $x_1 = -1$, then (4.8) admits p solutions if and only if $a_* = a_1^{-s_2 y} a_2^y$. Reasoning as above, if $x \neq -s_2 y$ there are no GF on G extending the assignment $\gamma(b) = \iota(a_*)\beta$.

4.4.6.2 Computations

By the discussion in Subsection 2.2.3 we can count the GF's as follows.

– Choose $\sigma \in \mathrm{GL}(2, p)$ without eigenvalues 1, and a RGF $\gamma : B \to \mathrm{Aut}(G)$ such that σ and γ satisfy (1.14) (q choices for γ corresponding to $\gamma(b) = \beta_1^{x_1}\beta_2^{-(x_1+1)}$ and $(p-1)(p-2)$ choices for σ as in equation (4.20)).

– By Proposition 1.26 each such assignment defines a unique function γ, and the GF's obtained in this way are distinct for $x_1 \neq 0, -1$ (namely when $\gamma(G)$ is centerless) and each of them is obtained p times when $x_1 = 0$ or -1 (namely when $Z(\gamma(G))$ is non trivial).

Now, let γ be a GF obtained for a choice of σ, B, x_1. Since γ is injective, $(G, \circ)$ is isomorphic to $\gamma(G)$. We have

$$\gamma(b)^{-1}\gamma(a)\gamma(b) = \gamma(b)^{-1}\iota(a^{-\sigma})\gamma(b) = \iota(a^{-\sigma T}) = \gamma(a^{\sigma T\sigma^{-1}}),$$

from which we obtain,

$$b^{\ominus 1} \circ a \circ b = a^{\sigma T\sigma^{-1}}.$$

Since $a^{\circ k} = a^k$, the action of $\iota(b)$ on A in $(G, \circ)$ is

$$Z_\circ \sim \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{x_1+1} \end{pmatrix}.$$

We obtain the following groups $(G, \circ)$.

Type 5 does not arise.

Type 6 when $x_1 = 0$ or $x_1 = -1$ and there are $2p(p-1)(p-2)$ groups.

Type 7 does not arise.

Type 8 when $x_1 \neq 0, -1, (q-1)/2$ and there are $p^2(p-1)(p-2)(q-3)$ groups. They are $2p^2(p-1)(p-2)$ groups isomorphic to G_s for every $s \in \mathcal{K}$.

Type 9 when $x_1 = (q-1)/2$ and there are $p^2(p-1)(p-2)$ groups.

As to the conjugacy classes, in the notation of Subsubsection 4.4.1.4, let $\varphi = \iota(x)\delta\psi \in \mathrm{Aut}(G)$. We have

$$\gamma^\varphi(a) = \varphi^{-1}\gamma(a^{S\delta^{-1}})\varphi = \psi^{-1}\delta^{-1}\iota(a^{-S\delta^{-1}\sigma})\delta\psi = \iota(a^{-S\delta^{-1}\sigma\delta S}),$$

so that $\gamma^\varphi(a) = \gamma(a)$ if and only if $\sigma^{-1}\delta S\sigma = \delta S$. The last condition yields $\delta_{22} = \delta_{11}$ if $S = 1$, and $\delta_{22} = \frac{s_2}{s_1}\delta_{11}$ if $S \neq 1$.

Now,

$$\gamma^\varphi(b) = \varphi^{-1}\gamma(b^{\varphi^{-1}})\varphi = \varphi^{-1}\gamma(x^{1-Z^{-r}}b^r)\varphi;$$

suppose first $\psi = 1$. Using Proposition 1.26, we obtain

$$\begin{aligned}
\gamma^\varphi(b) &= \varphi^{-1}\gamma(x^{1-Z^{-1}}b)\varphi \\
&= \varphi^{-1}\iota(x^{-(1-Z^{-1})T^{-1}\sigma})\beta\varphi \\
&= \delta^{-1}\iota(x^{-1+T^{-1}-(1-Z^{-1})T^{-1}\sigma})\beta\delta \\
&= \iota(x^{(-1+T^{-1}-(1-Z^{-1})T^{-1}\sigma)\delta})\beta,
\end{aligned}$$

so that $\gamma^\varphi(b) = \gamma(b)$ if and only if the system $x^{H_1} = 1$, where $H_1 := -1+T^{-1}-(1-Z^{-1})T^{-1}\sigma$, admits a solution. Since $\det(H_1) = (1-\lambda^{-x_1})(1-\lambda^{-x_1-1})$, there is one solution if $x_1 \neq 0, -1$, and p solutions otherwise.

Suppose now that $\psi \neq 1$. Since $\gamma(b^{-1}) = \beta^{-1}$, we have

$$\begin{aligned}\gamma^\varphi(b) &= \varphi^{-1}\gamma(x^{1-Z}b^{-1})\varphi \\ &= \varphi^{-1}\iota(x^{-(1-Z)T\sigma})\gamma(b^{-1})\varphi \\ &= \varphi^{-1}\iota(x^{-(1-Z)T\sigma})\beta^{-1}\varphi \\ &= \psi\delta^{-1}\iota(x^{-1+T-(1-Z)T\sigma})\beta^{-1}\delta\psi \\ &= \psi\iota(x^{(-1+T-(1-Z)T\sigma)\delta})\beta^{-1}\psi.\end{aligned}$$

If $H_2 := -1 + T - (1-Z)T\sigma$, we have that $\gamma^\varphi(b) = \gamma(b)$ if and only if

$$\iota(x^{H_2\delta})\beta^{-1} = \psi\beta\psi,$$

namely if and only if

$$\begin{cases} x^{H_2} = 1 \\ T^{-1} = STS. \end{cases}$$

Since $\det(H_2) = (1-\lambda^{x_1})(1-\lambda^{x_1+1})$, the system $x^{H_2} = 1$ has one solution if $x_1 \neq 0, -1$ and p solutions otherwise, while the condition $T^{-1} = STS$ is satisfied if and only if $x_1 = \frac{q-1}{2}$.

We obtain the following.

1. if $x_1 = 0, -1$, then the stabiliser has order $p(p-1)$. Here there are $2p(p-1)(p-2)$ groups $(G, \circ)$ of type 6, so that there are $p-2$ orbits of length $2p(p-1)$.

2. if $x_1 = \frac{q-1}{2}$, then $(G, \circ)$ is of type 9, and the stabiliser has order $2(p-1)$. Since there are $p^2(p-1)(p-2)$ groups, they split in $p-2$ orbits of length $p^2(p-1)$.

3. if $x_1 \neq 0, -1, \frac{q-1}{2}$, then $(G, \circ)$ is of type 8, and the stabiliser has order $p-1$. Since for every $s \in \mathcal{K}$ there are $2p^2(p-1)(p-2)$ groups isomorphic to G_s, they split in $p-2$ classes for every $s \in \mathcal{K}$.

If G is of type 7 and $q = 2$, reasoning as for the type 9 we find $2p(p-1)(p-2) \cdot \frac{1}{2}p(p+1) = p^2(p^2-1)(p-2)$ groups $(G, \circ)$ of type 6, which split in $p-2$ classes of length $p^2(p^2-1)$.

4.4.7 Results

For the type 8 and 9 we summarise our results in the following propositions. For the type 7 the results of this section, together with those in the next section, are collected in Proposition 4.10.

Proposition 4.8. *Let G be a group of order p^2q, $p > 2$, of type 9. Then in* $\mathrm{Hol}(G)$ *there are:*

1. *$4p^2$ groups of type 5, which split in two conjugacy classes of length p^2, and one conjugacy class of length $2p^2$;*

2. *$2p^2(4q + 3p - 7)$ groups of type 6, which split in 4 conjugacy classes of length $2p$, $4(q-2)$ conjugacy classes of length $2p^2$, $p+4$ conjugacy classes of length $2p(p-1)$, and two conjugacy classes of length $2p^2(p-1)$;*

   in total there are $4q + p + 2$ conjugacy classes;

3. *$2+4p+2p^2(2q-5)$ groups of type 7, which split in one conjugacy class of length 2, two conjugacy classes of length $2p$, and $2q-5$ conjugacy classes of length $2p^2$;*

   in total there are $2(q-1)$ conjugacy classes;

4. – *$2p(p^3+3p^2-14p+4pq-6)$ groups of type 8 isomorphic to G_2, which split in 8 conjugacy classes of length $2p$, $4(q-3)$ conjugacy classes of length $2p^2$, two conjugacy classes of length $2p(p-1)$, and $p+4$ conjugacy classes of length $2p^2(p-1)$;*
   – *for every $s \neq 2$, $s \in \mathcal{K}$, $2p(p^3 + 5p^2 - 18p + 4pq + 8)$ groups of type 8 isomorphic to G_s, which split in 8 conjugacy classes of length $2p$, $4(q-3)$ conjugacy classes of length $2p^2$, and $p+6$ conjugacy classes of length $2p^2(p-1)$;*

   in both the cases in total there are $4q + p + 2$ conjugacy classes for every isomorphism class G_s;

5. *if $q > 3$, $2 + 4p + p^2(p^2 + 5p + 4q - 16)$ groups of type 9, which split in two conjugacy classes of length 1, $2(q-2)$ conjugacy classes of length p^2, two conjugacy classes of length $2p$, $q-3$ conjugacy classes of length $2p^2$, $p-2$ conjugacy classes of length $p^2(p-1)$, and 4 conjugacy classes of length $2p^2(p-1)$;*

   in total there are $3q + p - 1$ conjugacy classes;

6. *if $q = 3$, $2 + 2p + p^3(p+3)$ groups of type 9, which split in two conjugacy classes of length 1, two conjugacy classes of length p^2, two conjugacy classes of length $2p$, $p-2$ conjugacy classes of length $p^2(p-1)$, one conjugacy class of length $2p(p-1)$, and 3 conjugacy classes of length $2p^2(p-1)$;*

   in total there are $8 + p$ conjugacy classes.

Proposition 4.9. *Let G be a group of order p^2q, $p > 2$, of type 8, so that G is isomorphic to G_k, where $k \neq 0, 1, -1$ determines the isomorphism class of G. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $4p^2$ *groups of type 5, which split in* 4 *conjugacy classes of length* p^2*;*

2. $8p^2(q+p-2)$ *groups of type 6, which split in* 8 *conjugacy classes of length* p*,* $8(q-2)$ *conjugacy classes of length* p^2*,* 8 *conjugacy classes of length* $p(p-1)$*, and* 8 *conjugacy classes of length* $p^2(p-1)$*;*

   in total there are $8(q+1)$ *conjugacy classes;*

3. $8p + 4p^2(q-3)$ *groups of type 7, which split in* 8 *conjugacy classes of length* p*, and* $4(q-3)$ *conjugacy classes of length* p^2*;*

   in total there are $4(q-1)$ *conjugacy classes;*

4. *if* G *is not isomorphic to* $G_{\pm 2}$*, then* $q > 5$ *and there are further*

   (a) *if either* k *or* k^{-1} *is a solution of* $x^2 - x - 1 = 0$*,*

      i. $2(1+5p+4p^2q-17p^2+7p^3)$ *groups of type 8 isomorphic to* G_s*, for* $s = k, 1-k$*, which split in two conjugacy classes of length* 1*,* 12 *conjugacy classes of length* p*,* $2(4q-11)$ *conjugacy classes of length* p^2*, two conjugacy classes of length* $p(p-1)$*, and* 14 *conjugacy classes of length* $p^2(p-1)$*;*

      ii. $4(3p + 2p^2q - 8p^2 + 3p^3)$ *groups of type 8 isomorphic to* G_{1+k}*, which split in* 16 *conjugacy classes of length* p*,* $8(q-3)$ *conjugacy classes of length* p^2*,* 4 *conjugacy classes of length* $p(p-1)$*, and* 12 *conjugacy classes of length* $p^2(p-1)$*;*

      iii. $8(2p + p^2q - 5p^2 + 2p^3)$ *groups of type 8 isomorphic to* G_s *for every* $s \in \mathcal{K}$*,* $s \neq k, 1+k, 1-k$*, which split in* 16 *conjugacy classes of length* p*,* $8(q-3)$ *conjugacy classes of length* p^2*, and* 16 *conjugacy classes of length* $p^2(p-1)$*;*

   in total there are $8(q+1)$ *conjugacy classes for every isomorphism class* G_s*;*

   (b) *if* k *and* k^{-1} *are the solutions of* $x^2 + x + 1 = 0$*,*

      i. $2(1+6p+4p^2q-19p^2+8p^3)$ *groups of type 8 isomorphic to* G_k*, which split in two conjugacy classes of length* 1*,* 12 *conjugacy classes of length* p*,* $2(4q-11)$ *conjugacy classes of length* p^2*, and* 16 *conjugacy classes of length* $p^2(p-1)$*;*

      ii. $2(1+4p+4p^2q-15p^2+6p^3)$ *groups of type 8 isomorphic to* G_{1+k}*, which split in two conjugacy classes of length* 1*,* 12 *conjugacy classes of length* p*,* $2(4q-11)$ *conjugacy classes of length* p^2*,* 4 *conjugacy classes of length* $p(p-1)$*, and* 16 *conjugacy classes of length* $p^2(p-1)$*;*

      iii. $2(7p+4p^2q-18p^2+7p^3)$ *groups of type 8 isomorphic to* G_s *for* $s = 1-k, 1-k^{-1}$*, which split in* 16 *conjugacy classes of length* p*,* $8(q-3)$ *conjugacy classes of length* p^2*, two conjugacy classes of length* $p(p-1)$*, and* 14 *conjugacy classes of length* $p^2(p-1)$*;*

iv. $8(2p+p^2q-5p^2+2p^3)$ *groups of type 8 isomorphic to* G_s *for every* $s \in \mathcal{K}$, $s \neq k, 1+k, 1-k, 1-k^{-1}$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

in total there are $8(q+1)$ *conjugacy classes for every isomorphism class* G_s;

(c) if k *and* k^{-1} *are the solutions of* $x^2-x+1=0$, *we obtain as many groups as in the previous case, but the isomorphism class depends on* $-k$ *instead of* k.

(d) if k *and* k^{-1} *are the solutions of* $x^2+1=0$,

i. $4(1+2p+2p^2q-9p^2+4p^3)$ *groups of type 8 isomorphic to* G_k, *which split in* 4 *conjugacy classes of length* 1, 8 *conjugacy classes of length* p, $4(2q-5)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

ii. $4(3p+2p^2q-8p^2+3p^3)$ *groups of type 8 isomorphic to* G_s, *for* $s = 1+k, 1-k$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, 4 *conjugacy classes of length* $p(p-1)$, *and* 12 *conjugacy classes of length* $p^2(p-1)$;

iii. $8(2p+p^2q-5p^2+2p^3)$ *groups of type 8 isomorphic to* G_s *for every* $s \in \mathcal{K}$, $s \neq k, 1+k, 1-k$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

in total there are $8(q+1)$ *conjugacy classes for every isomorphism class* G_s;

(e) if k *is not a solution of* $x^2-x-1=0$, $x^2+x-1=0$, $x^2+x+1=0$, $x^2-x+1=0$, $x^2+1=0$,

i. $2(1+6p+4p^2q-19p^2+8p^3)$ *groups of type 8 isomorphic to* G_s *for* $s = k, -k$, *which split in two conjugacy classes of length* 1, 12 *conjugacy classes of length* p, $2(4q-11)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

ii. $2(7p+4p^2q-18p^2+7p^3)$ *groups of type 8 isomorphic to* G_s *for* $s = 1+k, 1+k^{-1}, 1-k, 1-k^{-1}$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, *two conjugacy classes of length* $p(p-1)$, *and* 14 *conjugacy classes of length* $p^2(p-1)$;

iii. $8(2p+p^2q-5p^2+2p^3)$ *groups of type 8 isomorphic to* G_s *for every* $s \in \mathcal{K}$, $s \neq k, 1+k, 1-k, 1-k^{-1}, 1+k^{-1}, -k$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

in total there are $8(q+1)$ *conjugacy classes for every isomorphism class* G_s;

(f) $4p(2+p(q+2p-5))$ *groups of type 9, which split in* 8 *conjugacy classes of length* p, $4(q-3)$ *conjugacy classes of length* p^2, *and* 8 *conjugacy classes of length* $p^2(p-1)$;
in total there are $4(q+1)$ *conjugacy classes;*

5. *if* G *is isomorphic to* G_k *for* $k=\pm 2$ *and* $q>5$, *then there are further*

(a) $2(1+5p+4p^2q-17p^2+7p^3)$ *groups of type 8 isomorphic to* G_2, *which split in two conjugacy classes of length* 1, 12 *conjugacy classes of length* p, $2(4q-11)$ *conjugacy classes of length* p^2, *two conjugacy classes of length* $p(p-1)$, *and* 14 *conjugacy classes of length* $p^2(p-1)$;
in total there are $8(q+1)$ *conjugacy classes for every isomorphism class* G_s;

