BEAUVILLE STRUCTURES IN p-GROUPS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ŞÜKRAN GÜL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

NOVEMBER 2016

Approval of the thesis:

BEAUVILLE STRUCTURES IN p-GROUPS

submitted by **ŞÜKRAN GÜL** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Gülbin Dural Ünver
Dean, Graduate School of **Natural and Applied Sciences** ______________

Prof. Dr. Mustafa Korkmaz
Head of Department, **Mathematics** ______________

Prof. Dr. Gülin Ercan
Supervisor, **Mathematics Department, METU** ______________

Assoc. Prof. Dr. Gustavo Adolfo Fernández-Alcober
Co-supervisor, **Math. Dept., Univ. of the Basque Country** ______________

Examining Committee Members:

Prof. Dr. İsmail Şuayip Güloğlu
Mathematics Department, Doğuş University ______________

Prof. Dr. Gülin Ercan
Mathematics Department, METU ______________

Prof. Dr. Mustafa Hurşit Önsiper
Mathematics Department, METU ______________

Prof. Dr. Ergün Yalçın
Mathematics Department, Bilkent University ______________

Assoc. Prof. Dr. Ebru Solak
Mathematics Department, METU ______________

Date: ______________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: ŞÜKRAN GÜL

Signature :

ABSTRACT

BEAUVILLE STRUCTURES IN p-GROUPS

Gül, Şükran
Ph.D., Department of Mathematics
Supervisor : Prof. Dr. Gülin Ercan
Co-Supervisor : Assoc. Prof. Dr. Gustavo Adolfo Fernández-Alcober

November 2016, 107 pages

Given a finite group G and two elements $x, y \in G$, we denote by $\Sigma(x, y)$ the union of all conjugates of the cyclic subgroups generated by x, y and xy. Then G is called a *Beauville group* of unmixed type if the following conditions hold:

(i) G is a 2-generator group.

(ii) G has two generating sets $\{x_1, y_1\}$ and $\{x_2, y_2\}$ such that $\Sigma(x_1, y_1) \cap \Sigma(x_2, y_2) = 1$.

In this case, $\{x_1, y_1\}$ and $\{x_2, y_2\}$ are said to form a *Beauville structure* for G.

The main purpose of this thesis is to extend the knowledge about Beauville p-groups. We will first discuss the conditions under which a 2-generator p-group with a "nice power structure" is a Beauville group. These conditions are similar to the conditions for an abelian p-group to be a Beauville group. In particular, this result applies to all known families of p-groups with a good behavior with respect to powers: regular p-groups, powerful p-groups and more generally potent p-groups, and (generalized) p-central p-groups.

Secondly, we investigate Beauville structures in metabelian thin p-groups and in p-groups of maximal class which are either metabelian, or have a maximal subgroup of class ≤ 2.

We next determine which quotients of the Nottingham group over $\mathbb{F}_p$ for an odd prime p are Beauville groups. As a result, we get the first known infinite family of 3-groups admitting a Beauville structure.

Finally, we prove a conjecture of Boston: he conjectured that if $p \geq 5$, all p-central quotients of the free group on two generators and of the free product of two cyclic groups of order p are Beauville groups.

Keywords: Beauville groups, finite p-groups, thin p-groups, Nottingham group, group of maximal class, free group, free product

ÖZ

p-GRUPLARINDA BEAUVİLLE YAPILAR

Gül, Şükran

Doktora, Matematik Bölümü

Tez Yöneticisi : Prof. Dr. Gülin Ercan

Ortak Tez Yöneticisi : Doç. Dr. Gustavo Adolfo Fernández-Alcober

Kasım 2016 , 107 sayfa

Verilen bir sonlu grup G ve $x, y \in G$ için, x, y ve xy tarafından üretilen devirli alt grupların bütün eşleniklerinin birleşimini $\Sigma(x, y)$ ile gösteriyoruz. Eğer aşağıdaki şartlar sağlanırsa, G grubuna karışık türde olmayan *Beauville grup* denir:

(i) G 2-üreteçli grup.

(ii) G'nin öyle iki üreteç kümesi $\{x_1, y_1\}$ ve $\{x_2, y_2\}$ varki $\Sigma(x_1, y_1) \cap \Sigma(x_2, y_2) = 1$.

Bu durumda, $\{x_1, y_1\}$ ve $\{x_2, y_2\}$'ye G grubuna *Beauville yapısı* oluşturuyor denir.

Bu tezin asıl amacı Beauville p-grupları hakkındaki bilgiyi genişletmektir. İlk olarak "iyi kuvvet yapılı" 2-üreteçli p-grubun Beauville grup olması için gerekli şartları tartışacağız. Bu şartlar değişmeli bir p-grubun Beauville grup olabilmesi için gereken şartlara benzemektedir. Aslında bu sonuç kuvvetlere göre iyi davranış sergileyen bütün bilinen p-gruplar ailesine uygulanır: düzenli p-gruplar, kuvvetli p-gruplar ve daha da geneli potent p-gruplar, ve (genellenmiş) p-merkezsel p-gruplar.

İkinci olarak, metabelian ince p-gruplarda, ve metabelian olan ya da üstel sıfır sınıfı en fazla 2 olan bir azami alt grup içeren azami sınıflı gruplarda Beauville yapılarını inceleyeceğiz.

Daha sonra tek asal sayı p için, $\mathbb{F}_p$ üzerindeki Nottingham grubun hangi bölüm gruplarının Beauville grup olduğunu belirleyeceğiz. Sonuç olarak Beauville yapısına olanak sağlayan ilk bilinen sonsuz 3-gruplar ailesini elde etmiş olacağız.

Son olarak Boston'nın sanısını ispatlayacağız: eğer $p \geq 5$ ise, iki üreteçli serbest grubun ve derecesi p olan iki devirli grubun serbest çarpımının bütün p-merkezsel bölüm grupları Beauville gruptur.

Anahtar Kelimeler: Beauville gruplar, sonlu p-gruplar, ince p-gruplar, Nottingham grup, azami sınıflı gruplar, serbest grup, serbest çarpım

To my parents
&
to my twin sister

ACKNOWLEDGMENTS

Pursuing a Ph.D. is like diving into an ocean, deeper and deeper, and discovering a new environment accompanied with encouragement, trust and many people's help. I am grateful to people around me for making the time for my discovery an unforgettable experience.

First of all, I would like to express my gratitude to my advisor, Gülin Ercan, for her advice and encouragement during my studies. She is the one who led me to meet and like group theory. She accepted me as her Ph.D. student without any hesitation, and always guided me in the right direction. I cannot thank her enough since this study is the first fruit of the seeds that she spread many years ago. We call her "mother of algebra" in the department, and I am grateful to my "mother" for everything she taught me.

Many special thanks go to my co-advisor, Gustavo Fernández-Alcober. To work with him has been a pleasure for me, with heaps of fun and excitement. He has introduced me to many new subjects, and I enjoy a lot these subjects. I am so impressed by how optimistic he is towards difficulties. I remember he used to say "don't give up" to encourage me. Thanks to his perfectionist attitude and to his "red pen", which he has used to make corrections over and over again to mathematical writings, I have learned from him how to write mathematics properly. Above all, I will truly miss our daily meetings sometimes accompanied with some cups of tea or café con leche.

I would like to thank Norberto Gavioli and Carlo Maria Scoppola for their hospitality during my one-month visit to the University of L'Aquila. I had a great time in both L'Aquila and Rome.

I would never forget the beautiful moments I shared with some of my friends. Sincere thanks to Merve Gürbüz for her friendship over 9 years. She is the one who put up with me through the whole undergraduate and Ph.D. process. Thank you for all the fun we had together. Special thanks go to my housemate, Burcu Çuvaş, for giving me motivation and for enjoyable discussions about everything. Although I have a twin sister, we always feel like she is our triplet sister. I am indebted to Fuat Erdem for his helpful comments on my writings in English and for discussions in mathematics. I would also like to thank my fellow Ph.D. student Yasir Kızmaz. Especially in my early years in Ph.D., I really enjoyed brainstorming with him about algebra.

I will always remember the amount of hospitality I have experienced during my visits to Bilbao. I wish to thank my office mates Jone Uria Albizuri, Oihana Garaialde

Ocaña, Ainhoa Iñiguez Goizueta and Sheila Muñoz Gallardo for their kind and warm friendship. I am very grateful to all the members of GRECA Research Group who constantly welcome me every time I visited the University of the Basque Country. I wish to heartily thank Jon González Sánchez, who helped me in every way in the first weeks of my internship when I visited Bilbao for the first time. *¡Gracias por todo chicas y chicos!*

My warmest thanks to my mom, dad and sister for their endless support and unconditional love. My parents have always given me their full support to achieve my goals. They have never pushed me in any direction other than the directions I have chosen for myself. I wish to deeply thank my best friend in the world, my sister Büşra Gül Aksoy. No matter how far we are from each other, you were always there when I needed an ear to listen.