(b) *if* $q=7$,

i. $2(1+4p+13p^2+6p^3)$ *groups of type 8 isomorphic to* G_3, *which split in two conjugacy classes of length* 1, 12 *conjugacy classes of length* p, $2(4q-11)$ *conjugacy classes of length* p^2, 4 *conjugacy classes of length* $p(p-1)$, *and* 12 *conjugacy classes of length* $p^2(p-1)$;
in total there are 64 *conjugacy classes for every isomorphism class* G_s;

(c) *if* $q>7$,

i. $2(1+6p+4p^2q-19p^2+8p^3)$ *groups of type 8 isomorphic to* G_{-2}, *which split in two conjugacy classes of length* 1, 12 *conjugacy classes of length* p, $2(4q-11)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

ii. $2(7p+4p^2q-18p^2+7p^3)$ *groups of type 8 isomorphic to* G_s, *for* $s=3,\frac{3}{2}$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, *two conjugacy classes of length* $p(p-1)$ *and* 14 *conjugacy classes of length* $p^2(p-1)$;

iii. $8(2p+p^2q-5p^2+2p^3)$ *groups of type 8 isomorphic to* G_s, *for every* $s\in\mathcal{K}, s\neq 3,\frac{q+3}{2},2,q-2$, *which split in* 16 *conjugacy classes of length* p, $8(q-3)$ *conjugacy classes of length* p^2, *and* 16 *conjugacy classes of length* $p^2(p-1)$;

in total there are $8(q+1)$ *conjugacy classes for every isomorphism class* G_s;

(d) $2p(3+p(2q+3p-8))$ *groups of type 9, which split in* 8 *conjugacy classes of length* p, $4(q-3)$ *conjugacy classes of length* p^2, *two conjugacy classes of length* $p(p-1)$, *and* 6 *conjugacy classes of length* $p^2(p-1)$;
in total there are $4(q+1)$ *conjugacy classes;*

6. *If* $q=5$, *then* G *is isomorphic to* G_2 *and there are further*

(a) $4(1+p+3p^2(p+1))$ *groups of type 8 isomorphic to* G_2*, which split in* 4 *conjugacy classes of length* 1*,* 8 *conjugacy classes of length* p*,* 20 *conjugacy classes of length* p^2*,* 4 *conjugacy classes of length* $p(p-1)$*, and* 12 *conjugacy classes of length* $p^2(p-1)$*;*

in total there are 48 *conjugacy classes for every isomorphism class* G_s*;*

(b) $8p(1+p+2p(p^2-1))$ *groups of type 9, which split in* 8 *conjugacy classes of length* p*,* 8 *conjugacy classes of length* p^2*,* 4 *conjugacy classes of length* $p(p-1)$*, and* 4 *conjugacy classes of length* $p^2(p-1)$*.*

in total there are 24 *conjugacy classes;*

Proof. For the types 5, 6, 7 and 9, the number of $(G,\circ)$ is obtained just summing up the results in Sections 4.4.2, 4.4.3, 4.4.4, 4.4.5 and 4.4.6.

If $(G,\circ)$ is of type 8 and $q=5$, then there is only one isomorphism class of groups of type 8, so that also in this case we obtain the number of $(G,\circ)\simeq G_2$ simply summing up the results in the previous sections.

Suppose now $(G,\circ)$ of type 8 and $q>5$. To obtain the total number of $(G,\circ)$ for every isomorpism class of groups of type 8, we have to distinguish some cases.

Suppose first $k=\pm 2$, then by Subsections 4.4.4 and 4.4.5 the number of $(G,\circ)$ of type 8 depends on the isomorphis classes of the groups $G_2, G_3, G_{\frac{3}{2}}$ and G_{-2}. Since two groups of type 8, say G_{k_1} and G_{k_2}, are isomorphic if and only if $k_1=k_2$ or $k_1k_2=1$, in this case we have that the $G_3\simeq G_{\frac{3}{2}}\simeq G_{-2}\not\simeq G_2$ if $q=7$, and that $G_2, G_3, G_{\frac{3}{2}}$ and G_{-2} represent different isomorphism classes if $q>7$.

Suppose now $k\neq\pm 2$. By Subsections 4.4.4 and 4.4.5 the number of $(G,\circ)$ of type 8 depends on the isomorphis classes of the groups G_k, $G_{1+k^{-1}}$, G_{1+k}, $G_{1-k^{-1}}$, G_{1-k} and G_{-k}.

Suppose 5 is a quadratic residue modulo q; then $G_k\simeq G_{1+k^{-1}}$, $G_{1+k}\simeq G_{1-k^{-1}}$ and $G_{1-k}\simeq G_{-k}$ if and only if k is a solution of $x^2-x-1=0$. Moreover $G_k\simeq G_{1+k}$, $G_{1+k^{-1}}\simeq G_{1-k}$ and $G_{1-k^{-1}}\simeq G_{-k}$ if and only if k is a solution of $x^2+x-1=0$. Note also that if k is a solution of $x^2-x-1=0$, then k^{-1} is a solution of $x^2+x-1=0$. Therefore if $G\simeq G_k$ and either k or k^{-1} are solutions of $x^2-x-1=0$ then the groups above are in three different isomorphism classes, namely $G_k\simeq G_{1+k^{-1}}$, $G_{1+k}\simeq G_{1-k^{-1}}$, and $G_{1-k}\simeq G_{-k}$.

Suppose $q-3$ is a quadratic residue modulo q; then $G_{1+k^{-1}}\simeq G_{1+k}\simeq G_{-k}$ if and only if k is a solution of $x^2+x+1=0$. In that case k^{-1} is the other solution, and the groups above are in four different isomorphism classes. Similarly, if k is a solution of $x^2-x+1=0$ there are four different isomorphism classes. Note moreover that if α_1, α_2 are the solutions of $x^2+x+1=0$, then the solutions of $x^2-x+1=0$ are $-\alpha_1, -\alpha_2$. Therefore the last case can be obtained by the previous one changing k in $-k$.

Lastly suppose $q-4$ is a quadratic residue modulo q; then $G_k \simeq G_{-k}$, $G_{1+k} \simeq G_{1-k^{-1}}$ and $G_{1-k} \simeq G_{1+k^{-1}}$ if and only if k is a solution of $x^2+1=0$. Also here the other solution is k^{-1}.

Now, note that either k is a solution of exactly one of the above equations, or k is no a solution for any of them. In the last case the groups above form 6 different isomorphism classes.

In compliance with these facts, summing up the results of the previous subsections we obtain *(a)-(e)* in *4* and *(a)-(c)* in *5*. □

4.5 G of type 7, $\gamma(A) \not\leq \mathrm{Inn}(G)$

In this section we deal with the groups of type 7 in the case when $\gamma(A) \not\leq \mathrm{Inn}(G)$. As in the previous sections, we will count the number of GF distinguishing by the size of the kernel of γ. Note that we have to consider just the cases in which $p \mid |\gamma(G)|$.

Firstly we show that, appealing to duality, we can always suppose that $p \mid |\ker(\gamma)|$.

If $\gamma(A)$ has order p, then $p \mid |\ker(\gamma)|$. Moreover $\gamma(A) = \langle\, \iota(c)\alpha \,\rangle$, for some $c \in A$ and α in $\mathrm{GL}(2,p)$ of order p, therefore, by the discussion in Subsection 4.1.2, the kernel is the fixed point space of α.

Now suppose $|\gamma(A)| = p^2$. We show that there exists a subgroup C of order p which satisfies the hypotheses of Proposition 1.23, in the slightly more general version described in Remark 1.24.

Let $\gamma(A) = \langle\, \iota(c), \iota(d)\alpha \,\rangle$, for some $c, d \in A$, and $\alpha \in \mathrm{GL}(2,p)$ of order p. Since $1 = [\iota(c), \iota(d)\alpha] = \iota([c,\alpha])$, we have that α fixes c. Let $x_1, x_2 \in A$ be such that $\gamma(x_1) = \iota(c)$, and $\gamma(x_2) = \iota(d)\alpha$. Then

$$x_1^{\alpha} x_2 = x_1 \circ x_2 = x_2 \circ x_1 = x_2 x_1,$$

so that $x_1 \in \langle\, c \,\rangle$. It follows that $\gamma(c) = \iota(c^{-k})$ for some k. The subgroup $C = \langle\, c \,\rangle$ is $\gamma(G)$-invariant, as if $b \in G$ has order q, then $\gamma(A) \cap \iota(A)$ is normalised by $\langle\, \gamma(b) \,\rangle$, so that $\gamma(b)$ leaves C invariant. Since C is also normal in G, Proposition 1.23 and Remark 1.24 yield that $\gamma(c) = \iota(c^{-k})$ with $k = 0, 1$, namely either $C \leq \ker(\gamma)$ or $C \leq \ker(\tilde{\gamma})$. Now by Corollary 1.25 we can assume $C \leq \ker(\gamma)$.

4.5.1 The case $|\ker(\gamma)| = pq$

As explained in Subsection 4.4.3, since $K = \ker(\gamma)$ is isomorphic to $\mathcal{C}_p \rtimes \mathcal{C}_q$, then $(G, \circ)$ will have type 6. Moreover, we can choose K in $(p+1)p$ ways.

Let $K = \langle\, a_1, b \,\rangle$, and let $a_2 \in A$ be such that $A = \langle\, a_1, a_2 \,\rangle$.

Here there are no $\gamma(G)$-invariant complements of K, therefore let us consider $G = KA$. Proposition 1.13 yields that every GF on G is the lifting of a

RGF $\gamma' : A \to \mathrm{Aut}(G)$ with $\gamma(G) = \gamma'(A)$, and such that K is invariant under $\{\gamma'(x)\iota(x) : x \in A\}$. Conversely, every RGF γ' such that $\gamma'(\langle\, a_1 \,\rangle) = 1$, and which makes K invariant under $\{\gamma'(x)\iota(x) : x \in A\}$, can be lifted to G. Now we show that a such map is a morphism, and it is defined by

$$\gamma'(a_2) = \alpha\iota(a_1^j a_2^{-1}),$$

for some $0 \le j \le p-1$, and $\alpha \in \mathrm{GL}(2,p)$ of order p.

Indeed, since $\gamma'(A) = \gamma'(\langle\, a_2 \,\rangle)$ has order p, $\gamma'(a_2) = \alpha\iota(a)$ for some $a \in A$, and $\alpha \in \mathrm{GL}(2,p)$ of order p. By Subsection 4.1.2, $\langle\, a_1 \,\rangle$ is the space of the fixed points of α, so that $a_1^\alpha = a_1$. Moreover, we can write $a_2^\alpha = a_1^d a_2$, for some $1 \le d \le p-1$, and by Lemma A.2 in the Appendix, the RGF's are morphisms.

Now, if K is invariant under $\gamma'(x)\iota(x)$ for every $x \in A$, then $\gamma'(a_2)\iota(a_2) = \alpha\iota(aa_2)$ leaves K invariant, so that $aa_2 \in \langle\, a_1 \,\rangle$, namely $a = a_1^j a_2^{-1}$ for some j, $0 \le j \le p-1$. Conversely, choosing $a = a_1^j a_2^{-1}$ then $\gamma'(a_2)\iota(a_2) = \alpha\iota(a_1^j)$, and since γ' is a morphism, K is invariant under $\gamma'(x)\iota(x)$ for every $x \in \langle\, a_2 \,\rangle$, and so for every $x \in A$.

Since there are $p(p+1)$ choices for K, $p-1$ choices for α and p choices for $\iota(a_1^j a_2^{-1})$, we obtain $p^2(p^2-1)$ groups.

As to the conjugacy classes, let $\varphi = \iota(x)\delta \in \mathrm{Aut}(G)$. As in Subsection 4.4.3, $\gamma^\varphi(a_1) = \gamma(a_1)$ and $\gamma^\varphi(b) = \gamma(b)$ yields $\delta_{12} = 0$ and $x = 1$. Since

$$\begin{aligned}
\gamma^\varphi(a_2) &= \varphi^{-1}\gamma(a_2^{\delta^{-1}})\varphi \\
&= \delta^{-1}\alpha^{\delta_{22}^{-1}}\iota(a^{\alpha^{\delta_{22}^{-1}-1}+\cdots+\alpha+1})\delta \\
&= \delta^{-1}\alpha^{\delta_{22}^{-1}}\delta\iota(a^{\alpha^{\delta_{22}^{-1}-1}+\cdots+\alpha+1})^\delta,
\end{aligned}$$

φ stabilises γ if and only if both $\delta^{-1}\alpha^{\delta_{22}^{-1}}\delta = \alpha$, namely $\delta_{22}^2 = \delta_{11}$, and

$$\iota(a^{\alpha^{\delta_{22}^{-1}-1}+\cdots+\alpha+1})^\delta = \iota(a),$$

that is, $\delta_{21} = (j + \frac{d}{2})\delta_{22}(\delta_{22}-1)$. Therefore the stabiliser has order $p(p-1)$, and there is one orbit of length $p^2(p^2-1)$.

4.5.2 The case $|\ker(\gamma)| = p$

Let $\ker(\gamma) = \langle\, a_1 \,\rangle$. We claim that $\gamma(G) \cap \iota(A) = \{1\}$. Indeed, since $q \mid p-1$, $\gamma(G)$ (of order pq) has a unique subgroup of order p. Moreover A is the Sylow p-subgroup of both G and $(G, \circ)$, so that $\gamma(A) \le \gamma(G)$ and the order of $\gamma(A)$ is a divisor of p^2. Therefore the unique subgroup of order p of $\gamma(G)$ is necessarily $\gamma(A)$. Now, either $|\gamma(G) \cap \iota(A)| = 1$, and we are done, or $|\gamma(G) \cap \iota(A)| = p$. In the latter case $\gamma(G) \cap \iota(A) = \gamma(A)$, namely $\gamma(A) \le \mathrm{Inn}(G)$, contradiction.

Now, since $\gamma(G)$ intersects $\iota(A)$ trivially,

$$\gamma(G) = \langle\, \iota(c)\alpha, \beta \,\rangle,$$

where $c \in A$, $\alpha \in \mathrm{Aut}(G)$ has order p, and $\beta \in \mathrm{Aut}(G)$ has order q. So $\alpha_{|A}$ is an element of order p in $\mathrm{GL}(2,p)$, and $\beta_{|A}$ is an element of order q in $\mathrm{GL}(2,p)$. By Subsection 4.1.2 $\alpha_{|A}$ fixes $\langle\, a_1 \,\rangle$. Moreover, by Subsection 4.1.4, $\langle\, a_1 \,\rangle$ is an eigenspace for $\beta_{|A}$ too, and if $\langle\, a_2 \,\rangle$ is another eigenspace for $\beta_{|A}$ for a suitable choice of a_2 we can write

$$\alpha_{|A} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \beta_{|A} = \begin{pmatrix} \lambda^{x_1} & 0 \\ 0 & \lambda^{x_2} \end{pmatrix},$$

with respect to the basis $\{a_1, a_2\}$, where $\lambda \in \mathbb{F}_p^*$ of order q, and $0 \leq x_1, x_2 \leq q-1$ not both zero.

The subgroup $\langle\, \beta \,\rangle$ of $\mathrm{Aut}(G)$, of order q, acts on the set $\mathcal{Q}$ of the Sylow q-subgroups of G, and since $|\mathcal{Q}| = p^2$, this action has at least one fixed point. Suppose it is $\langle\, b \,\rangle$. We can suppose that $\langle\, b \,\rangle$ is fixed by α too, in fact otherwise it will be fixed by $\alpha' := \iota(x)\alpha$ for a suitable $x \in A$, and up to an appropriate adjustment of c, $\gamma(G) = \langle\, \iota(c)\alpha', \beta \,\rangle$.

Thus we assume in the following that $\alpha_{|A}$ and $\beta_{|A}$ are in the same copy of $\mathrm{GL}(2,p)$.

Note that the Sylow q-subgroups $\langle\, xb \,\rangle$ fixed by β are those for which x satisfies $x^{1-\beta} = 1$. Therefore there is a unique fixed Sylow q-subgroup when $x_1, x_2 \neq 0$, and there are p when either $x_1 = 0$ or $x_2 = 0$.

4.5.2.1 The case $\gamma(G)$ abelian

Suppose first $\gamma(G)$ is abelian. Then $[\alpha, \beta] = 1$ modulo $\iota(A)$, so that $\beta_{|A}$ is a non-trivial scalar matrix, namely $x_1 = x_2 \neq 0$. We can assume that $\beta_{|A}$ is scalar multiplication by λ. Moreover by the discussion above $\langle\, b \,\rangle$ is the unique β-invariant Sylow q-subgroup, as $x_1, x_2 \neq 0$.