Finally, I want to thank The Scientific and Technological Research Council of Turkey, TUBITAK, for supporting me financially both in Turkey and Spain. I also gratefully acknowledge the financial support of the Spanish Government, grant MTM2014-53810-C2-2-P, and of the Basque Government, grants IT753-13 and IT974-16.

TABLE OF CONTENTS

CHAPTERS

LIST OF SYMBOLS

$\lvert G : H\rvert = \lvert\{gH \mid g \in G\}\rvert$	the index of H in G
$C_G(H) = \{g \in G \mid g^{-1}xg = x \text{ for all } x \in H\}$	the centralizer of H in G
$\mathrm{Cl}_G(x) = \{g^{-1}xg \mid g \in G\}$	the conjugacy class of G containing x
$[A, B]$	the commutator subgroup of A and B
$[x,_i y]$	the higher commutator $[x, y, \overset{i}{\ldots}, y]$
$\mathrm{cl}(G)$	the nilpotency class of G
$d(G)$	the minimal number of generators of G
$Z(G)$	the center of G
$\Phi(G)$	the Frattini subgroup of G
$\exp G$	the exponent of G
$\Omega_{\{i\}}(G) = \{x \in G \mid x^{p^i} = 1\}$	the set of elements of order $\leq p^i$
$\Omega_i(G) = \langle x \in G \mid x^{p^i} = 1\rangle$	the subgroup generated by the elements of order $\leq p^i$
$G^{p^i} = \langle x^{p^i} \mid x \in G\rangle$	the subgroup generated by the p^ith powers of elements of G
$H \equiv K \pmod N$, for $N \trianglelefteq G$	$HN/N = KN/N$

CHAPTER 1

INTRODUCTION

Beauville groups were originally introduced in connection with a class of complex surfaces, known as Beauville surfaces. Beauville surfaces were introduced by Catanese in [13] generalizing the construction of Beauville in [6]. A **Beauville surface** S is a compact complex surface isomorphic to $(C_1 \times C_2)/G$, where C_1 and C_2 are algebraic curves of genera at least 2 and G is a finite group acting freely on $C_1 \times C_2$ by holomorphic transformations, and if $G_0 \leq G$ is the subgroup of index at most 2 consisting of the elements which preserve each of the factors, then G_0 acts effectively on each curve, in such a way that $C_i/G_0 \cong \mathbb{P}_1(\mathbb{C})$ and the covering map $C_i \to C_i/G_0$ is ramified over three points for $i = 1, 2$.

A Beauville surface is said to be of **mixed** or **unmixed type** according to whether $|G : G_0| = 2$ or $G = G_0$. Then G is said to be **Beauville group of mixed** or **unmixed type**, respectively. Clearly, any Beauville surface of mixed type $S = (C_1 \times C_2)/G$ gives rise to a Beauville surface of unmixed type $S_0 = (C_1 \times C_2)/G_0$.

The natural question that arises regarding Beauville surfaces is: which finite groups are Beauville groups?

Bauer, Catanese and Grunewald [4, 5] were able to characterize the groups appearing in the minimal presentations of Beauville surfaces in terms of the existence of the so-called *Beauville structure*. The group-theoretical reformulation of Beauville groups is as follows. For a couple of elements $x, y \in G$, we define

$$\Sigma(x, y) = \bigcup_{g \in G} \Big(\langle x \rangle^g \cup \langle y \rangle^g \cup \langle xy \rangle^g \Big),$$

that is, the union of all subgroups of G which are conjugate to $\langle x \rangle$, to $\langle y \rangle$ or to $\langle xy \rangle$.

Definition 1.0.1. *Let G be a finite group. An* ***unmixed Beauville structure*** *for G is a pair of generating sets $\{x_1, y_1\}$ and $\{x_2, y_2\}$ of G such that*

(i) $G = \langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle$,

(ii) $\Sigma(x_1, y_1) \cap \Sigma(x_2, y_2) = 1$.

We call $\{x_i, y_i, x_iy_i\}$ the ***triple*** *associated to $\{x_i, y_i\}$ for $i = 1, 2$. The* ***signature*** *of a triple is the tuple of orders of the elements in the triple.*

Remark 1.0.2. 1. The correspondence between the geometrical data of an unmixed Beauville surface and the group-theoretical data of an unmixed Beauville structure was given in [4, 5]. By this correspondence, a group G satisfying the conditions in Definition 1.0.1 gives rise to an unmixed Beauville surface, that it, G is an unmixed Beauville group.

2. Unmixed Beauville groups are 2-generator groups.

Definition 1.0.3. *Let G be a finite group. A* ***mixed Beauville structure*** *for G is a quadruple (G_0, x, y, z) where G_0 is a subgroup of G of index 2 and $x, y \in G_0$, $z \in G \setminus G_0$ are such that*

(i) $G_0 = \langle x, y \rangle$,

(ii) *For all $h \in G_0$, we have $(zh)^2 \notin \Sigma(x, y)$,*

(iii) $\Sigma(x, y) \cap \Sigma(x^z, y^z) = 1$.

Remark 1.0.4. By [4,5], a group G satisfying the conditions in Definition 1.0.3 gives rise to a mixed Beauville surface, that is, G is a mixed Beauville group.

In this thesis we study the unmixed case and we will use the term *Beauville group* to mean Beauville group of unmixed type.

Since 2000, many mathematicians such as Bauer, Catanese, Grunewald, Guralnick, Lubotzky and Malle have been interested in determining Beauville groups. Research in this regard has been carried out mostly for abelian groups and simple groups. However, in some sense most finite groups are p-groups [7, 8]. Therefore, it is natural to consider which finite p-groups are Beauville.

If p is a prime, the knowledge about Beauville p-groups is very scarce, and is restricted to either groups of small order or with a very simple structure. In this thesis, our main aim is to extend the knowledge about Beauville p-groups.

The thesis is organized as follows.

In Chapter 2, we first summarize some results on Beauville groups that we want to emphasize. We give the most fundamental results regarding abelian groups, simple groups and p-groups which admit Beauville structures. We next recall definitions and general group-theoretical results which will be relevant throughout this thesis. Further background material which is specific to a particular result or problem is included only in the chapter where it is used.

In Chapter 3, we study the existence of Beauville structures in p-groups with a "nice power structure". We provide a generalization of Catanese's characterization of abelian Beauville groups to these groups. The main result of this chapter is as follows:

Theorem 1.0.5. *Let G be a 2-generator finite p-group of exponent p^e such that one of the following conditions holds:*

(i) *G is semi-p^{e-1}-abelian, i.e. for every $x, y \in G$*

$$x^{p^{e-1}} = y^{p^{e-1}} \quad \textit{if and only if} \quad (xy^{-1})^{p^{e-1}} = 1.$$

(ii) *G is a potent p-group.*

Then G is a Beauville group if and only if $p \geq 5$ and $|G^{p^{e-1}}| \geq p^2$. If that is the case, then every lift of a Beauville structure in $G/\Phi(G)$ yields a Beauville structure of G.

This result applies to all known families of p-groups with a good behavior with respect to powers: regular p-groups, powerful p-groups and more generally potent p-groups, and (generalized) p-central p-groups. As another application of the theorem, we give the characterization of metacyclic Beauville p-groups. We also prove the following proposition to determine the condition $|G^{p^{e-1}}| \geq p^2$ easily.

Proposition 1.0.6. *Let $G = \langle a, b\rangle$ be a finite p-group of exponent p^e which is either semi-p^{e-1}-abelian or potent. Then $|G^{p^{e-1}}| \geq p^2$ if and only if $|\langle a^{p^{e-1}}, b^{p^{e-1}}\rangle| \geq p^2$.*

As an application of the proposition, we determine the number of Beauville groups of order p^6 by using the Lazard Correspondence.

We next analyze the Beauville structures which are not inherited by the Frattini quotients. In the last section, we give the characterization of regular Beauville groups without induced Beauville structures.

In Chapter 4, we investigate Beauville structures in thin p-groups. More specifically, we study metabelian thin p-groups and p-groups of maximal class which either are metabelian, or have a maximal subgroup of class ≤ 2.

If G is a p-group of order $\leq p^p$, then G is regular, and hence the existence of Beauville structure can be determined by using Theorem 1.0.5. Thus we concentrate on p-groups of maximal class of order $\geq p^{p+1}$. We prove the following main results.