Since $\gamma(G)$ is abelian, β has to centralise $\iota(c)\alpha$, and since

$$b^{\beta\iota(c)\alpha} = c^{(-1+\lambda^{-1})\alpha} b, \qquad b^{\iota(c)\alpha\beta} = c^{(-1+\lambda^{-1})\alpha\beta} b,$$

and β does not have fixed points in A, we get $c = 1$.

Therefore

$$\gamma(G) = \langle\, \alpha, \beta \,\rangle,$$

where both α and β fix $\langle\, b \,\rangle$ pointwise. In particular $\langle\, b \,\rangle$ is $\gamma(G)$-invariant.

We will have $\gamma(a_2) = \alpha^i$ for $i \neq 0$. Moreover, since b is fixed by $\gamma(G)$, $\gamma(b)^q = \gamma(b^q) = 1$, namely $\gamma(b) = \beta^j$. Now we show that necessarily $j = -1$.

In fact, in this case $(G, \circ)$ can be of type 5 or 6, as they are the only types which have an abelian quotient of order pq. We have

$$b^{\ominus 1} \circ a \circ b = b^{-1} a^{\gamma(b)} b = a^{\beta^j \iota(b)} = a^{\lambda^{j+1}}.$$

Denoting by $Z_\circ$ the action of $\iota(b)$ on A in $(G, \circ)$, and taking into account that

$$a_1^{\circ k} = a_1^k \;\text{ and }\; a_2^{\circ k} = a_1^{i\binom{k(k-1)}{2}} a_2^k,$$

we have that $Z_\circ$ has to be scalar multpilication by 1. In this case $j = -1$, $(G, \circ)$ is of type 5 and $\gamma(b) = \beta^{-1} = \iota(b^{-1})$.

Now we show that such an assignment extends to a gamma function, namely if $a = a_1^s a_2^t$ the maps defined by

$$\gamma(ab^k) = \alpha^{it\lambda^k}\beta^{-k}$$

satisfy the GFE. Let $a' = a_1^x a_2^y$. Then

$$\gamma(ab^k)\gamma(a'b^m) = \alpha^{it\lambda^k + iy\lambda^m}\beta^{-(k+m)},$$

and

$$\begin{aligned}\gamma((ab^k)^{\gamma(a'b^m)}a'b^m) &= \gamma(a^{\alpha^{iy\lambda^m}\beta^{-m}}b^k a'b^m)\\ &= \gamma((a_2^t)^{\alpha^{iy\lambda^m}\beta^{-m}}a_2^{y\lambda^{-k}}b^{k+m})\\ &= \gamma(a_2^{t\lambda^{-m}+y\lambda^{-k}}b^{k+m})\\ &= \alpha^{i(t\lambda^{-m}+y\lambda^{-k})\lambda^{k+m}}\beta^{-(k+m)}.\end{aligned}$$

Since there are $p+1$ choices for $\ker(\gamma)$, $p-1$ choices for i, and p^2 choices for the Sylow q-subgroup fixed by β, we obtain $p^2(p^2-1)$ groups $(G, \circ)$.

As to the conjugacy classes, $B = \langle\, b \,\rangle$ is the unique $\gamma(B)$-invariant Sylow q-subgroup, so that by Lemma 1.8(2) $\bar{B} = B^{\iota(a)}$ is the unique $\gamma^{\iota(a)}(\bar{B})$-invariant Sylow q-subgroup. Since $\iota(A)$ conjugates transitively the Sylow q-subgroups of G, all classes have order a multiple of p^2.

Suppose now $\delta \in \mathrm{GL}(2,p)$. Then $\gamma(a_1^{\delta^{-1}}) = 1$ if and only if $\delta_{12} = 0$. Moreover,

$$\gamma^\delta(a_2) = \delta^{-1}\gamma(a_2^{\delta_{22}^{-1}})\delta = \delta^{-1}\alpha^{i\delta_{22}^{-1}}\delta,$$

and it is equal to α^i when $\delta_{11} = \delta_{22}^2$. Since every δ stabilises β, as $[\delta, \beta] = 1$, we have that the stabiliser has order $p(p-1)$. Therefore there is one class of length $p^2(p^2-1)$.

4.5.2.2 The case $\gamma(G)$ non-abelian

Suppose now $\gamma(G)$ is non-abelian. Here β normalises but does not centralise $\iota(c)\alpha$. Therefore,

$$(\iota(c)\alpha)^\beta = \iota(c^\beta)\beta^{-1}\alpha\beta = \iota(c^\beta)\alpha^{\lambda^{x_1}-x_2}$$

is an element of $\langle\, \iota(c)\alpha \,\rangle$, and $x_1 \neq x_2$. Since $(\iota(c)\alpha)^k = \iota(c^{1+\alpha^{-1}+\cdots+\alpha^{-(k-1)}})\alpha^k$, we have that $(\iota(c)\alpha)^\beta \in \langle\, \iota(c)\alpha \,\rangle$ if and only if

$$c^\beta = c^{1+\alpha^{-1}+\cdots+\alpha^{-(\lambda^{x_1}-x_2-1)}}.$$

Writing $c = a_1^u a_2^v$, the latter yields

$$\begin{cases} u(1-\lambda^{-x_2}) = \frac{1}{2} v\lambda^{-x_2}(1-\lambda^{x_1-x_2}) \\ v\lambda^{x_2} = v\lambda^{x_1-x_2} \end{cases} . \tag{4.21}$$

From the second equation we obtain either $v = 0$ or $x_1 \equiv 2x_2 \bmod q$.

First case. If $v = 0$ the first equation yields $u = 0$ or $x_2 = 0$.

If $x_2 = 0$ and $u \neq 0$, we have

$$\gamma(G) = \langle\, \iota(a_1^u)\alpha, \beta \,\rangle,$$

where $\alpha_{|\langle b\rangle}, \beta_{|\langle b\rangle} = 1$. In this case there are p Sylow q-subgroups fixed by β, namely $\langle\, a_2^t b \,\rangle$. Among these, those fixed by $\iota(a_1^u)\alpha$ too are

$$a_2^t b = (a_2^t b)^{\iota(a_1^u)\alpha} = (a_2^t)^\alpha a_1^{u(-1+\lambda^{-1})\alpha} b = (a_2^t)^\alpha a_1^{u(-1+\lambda^{-1})} b,$$

that is, those with t such that $(a_2^t)^{1-\alpha} = a_1^{u(-1+\lambda^{-1})}$, namely $t = u(1-\lambda^{-1})$.

Since $\langle a_2^{u(1-\lambda^{-1})} b\rangle$ is fixed by both $\iota(a_1)\alpha$ and β, we can suppose that $\gamma(G) = \langle\, \alpha, \beta \,\rangle$ with α and β fixing the same Sylow q-subgroup (which will still denote by $\langle\, b \,\rangle$).

By the discussion above, when $v = 0$ we can always suppose

$$\gamma(G) = \langle\, \alpha, \beta \,\rangle,$$

with α, β fixing $\langle\, b \,\rangle$. Moreover a Sylow q-subgroup $\langle\, yb \,\rangle$ is $\gamma(G)$-invariant if and only if $y^\alpha = y^\beta = y$. The latter has $y = 1$ has unique solution except when $x_1 = 0$, which gives the p solutions $y \in \langle\, a_1 \,\rangle$.

We will have $\gamma(a_2) = \alpha^i$, $i \neq 0$, and up to change β with another element of order q in $\gamma(G)$ we can suppose $\gamma(b) = \beta$.

Now we show that such an assignment extends to a gamma function if and only if $x_1 = 2x_2 + 1$. If $a = a_1^s a_2^t$, consider the maps defined by

$$\gamma(ab^k) = \alpha^{it\lambda^{-kx_2}} \beta^k.$$

With computations similar to the previous case, for $a' = a_1^x a_2^y$ we find that

$$\gamma(ab^k)\gamma(a'b^m) = \alpha^{it\lambda^{-kx_2} + iy\lambda^{-mx_2 - k(x_1-x_2)}} \beta^{k+m},$$

and

$$\gamma((ab^k)^{\gamma(a'b^m)} cb^m) = \alpha^{i(t\lambda^{-kx_2} + y\lambda^{-k-(k+m)x_2})} \beta^{k+m},$$

so that they are equal precisely when $x_1 = 2x_2 + 1$.

Since there are $p+1$ choices for the kernel $\langle\, a_1 \,\rangle$, p choices for $\langle\, a_2 \,\rangle$, $p-1$ for the image of a_2, $q-1$ for x_2 such that $\beta_{|A}$ is non-scalar, and p^2 for the Sylow q-subgroup $\langle\, b \,\rangle$ fixed by α and β, we have $p^3(p^2-1)(q-1)$ GF. They are

all distinct if $\langle b \rangle$ is the unique $\gamma(G)$-invariant Sylow q-subgroup. Otherwise, when $x_2 = \frac{q-1}{2}$, the p choices for a $\gamma(G)$-invariant Sylow q-subgroups yield the same GF, so there are $p^2(p^2-1)$ distinct GF.

Note that we do not consider the choices for the images of b, as if $\gamma(b) = \alpha^i\beta^k$, then the choices for k correspond to the choices for x_2, and since $\alpha^i\beta^k$ will have eigenspaces $\langle a_1 \rangle, \langle a_3 \rangle$, for $a_3 \in A \setminus \langle a_1 \rangle$, the choices for i correspond to the choices for the second eigenspace, namely to the choice for $\langle a_2 \rangle$.

Since

$$b^{\ominus 1} \circ a \circ b = a^{\gamma(b)\iota(b)},$$

and $a_1^{\circ k} = a_1^k$, $a_2^{\circ k} = a_2^k$ modulo $\langle a_1 \rangle$, denoting by $Z_\circ$ the action of $\iota(b)$ on A in $(G, \circ)$, we have

$$Z_\circ \sim \begin{pmatrix} \lambda^{2x_2+2} & 0 \\ 0 & \lambda^{x_2+1} \end{pmatrix}.$$

If $q = 2$ the unique choice for x_1, x_2 compatible with the conditions β non-scalar and $x_1 = 2x_2 + 1$ is $x_1 = 1$ and $x_2 = 0$. Therefore $Z_\circ = \mathrm{diag}(1, \lambda)$, and $(G, \circ)$ is of type 6. Therefore:

Type 6 is for $q = 2$ and $x_2 = 0$. Since $x_1 \neq 0$ we obtain $p^3(p^2-1)$ groups.

Suppose now $q > 2$. In this case if $x_2 = -1$, then $x_1 = -1$ too so that β is scalar, against the assumption $\gamma(G)$ non-abelian. So suppose $x_2 \neq -1$, so that the groups $(G, \circ)$ can have only types 8 or 9.

Type 9 is when $\det(Z_\circ) = 1$, namely for $3(x_2+1) = 0$. If $q > 3$ then there are no groups of type 9. If $q = 3$ then for $x_2 = 0$ there is a unique invariant Sylow q-subgroup, and we have $p^3(p^2-1)$ groups. If $x_2 = 1$ there are p invariant Sylow q-subgroups, and there are $p^2(p^2-1)$ groups. Thus in total $p^2(p^2-1) + p^3(p^2-1)$ groups.

Type 8 is when $q > 3$ and $\det(Z_\circ) \neq 1$, namely $x_2 \neq -1$. For each choice of x_2 there are $p^3(p^2-1)$ groups, except when $x_2 = \frac{q-1}{2}$, in which there are $p^2(p^2-1)$ groups. Thus in total $p^2(p^2-1) + p^3(p^2-1)(q-2)$ groups.

Note that in this case $Z_\circ \sim \mathrm{diag}(\mu^2, \mu)$, where $\mu = \lambda^{x_2+1}$, therefore the groups $(G, \circ)$ are all isomorphic to G_2.

As to the conjugacy classes, when there is a unique Sylow q-subgroup B which is $\gamma(B)$-invariant, as in the previous case, all classes have order a multiple of p^2. Otherwise $x_1 = 0$ and there are p invariant Sylow q-subgroups. In this case $\iota(x)$ stabilises γ if and only if $\iota(x)$ commutes with both α and β, namely when $x \in \langle a_1 \rangle$.

Now suppose $\delta = (\delta_{ij}) \in \mathrm{GL}(2, p)$. As above, $\gamma^\delta(a_1) = 1$ and $\gamma^\delta(a_2) = \gamma(a_2)$ if and only if $\delta_{12} = 0$ and $\delta_{11} = \delta_{22}^2$. Moreover

$$\gamma^\delta(b) = \delta^{-1}\gamma(b)\delta = \delta^{-1}\beta\delta,$$

and β, which is non-scalar, is centralised by δ when δ is a diagonal matrix.

Therefore the orbits have length $p^3(p^2-1)$ if $x_1 \neq 0$ and $p^2(p^2-1)$ if $x_1 = 0$.

Second case. Suppose now $v \neq 0$ and $x_1 \equiv 2x_2 \bmod q$. Then (4.21) yields $v = -2u$ and we have

$$\gamma(G) = \langle\, \iota(c)\alpha, \beta \,\rangle\,,$$

where α and β fix $\langle\, b \rangle$, and $c = a_1^u a_2^{-2u}$.

Up to change a_1 with a suitable element in $\langle\, a_1 \,\rangle$ we can suppose $u = \frac{1}{2}$.

We will have $\gamma(a_2) = (\iota(c)\alpha)^i$ for some $i \neq 0$, and $\gamma(b) = (\iota(c)\alpha)^j\beta^k$, with $k \neq 0$, as it is an element of order q in $\gamma(G)$. Up to change β with a suitable element in $\langle\, \beta \,\rangle$ we can suppose that $k = 1$.

Now we show that if the assignment above extends to a GF, then $i = 1$. In fact, denoting by M_i the matrix $1 + \alpha^{-1} + \cdots + \alpha^{-(i-1)}$, we will have

$$\begin{aligned} b^{\ominus 1} \circ a_2 \circ b &= (b^{\gamma(b)^{-1}\gamma(a_2)\gamma(b)})^{-1} a_2^{\gamma(b)} b \\ &= (b^{\iota(c^{M_i})\alpha^i\beta})^{-1} a_2^{\alpha^j\beta} b \\ &= b^{-1} c^{(1-\lambda^{-1})M_i\alpha^i\beta} a_2^{\alpha^j\beta} b \\ &= c^{(\lambda-1)M_i\alpha^i\beta} a_2^{\lambda\alpha^j\beta} \\ &= a_1^{(\frac{1}{2}(1-\lambda)i^2 + j\lambda)\lambda^{2x_2}} a_2^{((1-\lambda)i+\lambda)\lambda^{x_2}}. \end{aligned}$$

Applying γ to both the sides we obtain

$$\gamma(b)^{-1}\gamma(a_2)\gamma(b) = \gamma(a_2)^{((1-\lambda)i+\lambda)\lambda^{x_2}},$$

and comparing with

$$\gamma(b)^{-1}\gamma(a_2)\gamma(b) = \beta^{-1}\iota(c^{M_i})\alpha^i = \iota(c^{M_i\beta})\alpha^{i\lambda^{x_2}}$$

we obtain $(1-\lambda)i + \lambda = i$, so that $i = 1$.

Now we show that if the map γ extends to a GF then there always exist at least one Sylow q-subgroup B which is $\gamma(B)$-invariant.

Write $x = a_1^w a_2^z$ for an element in A. If γ extends to a GF, then

$$\gamma(xb) = \gamma(a_2^{z\lambda^{-x_2}})\gamma(b) = \iota(c^{M_K})\alpha^K\beta,$$

where $K := j + z\lambda^{x_2}$.

Since

$$(xb)^{\gamma(xb)} = (xb)^{\iota(c^{M_K})\alpha^K\beta} = (xc^{(-1+\lambda^{-1})M_K})^{\alpha^K\beta}b,$$

$(xb)^{\gamma(xb)}$ belongs to $\langle\, xb \,\rangle$ if and only if

$$x^{1-\alpha^K\beta} = c^{(-1+\lambda^{-1})M_K\alpha^K\beta}. \tag{4.22}$$

Writing x and c in the basis $\langle\, a_1, a_2 \,\rangle$ and looking at their second component in (4.22) we find

$$z(\lambda^{-1} - \lambda^{x_2}) = j\lambda^{x_2}(1 - \lambda^{-1}). \tag{4.23}$$

If $x_2 \neq -1$ then there is a unique solution for z and in this case the first component (4.22) yields

$$w(1-\lambda^{2x_2}) = j^2\lambda^{2x_2}\frac{(1-\lambda^{-1})}{2(\lambda^{-1}-\lambda^{x_2})^2}(1-\lambda^{2x_2}),$$

so that, since $q > 2$ (as $x_2 \neq 0, -1$), there is a unique invariant Sylow q-subgroup.

Suppose now $x_2 = -1$. By induction one can show that in this case if the map γ is a GF then

$$\gamma(b^m) = \gamma(a_2)^{j(m-(1+\lambda+\cdots+\lambda^{m-1}))}\gamma(b)^m.$$

Looking at the exponent of α in $\gamma(b^q) = 1$ we obtain that $jq = 0$, namely $j = 0$.

Therefore (4.23) yields that there are p solutions for z. Moreover in this case

$$w(1-\lambda^{-2}) = \frac{1}{2}z^2(1+\lambda^{-1}),$$

so that there are p invariant Sylow q-subgroups when $q > 2$ and p^2 when $q = 2$.

Now, since the Sylow q-subgroup $\langle\, b \,\rangle$ is invariant, $\gamma(b) = \beta^k$.

With computations similar to the previous cases one can show that the assignment

$$\begin{cases} \gamma(a_2) = \iota(c)\alpha \\ \gamma(b) = \beta \end{cases}$$

extends to a GF, namely if $a = a_1^s a_2^t$ then the map defined as

$$\gamma(ab^k) = \iota(c^{M_{t\lambda^{-kx_2}}})\alpha^{t\lambda^{-kx_2}}\beta^k$$

satisfies the GFE.

Since there are $p+1$ choices for $\langle\, a_1 \,\rangle$, p choices for $\langle\, a_2 \,\rangle$, $p-1$ choices for a_2 in $\langle\, a_2 \,\rangle$, $q-1$ choices for x_2, and p^2 choices for the Sylow q-subgroup fixed by α and β, we have $p^3(p^2-1)(q-1)$ GF. They are all distinct if $\langle\, b \,\rangle$ is the unique invariant Sylow q-subgroup. Otherwise, when $x_2 = -1$, the p (respectively p^2 when $q = 2$) choices for an invariant Sylow q-subgroup yield the same GF, and so there are $p^2(p^2-1)$ (respectively $p(p^2-1)$) distinct GF.

We have

$$b^{\ominus 1} \circ a_1 \circ b = a_1^{\lambda^{2x_2+1}},$$
$$b^{\ominus 1} \circ a_2 \circ b = a_1^{\frac{1}{2}(1-\lambda)\lambda^{2x_2}} a_2^{\lambda^{x_2}},$$

and since $a_1^{\circ k} = a_1^k$ and $a_2^{\circ k} = a_2^k$ modulo $\langle\, a_1 \,\rangle$, denoting as usual by $Z_\circ$ the action of $\iota(b)_{|A}$ in $(G, \circ)$, we have

$$Z_\circ \sim \begin{pmatrix} \lambda^{2x_2+1} & 0 \\ 0 & \lambda^{x_2} \end{pmatrix}.$$

Type 6 when $Z_\circ$ has an eigenvalue 1, namely for $x_2 = \frac{q-1}{2}$. In this case there are $p^3(p^2-1)$ groups.

Type 7 when $Z_\circ$ is scalar, namely for $x_2 = -1$. In this case there are $p^2(p^2-1)$ groups if $q > 2$ and $p(p^2-1)$ if $q = 2$. (Note that for $x_1 = -1$, $b^{\ominus 1} \circ a_2 \circ b = a_2^{\circ \lambda^{x_2}}$, so that $Z_\circ$ is actually a scalar matrix.)

Type 8 when $q > 3$ and $x_2 \neq -1, \frac{q-1}{2}, \frac{q-1}{3}$, so there are $p^3(p^2-1)(q-4)$ groups of type 8.

Here each group $(G, \circ)$ is isomorphic to $G_{2+x_2^{-1}}$ for a certain x_2. For each $s \neq 2$, $s \in \mathcal{K}$, there are $2p^3(p^2-1)$ groups isomorphic to G_s, namely those obtained for x_2 such that $2 + x_2^{-1} = s$ and $2 + x_2^{-1} = s^{-1}$, while there are $p^3(p^2-1)$ groups isomorphic to G_2, as they can be obtained just for x_2 such that $2 + x_2^{-1} = 2^{-1}$.

Type 9 when $x_2 \neq -1, \frac{q-1}{2}$ and $Z_\circ$ has determinant equal to 1, namely when $x_2 = \frac{q-1}{3}$ and $q > 3$. In this case we obtain $p^3(p^2-1)$ groups.

As to the conjugacy classes, with computations similar to the previous cases we obtain orbits of length $p^3(p^2-1)$ when $x_2 \neq -1$, otherwise $x_2 = -1$ and there is unique orbit of length $p^2(p^2-1)$ if $q > 2$, and $p(p^2-1)$ if $q = 2$.

Summing up the results of this section with those of the previous section we obtain the following.

Proposition 4.10. *Let G be a group of order p^2q, $p > 2$, of type 7. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $p^3(3p+1)$ *groups of type 5, which split in two conjugacy classes of length p^2, one conjugacy class of length $p^3(p+1)$ and two conjugacy classes of length $p^2(p^2-1)$;*
2. *if $q = 2$*
   (a) $p^3(p+1)(3p+1)$ *groups of type 6, which split in* 4 *conjugacy classes of length $p^2(p+1)$, $p+4$ conjugacy classes of length $p^2(p^2-1)$, and two conjugacy classes of length $p^3(p^2-1)$;*
   in total $10+p$ conjugacy classes;
   (b) $2 + p(p+1)(2p-1)$ *groups of type 7, which split in two conjugacy classes of length* 1*, two conjugacy classes of length $p(p^2-1)$, and one conjugacy class of length $p(p+1)$;*
   in total 5 *conjugacy classes;*
3. *if $q > 2$*

(a) $4p^2(p+1)(p^2+pq-2p)$ *groups of type 6, which split in* 4 *conjugacy classes of length* $p^2(p+1)$, $4(q-2)$ *conjugacy classes of length* $p^3(p+1)$, 4 *conjugacy classes of length* $p^2(p^2-1)$, *and* 4 *conjugacy classes of length* $p^3(p^2-1)$;

in total $4(q+1)$ *conjugacy classes;*

(b) $2+p^2(2p^2+pq+2q-4)$ *groups of type 7, which split in two conjugacy classes of length* 1, $2(q-2)$ *conjugacy classes of length* p^2, *two conjugacy classes of length* $p^2(p+1)$, *two conjugacy classes of length* $p^2(p^2-1)$, *and* $q-3$ *conjugacy classes of length* $p^3(p+1)$;

in total $3q-1$ *conjugacy classes;*

(c) *if* $q=3$, $p(p+1)(2p^3+3p^2-2p+1)$ *groups of type 9, which split in one conjugacy class of length* $p^3(p+1)$, *two conjugacy classes of length* $p^2(p+1)$, *one conjugacy class of length* $p(p+1)$, *two conjugacy classes of length* $p^3(p^2-1)$, *and* 4 *conjugacy classes of length* $p^2(p^2-1)$;

in total 10 *conjugacy classes;*

(d) *if* $q>3$,

- $2p^2(p+1)(p^2q+pq-4p+2)$ *groups of type 8 isomorphic to* G_2, *which split in* $4(q-3)$ *conjugacy classes of length* $p^3(p+1)$, 8 *conjugacy classes of length* $p^2(p+1)$, 4 *conjugacy classes of length* $p^2(p^2-1)$, *and* $2q$ *conjugacy classes of length* $p^3(p^2-1)$;
- *for every* $s \in \mathcal{K}$, $s \neq 2$, $4p^2(p+1)(2p^2-5p+pq+2)$ *groups of type 8 isomorphic to* G_s, *which split in* $4(q-3)$ *conjugacy classes of length* $p^3(p+1)$, 8 *conjugacy classes of length* $p^2(p+1)$, *and* 8 *conjugacy classes of length* $p^3(p^2-1)$;

in total $6q$ *conjugacy classes of groups isomorphic to* G_2 *and* $4(q+1)$ *conjugacy classes of groups isomorphic to* G_s *for every* $s \neq 2$;

(e) *if* $q>3$, $4p^5+p^4(q-2)+p^3(2q-7)+3p^2+p$ *groups of type 9, which split in* $2q-5$ *conjugacy classes of length* $p^3(p+1)$, *two conjugacy classes of length* $p^2(p+1)$, *one conjugacy class of length* $p(p+1)$, *and* 4 *conjugacy classes of length* $p^3(p^2-1)$;

in total $2(q+1)$ *conjugacy classes;*

4.6 G of type 10

In this case $q \mid p+1$, where $q>2$, and $G=(\mathcal{C}_p \times \mathcal{C}_p) \rtimes_C \mathcal{C}_q$. The Sylow p-subgroup $A=\langle a_1, a_2 \rangle$ is characteristic and a generator b of a Sylow q-subgroup acts on A as a suitable power Z of a Singer cycle, namely $a^b=a^Z$ for $a \in A$. We know that Z has determinant 1 and two (conjugate) eigenvalues $\lambda, \lambda^p=\lambda^{-1} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

The divisibility condition on p and q implies that $(G, \circ)$ can only be of type 5 or 10.

According to Subsections 4.1 and 4.4 of [CCDC21], we have

$$\mathrm{Aut}(G) = (\mathcal{C}_p \times \mathcal{C}_p) \rtimes (\mathcal{C}_{p^2-1} \rtimes \mathcal{C}_2),$$

where $\mathcal{C}_p \times \mathcal{C}_p = \iota(A)$, and for $\mu \in \mathcal{C}_{p^2-1}$ and $\psi \in \mathcal{C}_2$ we write

$$\mu : \begin{cases} a \mapsto a^M \\ b \mapsto b \end{cases}, \ \psi : \begin{cases} a \mapsto a^S \\ b \mapsto b^r \end{cases}, \tag{4.24}$$

where $M = uI + vZ \in \mathrm{GL}(2, p)$, for $u, v \in \mathbb{F}_p$ not both zero, and S, r are such that either $r = 1$ and $S = 1$, or $r = -1$ and

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The Sylow p-subgroup of $\mathrm{Aut}(G)$ has order p^2 and is characteristic and a Sylow q-subgroup is cyclic, so $\gamma(G)$ of order a divisor of p^2q is always contained in $\mathrm{Inn}(G)$.

Moreover

- since A is characteristic, it is also a Sylow p-subgroup of $(G, \circ)$, so $\gamma(A)$ is a subgroup of $\iota(A)$, the Sylow p-subgroup of $\mathrm{Aut}(G)$.
- $\gamma_{|A} : A \to \mathrm{Aut}(G)$ is a morphism, as for each $a \in A$ the automorphism $\iota(a)$ acts trivially on the abelian group A, and so

  $$\gamma(a)\gamma(a') = \gamma(a^{\gamma(a')}a') = \gamma(aa').$$

  Therefore, $\gamma(a) = \iota(a^{-\sigma})$ for each $a \in A$, where $\sigma \in \mathrm{End}(A)$.

In the following assume $\gamma \neq 1$.

4.6.1 The case $|\ker(\gamma)| = p$

This case does not arise, in fact the group $(G, \circ)$ can not have type 5, since $\mathrm{Inn}(G)$ does not contain an abelian subgroup of order pq. $(G, \circ)$ can neither be of type 10, since a group of type 10 has no normal subgroups of order p.

4.6.2 The case $|\ker(\gamma)| = p^2$

Here $\ker(\gamma) = A$ and $|\gamma(G)| = q$, so $\gamma(G) = \langle\, \iota(b) \,\rangle$ where b is a q-element of G. In this case $B = \langle\, b \,\rangle$ is the unique $\gamma(G)$-invariant Sylow q-subgroup, therefore by Subsection 2.2.1 each γ is the lifting of exactly one RGF defined on the unique $\gamma(G)$-invariant Sylow q-subgroup. So, for each choice of $B = \langle\, b \,\rangle$ (p^2 possibilities), we can define $\gamma(b) = \iota(b^{-s})$, with $1 \leq s \leq q-1$ ($q-1$ choices).

Since $[B, \gamma(B)] = 1$, by Lemma 1.12 the RGF's correspond to the morphisms.

For $s = 1$ we obtain a group of type 5 and for $s \neq 1$ ($q - 2$ choices) we obtain a group of type 10. In conclusion there are

(i) p^2 groups of type 5;

(ii) $p^2(q-2)$ groups of type 10.

As to the conjugacy classes, here the kernel A is characteristic, so that every $\varphi \in \mathrm{Aut}(G)$, stabilises $\gamma_{|A}$.

All orbits here have length a multiple of p^2, as

$$\gamma^{\iota(x)}(b) = \iota(x^{-1})\gamma(b)\iota(x) = \iota(x^{-1+Z^s}b^{-s}) = \iota(x^{-1+Z^s})\gamma(b).$$

Now, let $\varphi = \mu\psi$, where μ and ψ are as in (4.24). Then

$$\gamma^{\varphi}(b) = \varphi^{-1}\iota(b^{-sr})\varphi = \psi^{-1}\iota(b^{-sr})\psi = \iota(b^{-s}) = \gamma(b),$$

so that the orbits have length exactly p^2.

4.6.3 The case $q \mid |\ker(\gamma)|$

In this case $(G, \circ)$ can only be of type 5, as a group of type 10 has no normal subgroups of order q or pq.

Let $B \leq \ker(\gamma)$. Since A is characteristic, by Subsection 2.2.1 each GF on G is the lifting of a RGF defined on A, and a RGF on A can be lifted to G if and only if B is invariant under $\{\gamma(a)\iota(a) \mid a \in A\}$.

Now, for each $a \in A$, $\gamma(a) = \iota(a^{-\sigma})$, where $\sigma \in \mathrm{End}(A)$, so that $\gamma(a)\iota(a) = \iota(a^{1-\sigma})$. Since every Sylow q-subgroup of G is self-normalising, necessarily $\sigma = 1$, so that for each $a \in A$

$$\gamma(a) = \iota(a^{-1}).$$

Since $[A, \gamma(A)] = 1$, by Lemma 1.12 the RGF's correspond to the morphisms. So, for each of the p^2 choices for B there is a unique RGF on A which lifts to G.

In conclusion we obtain p^2 groups of type 5. Note that for all the GF's of this case $|\ker(\gamma)| = q$, namely there are no GF's on G with $|\ker(\gamma)| = pq$.

As to the conjugacy classes, as in Subsection 4.4.2, since $\iota(A)$ conjugates transitively the p^2 Sylow q-subgroups of G, the p^2 GF's are conjugate.

4.6.4 The case $\ker(\gamma) = \{1\}$

As in Subsection 4.4.6, the GF's of this case can be divided into subclasses according to the size of $\ker(\tilde{\gamma})$.

In this case $\gamma(G) = \mathrm{Inn}(G) \cong (G, \circ)$, so that all the GF's correspond to groups of type 10.

Let $\gamma(a) = \iota(a^{-\sigma})$ for some $\sigma \in \mathrm{GL}(2, p)$.

Consider first the case $\sigma = 1$, namely $\gamma(a) = \iota(a^{-1})$. In this case $p^2 \mid |\ker(\tilde{\gamma})|$, since $\tilde{\gamma}(x) = \gamma(x^{-1})\iota(x^{-1})$ for all $x \in G$. By Subsection 4.6.2, $\tilde{\gamma}(b) = \iota(b^{-s})$, therefore $\gamma(b) = \tilde{\gamma}(b^{-1})\iota(b^{-1}) = \iota(b^{s-1})$, and $q \mid |\ker(\gamma)|$ precisely when $s = 1$. Therefore, the p^2 GF's $\tilde{\gamma}$ corresponding to $(G, \circ)$ of type 5 are such that the corresponding γ have kernel of size q, and these have already been considered in Subsection 4.6.3. All the other $\tilde{\gamma}$ correspond to γ with kernel of size 1. The latter are $p^2(q-2)$, plus the right regular representation, and all of them correspond to groups of type 10.

Let now $\sigma \neq 1$. In this case 1 is not an eigenvalue of σ, in fact otherwise $p \mid |\ker(\tilde{\gamma})|$, but, as seen before, this implies $p^2 \mid |\ker(\tilde{\gamma})|$, and hence $\sigma = 1$. Therefore here both σ and $(1 - \sigma^{-1})$ are invertible.

Let b be a q-element and let $\gamma(b) = \iota(a_0 b^{-s})$ for some $a_0 \in A$ and $s \not\equiv 0 \bmod q$. Then Subsection 2.2.1.2 yields (2.2), which in our notation here is

$$(\sigma^{-1} - 1)^{-1} Z^{-s} (\sigma^{-1} - 1) = Z^{1-s}. \tag{4.25}$$

Recall that Z has order q and has two conjugate eigenvalues λ and λ^{-1} in the extension $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. An easy computation shows that the corresponding eigenspaces are $\langle\, v_1 \,\rangle$ and $\langle\, v_2 \,\rangle$ with $v_1 = a_1 + \lambda a_2$, $v_2 = a_1 + \lambda^{-1} a_2$.