Lemma 1.0.7. *Let G be a p-group of maximal class of order $\geq p^{p+1}$. Suppose that G satisfies one of the following:*

(i) *All elements of $G \setminus G_1$ are of order p^2.*

(ii) *There exists $s \in G \setminus G_1$ such that $o(s) = p$ and all elements outside $G_1 \cup \langle s, G' \rangle$ are of order p^2.*

Then G is not a Beauville group.

Theorem 1.0.8. *Let G be a p-group of maximal class of order $p^n \geq p^{p+1}$, where p is odd, such that either G is metabelian or $\mathrm{cl}(G_1) \leq 2$. Suppose that G is not as in Lemma 1.0.7. Then one of the following holds:*

(i) *All elements of $G \setminus G_1$ are of order p.*

(ii) *There exist a uniform element s and $s_1 \in G_1 \setminus G'$ such that $o(s) = o(ss_1) = p$ and all elements outside $G_1 \cup \langle s, G' \rangle \cup \langle ss_1, G' \rangle$ are of order p^2.*

Theorem 1.0.9. *Let G be as in Theorem 1.0.8. Then G is a Beauville group if and only if $p \geq 5$ and one of the following two cases holds:*

1. (i) holds.

2. *(ii) holds, and either $n \neq k(p-1)+2$ with $k \geq 1$, or $n = p+1$ and $\exp G_1 = p$.*

If G is a metabelian thin p-group, then $\mathrm{cl}(G) \leq p+1$. If $\mathrm{cl}(G) < p$, then the group is regular, and hence Theorem 1.0.5 can be used to determine Beauville structures. Thus we focus on metabelian thin p-groups of class p or $p+1$. The main results are as follows.

Theorem 1.0.10. *Let G be a metabelian thin p-group with $\mathrm{cl}(G) = p$ such that $|\gamma_p(G)| = p^2$, where $p \geq 5$. Then G has a Beauville structure in which one of the two triples has all elements of order p^2.*

Theorem 1.0.11. *Let G be a metabelian thin p-group with $\mathrm{cl}(G) = p+1$, where $p \geq 5$. Then G has a Beauville structure.*

We next analyze the case $\mathrm{cl}(G) = p$ and $|\gamma_p(G)| = p$. There are two possibilities:

(i) $G^p = \gamma_{p-1}(G)$,

(ii) $G^p = \gamma_p(G)$.

Theorem 1.0.12. *Let G be a group in case (i). Then G has a Beauville structure.*

Theorem 1.0.13. *Let G be a group in case (ii). Then G has a Beauville structure if and only if it has at least three maximal subgroups of exponent p.*

In Chapter 5, we study Beauville structures in quotients of the Nottingham group over $\mathbb{F}_p$, for an odd prime p. As a consequence, we give the first explicit infinite family of Beauville 3-groups, and we show that there are Beauville 3-groups of order 3^n for every $n \geq 5$. The main result of this chapter is the following:

Theorem 1.0.14. *Let $\mathcal{N}$ be the Nottingham group over $\mathbb{F}_p$, where p is an odd prime, and let $\mathcal{W}$ be a normal subgroup of $\mathcal{N}$ of index $\geq p^2$ or p^5, according as $p > 3$ or $p = 3$. Then $\mathcal{N}/\mathcal{W}$ is a Beauville group if and only if $\mathcal{W} \neq \mathcal{N}_{z_m}, \langle e, \mathcal{N}_{z_m+1}\rangle$, where e is the automorphism given by $e(t) = t + t^{z_m}$ for all $m \geq 1$ or $m \geq 2$, according as $p > 3$ or $p = 3$ and $z_m = p^m + p^{m-1} + \cdots + p + 2$.*

Finally, in Chapter 6, we prove a conjecture of Boston: he conjectured that if $p \geq 5$, all p-central quotients of the free group on two generators and of the free product of two cyclic groups of order p are Beauville groups. In the case of the free product, we also deal with $p = 3$, and we get an infinite family of Beauville 3-groups which is different from the one given in Chapter 5. The main results of this chapter as follow.

Theorem 1.0.15. *Let $F = \langle x, y \rangle$ be the free group on two generators. Then a p-central quotient $F/\lambda_n(F)$ is a Beauville group if and only if $p \geq 5$ and $n \geq 2$.*

Let $F = \langle x, y \mid x^p, y^p \rangle$ be the free product of two cyclic groups of order p.

Theorem 1.0.16. *If $p \geq 5$ then the p-central quotient $F/\lambda_n(F)$ is a Beauville group for every $n \geq 2$.*

Theorem 1.0.17. *Let $p = 3$. Then the following hold.*

(i) *The p-central quotient $F/\lambda_n(F)$ is a Beauville group if and only if $n \geq 4$.*

(i) *The series $\{\lambda_n(F)\}_{n \geq 4}$ can be refined to a normal series of F such that two consecutive terms of the series have index p and for every term N of the series F/N is a Beauville group.*

Theorem 1.0.18. *Let $N \neq \gamma_4(F)$ be a normal subgroup of F such that F/N is a Beauville group. Then F/N is not isomorphic to any quotient of $\mathcal{N}$ which is a Beauville group. On the other hand, $F/\gamma_4(F)$ is isomorphic to $\mathcal{N}/\gamma_4(\mathcal{N})$.*

CHAPTER 2

BACKGROUND MATERIAL

2.1 Known results on Beauville groups

Research activity around Beauville groups has been very intense since the beginning of this century; see, for example, the recent survey papers [9, 17, 34]. We briefly mention some results that we want to highlight.

In 2000, Catanese proved a result regarding abelian groups.

Theorem 2.1.1. [13] A finite abelian group is a Beauville group if and only if it is isomorphic to $C_n \times C_n$, where $n > 1$ and $\gcd(n, 6) = 1$.

The following is a corollary of Catanese's criterion for abelian Beauville p-groups.

Corollary 2.1.2. *There are no abelian Beauville 2-groups or 3-groups. Thus an abelian p-group G is a Beauville group if and only if $G \cong C_{p^n} \times C_{p^n}$, where $n \geq 1$ and $p \geq 5$.*

This result can be stated in a different way:

Corollary 2.1.3. *Let $p \geq 5$, and let G be an abelian 2-generator p-group. If the exponent of G is p^e then G is a Beauville group if and only if $|G^{p^{e-1}}| = p^2$.*

The following groups also admit Beauville structures.

Theorem 2.1.4. [4, 5, 22]

(i) The alternating groups A_n are Beauville groups if and only if $n \geq 6$,

(ii) The symmetric groups S_n are Beauville groups if and only if $n \geq 5$,

(iii) The groups $SL(2,p)$ and $PSL(2,p)$ are Beauville groups for every prime $p \neq 2,3,5$.

Part (i) was proven in [4, 5] for n large enough, and it was later generalized in [22]. Part (ii) was proven for $n \geq 7$ in [5], and it was later improved in [22]. Part (iii) appeared in [4].

In 2006, Bauer, Catanese, and Grunewald made the following conjecture.

Conjecture 2.1.5. [5, Conjecture 7.17] Every non-abelian finite simple group other than A_5 is a Beauville group.

By using probabilistic methods, Garion, Larsen, and Lubotzky [24] showed in 2012 that the conjecture is true if the order of the group is large enough. Soon afterwards, Guralnick and Malle [28] gave a complete proof of the conjecture. Then Fairbairn, Magaard and Parker proved that:

Theorem 2.1.6. [18, 19] All finite quasisimple groups other than A_5 and $SL(2,5)$ are Beauville groups.

Bauer, Catanese and Grunewald have showed the following result.

Theorem 2.1.7. [4, Lemma 3.7] Let G be a non-trivial finite quotient of the infinite dihedral group $D_\infty = \langle x, y \mid x^2, y^2 \rangle$, that is, G is a finite dihedral group. Then G is not a Beauville group.

After the abelian groups, the next most natural class of finite groups to consider are the nilpotent groups. In [2], the following lemma was stated.

Lemma 2.1.8. [2, Lemma 3] Let G and G' be Beauville groups and let $\{\{x_1, y_1\}, \{x_2, y_2\}\}$ and $\{\{x_1^{'}, y_1^{'}\}, \{x_2^{'}, y_2^{'}\}\}$ be their Beauville structures, respectively. Suppose that for $i = 1, 2$

$$\gcd(o(x_i), o(x_i^{'})) = \gcd(o(y_i), o(y_i^{'})) = 1.$$

Then $\{(x_1, x_1^{'}), (y_1, y_1^{'})\}$, $\{(x_2, x_2^{'}), (y_2, y_2^{'})\}$ is a Beauville structure for $G \times G'$.

More generally we have the following lemma.

Lemma 2.1.9. *Let G and G' be 2-generator groups of coprime order. Then $G \times G'$ is a Beauville group if and only if both G and G' are Beauville groups.*

Proof. If G and G' are Beauville groups, then since they have coprime order, Lemma 2.1.8 implies that $G \times G'$ is a Beauville group.