From (4.25) we get $\{\lambda^{-s}, \lambda^s\} = \{\lambda^{1-s}, \lambda^{-1+s}\}$, which is possible only for $\lambda^{-s} = \lambda^{-1+s}$: this gives the condition $2s \equiv 1 \bmod q$ and means that $\sigma^{-1} - 1$ exchanges the two eigenspaces of Z. Therefore, with respect to the basis $\{v_1, v_2\}$,

$$\sigma^{-1} - 1 = \begin{pmatrix} 0 & \nu^p \\ \nu & 0 \end{pmatrix},$$

where $\nu \in \mathbb{F}_{p^2}^*$. The condition that σ has not 0 and 1 as eigenvalues reads here as $\det(\sigma^{-1} - 1) = \nu^{p+1} \neq 0$ and $\det(\sigma^{-1}) = 1 - \nu^{p+1} \neq 0$, so we have $p^2 - 1 - (p+1) = (p+1)(p-2)$ choice for $\sigma^{-1} - 1$ and hence for σ. Since $2s \equiv 1 \bmod q$, there are $(p+1)(p-2)$ choices for the couple (σ, s).

As discussed in Subsection 2.2.3, the next Proposition shows that all the GF's of this case can be constructed via gluing.

Proposition 4.11. *Let γ be a GF on a group G of type 10. If $|\ker(\gamma)| = 1$, then there is a unique Sylow q-subgroup B of G invariant under $\gamma(B)$.*

Proof. Let $B = \langle\, b \,\rangle$ a Sylow q-subgroup of G. Then, a Sylow q-subgroup $\langle\, b^x \,\rangle$, where $x \in A$, is invariant when $(b^x)^{\gamma(b^x)} \in \langle\, b^x \,\rangle$, that is,

$$\gamma(b^x) \in \mathrm{Norm}_{\mathrm{Aut}(G)}(\iota(b^x)).$$

Since $\gamma(b^x)$ is a q-element, the latter means that

$$\gamma(b^x) \in \langle\, \iota(b^x) \,\rangle. \tag{4.26}$$

Since

$$\begin{aligned}\gamma(b^x) &= \gamma(x^{-1+Z^{-1}}b)\\ &= \gamma(x^{(-1+Z^{-1})\iota(b^s)})\gamma(b)\\ &= \iota(x^{(1-Z^{-1})Z^s\sigma})\iota(a_0b^{-s})\\ &= \iota(b^{-s})\iota(x^{(1-Z^{-1})Z^s\sigma Z^{-s}}a_0^{Z^{-s}}),\end{aligned}$$

(4.26) becomes

$$\iota(b^{-s})\iota(x^{(1-Z^{-1})Z^s\sigma Z^{-s}}a_0^{Z^{-s}}) = \iota(x^{-1+Z^{-1}}b)^{-s},$$

which is equivalent to

$$b^{-s}x^{(1-Z^{-1})Z^s\sigma Z^{-s}}a_0^{Z^{-s}} = b^{-s}x^{-Z^{-s}+1}.$$

Therefore, we are left with show that the equation

$$x^{(1-Z^{-1})Z^s\sigma Z^{-s}}a_0^{Z^{-s}} = x^{-Z^{-s}+1} \tag{4.27}$$

has a unique solution x for each choice of $a_0 \in A$, namely that the matrix

$$D = (1-Z^{-1})Z^s + (1-Z^s)\sigma^{-1}$$

is invertible. One can easily compute D and $\det(D) = (1-\lambda^s)(1-\lambda^{-s})(1-\nu^{p+1})$, and since the latter is non-zero, D is invertible and (4.27) has a unique solution x. □

Summarising, each γ admits a unique invariant Sylow q-subgroup, so that it is a gluing of a RGF $\gamma_B : B \to \mathrm{Aut}(G)$ and a RGF γ_A determined by σ, with the condition that equation (4.25) holds. Necessarily, $\gamma_B(b) = \iota(b^{-s})$ for some s, and by (4.25) we get $2s \equiv 1 \bmod q$. Therefore for each B (p^2 choices), we have only one RGF on B and $(p+1)(p-2)$ choices for σ, so there are $p^2(p+1)(p-2)$ distinct GF, corresponding to groups of type 10.

As to the conjugacy classes, since each γ has a unique Sylow q-subgroup B which is $\gamma(B)$-invariant, by Lemma 1.8(2), for $a \in A$, $\gamma^{\iota(a)}$ has $\bar{B} = B^{\iota(a)}$ as $\gamma(\bar{B})$-invariant Sylow p-subgroup. Now $\iota(A)$ conjugates transitively the Sylow p-subgroups of G, so that all classes have order a multiple of p^2.

Consider $\varphi = \mu\psi \in \mathrm{Aut}(G)$, where μ and ψ are as in (4.24). μ centralises both b and $\gamma(b)$, so that it stabilises $\gamma_{|B}$. Moreover ψ has order 2, and $b^\psi = b^r$, $\iota(b)^\psi = \iota(b^r)$, so that ψ stabilises $\gamma_{|B}$ as well.

As for $\gamma_{|A}$, we have $a^{\varphi^{-1}} = a^{\psi\mu^{-1}} = a^{SM^{-1}}$, so that

$$\gamma^\varphi(a) = \varphi^{-1}\gamma(a^{SM^{-1}})\varphi = \varphi^{-1}\iota(a^{-SM^{-1}\sigma})\varphi,$$

and it coincides to $\gamma(a) = \iota(a^{-\sigma})$ if and only if $a^{SM^{-1}\sigma MS} = a^{\sigma}$, namely if and only if $\sigma MS\sigma^{-1} = MS$. The latter can be written as

$$(\sigma^{-1} - 1)^{-1} MS(\sigma^{-1} - 1) = MS. \tag{4.28}$$

If $S = 1$, (4.28) yields $u + v\lambda^{-1} = u + v\lambda$, namely $v = 0$, so that there are $p - 1$ choices for μ. If $S \neq 1$, (4.28) yields $(u + v\lambda^{-1})\nu^{p-1} = u + v\lambda$, namely

$$\frac{u}{v} = \frac{\lambda - \lambda^{-1}\nu^{p-1}}{\nu^{p-1} - 1}.$$

Since it is fixed by the Frobenius endomorphism, it is actually in $\mathbb{F}_p$, and there are $p - 1$ choices for μ.

Therefore, the stabiliser has order $2(p - 1)$, and there are $p - 2$ orbits of length $p^2(p + 1)$.

We summarise, including the right and left regular representations.

Proposition 4.12. *Let G be a group of order p^2q, $p > 2$, of type 10. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $2p^2$ *groups of type 5, which split in two conjugacy classes of length p^2;*
2. $2 + p^2(2(q - 2) + (p + 1)(p - 2))$ *groups of type 10, which split in two conjugacy classes of length* 1, $2(q-2)$ *conjugacy classes of length p^2, and $p - 2$ conjugacy classes of length $p^2(p + 1)$.*

4.7 G of type 11

In this case $p \mid q - 1$ and $G = \mathcal{C}_p \times (\mathcal{C}_p \ltimes \mathcal{C}_q)$. Let $Z = \langle\, z \,\rangle$ be the center of G, and $B = \langle\, b \,\rangle$ the Sylow q-subgroup.

According to Subsection 4.6 of [CCDC21],

$$\mathrm{Aut}(G) = \mathrm{Hol}(C_p) \times \mathrm{Hol}(C_q),$$

so that a Sylow p-subgroup of $\mathrm{Aut}(G)$ is of the form $\mathcal{C}_p \times \mathcal{P}$, where $\mathcal{C}_p$ is generated by a central automorphism and $\mathcal{P}$ is a Sylow p-subgroup of $\mathrm{Hol}(\mathcal{C}_q)$. Therefore, a subgroup of order p^2 in $\mathrm{Aut}(G)$ is generated by an inner automorphism $\iota(a)$, for some non-central element a of order p, and the central automorphism

$$\psi : \begin{cases} z \mapsto z, \\ a \mapsto az, \\ b \mapsto b \end{cases} . \tag{4.29}$$

By Subsection 2.2.1 in counting the GF's we can suppose $B \leq \ker(\gamma)$. Therefore the image $\gamma(G)$ is contained in a subgroup of $\mathrm{Aut}(G)$ of order p^2, that is,

$$\gamma(G) \leq \langle\, \iota(a), \psi \,\rangle,$$

for $a \in A \setminus Z$, and ψ as in (4.29).

Theorem 2.3 yields that there exists at least one Sylow p-subgroup A of G which is $\gamma(G)$-invariant. More precisely $A = \langle a, z \rangle$ is $\gamma(G)$-invariant, and it is the unique $\gamma(G)$-invariant Sylow p-subgroup if $\gamma(G) \cap \mathrm{Inn}(G) \neq \{1\}$; otherwise $\gamma(G) \leq \langle \psi \rangle$, and every Sylow p-subgroup is $\gamma(G)$-invariant.

We may thus apply Proposition 1.13, and look for the functions

$$\gamma' : A \to \mathrm{Aut}(G)$$

which satisfy the GFE (we will just wrote γ in the following). Since $(A, \circ)$ is abelian, we have

$$a^{\gamma(z)} z = a \circ z = z \circ a = z^{\gamma(a)} a = za,$$

so that $a^{\gamma(z)} = a$, namely

$$\gamma(z) = \iota(a)^s, \tag{4.30}$$

for some $0 \leq s \leq p-1$. We also have

$$\gamma(a) = \iota(a)^t \psi^u, \tag{4.31}$$

for some $0 \leq t, u \leq p-1$.

If both $s = 0$ and $u = t = 0$, then $\ker(\gamma) = G$ and we get the right regular representation.

Proposition 1.13 yields also that the RGF's on A with kernel of size 1, respectively p, correspond to the GF's on G with kernel of size q, respectively qp. In the following we suppose $\gamma(G) \neq \{1\}$.

4.7.1 The case $|\ker(\gamma)| = q$

Here $\gamma(G) = \langle \iota(a), \psi \rangle$ and $A = \langle a, z \rangle$ is the unique Sylow p-subgroup of G which is $\gamma(G)$-invariant. By the discussion above, we look for the RGF's γ on A extending the assignments (4.30), (4.31), and with trivial kernel, namely $s \neq 0$ and $u \neq 0$. By Lemma A.1 in the Appendix there is a unique RGF γ like that, and since there are q choices for A, we get $qp(p-1)^2$ maps.

As to the circle operation, for every $x \in A$, $x^{\ominus 1} \circ b \circ x = b^{\gamma(x)\iota(x)}$, so that

$$a^{\ominus 1} \circ b \circ a = b^{\iota(a^{t+1})\psi^u}, \ z^{\ominus 1} \circ b \circ z = b^{\iota(a^s z)}.$$

Since $b^{\circ k} = b^k$ and $s \neq 0$, all groups $(G, \circ)$ are of type 11.

As to the conjugacy classes, let $\varphi \in \mathrm{Aut}(G)$. Write $\varphi = \varphi_1 \varphi_2$, where $\varphi_1 \in \mathrm{Hol}(\mathcal{C}_p)$ and $\varphi_2 \in \mathrm{Hol}(\mathcal{C}_q)$, so that

$$\varphi_1 : \begin{cases} z \mapsto z^i \\ a \mapsto az^j \\ b \mapsto b \end{cases}, \varphi_2 : \begin{cases} z \mapsto z \\ a \mapsto b^m a \\ b \mapsto b^k \end{cases}. \tag{4.32}$$

Since the kernel B is characteristic, then $\gamma_{|B}$ is stabilised by every automorphism of G.

Moreover

$$\begin{aligned}\gamma^{\varphi}(a) &= \varphi^{-1}\gamma(az^{-ji^{-1}})\varphi \\ &= \varphi^{-1}\gamma(a)\gamma(z)^{-ji^{-1}}\varphi \\ &= \varphi^{-1}\iota(a^{t-sji^{-1}})\psi^{u}\varphi \\ &= (\iota(a^{t-sji^{-1}}))^{\varphi_2}(\psi^{u})^{\varphi_1},\end{aligned}$$

and

$$\begin{aligned}\gamma^{\varphi}(z) &= \varphi^{-1}\gamma(z^{i^{-1}})\varphi \\ &= \varphi^{-1}\iota(a^{si^{-1}})\varphi \\ &= (\iota(a^{si^{-1}}))^{\varphi_2},\end{aligned}$$

so that φ stabilises γ if and only if $\varphi_1 = 1$ and $\varphi_2 \in \mathcal{C}_{q-1}$.

Therefore, the stabiliser has order $q-1$ and there are $p-1$ orbits of length $qp(p-1)$.

4.7.2 The case $|\ker(\gamma)| = pq$

Here $\gamma(G)$ is a subgroup of order p of $\langle\, \iota(a), \psi \,\rangle$. We look for the RGF's γ on A extending the assignments (4.30), (4.31), and with kernel of size p, namely $s = 0$ or $u = 0$.

Suppose first that $s = 0$, so that the kernel is ZB and $\gamma(a) = \iota(a)^t\psi^u$. By Lemma A.2 in the Appendix the RGF's on A with kernel of size p are precisely the morphisms.

1. If $t = 0$, then $\gamma(a) = \psi^u$ and every Sylow p-subgroup is $\gamma(G)$- invariant. Therefore here we obtain $p-1$ groups, and they are all of type 11 as b is $\gamma(b)$-invariant and
$$a^{\ominus 1} \circ b \circ a = b^{\iota(a)}.$$

2. If $t \neq 0$, then $\gamma(a) = \iota(a)^t\psi^u$, and $A = \langle\, a, z \,\rangle$ is the unique $\gamma(G)$-invariant Sylow p-subgroup, so that we have q choices for A, $p-1$ for t and p for u, namely $qp(p-1)$ functions. Since
$$a^{\ominus 1} \circ b \circ a = b^{\iota(a)^{t+1}},$$
they correspond to qp groups of type 5 and $qp(p-2)$ groups of type 11.

As to the conjugacy classes, here the kernel ZB is charactertistic, so that $\gamma_{|ZB}$ is stabilised by every automorphism of G.

Now, since $a^\varphi \equiv a \bmod \ker(\gamma)$, we have

$$\gamma^\varphi(a) = \varphi^{-1}\gamma(a)\varphi = \varphi^{-1}\iota(a^t)\psi^u\varphi = (\iota(a^t))^{\varphi_2}(\psi^u)^{\varphi_1},$$

so that φ stabilises γ if and only if it centralises $\gamma(a)$.

If $t = 0$, the last condition is equivalent to say that $\varphi_1 \in \langle\, \psi \,\rangle$ and $\varphi_2 \in \mathrm{Hol}(\mathcal{C}_q)$, so that the $p-1$ groups of type 11 form one orbit of length $p-1$.

If $t \neq 0$, then φ centralises $\gamma(a)$ if and only if $\varphi_2 \in \mathcal{C}_{q-1}$, and either $u \neq 0$ and $\varphi_1 \in \langle\, \psi \,\rangle$, or $u = 0$ and $\varphi_1 \in \mathrm{Hol}(\mathcal{C}_p)$. In the first case the stabiliser has order $p(q-1)$, and there is one orbit of length $q(p-1)$ for the type 5, and $p-2$ orbits of length $q(p-1)$ for the type 11. In the second case the stabiliser has order $p(p-1)(q-1)$, and there is one orbit of length q for the type 5, and $p-2$ orbits of length q for the type 11.

Suppose now $u = 0$, so that $\gamma(a) = \iota(a^t)$ and $\gamma(z) = \iota(a^s)$. Here $\ker(\gamma) = \langle\, v \,\rangle$, where $v = z^e a^f$ is such that $tf + se = 0$. Up to change the basis of A, we can appeal again to Lemma A.2, which yields that the RGF's here are exactly the morphisms. Again, $A = \langle\, a, z \,\rangle$ is the unique $\gamma(G)$-invariant Sylow p-subgroup, and we obtain $qp(p-1)$ functions. Since

$$z^{\ominus 1} \circ b \circ z = b^{\iota(a^s)}$$

they correspond to groups of type 11.

As to the conjugacy classes, since $B \leq \ker(\gamma)$ is characteristic, $\gamma_{|B}$ is stabilised by every automorphism φ. Moreover , let $\varphi = \varphi_1\varphi_2$ where φ_1, φ_2 are as in (4.32). We have

$$\gamma^\varphi(a) = \varphi^{-1}\gamma(az^{-ji^{-1}})\varphi = (\iota(a^{t-sji^{-1}}))^{\varphi_2},$$
$$\gamma^\varphi(z) = \varphi^{-1}\gamma(z^{i^{-1}})\varphi = (\iota(a^{si^{-1}}))^{\varphi_2},$$

so that φ stabilises γ if and only if $\varphi_1 = \mathrm{id}$ and $\varphi_2 \in \mathcal{C}_{q-1}$, namely the stabiliser has order $q-1$, and there is one orbit of length $qp(p-1)$.

We summarise, including the right and left regular representations.