Conversely, assume that $\{(x_1, x_1^{'}), (y_1, y_1^{'})\}$, $\{(x_2, x_2^{'}), (y_2, y_2^{'})\}$ is a Beauville structure for $G \times G'$. We will show that G is a Beauville group, and the same arguments apply to G'.

Let $A = \{(x_1, x_1^{'}), (y_1, y_1^{'}), (x_1y_1, x_1^{'}y_1^{'})\}$ and $B = \{(x_2, x_2^{'}), (y_2, y_2^{'}), (x_2y_2, x_2^{'}y_2^{'})\}$. Then for every $(a, a^{'}) \in A$ and $(b, b^{'}) \in B$ we have

$$\langle (a, a^{'}) \rangle^{(g,g^{'})} \cap \langle (b, b^{'}) \rangle^{(h,h^{'})} = (1, 1), \tag{2.1}$$

for all $g, h \in G$ and $g^{'}, h^{'} \in G^{'}$. Let $|G| = l$ and $|G'| = m$, where $\gcd(l, m) = 1$. Then by equation (2.1), we get

$$\langle ((a^m)^g, 1) \rangle \cap \langle ((b^m)^h, 1) \rangle = (1, 1),$$

and hence $\langle a^m \rangle^g \cap \langle b^m \rangle^h = 1$. Since $\gcd(l, m) = 1$, it then follows that $\langle a \rangle^g \cap \langle b \rangle^h = 1$. Thus G is a Beauville group. □

Since a finite group is nilpotent if and only if it is a direct product of its Sylow subgroups, by the above lemma, the study of nilpotent Beauville groups is reduced to the study of Beauville p-groups.

Recently Stix and Vdovina [49] have constructed infinite series of Beauville p-groups. In particular this gives the first examples of non-abelian Beauville p-groups of arbitrarily large order and any prime $p \geq 5$. The existence of a non-abelian Beauville p-group of order p^n for every $p \geq 5$ and every $n \geq 3$ is also proved in [2]. On the other hand, as a consequence of the main theorem in [3], there are Beauville 2-groups of arbitrarily high order. The existence of infinitely many Beauville 3-groups has been settled in the affirmative in [49] and [25]. In particular, Stix and Vdovina [49, Theorem 2] have showed that there are quotients of the ordinary triangle group $T = \langle x, y \mid x^3 = y^3 = (xy)^9 = 1\rangle$ which are Beauville 3-groups of every order greater than or equal to 3^5. In all these groups, the signature of one of the triples of the Beauville structure takes the constant value $(3, 3, 9)$. They have also proved the following theorem, which generalizes the reformulation of Catanese's criterion for abelian p-groups .

Theorem 2.1.10. [49, Theorem 3] A split metacyclic p-group G is a Beauville group if and only if $p \geq 5$ and G is a semidirect product of two cyclic groups of the same order.

Barker, Boston and Fairbairn have determined the smallest non-abelian Beauville p-group for all primes p. In the below presentations of these groups, we have omitted all commutators between generators which are trivial.

Theorem 2.1.11. [2, Corollary 9]

(i) For $p = 2$, `SmallGroup`$(2^7, 36)$, that is the group

$$\langle x, y \mid x^4 = y^4 = [x, y]^2 = [x, y^2]^2 = [x^2, y]^2 = 1\rangle$$

of order 2^7.

(ii) For $p = 3$, `SmallGroup`$(3^5, 3)$, that is the group

$$\langle x, y, z, w, t \mid x^3 = y^3 = z^3 = w^3 = t^3 = 1, [y, x] = z, [z, x] = w, [z, y] = t\rangle$$

of order 3^5.

(iii) For $p \geq 5$, the group

$$\langle x, y, z \mid x^p = y^p = z^p = 1,\ [x, y] = z\rangle$$

of order p^3.

Also, by using the computer algebra system MAGMA for $p = 3, 5$ and by giving the direct proof for $p \geq 7$, they have showed that:

Theorem 2.1.12. [2, pages 5,6,9]

(i) There is only one Beauville group of order 3^5, namely `SmallGroup`$(3^5, 3)$.

(ii) There are only three Beauville groups of order 3^6, namely $\texttt{SmallGroup}(3^6, n)$ for $n = 34, 37, 40$.

(iii) There is only one Beauville group of order p^3 for $p \geq 5$, namely the one given in (iii) above.

In [2], they have also determined all Beauville p-groups of order at most p^4, and have found estimates for the number of Beauville groups of orders p^5 and p^6.

Theorem 2.1.13. [17, Theorem 4.6] Let G be a finite group of exponent $n = p^e > 1$ for some prime $p \geq 5$ such that the abelianization $G/G' \cong C_n \times C_n$. Then G is a Beauville group.

As a corollary of the above theorem, we have the following.

Corollary 2.1.14. [17, Corollary 4.7] Let G be a 2-generator finite p-group of exponent p for some prime $p \geq 5$. Then G is a Beauville group.

2.2 General group-theoretical results

In this section, we recall some results which will be required throughout this thesis. These results will be used without reference in later chapters. Most of them are well known results and the proofs can be seen in the given references.

Definition 2.2.1. *Let G be a group. We define the* ***commutator subgroup*** *G' to be*

$$G' = \langle [g, h] = g^{-1}h^{-1}gh \mid g, h \in G \rangle.$$

Lemma 2.2.2. [32, pages 113,114] *Let G be a group and $g, h, k \in G$. Then the following identities hold:*

(i) $[g, h][h, g] = 1$.

(ii) $[gh, k] = [g, k]^h[h, k]$.

(iii) $[g, hk] = [g, k][g, h]^k$.

Definition 2.2.3. *Let G be a group and let $H, K \leq G$ be subgroups. Then the commutator of H and K, denoted $[H, K]$, is defined to be*

$$[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle.$$

Since the generators of $[H, K]$ are the inverses of the generators of $[K, H]$, we have $[H, K] = [K, H]$.

Lemma 2.2.4. [32, Lemma 4.1] *Let G be a group and $H, K \leq G$ be subgroups. Then $[H, K] \trianglelefteq \langle H, K\rangle$.*

Lemma 2.2.5. *Let G be a group and let N be a normal subgroup of G such that G/N is cyclic. Then $G' = [G, N]$.*

Proof. Clearly $[G, N] \leq G'$. To prove the other inclusion, it is enough to show that $[g, h] \in [G, N]$ for any $g, h \in G$. Let $G/N = \langle aN\rangle$ for some $a \in G$. Write $g = a^i n_1$, $h = a^j n_2$ for some $n_1, n_2 \in N$ and for some integers i, j. Then

$$\begin{aligned}[g, h] = [a^i n_1, a^j n_2] =&[a^i, a^j n_2]^{n_1}[n_1, a^j n_2]\\ =&[a^i, n_2]^{n_1}[n_1, n_2][n_1, a^j]^{n_2} \in [G, N].\end{aligned}$$

□

We can define higher commutators as follows.

Definition 2.2.6. *Let G be a group and $g_1, g_2, \ldots, g_n \in G$. For $n > 2$, we define*

$$[g_1, g_2, \ldots, g_n] = [[g_1, g_2, \ldots, g_{n-1}], g_n].$$

Notation: For any group G and $x, y \in G$, we will use the notation $[x,_i y]$ to denote the higher commutator $[x, y, \overset{i}{\ldots}, y]$ for $i \geq 1$.

Definition 2.2.7. *Let G be a group. Let $\gamma_1(G) = G$ and define recursively $\gamma_{i+1}(G) = [\gamma_i(G), G]$ for all $i \geq 1$. The chain of normal subgroups*

$$G = \gamma_1(G) \geq \gamma_2(G) = G' \geq \gamma_3(G) \geq \ldots$$

*is called the **lower central series** of G. If for some $n \in \mathbb{N}$, we have $\gamma_{n+1}(G) = 1$, then G is said to be **nilpotent**. The smallest such integer n is said to be **nilpotency class** of G.*

Theorem 2.2.8. [32, Theorem 4.11] *For any group G, $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ for all $i, j \geq 1$.*

Theorem 2.2.9. [20, Theorem 1.11] *Let G be a group and let N be a normal subgroup of G. Then $\gamma_i(G/N) = \gamma_i(G)N/N$ for all $i \geq 1$.*

Definition 2.2.10. *Let G be a group. Let $Z_0(G) = 1$ and $Z_1(G) = Z(G)$ and define $Z_i(G)$ inductively as the unique subgroup such that $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. The chain of normal subgroups*

$$1 = Z_0(G) \leq Z_1(G) = Z(G) \leq Z_2(G) \leq \dots$$

is called the ***upper central series*** *of G.*

Lemma 2.2.11. [20, Lemma 1.12] *Let G be a nilpotent group of class n. Then $\gamma_{n+1-i}(G) \leq Z_i(G)$ for all $0 \leq i \leq n$.*

Theorem 2.2.12. [20, Theorem 1.13] *A group G is nilpotent of class n if and only if $Z_n(G) = G$ and $Z_{n-1}(G) \neq G$.*

Corollary 2.2.13. [20, Corollary 1.14] *Any finite p-group is nilpotent.*

Definition 2.2.14. *For a finite group G, the intersection of its maximal subgroups is called the* ***Frattini subgroup*** *of G and is denoted by $\Phi(G)$.*

Theorem 2.2.15. [20, Theorem 1.6] ***(Burnside's Basis Theorem)*** *Let G be a finite p-group. Then*

(i) *$G/\Phi(G)$ is an elementary abelian p-group, and consequently it may be viewed as a vector space over $\mathbb{F}_p$.*

(ii) *The set $\{g_1, g_2, \dots, g_d\}$ is a minimal generating set of G if and only if $\{g_1\Phi(G), \dots, g_d\Phi(G)\}$ is a basis of $G/\Phi(G)$.*

(iii) *If d is the minimal number of generators of G, then $|G : \Phi(G)| = p^d$.*

Definition 2.2.16. *Let G be a p-group. For any $i \geq 0$ we define*

$$\Omega_i(G) = \langle x \in G \mid x^{p^i} = 1 \rangle,$$

that is, the subgroup generated by the elements of G whose orders are $\leq p^i$, and

$$G^{p^i} = \langle x^{p^i} \mid x \in G \rangle.$$

It is clear that both $\Omega_i(G)$ and G^{p^i} are characteristic subgroups of G.

Definition 2.2.17. *Let G be a finite group. The* ***exponent*** *of G, denoted by $\exp G$, is the least common multiple of the orders of its elements. If G is a p-group, it is simply the maximum of the orders of all elements of G.*

If $\exp G = p^e$ then $x^{p^e} = 1$ for all $x \in G$, so that $\Omega_e(G) = G$ and $G^{p^e} = 1$. Thus we have the following series :

$$1 = \Omega_0(G) \leq \Omega_1(G) \leq \cdots \leq \Omega_{e-1}(G) \leq \Omega_e(G) = G,$$

and

$$G \geq G^p \geq \cdots \geq G^{p^{e-1}} \geq G^{p^e} = 1.$$

Theorem 2.2.18. [20, Theorem 2.4] *Let G be a finite p-group and $N \trianglerighteq G$. Then $(G/N)^{p^i} = G^{p^i}N/N$ for all $i \geq 0$.*

Theorem 2.2.19. [30, Theorem III.3.14] *Let G be a p-group. Then*

(i) *$\Phi(G)$ is the smallest subgroup N of G such that G/N is elementary abelian.*

(ii) *$\Phi(G) = G'G^p$.*

(iii) *If $N \trianglelefteq G$ then $\Phi(G/N) = \Phi(G)N/N$.*

The following remarkable formula relates x^ny^n to $(xy)^n$ in any group by using commutators in x and y.

Theorem 2.2.20. [30, Theorem III.9.4] ***(Hall-Petrescu Formula)*** *Let G be a group and $x, y \in G$. Then there exist elements $c_i = c_i(x, y) \in \gamma_i(\langle x, y\rangle)$ such that*

$$x^ny^n = (xy)^n c_2^{\binom{n}{2}} c_3^{\binom{n}{3}} \ldots c_n^{\binom{n}{n}}$$

for all $n \in \mathbb{N}$.

Under some particular conditions on the group, there is a more interesting formula that gives an explicit expression for the elements $c_i(x, y)$ in the Hall-Petrescu formula.

Lemma 2.2.21. *Let G be a group and let $x, y \in G$. Write $H = \langle x, y\rangle$ and assume that $\langle y, H'\rangle$ is abelian. Then for any $n \in \mathbb{N}$*

$$(xy)^n = x^ny^n[y, x]^{\binom{n}{2}}[y, x, x]^{\binom{n}{3}} \ldots [y, x, \overset{n-1}{\ldots}, x]^{\binom{n}{n}}.$$

Proof. First of all, notice that

$$(xy)^n = x^n y^{x^{n-1}} y^{x^{n-2}} \ldots y^{x^2} y^x y.$$

Since $y^{x^i} = y[y, x^i]$ for any $i \in \mathbb{N}$, and $\langle y, H' \rangle$ is abelian, we deduce that

$$(xy)^n = x^n y^n [y, x^{n-1}][y, x^{n-2}] \ldots [y, x].$$

Next by using induction on i and by taking into account that $\langle y, H' \rangle$ is abelian, it can be seen that

$$[y, x^i] = [y, x]^i [y, x, x]^{\binom{i}{2}} [y, x, x, x]^{\binom{i}{3}} \ldots [y, x, \overset{i}{\ldots}, x]. \tag{2.2}$$

Then (2.2) and the relation $\sum_{i=k}^{n-1} \binom{i}{k} = \binom{n}{k+1}$ for binomial coefficients imply that

$$(xy)^n = x^n y^n [y, x]^{\binom{n}{2}} [y, x, x]^{\binom{n}{3}} \ldots [y, x, \overset{n-1}{\ldots}, x]^{\binom{n}{n}}.$$

□

We will use the following results in Chapter 5.

Theorem 2.2.22. [1, Theorem 5.25] ***(Wolstenholme's Theorem)*** *For any prime $p \geq 5$, we have*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}.$$

Theorem 2.2.23. [16, Theorem 13.6] ***(Kummers's Theorem)*** *The power of a prime p that divides the binomial coefficient $\binom{n}{m}$ is given by the number of "carries" when we add m and $n-m$ in base p.*

We have the following corollary of Kummer's Theorem.

Corollary 2.2.24. *If $1 \leq i \leq p^l$ is such that $p^r \leq i < p^{r+1}$, then the binomial coefficient $\binom{p^l}{i}$ is divisible by p^{l-r}.*

We next give the results regarding extensions with cyclic factor group and with abelian factor group.

Theorem 2.2.25. [54, pages 128,129] ***(Extension with cyclic factor group)*** *Let N be a group and let $\sigma : N \longrightarrow N$ be an automorphism of N with the following property:*

(i) *There exists* $a \in N$ *such that* $\sigma(a) = a$ *and* $\sigma^n(x) = a^{-1}xa$ *for all* $x \in N$ *and for some* $n \in \mathbb{N}$.

Then there exists one and only one extension group G *of* N *such that* $G/N = \langle gN \rangle$ *is cyclic of order* n, $g^n = a$, *and* $\sigma(x) = g^{-1}xg$ *for all* $x \in N$.

We next state a special case of extensions with abelian factor group.

Theorem 2.2.26. [54, pages 130,133] ***(Extension with abelian factor group)*** *Let* N *be an abelian group. Let* a_i, $a_{i,k}$ $(i, k = 1, 2 \ldots r; i \neq k)$ *be elements of* N *and let* σ_i *be automorphisms of* N *with the following properties:*

(i) $\sigma_i^{n_i}(a) = a$ *for all* $a \in N$,

(ii) $\sigma_i\sigma_k(a) = \sigma_k\sigma_i(a)$ *for all* $a \in N$,
and $a_{i,k}a_{k,i} = 1$,

(iii) $(\sigma_i - 1)(a_k) = (1 + \sigma_k + \sigma_k^2 + \cdots + \sigma_k^{n_k-1})(a_{i,k})$,

(iv) $(\sigma_l - 1)(a_{i,k})(\sigma_i - 1)(a_{k,l})(\sigma_k - 1)(a_{l,i}) = 1$ *for* $i < k < l$.

Then there exists an extension G *of* N *such that* $G/N = \langle s_1N \rangle \times \langle s_2N \rangle \times \cdots \times \langle s_rN \rangle$, *where* $o(s_iN) = n_i$ *and the following relations hold:*

1. $\sigma_i(a) = s_i^{-1}as_i$ *for all* $a \in N$,
2. $s_i^{n_i} = a_i$,
3. $[s_i, s_k] = a_{i,k}$.

2.3 Some useful lemmas

In this section, we shall give some lemmas which will be used in the proof of the main theorems.