Proposition 4.13. *Let G be a group of order p^2q, $p > 2$, of type 11. Then in* $\mathrm{Hol}(G)$ *there are:*

1. *$2pq$ groups of type 5, which split in two conjugacy classes of length q, and two conjugacy classes of length $q(p-1)$;*
2. *$2p(1 + q(p^2-2))$ groups of type 11, which split in*
   - *(a) two conjugacy classes of length 1;*
   - *(b) two conjugacy classes of length $p-1$;*
   - *(c) two conjugacy classes of length $qp(p-1)$;*
   - *(d) $2(p-1)$ conjugacy classes of length $qp(p-1)$;*
   - *(e) $2(p-2)$ conjugacy classes of length $q(p-1)$;*
   - *(f) $2(p-2)$ conjugacy classes of length q.*

4.8 Proof of Theorems 2 and 4

From Theorem 1 we have that, for each pair of finite groups Γ, G with $|\Gamma| = |G|$,

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} e'(\Gamma, G).$$

If the Sylow p-subgroups of the groups Γ and G are isomorphic, then the values of $e'(\Gamma, G)$ computed in Propositions 3.1, 3.2, 3.3, 3.4, 4.1, 4.2, 4.8, 4.9, 4.10, 4.12 and 4.13 and the cardinalities of the automorphism groups given in Table 2.1 yield the values of $e(\Gamma, G)$.

Propositions 3.1, 3.2, 3.3, 3.4, 4.1, 4.2, 4.8, 4.9, 4.10, 4.12 and 4.13 also yield, for $G = (G, \cdot)$, the numbers of conjugacy classes of regular subgroups of $\mathrm{Hol}(G)$, that is, the numbers of isomorphism classes of skew braces $(G, \cdot, \circ)$.

If the Sylow p-subgroups of the groups Γ and G are not isomorphic, then Corollary 2.4 yields $e'(\Gamma, G) = e(\Gamma, G) = 0$.

Chapter 5

Groups of order $4q$

In this chapter we deal with the case $p = 2$.

In [Koh07, Proposition 6.1] Kohl enumerates the Hopf-Galois structures on a Galois extension of degree $4q$, for $q > 3$. The Hopf-Galois structures on a Galois extension of degree 12 are enumerated by Byott in [SV18, Table A.2].

We will do this by using the gamma functions, and in addition we provide the number of isomorphism classes of skew braces $(G, \cdot, \circ)$ such that $\Gamma \simeq (G, \circ)$, where $\Gamma = \mathrm{Gal}(L/K)$.

We will prove the following (where the first and the second table are the results of Kohl, respectively Byott).

Theorem 5.1. *Let L/K be a Galois field extension of order $4q$ and let $\Gamma = \mathrm{Gal}(L/K)$.*

Then the following tables give the numbers $e(\Gamma, G)$ of Hopf-Galois structures on L/K of type G for each group G of order $4q$.

1. *If $q > 3$,*

Γ \ G	*1*	*2*	*3*	*5*	*11*
1	1	2	4	1	2
2	q	2	$4q$	q	2
3	q	$2q$	$2q+2$	q	$2q$
5	3	6	–	1	6
11	$3q$	$4q+2$	–	q	$4q+2$

2. If $q = 3$,

Γ \ G	*1*	*2*	*5*	*10*	*11*
1	1	2	1	-	2
2	3	2	3	12	2
5	3	6	1	4	6
10	-	-	4	10	-
11	9	14	3	-	14

Moreover the following tables give the numbers of isomorphism classes of skew braces $(G, \cdot, \circ)$ such that $\Gamma \cong (G, \circ)$.

1. If $q > 3$,

Γ \ G	*1*	*2*	*3*	*5*	*11*
1	1	2	2	1	2
2	1	2	2	1	2
3	1	2	4	1	2
5	1	2	–	1	2
11	2	4	–	1	4

2. If $q = 3$,

Γ \ G	*1*	*2*	*5*	*10*	*11*
1	1	2	1	-	2
2	1	2	1	2	2
5	1	2	1	2	2
10	-	-	1	4	-
11	2	4	1	-	4

The lengths of the conjugacy classes are spelled out in Propositions 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

Hereafter, we proceed to prove Theorem 5.1.

The case $p = 2$ is special since, as the tables above show, the isomorphism class of the Sylow 2-subgroups may change from G to $(G, \circ)$. This is due to the elementary fact that the regular subgroups

$$\langle\, (1234) \,\rangle\,, \quad \text{and} \quad \langle\, (12)(34), (13)(24) \,\rangle$$

of $\mathcal{S}_4$ normalise each other, as they are both maximal in the common Sylow 2-subgroup $\langle\, (1234), (12)(34) \,\rangle$.

Let G be a group of order $4q$. Then G can be of type 1, 2, 3, 5, or 11 if $q > 3$, and of type 1, 2, 5, 10, or 11 if $q = 3$.

As usual, A denotes a Sylow 2-subgroup (so $A \simeq \mathcal{C}_4$ or $\mathcal{C}_2 \times \mathcal{C}_2$) and B a Sylow q-subgroup, which is always characteristic if $q > 3$.

Let γ be a GF on G.

If G is cyclic (type 1), then there are no elements of order q in $\mathrm{Aut}(G)$, thus $B \leq \ker(\gamma)$. The same is true also for G of type 5 when $q > 3$.

If G is of type 2, 3 or 11, we are under the assumptions of Proposition 2.1 with $H = B$, thus we can just consider the case when $B \leq \ker(\gamma)$. Moreover for G as above, by Theorem 2.3, there exists a Sylow p-subgroup A of G which is $\gamma(A)$-invariant, thus, by Proposition 1.13, each GF such that B is contained into the kernel is the lifting of a RGF defined on an invariant Sylow 2-subgroup A.

Since A is always $\gamma(A)$-invariant, if $\gamma : A \to \mathrm{Aut}(G)$ is a RGF, then the map $a \mapsto \gamma(a)_{|A}$ is a GF on A.

The following proposition gives an easy criterion to establish when $(A, \circ)$ changes the isomorphism type.

Proposition 5.2. *Let A be a group of order 4 and γ a GF on A. Then*

$$(A, \circ) \cong A \quad \textit{if and only if} \quad \gamma(A) = \{1\}.$$

Proof. Since $\mathrm{Aut}(\mathcal{C}_4) = \{\pm 1\}$ and $\mathrm{Aut}(V_4) \cong S_3$, $|\gamma(A)| \mid (|\mathrm{Aut}(A)|, 4) = 2$. Therefore, $\gamma(A) = \{1\}$ or $\gamma(A) = \langle \alpha \rangle$ where α is the inversion $a \mapsto a^{-1}$ if A is cyclic, and α is the transposition of two elements of order 2, say a_1 and a_2, if A is elementary abelian.

If $\gamma(A) = \{1\}$, then γ is a morphism and $(A, \circ) \cong A$.

Suppose now $\gamma(A) = \langle \alpha \rangle$. If $A = \langle a \rangle$, then $\ker(\gamma) = \langle a^2 \rangle$ and $a^{\circ 2} = a^\alpha a = 1$, thus $(A, \circ)$ is elementary abelian since both a and a^2 have order 2. If A is elementary abelian then $a_1^{\circ 2} = a_1^\alpha a_1 = a_2 a_1 \neq 1$, so that $(A, \circ)$ is cyclic. Therefore, in both the cases $(A, \circ) \not\cong A$, proving the proposition. □

5.1 G of type 1

In this case $G = \mathcal{C}_4 \times \mathcal{C}_q$ and $\mathrm{Aut}(G) = \mathcal{C}_2 \times \mathcal{C}_{q-1}$. Let $A = \langle a \rangle$ be the Sylow 2-subgroup, and $B = \langle b \rangle$ the Sylow q-subgroup.

As said above, if $q > 3$ then $B \leq \ker(\gamma)$. In this case, also for $q = 3$ in $\mathrm{Aut}(G)$ there are no elements of order 3, so let $B \leq \ker(\gamma)$. We look for the RGF's $A \to \mathrm{Aut}(G)$ (which we still denote by γ).

Consider the automorphisms of G

$$\alpha : \begin{cases} a \mapsto a^{-1} \\ b \mapsto b \end{cases}, \qquad \beta_k : \begin{cases} a \mapsto a \\ b \mapsto b^k \end{cases}, \tag{5.1}$$

with $k \in \mathcal{C}_q^*$. $\gamma(a)_{|A}$ is either 1 or α, and, according to Proposition 5.2, this corresponds to $(A, \circ)$ being cyclic or not. Here

$$a^{\ominus 1} \circ b \circ a = a^{-\gamma(a)^{-1}\gamma(b)\gamma(a)} b^{\gamma(a)} a = b^{\gamma(a)}.$$

If $\gamma(a)_{|A} = 1$ then γ is a morphism, and there are the following possibilities.

1. $\gamma(a) = 1$, namely the right regular representation;
2. $\gamma(a) = \beta_{-1}$, which corresponds to a group of type 2;
3. if moreover $4 \mid q-1$, we can also have $\gamma(a) = \beta_j^{\pm 1}$, where j has order 4, and we get further 2 groups of type 3.

If $\gamma(a)_{|A} = \alpha$, then $(A, \circ)$ is elementary abelian. An easy computation shows that the image $\gamma(a)_{|A}$ determines also $\gamma(a^{-1})_{|A}$ and $\gamma(a^2)_{|A}$, as we have $\gamma(a)_{|A} = \gamma(a^{-1})_{|A}$ and $\gamma(a^2)_{|A} = 1$. Since $\gamma : (A, \circ) \to \mathrm{Aut}(G)$ is a morphism, each γ of this case is defined by $\gamma(a) = \alpha\beta_{-1}^l$, $\gamma(a^2) = \beta_{-1}^m$ with $l, m \in \{0, 1\}$.

For $l = m = 0$ we get a group of type 5; otherwise, in the other three cases, we get groups of type 11.

As to the conjugacy classes, let α and β_k as in (5.1). Since $\mathrm{Aut}(G)$ is abelian and β_k centralises a, then $\langle\, \beta_k \,\rangle$ stabilises γ. Moreover,

$$\gamma^\alpha(a) = \gamma(a^{\alpha^{-1}}) = \gamma(a^{-1}).$$

If $\gamma(a)_{|A} = 1$ then $\gamma(a) = \beta_j$ with $\mathrm{ord}(j) \mid 4$, so that α stabilises γ precisely when $\mathrm{ord}(j) \mid 2$. In these cases we get one orbit of length 1, while for j of order 4 the stabiliser has order $q-1$, and there is one orbit of length 2.

If $\gamma(a)_{|A} = \alpha$ then α stabilises γ if and only if $\gamma(a)_{|B} = \gamma(a^{-1})_{|B}$ (two possibilities); in this case we get 2 classes of length 1. Otherwise $\gamma(a)_{|B} \neq \gamma(a^{-1})_{|B}$ and the stabiliser has order $q-1$, therefore we get one orbit of length 2.

We summarise our results in the next Proposition.

Proposition 5.3. *Let G be a group of order $4q$ of type 1. Then in* $\mathrm{Hol}(G)$ *there are:*

1. 1 *group of type 1, which forms one conjugacy class of length* 1*;*
2. 1 *group of type 2, which forms one conjugacy class of length* 1*;*
3. *if* $4 \mid q-1$*, further* 2 *groups of type 3, which form one conjugacy class of length* 2*;*
4. 1 *group of type 5, which forms one conjugacy class of length* 1*;*
5. 3 *groups of type 11, which split in one conjugacy class of length* 1*, and one conjugacy class of length* 2*.*

5.2 G of type 2

Here $G = \mathcal{C}_q \rtimes_2 \mathcal{C}_4$ and $\mathrm{Aut}(G) = C_2 \times \mathrm{Hol}(\mathcal{C}_q)$.

The automorphism α of order 2 in the centre of $\mathrm{Aut}(G)$ is the identity on B, and acts as inversion on any Sylow 2-subgroup. If $4 \mid q-1$, let $\beta \in \mathrm{Hol}(\mathcal{C}_q)$ be such that $\beta^2 = \iota(a)$.

The Sylow q-subgroup B can be assumed to be in the kernel of γ. Moreover, as usual, there is (at least) one $\gamma(G)$-invariant Sylow 2-subgroup $A = \langle\, a \,\rangle$, and $\gamma(G) = \gamma(A)$. Notice that in all cases when $\iota(a) \in \gamma(G)$ then $A = \langle\, a \,\rangle$ is the only invariant Sylow 2-subgroup of G.

As for the operation $\circ$, for each $a' \in A$, we have

$$a'^{\ominus 1} \circ b \circ a' = a'^{-1} b^{\gamma(a')} a' = b^{\gamma(a')\iota(a')}.$$

If $\gamma(a)_{|A} = 1$, then $(A, \circ)$ is cyclic and γ is a morphism, so we get, before doubling,

1. 1 group of type 2, namely the right regular represention, when $\gamma(G) = \{1\}$;
2. q groups of type 1, for the q choices of A, and $\gamma(a) = \iota(a)$;
3. when $4 \mid q-1$, further $2q$ groups of type 3 for the q choices of A and $\gamma(a) = \beta^{\pm 1}$.

If $\gamma(a)_{|A} = \alpha$, then $(A, \circ)$ is elementary abelian, $\gamma(a)$ has order 2, and $\gamma(a^2)_{|A} = 1$. We distinguish two cases:

1. if $|\gamma(A)| = 4$, then $\gamma(a^2) = \iota(a)$, and $\gamma(a)$ is either α or $\alpha\iota(a)$, so that we obtain $2q$ groups of type 11;
2. if $|\gamma(A)| = 2$, then $\gamma(a^2) = 1$ and either $\gamma(a) = \alpha$, so that the choice of A is irrelevant and we get one group of type 11, or $\gamma(a) = \alpha\iota(a)$, so that we get q groups of type 5.

As to the conjugacy classes, an automorphism $\mu \in \mathcal{C}_{q-1}$ centralises a and $\gamma(a)$, so that $\langle\, \mu \,\rangle$ is in the stabiliser of each γ.

Moreover

$$\gamma^{\alpha}(a) = \alpha^{-1}\gamma(a^{\alpha^{-1}})\alpha = \gamma(a^{-1}),$$
$$\gamma^{\iota(b)}(a) = \iota(b^{-1})\gamma(a^{\iota(b^{-1})})\iota(b) = \iota(b^{-1})\gamma(a)\iota(b).$$

Thus all classes, except those corresponding to $\gamma(a) = 1$ and $\gamma(a) = \alpha$, have order a multiple of q.

Suppose $\gamma(a)_{|A} = 1$; if $\gamma(a) = 1$ we get one class of length 1. If $\gamma(a) = \gamma(a^{-1})$, namely $\gamma(a)^2 = 1$ and so $\gamma(a) = \iota(a)$, we get one class of length q. The

case $\gamma(a) \neq \gamma(a^{-1})$ can happen only if $4 \mid q-1$ and $\gamma(a) = \beta^{\pm 1}$, and here we get one class of length $2q$.

Now assume $\gamma(a)_{|A} = \alpha$; if $\gamma(a) = \gamma(a^{-1}) = \alpha$ we get one class of length 1; since $\gamma(a^{-1}) = \gamma(a^2)\gamma(a)$, this happens when $(G, \circ)$ is of type 11. If $\gamma(a) = \gamma(a^{-1}) = \iota(a)\alpha$, then $(G, \circ)$ is of type 11 and we obtain one class of length q. For $\gamma(a) \neq \gamma(a^{-1})$ we get one class of length $2q$.

Proposition 5.4. *Let G be a group of order $4q$ of type 2. Then in* $\mathrm{Hol}(G)$ *there are:*

1. $2q$ *groups of type 1, which split in two conjugacy classes of length q;*
2. 2 *groups of type 2, which split in two conjugacy classes of length* 1*;*
3. *if $4 \mid q-1$, further $4q$ groups of type 3, which split in two conjugacy classes of length $2q$;*
4. $2q$ *groups of type 5, which split in two conjugacy classes of length q;*
5. $4q+2$ *groups of type 11, which split in two conjugacy classes of length* 1*, and two conjugacy classes of length $2q$.*

5.3 G of type 3

Here $G = \mathcal{C}_q \rtimes \mathcal{C}_4$, with $4 \mid q-1$ (so that $q > 3$), and $\mathrm{Aut}(G) = \mathrm{Hol}(\mathcal{C}_q)$.

As usual, we may assume that the Sylow q-subgroup B is contained in $\ker(\gamma)$. By Lemma 1.12 all the GF's here are morphisms.

Since $|\gamma(G)| \mid 4$, we have that $\gamma(G)$ is a cyclic subgroup of $\langle\, \iota(a) \,\rangle$, for some $a \in G$, $\mathrm{ord}(a) = 4$, and if $\gamma(G) \neq \{1\}$, then $A = \langle\, a \,\rangle$ is the unique $\gamma(G)$-invariant Sylow 2-subgroup of G.