Lemma 2.3.1. *Let* $G = \langle a, b \rangle$ *be a* 2*-generator* p*-group and* $o(a) = p$, *for some prime* p. *Then*

$$\Big(\bigcup_{g\in G} \langle a \rangle^g\Big) \bigcap \Big(\bigcup_{g\in G} \langle b \rangle^g\Big) = 1.$$

Proof. Let x be an arbitrary element of this intersection such that $x = (a^i)^g = (b^j)^h$ for some g, $h \in G$ and $i, j \in \mathbb{Z}$. Then in the quotient $\overline{G} = G/\Phi(G) = \langle \overline{a} \rangle \times \langle \overline{b} \rangle$, we have $\overline{x} \in \langle \overline{a} \rangle \cap \langle \overline{b} \rangle = \overline{1}$ implying that $x \in \Phi(G)$. On the other hand, $x \in \langle a^g \rangle$, where a^g is of order p and $a^g \notin \Phi(G)$. It then follows that $x = 1$. □

Lemma 2.3.2. *Let G be a finite p-group and let $x \in G \setminus \Phi(G)$ be an element of order p. If $t \in \Phi(G) \setminus \{[x, g] \mid g \in G\}$ then*

$$\Big(\bigcup_{g \in G} \langle x \rangle^g \Big) \bigcap \Big(\bigcup_{g \in G} \langle xt \rangle^g \Big) = 1.$$

Proof. Let h be an arbitrary element of this intersection, that is $h = (x^i)^{g_1} = ((xt)^j)^{g_2}$ for some $g_1, g_2 \in G$ and $i, j \in \mathbb{Z}$. In the quotient $\overline{G} = G/\Phi(G)$, we have $\overline{h} = \overline{x}^i = \overline{x}^j$ as $t \in \Phi(G)$, and so $i \equiv j \pmod{p}$. Then $(x^j)^{g_1} = ((xt)^j)^{g_2}$ since $o(x) = p$. If $p | j$, then we are done. Thus we assume that $p \nmid j$. Since G is a finite p-group, we have $\gcd(o(xt), j) = 1$, and by Bézout's identity, there exist some integers k, l such that $o(xt)l + jk = 1$. Then $(x^{jk})^{g_1} = ((xt)^{jk})^{g_2}$, that is $x^{g_1} = (xt)^{g_2}$. Hence $t = [x, g_1 {g_2}^{-1}]$, which is a contradiction. □

Lemma 2.3.3. *Let G be a group and $g \in G$. Then the set*

$$Z = \{[g, x] \mid x \in G\} \cap Z(G)$$

is a subgroup of G.

Proof. Let $[g, x_1], [g, x_2] \in Z$ for some $x_1, x_2 \in G$. Then $[g, x_2 x_1] = [g, x_1][g, x_2]^{x_1} = [g, x_1][g, x_2] \in Z$ and $[g, x_1]^{-1} = [g, x_1^{-1}] \in Z$. Hence Z is a subgroup of G. □

Lemma 2.3.4. [23, Lemma 4.2] *Let G be a finite group and let $\{x_1, y_1\}$ and $\{x_2, y_2\}$ be two sets of generators of G. Assume that, for a given $N \trianglelefteq G$, the following hold:*

(i) $\{x_1 N, y_1 N\}$ *and* $\{x_2 N, y_2 N\}$ *is a Beauville structure for* G/N,

(ii) $o(u) = o(uN)$ *for every* $u \in \{x_1, y_1, x_1 y_1\}$.

Then $\{x_1, y_1\}$ and $\{x_2, y_2\}$ is a Beauville structure for G.

Proof. Let $1 \neq x \in \left(\bigcup_{g\in G} \langle u\rangle^g\right) \bigcap \left(\bigcup_{g\in G} \langle v\rangle^g\right)$, where $u \in \{x_1, y_1, x_1y_1\}$ and $v \in \{x_2, y_2, x_2y_2\}$. Then $x = (u^i)^{g_1} = (v^j)^{g_2}$ for some $g_1, g_2 \in G$ and $1 \leq i < o(u), 1 \leq j < o(v)$.

In the quotient G/N, we have $xN \in \langle uN\rangle^{g_1N} \cap \langle vN\rangle^{g_2N}$. Since $\{x_1N, y_1N\}$ and $\{x_2N, y_2N\}$ is a Beauville stucture for G/N, it follows that $xN = N$, that is $x \in N$. On the other hand, $x = (u^i)^{g_1}$ implies that $x^{g_1^{-1}} = u^i \in N$,which contradicts our assumption that $o(u) = o(uN)$, and hence $x = 1$. Thus $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G. □

Recall that by Corollary 2.1.14, a 2-generator finite p-group of exponent p for some prime $p \geq 5$ is a Beauville group. Indeed, we can give a more general result.

Lemma 2.3.5. *Let $p \geq 5$, and let G be a 2-generator finite p-group such that it has at least three maximal subgroups of exponent p. Then G has a Beauville structure.*

Proof. First of all, our aim is to find a triple so that every element in the triple is of order p. Let M_i be maximal subgroups of G of exponent p for $i = 1, 2, 3$. Choose $x \in M_1 \smallsetminus \Phi(G)$ and $y \in M_2 \smallsetminus \Phi(G)$. Since each element in the set $\{xy^j \mid 1 \leq j \leq p-1\}$ falls into different maximal subgroups, there exists $1 \leq j \leq p-1$ such that $xy^j \in M_3 \smallsetminus \Phi(G)$. Thus if we put $x_1 = x$ and $y_1 = y^j$, then every element in the triple $\{x_1, y_1, x_1y_1\}$ is of order p. We choose $\{x_1, y_1\}$ as one of the generating sets of G.

Now let $\{z, t\}$ be another set of generators of G such that $z, t \notin M_i$ for $i = 1, 2, 3$. Again as in the previous paragraph each element in the set $\{zt^k \mid 1 \leq k \leq p-1\}$ falls into different maximal subgroups. Since $p \geq 5$, we have $p + 1 \geq 6$ maximal subgroups, and hence there exists $1 \leq k \leq p-1$ such that $zt^k \notin M_i$ for $i = 1, 2, 3$. Then if we put $x_2 = z$ and $y_2 = t^k$, then each pair of elements in the set $\{x_i, y_i, x_iy_i \mid i = 1, 2\}$ is linearly independent modulo $\Phi(G)$.

We claim that $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G. Set $A = \{x_1, y_1, x_1y_1\}$ and $B = \{x_2, y_2, x_2y_2\}$. Since $o(a) = p$ for all $a \in A$, and $G = \langle a, b\rangle$ for all $b \in B$, Lemma 2.3.1 implies that $\langle a^g\rangle \cap \langle b^h\rangle = 1$, for all $g, h \in G$. □

We close this section by a remark regarding the order of generators of G in a Beauville structure.

Remark 2.3.6. If $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G, then the order of x_1 and y_1 (similarly the order of x_2 and y_2) is irrelevant, that is, $\{y_1, x_1\}$ and $\{x_2, y_2\}$ also form a Beauville structure for G. Since $\langle x_1 y_1\rangle^g \cap \langle a\rangle = 1$ for all $a \in \{x_2, y_2, x_2 y_2\}$ and $y_1 x_1 = x_1 y_1^{x_1}$, it follows that $\langle x_1 y_1^{x_1}\rangle^{x_1^{-1}g} \cap \langle a\rangle = 1$ for all $g \in G$.

CHAPTER 3

p-GROUPS WITH A NICE POWER STRUCTURE

In this chapter, we extend Catanese's criterion for abelian Beauville groups to finite p-groups satisfying certain conditions which are much weaker than commutativity. This result applies to all known families of p-groups with a good behaviour with respect to powers: regular p-groups, powerful p-groups and more generally potent p-groups, and (generalized) p-central p-groups. Then we give some applications of the result. We next focus on Beauville structures of those groups which are not inherited by the Frattini quotients. In the last section, we give the characterization of regular Beauville groups without induced Beauville structures.

3.1 Preliminaries

In this section, we present some preliminaries for p-groups with a "nice power structure". The results can be found with detailed proofs in the given references. Where results may not be found, the author provides a proof.

Definition 3.1.1. *Let G be a finite p-group. We call G a **regular p-group** if $x^py^p \equiv (xy)^p \pmod{(\langle x, y\rangle^{'})^p}$ for every $x, y \in G$.*

Theorem 3.1.2. [50, Lemma 3.13]

(i) *Any p-group of class less than p is regular. In particular, any p-group of order $\leq p^p$ is regular.*

(ii) *Let G be a p-group. If $\gamma_{p-1}(G)$ is cyclic, then G is regular. Hence if $p > 2$ and G' is cyclic, then G is regular.*

(iii) *A regular* 2*-group is abelian.*

The elementary properties of regular p-groups are collected in the following theorem.

Theorem 3.1.3. [50, Theorem 3.14] *Let G be a regular* p*-group. Then the following properties hold for any* $i \geq 0$ *:*

(i) *For any* $x, y \in G$*, we have* $x^{p^i} = y^{p^i}$ *if and only if* $(x^{-1}y)^{p^i} = 1$.

(ii) $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(iii) $G^{p^i} = \{x^{p^i} \mid x \in G\}$.

(iv) $|G : \Omega_i(G)| = |G^{p^i}|$*, and consequently also* $|G : G^{p^i}| = |\Omega_i(G)|$.

Corollary 3.1.4. [20, Corollary 2.11] *If a regular* p*-group is generated by elements of order* p^e*, then* $\exp G \leq p^e$.

Another family of p-groups with a nice power structure is powerful p-groups.

Definition 3.1.5. *A finite* p*-group* G *is called* ***powerful*** *if* $G' \leq G^p$ *for odd prime* p*, or if* $G' \leq G^4$ *for* $p = 2$.

Theorem 3.1.6. [[35], Theorem 11.10, [21], Theorem 1 and Theorem 4] *Let G be a powerful* p*-group. Then the following properties hold for any* $i \geq 0$*:*

(i) $G^{p^i} = \{x^{p^i} \mid x \in G\}$.

(ii) *If p is odd, then* $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(iii) $|G : G^{p^i}| = |\Omega_{\{i\}}(G)|$.

Lemma 3.1.7. [21, Lemma 3] *Let G be a powerful* p*-group of exponent* p^e*. Then for every* $0 \leq i \leq e - 1$*, and every* $x \in G$*,* $y \in G^{p^{e-i-1}}$*, we have* $(xy)^{p^i} = x^{p^i} y^{p^i}$.

If G is a powerful p-group of exponent p^e, then Lemma 3.1.7 implies that for any $x, y \in G$, $x^{p^{e-1}} = y^{p^{e-1}}$ if and only if $(x^{-1}y)^{p^{e-1}} = 1$.

Theorem 3.1.8. [40, Corollary 1.9] *Let* $G = \langle g_1, g_2, \ldots, g_n \rangle$ *be a powerful* p*-group. Then for any* $i \geq 1$*, we have* $G^{p^i} = \langle g_1^{p^i}, g_2^{p^i}, \ldots, g_n^{p^i} \rangle$.

We next define a family of finite p-groups which are in many respect dual to powerful p-groups.

Definition 3.1.9. *Let G be a finite p-group. We call G **p-central** if $\Omega_1(G) \leq Z(G)$ for odd prime p, or if $\Omega_2(G) \leq Z(G)$ for $p = 2$.*

It is clear that the property of being p-central or regular is hereditary for subgroups. On the other hand, subgroups of a powerful p-group need not be powerful. The property of being regular or powerful is clearly inherited by quotients, but quotients of a p-central p-group are not necessarily p-central.

Next we consider a family of p-groups which are generalizations of p-central p-groups.

Definition 3.1.10. *Let G be a finite p-group. We call G **generalized p-central** if $\Omega_1(G) \leq Z_{p-2}(G)$ for odd prime p, or if $\Omega_2(G) \leq Z(G)$ for $p = 2$.*

Clearly, every subgroup of a generalized p-central p-group is generalized p-central.

Theorem 3.1.11. [27, Theorem B] *Let G be a generalized p-central p-group. Then for all $i \geq 1$*

(i) $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(ii) *$G/\Omega_i(G)$ is also a generalized p-central p-group.*

Definition 3.1.12. *Let i be any positive integer. We call a finite p-group G **semi-p^i-abelian** if for any $x, y \in G$, $x^{p^i} = y^{p^i}$ if and only if $(x^{-1}y)^{p^i} = 1$.*

Definition 3.1.13. *We call a finite p-group G **strongly semi-p-abelian**, if G is semi-p^i-abelian for every positive integer i.*

The following lemma contains some elementary properties of semi-p^i-abelian p-groups.

Lemma 3.1.14. [52, Lemma 1] *Let G be a finite semi-p^i-abelian p-group. Then the following properties hold:*

(i) $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(ii) $[x,y]^{p^i} = 1$ *if and only if* $[x^{p^i}, y] = 1$ *if and only if* $[x, y^{p^i}] = 1$.

(iii) $|G : \Omega_i(G)| = |\{x^{p^i} \mid x \in G\}|$.

By Theorem 3.1.3, regular p-groups are strongly semi-p-abelian. On the other hand, as a consequence of Lemma 3.1.7, a powerful p-group of exponent p^e is semi-p^{e-1}-abelian, and note that it need not be strongly semi-p-abelian. We next show that a generalized p-central p-group G is strongly semi-p-abelian. This applies in particular to p-central p-groups. We start by proving that G is semi-p-abelian.

Theorem 3.1.15. *A generalized p-central p-group is semi-p-abelian.*

Proof. We prove the theorem by induction on $|G|$. We assume that the conclusion holds for any p-group of order less than $|G|$.

Claim 1: If $a, b \in G$ and $a^p = b^p$, then $(a^{-1}b)^p = 1$.

Set $H = \langle a, b \rangle$. If $H < G$ then by induction hypothesis, H is semi-p-abelian, and hence we are done. Thus we assume that $G = \langle a, b \rangle$. Since $a^p = b^p$, we have $[a^p, b] = 1$, that is $a^p = (b^{-1}ab)^p$. If we set $K = \langle a, b^{-1}ab \rangle$, then K is a proper subgroup of G. The induction hypothesis implies that K is semi-p-abelian, so we get $(a^{-1}b^{-1}ab)^p = [a,b]^p = 1$. Since G is a 2-generator p-group generated by a and b, we have $G' = \langle [a,b]^g \mid g \in G \rangle$, where all generators of G' are of order p. It then follows that $G' \leq \Omega_1(G)$. If p is odd, then $G' \leq Z_{p-2}(G)$, and $\gamma_p(G) = [G', G, \overset{p-2}{\ldots}, G] = 1$. Thus G is regular, by Theorem 3.1.2, and hence $(a^{-1}b)^p = 1$. If $p = 2$ then, since $a^2 = b^2$, we have $G/G' = C/G' \times D/G'$ with C/G' and D/G' cyclic, and $D/G' \cong C_2$. Then $D \leq \Omega_2(G) \leq Z(G)$ and $G/Z(G)$ is cyclic. Thus G is abelian and the result is valid also in this case.

Claim 2: If $a, b \in G$ and $(a^{-1}b)^p = 1$, then $a^p = b^p$.

We may assume that $G = \langle a, b \rangle$. Since $(a^{-1}b)^p = 1$, we have $[(a^{-1}b)^p, a] = 1$, that is $(a^{-1}b)^p = ((a^{-1}b)^p)^a = ((a^{-1}b)^a)^p = (a^{-2}ba)^p$. By Claim 1, we get $[b,a]^p = 1$. Consequently again $G' \leq \Omega_1(G)$ and then, as above, G is regular if p is odd, or abelian if $p = 2$. Then the result holds. □

Theorem 3.1.16. *A generalized p-central p-group is strongly semi-p-abelian.*

Proof. Given $a, b \in G$, we prove that $a^{p^i} = b^{p^i}$ if and only if $(ab^{-1})^{p^i} = 1$ by induction on $i \geq 1$. By Theorem 3.1.15, the results holds for $i = 1$. Thus we consider the case $i > 1$. Since G is semi-p-abelian, we have $a^{p^i} = b^{p^i}$ if and only if $(a^{p^{i-1}}b^{-p^{i-1}})^p = 1$ which is in turn equivalent to $a^{p^{i-1}}\Omega_1(G) = b^{p^{i-1}}\Omega_1(G)$. Now, $G/\Omega_1(G)$ is again a generalized p-central p-group, by Theorem 3.1.11. By the induction hypothesis, the last equality is equivalent to $(ab^{-1})^{p^{i-1}} \in \Omega_1(G)$, and this means exactly that $(ab^{-1})^{p^i} = 1$, since $\Omega_1(G) = \{x \in G \mid x^p = 1\}$. □

Finally, we define a class of p-groups which are generalizations of powerful p-groups.

Definition 3.1.17. *Let G be a finite p-group. We call G* ***potent*** *if $\gamma_{p-1}(G) \leq G^p$ for $p > 2$, or $G' \leq G^4$ for $p = 2$.*

Potent p-groups can be seen as the dual analogue of generalized p-central p-groups. Also, the property of being potent is clearly inherited by quotients. Note also that if $p = 2$ or 3, then a potent p-group is a powerful p-group.

Definition 3.1.18. *Let G be a finite p-group. We call G* ***power abelian*** *if it satisfies the following three properties for any $i \geq 0$:*

(i) $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$.

(ii) $G^{p^i} = \{x^{p^i} \mid x \in G\}$.

(iii) $|G^{p^i}| = |G : \Omega_i(G)|$.