As for the operation $\circ$, we have

$$a^{\ominus 1} \circ b \circ a = a^{-1} b^{\gamma(a)} a = b^{\gamma(a)\iota(a)}.$$

Therefore, before doubling, we get

1. one group of type 3, namely the right regular representation, if $\gamma(a) = 1$;
2. q groups of type 2, one for each choice of A, if $\gamma(a) = \iota(a)$.
3. q groups of type 3 if $\gamma(a) = \iota(a^2)$;
4. q groups of type 1 if $\gamma(a) = \iota(a^{-1})$;

As to the conjugacy classes, as in the previous case each element of $\mathcal{C}_{q-1}$ stabilises γ. The action of $\iota(B)$ is

$$\gamma^{\iota(b)}(a) = \iota(b^{-1})\gamma(a^{\iota(b^{-1})})\iota(b) = \iota(b^{-1})\gamma(a)\iota(b),$$

so that all classes have order q, except when $\gamma(a) = 1$.

Therefore we get one class of length 1, and 3 classes of length q, corresponding to $\gamma(a) \neq 1$.

Proposition 5.5. *Let G be a group of order $4q$ of type 3. Then in* $\mathrm{Hol}(G)$ *there are:*

1. *$2q$ groups of type 1, which split in two conjugacy classes of length q;*
2. *$2q$ groups of type 2, which split in two conjugacy classes of length q;*
3. *$2q + 2$ groups of type 3, which split in two conjugacy classes of length q and two conjugacy classes of length* 1.

5.4 G of type 5

Here $G = \mathcal{C}_2 \times \mathcal{C}_2 \times C_q$ and $\mathrm{Aut}(G) = \mathrm{GL}(2,2) \times \mathcal{C}_{q-1}$.

The case $q > 3$. Suppose first $q > 3$, so that $B \leq \ker(\gamma)$. Here there is a unique Sylow 2-subgroup $A = \{1, a_1, a_2, a_3\}$ which is characteristic, so we look for the RGF's $A \to \mathrm{Aut}(G)$, which we still denote by γ.

For $i = 1, 2, 3$ and $k \in \mathcal{C}_q^*$, consider the automorphisms of G

$$\alpha_i : \begin{cases} a_j \mapsto a_l \text{ for } \{i,j,l\} = \{1,2,3\} \\ a_i \mapsto a_i \\ b \mapsto b \end{cases}, \quad \beta_k : \begin{cases} a_h \mapsto a_h \text{ for } h = 1,2,3 \\ b \mapsto b^k \end{cases}.$$

We have $\gamma(A) \leq \langle\, \alpha_i, \beta_k \mid i = 1,2,3,\ \mathrm{ord}(k) \mid 4 \,\rangle$.

Consider first the case $\gamma(A)_{|A} = \{1\}$, so $(A, \circ)$ is elementary abelian and the RGF's on A are precisely the morphisms. If $\gamma(A) = \{1\}$, then we get the right regular representation, namely one group of type 5. We have further three RGF's with $\gamma(A)_{|A} = \{1\}$, for which $\gamma(A) = \langle\, \beta_{-1} \,\rangle$. They are defined by $\gamma(a_l) = 1$ and $\gamma(a_i) = \gamma(a_j) = \beta_{-1}$, and they give 3 groups of type 11.

Suppose now $\gamma(A)_{|A} \neq \{1\}$, so that $\gamma(A)_{|A} = \langle \alpha_l \rangle$ for a certain l. Here $(A, \circ)$ is cyclic, and since $a_l^{\circ 2} = 1$, $(A, \circ)$ is generated by a_i, for $i \neq l$. Moreover, an easy computation shows that the image $\gamma(a_i)_{|A}$ determines also $\gamma(a_j)_{|A}$ and $\gamma(a_l)_{|A}$, namely $\gamma(a_i)_{|A} = \gamma(a_j)_{|A}$ and $\gamma(a_l)_{|A} = 1$. Now, the RGF's are the morphisms $(A, \circ) \to \mathrm{Aut}(G)$, thus they are defined by $\gamma(a_i) = \alpha_l \beta_k$, where $k \in \mathcal{C}_{q-1}$ and $\mathrm{ord}(k) \mid 4$. Since

$$a_i^{\ominus 1} \circ b \circ a_i = a_i^{-1} b^{\gamma(a_i)} a_i = b^{\beta_k},$$

for $k = 1$ and for each l (3 cases) we get groups of type 1, for $k = -1$ and for each l (3 cases), groups of type 2, and when $4 \mid q - 1$ for $\mathrm{ord}(k) = 4$ and for each l (6 cases) we get groups of type 3.

As to the conjugacy classes, the subgroup $\mathcal{C}_{q-1}$ of $\mathrm{Aut}(G)$ is in the stabiliser of each γ.

Let π be a permutation in $\mathcal{S}_3 \simeq \mathrm{GL}(2,2)$. We have

$$\gamma^\pi(a_i) = \pi^{-1}\gamma(a_i^{\pi^{-1}})\pi = \pi^{-1}\gamma(a_{\pi^{-1}(i)})\pi,$$

so that a 3-cycle is not in the stabiliser of any γ, except when γ is the right regular representation, and a transposition (i,j) stabilises γ if and only if $\gamma(a_i) = \gamma(a_j)$. Note that for $\pi = (i,j)$, $\gamma^\pi(a_i)_{|A} = \gamma(a_j)_{|A}$.

If $\gamma(A)_{|A} = \{1\}$, then we get one class of length 1 for the right regular representation; moreover the GF's $\gamma(a_l) \neq \gamma(a_i) = \gamma(a_j)$ have (i,j) in their stabiliser, so that for each of these three GF's the stabiliser has order $2(q-1)$ and we get one orbit of length 3.

If $\gamma(A)_{|A} \neq \{1\}$, then each orbit has length a multiple of 3, as a 3-cycle is not in the stabiliser of γ. Moreover, $\gamma(a_i) = \alpha_l\beta_k$ has (i,j) in its stabiliser precisely when $\gamma(a_i)_{|B} = \gamma(a_j)_{|B}$. Therefore each of the two cases in which $\mathrm{ord}(k) \mid 2$ yields one orbit of length 3, and in the case $4 \mid q-1$ and $\mathrm{ord}(k) = 4$ we get one orbit of length 6.

The case $q = 3$. If $q = 3$, when $\gamma(A) = 1$, then the GF's on G correspond to the RGF's on B, and these are precisely the morphisms $B \to \mathrm{Aut}(G)$. We can choose the image in two non trivial ways, and the commutation rule with respect to the circle operation yields 2 groups of type 10 (note that b is $\gamma(b)$-invariant). As to the conjugacy classes, the stabiliser here consist of the elements $\beta_{-1}^l\pi$, where if $l = 0$ then π is a 3-cycle, and if $l = 1$ then π is a transposition. Therefore there is one conjugacy class of length 2.

Reasoning as for the case $q > 3$ we obtain as many group $(G,\circ)$ of type 1, 2, 5, and 11 as above. Moreover there are no other cases, as if $\gamma(A) = \langle\, \beta_{-1} \,\rangle$ and $\gamma(b) \in \mathrm{GL}(2,p)$ then $\gamma(a)$ and $\gamma(b)$ commute, so that $(G,\circ)$ can have only type 5. Now the commutation rule in $(G,\circ)$ yields $\gamma(b) = 1$. If $\gamma(A) = \langle\, \alpha_l \,\rangle$, then $(G,\circ)$ can be of type 1 or 2. Keeping in mind that $\gamma : (G,\circ) \to \mathrm{Aut}(G)$ is a morphism, it is easy to see that in both the cases necessarily $\gamma(b) = 1$.

Proposition 5.6. *Let G be a group of order $4q$ of type 5. Then in* $\mathrm{Hol}(G)$ *there are:*

1. 3 *groups of type 1, which form one conjugacy class of length* 3*;*
2. 3 *groups of type 2, which form one conjugacy class of length* 3*;*
3. *if* $4 \mid q-1$, *further* 6 *groups of type 3, which form one conjugacy class of length* 6*;*
4. 1 *group of type 5, which forms one conjugacy class of length* 1*;*
5. 3 *groups of type 11, which form one conjugacy class of length* 3*.*
6. *If* $q = 3$, 2 *groups of type 10, which form one conjugacy class of length* 2*;*

5.5 G of type 11

Here $G = \mathcal{C}_2 \times (\mathcal{C}_2 \ltimes \mathcal{C}_q)$ and $\mathrm{Aut}(G) = \mathcal{C}_2 \times \mathrm{Hol}(\mathcal{C}_q)$.

As usual, we may just consider the case when the Sylow q-subgroup B is contained in the kernel of γ, so that there is a $\gamma(G)$-invariant Sylow 2-subgroup A, and $\gamma(G) = \gamma(A)$. Write $A = \langle\, z, a \,\rangle$, where $z \in Z(G)$, and a lies in the $\mathcal{C}_q \rtimes \mathcal{C}_2$ dihedral factor. The central factor $\mathcal{C}_2$ of $\mathrm{Aut}(G)$ is spanned by the central automorphism

$$\alpha : \begin{cases} a \mapsto az \\ z \mapsto z \\ b \mapsto b \end{cases} .$$

As to the circle operation, we have

$$a^{\ominus 1} \circ b \circ a = b^{\gamma(a)\iota(a)}$$
$$z^{\ominus 1} \circ b \circ z = b^{\gamma(z)}.$$

Suppose first $\gamma(A)_{|A} = \{1\}$, so that $(A, \circ)$ is elementary abelian and the RGF's on A are precisely the morphisms $A \to \mathrm{Aut}(G)$. If $\gamma(a) = \gamma(z) = 1$ we get the right regular representation, namely one group of type 11. If $\gamma(a) = \iota(a)$ and $\gamma(z) = 1$ we get q groups of type 5, as there are q choices for an invariant Sylow 2-subgroup A. The other two cases, namely $\gamma(a) = 1, \gamma(z) = \iota(a)$ and $\gamma(a) = \gamma(z) = \iota(a)$, yield $2q$ groups of type 11.

Suppose now $\gamma(A)_{|A} \neq \{1\}$, so that $(A, \circ)$ is cyclic. Since $z \circ z = z^{\gamma(z)} z = 1$, $(A, \circ)$ is generated by a. Moreover $\gamma(a)_{|A} = \gamma(az)_{|A}$ and $\gamma(z)_{|A} = 1$. The RGF's on A are the morphisms $(A, \circ) \to \mathrm{Aut}(G)$, therefore there are the following possibilities.

1. $\gamma(a) = \alpha$, and this yields 1 group of type 2, as here the choice of A is irrelevant;

2. $\gamma(a) = \alpha\iota(a)$, and this yields q groups of type 1, as there are q choices for A;

3. if $4 \mid q - 1$, let β an element of order 4 in $\mathrm{Aut}(G)$ such that $\beta^2 = \iota(a)$; then $\gamma(a) = \alpha\beta^{\pm 1}$ yields futher $2q$ groups of type 3.

As to the conjugacy classes, also in this case the subgroup $\mathcal{C}_{q-1}$ of $\mathrm{Aut}(G)$ is in the stabiliser of each γ. Moreover, the automorphisms α and $\iota(b)$ centralise z and $\gamma(z)$, so that they centralise $\gamma_{|Z}$.

Now,

$$\gamma^{\alpha}(a) = \alpha\gamma(a^{\alpha})\alpha = \gamma(a)\gamma(z),$$
$$\gamma^{\iota(b)}(a) = \iota(b^{-1})\gamma(a^{\iota(b^{-1})})\iota(b) = \iota(b^{-1})\gamma(a)\iota(b).$$

Therefore α stabilises γ if and only if $\gamma(z) = 1$, and $\iota(B)$ stabilises γ if and only if $\gamma(a)$ commutes with $\iota(B)$, namely when $\gamma(a) \in \{1, \alpha\}$.

If $\gamma(A)_{|A} = \{1\}$ we have one orbit of length 1 for the right regular representation, one orbit of length q for $\gamma(a) = \iota(a), \gamma(z) = 1$, as in this case the stabiliser has order $2(q-1)$, and one orbit of length $2q$, as for the remaining cases the stabiliser has order $q-1$.

If $\gamma(A)_{|A} \neq \{1\}$, when $\gamma(a) = \alpha$, it is stabilised by any automorphism, so that there is an orbit of length 1. If $\gamma(a) = \alpha\iota(a)$, then α is in the stabiliser, since $\gamma(z) = 1$ here, so that this yields one orbit of length q. Lastly, the GF's $\gamma(a) = \alpha\beta^{\pm 1}$ yield one orbit of length $2q$, as the stabiliser here has length $q-1$.

Proposition 5.7. *Let G be a group of order $4q$ of type 11. Then in* $\mathrm{Hol}(G)$ *there are:*

1. *$2q$ groups of type 1, which split in two conjugacy classes of length q;*
2. *2 groups of type 2, which split in two conjugacy classes of length 1;*
3. *if $4 \mid q-1$, further $4q$ groups of type 3, which split in two conjugacy classes of length $2q$;*
4. *$2q$ groups of type 5, which split in two conjugacy classes of length q;*
5. *$4q+2$ groups of type 11, which split in two conjugacy classes of length 1, and two conjugacy classes of length $2q$.*

5.6 G of type 10

If G is of type 10 then $q = 3$. Here $G = (\mathcal{C}_2 \times \mathcal{C}_2) \rtimes_C \mathcal{C}_3$ and $\mathrm{Aut}(G) = (\mathcal{C}_2 \times \mathcal{C}_2) \rtimes (\mathcal{C}_3 \rtimes \mathcal{C}_2)$.

Let γ be a GF on G. If $\gamma(A)_{|A} = 1$ then $(A, \circ)$ is elementary abelian and $\gamma(A) \leq \mathrm{Inn}(G)$. Reasoning as in the general case for $p > 2$ (Section 4.6) we obtain

1. 8 groups of type 5, which split in 2 classes of length 4,
2. 10 groups of type 10, which split in 2 classes of length 1 and 2 classes of length 4.

Suppose now $\gamma(A)_{|A} \neq 1$. Then $(A, \circ)$ is cyclic and $(G, \circ)$ can be of type 1 or 2. If $(G, \circ)$ is of type 1, then $|\gamma(G)| \neq 6, 12$, as $\gamma : (G, \circ) \to \mathrm{Aut}(G)$ is a morphism. Moreover in both the cases $|\gamma(G)| = 2, 3$ the commutation rule with respect to the circle operation yields a contradiction. Therefore $(G, \circ)$ is of type 2. Since $\ker(\gamma)$ is a normal subgroup of $(G, \circ)$, it can have size 6, 3 or 2 (recall that the type 2 has centre of order p). If $3 \mid |\ker(\gamma)|$, the GF's on G correspond to the RGF's on A such that B is invariant under $\{\gamma(a)\iota(a) : a \in A\}$, namely

$\gamma(a) = \psi\iota(a^{-1})$, where ψ is defined in (4.24). Therefore there are 12 groups of type 2. If $|\ker(\gamma)| = 2$ there are further 12 morphisms $(G, \circ) \to \mathrm{Aut}(G)$. Routine computations show that they split in 2 classes of length 12.

Proposition 5.8. *Let G be a group of order 12 of type 10. Then in $\mathrm{Hol}(G)$ there are:*

1. *24 groups of type 2, which split in two conjugacy classes of length 12;*
2. *8 groups of type 5, which split in two conjugacy classes of length 4;*
3. *10 groups of type 10, which split in two conjugacy classes of length 1, and two conjugacy classes of length 4.*

5.7 Proof of Theorem 5.1

The values of $e'(\Gamma, G)$ computed in Propositions 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8 and the cardinalities of the automorphism groups given in Table 2.1 yield the values of $e(\Gamma, G)$ (via Theorem 1).

The same propositions also yields the numbers of conjugacy classes of regular subgroups of $\mathrm{Hol}(G)$, that is, the numbers of isomorphism classes of skew braces $(G, \cdot, \circ)$.

Appendix A

In showing that a map γ is a gamma function, for some types of group there is a recurring argument. We collect here two results: the first applies to the groups of type 5 and 11, when γ has kernel of size q, and the second applies to the groups of type 5, 7, and 11, in the case $|\ker(\gamma)| = pq$.

The following Lemma proves that the maps found in Subsections 4.2.2, 4.7.1 in the case $|\ker(\gamma)| = q$ are gamma functions.

Lemma A.1. *Let G be a group of type 5 or 11, B its Sylow q-subgroup, and $A = \langle\, a_1, a_2 \,\rangle$ a Sylow p-subgroup.*

Let $\gamma : A \to \mathrm{Aut}(G)$ a map such that

$$\begin{cases} \gamma(a_1) & = \eta_1 \\ \gamma(a_2) & = \eta_2, \end{cases} \tag{A.1}$$

where $\eta_{1|A} = 1$, $a_1^{\eta_2} = a_1$, $a_2^{\eta_2} = a_2 a_1^k$, $1 \leq k < p$.

Then

$$\gamma(a_1^n a_2^m) = \eta_1^{n-k(1+\cdots+(m-1))}\eta_2^m$$

is the unique RGF extending the assignment above.

Proof. By our assumptions A is clearly $\gamma(A)$-invariant. Moreover

$$\begin{aligned} \gamma((a_1^n a_2^m)^{\gamma(a_1^e a_2^f)} a_1^e a_2^f) &= \gamma((a_1^n a_2^m)^{\eta_1^{e-k(1+\cdots+(f-1))}\eta_2^f} a_1^e a_2^f) \\ &= \gamma(a_1^n (a_2^m)^{\eta_2^f} a_1^e a_2^f) \\ &= \gamma(a_1^{n+e+kfm} a_2^{m+f}) \\ &= \eta_1^{n+e+kfm-k(1+\cdots+(m+f-1))}\eta_2^{m+f}, \end{aligned}$$

and, on the other hand,

$$\begin{aligned} \gamma(a_1^n a_2^m)\gamma(a_1^e a_2^f) &= \eta_1^{n-k(1+\cdots+(m-1))}\eta_2^m \eta_1^{e-k(1+\cdots+(f-1))}\eta_2^f \\ &= \eta_1^{n-k(1+\cdots+(m-1))+e-k(1+\cdots+(f-1))}\eta_2^{m+f}. \end{aligned}$$

Therefore γ satisfies the GFE if and only if

$$-k(\sum_{s=1}^{m+f-1} s) + fkm \equiv -k(\sum_{s=1}^{m-1} s + \sum_{s=1}^{f-1} s) \bmod p,$$

that is,

$$\sum_{s=m}^{m+f-1} s - fm \equiv \sum_{s=1}^{f-1} s \bmod p.$$

Since $m+(m+1)+\cdots+(m+f-1) = fm+(1+\cdots+f-1)$, the last condition holds true, and γ is a RGF on A.

Now let γ' be a RGF on A extending the assignment (A.1). Since $\eta_{1|A} = 1$, necessarily $a_1^{\circ n} = a_1^n$, so

$$\gamma'(a_1^n a_2^m) = \gamma'((a_2^m)^{\gamma'(a_1^n)^{-1}})\gamma'(a_1^n) = \gamma'(a_2^m)\gamma'(a_1)^n.$$

Moreover

$$\begin{aligned}\gamma'(a_2^m) &= \gamma'((a_2^{m-1})^{\gamma'(a_2)^{-1}})\gamma'(a_2)\\ &= \gamma'(a_1^{-k(m-1)}a_2^{m-1})\gamma'(a_2)\\ &= \gamma'(a_1)^{-k(m-1)}\gamma'(a_2^{m-1})\gamma'(a_2).\end{aligned}$$

By induction we obtain $\gamma'(a_2^m) = \gamma'(a_1)^{-k((m-1)+(m-2)+\cdots+1)}\gamma'(a_2)^m$, so that

$$\gamma'(a_1^n a_2^m) = \gamma'(a_1)^{n-k((m-1)+(m-2)+\cdots+1)}\gamma'(a_2)^m,$$

namely $\gamma' = \gamma$. □

The following Lemma proves that the maps γ in Subsections 4.2.2, 4.5.1 and 4.7.2, in the case $|\ker(\gamma)| = pq$, satisfy the assumptions of Lemma 1.12.

Lemma A.2. *Let G be a group of order p^2q, $A = \langle a_1, a_2 \rangle$ a Sylow p-subgroup of G, and $\gamma : A \to \mathrm{Aut}(G)$ a map such that*

$$\begin{cases} \gamma(a_1) = \varphi \text{ (possibly modulo } \iota(A)) \\ \gamma(a_2) = 1 \end{cases},$$

where $a_2^\varphi = a_2$, $a_1^\varphi = a_1 a_2^{k_\varphi}$ for a certain k_φ.

Then γ extends to a unique RGF on A if and only if γ is a morphism.

Proof. We show that

$$[A, \gamma(A)] = [A, \gamma(\langle a_1 \rangle)] \subseteq \langle a_2 \rangle,$$

and then, by Lemma 1.12, the RGF's on A with kernel $\langle a_2 \rangle$ correspond to the morphisms $A \to \mathrm{Aut}(G)$.

Note that if γ is a RGF or a morphism, then $\gamma(a_1^s) = \gamma(a_1)^s$, as $\ker(\gamma) = \langle a_2 \rangle$. Thus we have

$$(a_2^m a_1^t)^{-1}(a_2^m a_1^t)^{\gamma(a_1^s)} = (a_2^m a_1^t)^{-1+\varphi^s} = (a_1^t)^{-1+\varphi^s} = a_2^{tk_{\varphi^s}} \in \langle a_2 \rangle.$$

□

Appendix B

Table B.1: Number of GF on a group G of type 8, $|\ker(\gamma)| = p$

$G8$	T5	T6	T7
A1+A1*	0	$2p(p^2-1)$	0
A2+A2*	0	$2p^2(p-1)$	0
A3+A3*	$2p^2$	$2p+4p^2(q-2)$	$4p+2p^2(q-3)$
B1+B1*	0	$2p(p-1)+2p^2(p-1)$	0

$G8$	T8		T9	
A1	$2p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$p(p-1)$	if $k=-1/2$
	$2p^2(p-1)$	G_s, $\forall s \neq 1+k^{-1}$	$p^2(p-1)$	if $k \neq -1/2$
	$p(p-1)+p^2(p-1)$	$G_{1+k^{-1}}$		
A2	$2p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$p(p-1)$	if $k=1/2$
	$2p^2(p-1)$	G_s, $\forall s \neq 1-k^{-1}$	$p^2(p-1)$	if $k \neq 1/2$
	$p(p-1)+p^2(p-1)$	$G_{1-k^{-1}}$		
A3	$1+2p+p^2(2q-5)$	G_{-k}	$2p+p^2(q-3)$	
	$4p+2p^2(q-3)$	G_s, $\forall s \neq -k$		
A1*	$2p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$p(p-1)$	if $k=-2$
	$2p^2(p-1)$	G_s, $\forall s \neq 1+k$	$p^2(p-1)$	if $k \neq -2$
	$p(p-1)+p^2(p-1)$	G_{1+k}		
A2*	$2p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$p(p-1)$	if $k=2$
	$2p^2(p-1)$	G_s, $\forall s \neq 1-k$	$p^2(p-1)$	if $k \neq 2$
	$p(p-1)+p^2(p-1)$	G_{1-k}		
A3*	$1+2p+p^2(2q-5)$	$G_{-k^{-1}}$	$2p+p^2(q-3)$	
	$4p+2p^2(q-3)$	G_s, $\forall s \neq -k^{-1}$		
B1	$2p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$p(p-1)$	if $k=1/2$
	$2p^2(p-1)$	G_s, $\forall s \neq 1-k^{-1}$	$p^2(p-1)$	if $k \neq 1/2$
	$p(p-1)+p^2(p-1)$	$G_{1-k^{-1}}$		
B1*	$2p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$p(p-1)$	if $k=2$
	$2p^2(p-1)$	$\forall s \neq 1-k$	$p^2(p-1)$	if $k \neq 2$
	$p(p-1)+p^2(p-1)$	G_{1-k}		

Table B.2: Number of GF on a group G of type 7, $|\ker(\gamma)| = p$

$G7$	T5	T6
A1+A1*	0	$p^2(p+1)(p^2-1)$
A2+A2*	0	$2p(p-1)$
A3+A3*	$p^3(p+1)$	$2p(1+p^2(p+1)(q-2))$
B2	0	$p^2(p-1)$
Sec 4.5	$p^2(p^2-1)$	$p^3(p^2-1)$

$G7$	T7	T9
A1+A1*	0	$p^e(p^2-1)$
A2+A2*	0	$2p^2(p-1)$
A3+A3*	$2p^2(p+1)+p^3(p+1)(q-3)$	$2p^2+p(p+1)(1+p^2(q-3))$
B2	0	$p^3(p-1)$
Sec 4.5	$p^f(p^2-1)$	$p^3(p^2-1)$ if $q>3$ $p^2(p+1)(p^2-1)$ if $q=3$

$G7$	T8	
A1+A1*	$2p^3(p^2-1)$	G_s, $\forall s \neq 2$
	$p^2(p^2-1)+p^3(p^2-1)$	G_2
A2+A2*	$4p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$
A3+A3*	$4p^2+4p^2(p+1)+2p^3(p+1)(q-3)$	G_s, $\forall s \in \mathcal{K}$
B2	$2p^3(p-1)$	G_s, $\forall s \in \mathcal{K}$
Sec 4.5	$2p^3(p^2-1)$	G_s $\forall s \neq 2$
	$p^2(p^2-1)+p^3(p^2-1)(q-1)$	G_2

In the second table $e = 2$ if $q = 3$ and $e = 3$ if $q > 3$; $f = 2$ if $q > 2$ and $f = 1$ if $q = 2$.

Table B.3: Number of GF on a group G of type 9, $|\ker(\gamma)| = p$

$G9$	T5	T6	T7
A1+A1*	0	$4p(p-1)$	0
A2+A2*	0	$2p^2(p-1)$	0
A3+A3*	$2p^2$	$2p+4p^2(q-2)$	$2+2p^2(q-2)$
B1+B1*	0	$2p(p-1)+2p^2(p-1)$	0

$G9$	T8		T9
A1+A1*	$4p^2(p-1)$	G_s, $\forall s \in \mathcal{K}$	$2p^2(p-1)$
A2+A2*	$4p^2(p-1)$	G_s, $\forall s \neq 2$	$2p^e(p-1)$
	$4p(p-1)+4p^2(p-1)$	G_2	
A3+A3*	$4p+2p^2(q-3)$	G_s, $\forall s \in \mathcal{K}$	$4p+2p^2(q-3)$
B1+B1*	$4p^2(p-1)$	G_s, $\forall s \neq 2$	$2p^2(p-1)$
	$2p(p-1)+2p^2(p-1)$	G_2	

In the second table, $e = 1$ if $q = 3$ and $e = 2$ if $q > 3$.

Bibliography

[AB18] Ali A. Alabdali and Nigel P. Byott, *Counting Hopf-Galois structures on cyclic field extensions of squarefree degree*, J. Algebra **493** (2018), 1–19. MR 3715201

[AB20a] Emiliano Acri and Marco Bonatto, *Skew braces of size p^2q I: abelian type*, 2020, `https://arxiv.org/abs/2004.04291`.

[AB20b] Emiliano Acri and Marco Bonatto, *Skew braces of size p^2q II: non-abelian type*, 2020, https://doi.org/10.1142/S0219498822500621.

[AB20c] Emiliano Acri and Marco Bonatto, *Skew braces of size pq*, Comm. Algebra **48** (2020), no. 5, 1872–1881. MR 4085764

[Bac16] David Bachiller, *Counterexample to a conjecture about braces*, J. Algebra **453** (2016), 160–176. MR 3465351

[BC12] Nigel P. Byott and Lindsay N. Childs, *Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures*, New York J. Math. **18** (2012), 707–731. MR 2991421

[BML22] Nigel P. Byott and Isabel Martin-Lyons, *Hopf-Galois structures on non-normal extensions of degree related to Sophie Germain primes*, J. Pure Appl. Algebra **226** (2022), no. 3, Paper No. 106869, 20. MR 4295182

[Byo96] Nigel P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555

[Byo04] Nigel P. Byott, *Hopf-Galois structures on Galois field extensions of degree pq*, J. Pure Appl. Algebra **188** (2004), no. 1-3, 45–57. MR 2030805

[Byo13] Nigel P. Byott, *Nilpotent and abelian Hopf-Galois structures on field extensions*, J. Algebra **381** (2013), 131–139. MR 3030514

[Byo15] Nigel P. Byott, *Solubility criteria for Hopf-Galois structures*, New York J. Math. **21** (2015), 883–903. MR 3425626

[Car18] Andrea Caranti, *Multiple holomorphs of finite p-groups of class two*, J. Algebra **516** (2018), 352–372. MR 3863482

[CCDC20] Elena Campedel, Andrea Caranti, and Ilaria Del Corso, *Hopf-Galois structures on extensions of degree p^2q and skew braces of order p^2q: the cyclic Sylow p-subgroup case*, J. Algebra **556** (2020), 1165–1210. MR 4089566

[CCDC21] Elena Campedel, Andrea Caranti, and Ilaria Del Corso, *The automorphism groups of groups of order p^2q*, Int. J. Group Theory **10** (2021), no. 3, 149–157. MR 4223627

[CDC21] Andrea Caranti and Ilaria Del Corso, *On the ranks of the additive and the multiplicative groups of a brace*, 2021, `https://arxiv.org/abs/2104.03211`, to appear in Rivista di Matematica della Università di Parma.

[CDV17] Andrea Caranti and Francesca Dalla Volta, *The multiple holomorph of a finitely generated abelian group*, J. Algebra **481** (2017), 327–347. MR 3639478

[CDV18] Andrea Caranti and Francesca Dalla Volta, *Groups that have the same holomorph as a finite perfect group*, J. Algebra **507** (2018), 81–102. MR 3807043

[CDVS06] Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308. MR 2273982

[CF64] Roger Carter and Paul Fong, *The sylow 2-subgroups of the finite classical groups*, Journal of Algebra **1** (1964), no. 2, 139–151.

[Chi89] Lindsay N. Childs, *On the Hopf Galois theory for separable field extensions*, Comm. Algebra **17** (1989), no. 4, 809–825. MR 990979

[Chi00] Lindsay N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499

[Chi05] Lindsay N. Childs, *Elementary abelian Hopf Galois structures and polynomial formal groups*, J. Algebra **283** (2005), no. 1, 292–316. MR 2102084

[Cre21] Teresa Crespo, *Hopf galois structures on field extensions of degree twice an odd prime square and their associated skew left braces*, J. Algebra **565** (2021), 282–308. MR 4150347

[CS19] Teresa Crespo and Marta Salguero, *Hopf Galois structures on separable field extensions of odd prime power degree*, J. Algebra **519** (2019), 424–439. MR 3880638

[Cur08] M. John Curran, *Automorphisms of semidirect products*, Math. Proc. R. Ir. Acad. **108** (2008), no. 2, 205–210. MR 2475812

[Die18] Carsten Dietzel, *Braces of order p^2q*, 2018, `https://arxiv.org/abs/1801.06911`.

[FCC12] Stephen C. Featherstonhaugh, Andrea Caranti, and Lindsay N. Childs, *Abelian Hopf Galois structures on prime-power Galois field extensions*, Trans. Amer. Math. Soc. **364** (2012), no. 7, 3675–3684. MR 2901229

[GP87] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476

[GV17] Leandro Guarnieri and Leandro Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534. MR 3647970

[Höl93] Otto Hölder, *Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4*, Math. Ann. **43** (1893), no. 2-3, 301–412. MR 1510814

[Koh98] Timothy Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*, J. Algebra **207** (1998), no. 2, 525–546. MR 1644203

[Koh07] Timothy Kohl, *Groups of order $4p$, twisted wreath products and Hopf-Galois theory*, J. Algebra **314** (2007), no. 1, 42–74. MR 2331752

[KT20] Alan Koch and Paul J. Truman, *Opposite skew left braces and applications*, J. Algebra **546** (2020), 218–235. MR 4033084

[NZ18] Kayvan Nejabati Zenouz, *On Hopf-Galois Structures and Skew Braces of Order p^3*, PhD thesis, The University of Exeter (2018), `https://ore.exeter.ac.uk/repository/handle/10871/32248`.

[NZ19] Kayvan Nejabati Zenouz, *Skew Braces and Hopf-Galois structures of Heisenberg type*, J. Algebra **524** (2019), 187–225. MR 3905210

[PS18] Cheryl E. Praeger and Csaba Schneider, *Permutation groups and Cartesian decompositions*, London Mathematical Society Lecture Note Series, vol. 449, Cambridge University Press, Cambridge, 2018. MR 3791829

[Rum07a] Wolfgang Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170. MR 2278047

[Rum07b] Wolfgang Rump, *Classification of cyclic braces*, J. Pure Appl. Algebra **209** (2007), no. 3, 671–685. MR 2298848

[SV18] Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86. MR 3763907

[TQ20] Cindy Tsang and Chao Qin, *On the solvability of regular subgroups in the holomorph of a finite solvable group*, Internat. J. Algebra Comput. **30** (2020), no. 2, 253–265. MR 4077413

[Tsa19] Cindy Tsang, *Hopf-Galois structures on a Galois S_n-extension*, J. Algebra **531** (2019), 349–360. MR 3953015

[Ven19] Leandro Vendramin, *Problems on skew left braces*, Adv. Group Theory Appl. **7** (2019), 15–37. MR 3974481