Theorem 3.1.19. [26, Theorem 1.1] *Let p be odd, and let G be a potent p-group. If $N \trianglelefteq G$ then N is power abelian.*

Potent p-groups are not in general strongly semi-p-abelian. Indeed, they need not be even semi-p^{e-1}-abelian as powerful p-groups, given that $\exp G = p^e$.

Example 3.1.20. Let $p > 3$ be a prime and let

$$A = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_p \rangle \cong C_p \times \overset{p-2}{\cdots} \times C_p \times C_{p^2} \times C_{p^2}.$$

be an abelian group.

We define an automorphism α of A by means of

$$\alpha(a_i) = a_i a_{i+1}, \quad \text{for } i = 1, \ldots, p-3,$$

$$\alpha(a_{p-2}) = a_{p-2} a_{p-1}^p,$$

$$\alpha(a_{p-1}) = a_{p-1} a_p,$$

$$\alpha(a_p) = a_p.$$

If we set $x_i = a_i$ for $i = 1, \ldots, p-2$, $x_{p-1} = a_{p-1}^p$, $x_p = a_p^p$ and $x_i = 1$ for $i > p$, then we have $\alpha(x_i) = x_i x_{i+1}$. Since every x_i is of order at most p, we get

$$\alpha^p(x_i) = x_i x_{i+1}^{\binom{p}{1}} x_{i+2}^{\binom{p}{2}} \ldots x_{i+p-1}^{\binom{p}{p-1}} x_{i+p} = x_i$$

for all $i \geq 1$. Also,

$$\alpha^p(a_{p-1}) = a_{p-1} a_p^p.$$

It then follows that $\alpha^{p^2}(a_{p-1}) = a_{p-1}$. Thus α is an automorphism of A of order p^2.

Let $G = A \rtimes \langle b \rangle$, where b is of order p^2 and acts on A via α. Then we have $G' = \langle a_2, a_3, \ldots, a_{p-2}, a_{p-1}^p, a_p \rangle$, and $\gamma_i(G) = \langle a_i, a_{i+1}, \ldots, a_{p-2}, a_{p-1}^p, a_p^p \rangle$ for $3 \leq i \leq p-2$. Thus $\gamma_{p-1}(G) = \langle a_{p-1}^p, a_p^p \rangle \leq G^p$, and hence G is potent. Furthermore, it is a 3-generator potent p-group as $G = \langle b, A \rangle = \langle b, a_1, \ldots, a_{p-1}, a_p \rangle = \langle b, a_1, a_{p-1} \rangle$.

We will show that $\exp G = p^2$. If we set $N = \langle b^p, a_1, \ldots, a_{p-2}, a_{p-1}^p, a_p^p \rangle \leq G$, then we see that N is an abelian normal subgroup of exponent p. Since $\alpha^p(x_i) = x_i$ for all $i \geq 1$, b^p commutes with all x_i, and hence N is abelian. Then we have $\exp N = p$, since N is abelian and each generator of N is of order p. To show $N \trianglelefteq G$, we only need to show that $[b^p, a] \in N$ for all $a \in A$. Now

$$[b^p, a_i] = a_i, \quad \text{for } i = 1, \ldots, p-2,$$

$$[b^p, a_{p-1}] = a_p^p, \quad [b^p, a_p] = 1.$$

Hence we conclude that N is normal in G. We next consider the quotient group $\overline{G} = G/N = \langle \overline{b}, \overline{a_{p-1}} \rangle$. Since $[\overline{b}, \overline{a_{p-1}}] = \overline{a_p} \in Z(\overline{G})$, this implies that $\overline{G}$ is of class $2 < p$. Thus by Theorem 3.1.2, $\overline{G}$ is a regular p-group in which each generator is of order p. Then according to Corollary 3.1.4, $\exp \overline{G} = p$, and this, together with $\exp N = p$, yields that $\exp G = p^2$.

We next show that G is not semi-p-abelian. Observe that $\langle a_1, G' \rangle$ is abelian. Then by Lemma 2.2.21, we have

$$\begin{aligned}(ba_1)^p &= b^p a_1^p [a_1, b]^{\binom{p}{2}} [a_1, b, b]^{\binom{p}{3}} \dots [a_1, b, \overset{p-1}{\dots}, b]^{\binom{p}{p}} \\ &= b^p a_p^p = (ba_p)^p.\end{aligned}$$

The last equality is due to the fact that $a_p \in Z(G)$. On the other hand, $(a_p^{-1} b^{-1} b a_1)^p = (a_p^{-1} a_1)^p = a_p^{-p} \neq 1$.

Hence G is a 3-generator potent p-group of exponent p^2 which is not semi-p-abelian.

3.2 Main result

Recall that Catanese's criterion for abelian Beauville groups implies that a 2-generator abelian p-group of exponent p^e is a Beauville group if and only if $p \geq 5$ and $|G^{p^{e-1}}| = p^2$. In this section, we give a generalization of this result to a wide class of finite p-groups with a nice power structure. Then we will give a number of application of this result.

We start with a proposition that can be used to prove the non-existence of Beauville structures.

Proposition 3.2.1. *Let G be a* 2*-generator finite* p*-group of exponent* p^e*, and suppose that:*

(i) $\Omega_{\{e-1\}}(G)$ *is contained in the union of two maximal subgroups of G.*

(ii) $|G^{p^{e-1}}| = p$*.*

Then G is not a Beauville group.

Proof. We argue by way of contradiction. Suppose $\{x_1, y_1\}$ and $\{x_2, y_2\}$ are two systems of generators of G such that $\Sigma(x_1, y_1) \cap \Sigma(x_2, y_2) = 1$. Since no two of the elements x_1, y_1 and $x_1 y_1$ can lie in the same maximal subgroup of G, it follows from (i) that one of these elements, say x_1, is of order p^e. Similarly, we may assume that the order of x_2 is also p^e. Since $G^{p^{e-1}}$ is of order p, we conclude that $\langle x_1^{p^{e-1}} \rangle = \langle x_2^{p^{e-1}} \rangle$, which is a contradiction. □

We will see later in Chapter 5 that we cannot relax condition (i) in Proposition 3.2.1, since there are examples of groups G in which $\Omega_{\{e-1\}}(G)$ is contained in the union of three maximal subgroups, and which are Beauville groups even if $G^{p^{e-1}}$ is of order p.

We next give the main result of this chapter which can be applied to all classes of finite p-groups given in Section 3.1.

Theorem 3.2.2. *Let G be a 2-generator finite p-group of exponent p^e such that one of the following conditions holds:*

(i) *G is semi-p^{e-1}-abelian, i.e. for every $x, y \in G$*

$$x^{p^{e-1}} = y^{p^{e-1}} \quad \textit{if and only if} \quad (xy^{-1})^{p^{e-1}} = 1. \tag{3.1}$$

(ii) *G is a potent p-group.*

Then G is a Beauville group if and only if $p \geq 5$ and $|G^{p^{e-1}}| \geq p^2$. If that is the case, then every lift of a Beauville structure in $G/\Phi(G)$ yields a Beauville structure of G.

Proof. First of all, notice that if (3.1) holds in G, then according to Lemma 3.1.14, $\Omega_{e-1}(G) = \{g \in G \mid g^{p^{e-1}} = 1\}$. It then follows from (3.1) that $x^{p^{e-1}} = y^{p^{e-1}}$ if and only if $\Omega_{e-1}(G)x = \Omega_{e-1}(G)y$, and therefore the cardinality of the set

$$X = \{g^{p^{e-1}} \mid g \in G\}$$

coincides with the index $|G : \Omega_{e-1}(G)|$.

Let us first show that G is a Beauville group if $p \geq 5$ and $|G^{p^{e-1}}| \geq p^2$. We claim that $\Omega_{e-1}(G)$ is contained in $\Phi(G)$. Since $\Phi(G) = G'G^p \subseteq G'\Omega_{e-1}(G)$, we have

$$\begin{aligned} |G/\Omega_{e-1}(G) : (G/\Omega_{e-1}(G))'| &= |G : G'\Omega_{e-1}(G)| \\ &= |G : \Phi(G)\Omega_{e-1}(G)| \leq |G : \Phi(G)| = p^2. \end{aligned} \tag{3.2}$$

If $|G/\Omega_{e-1}(G) : (G/\Omega_{e-1}(G))'| \leq p$, then the quotient $G/\Omega_{e-1}(G)$ is cyclic, and so it has order at most p. If (3.1) holds in G, then by the first paragraph of the proof, we have $|X| \leq p$, and then the subgroup $G^{p^{e-1}}$ coincides with X. If G is potent, then by Theorem 3.1.19, it is power abelian, and hence $|G : \Omega_{e-1}(G)| = |G^{p^{e-1}}|$, and $G^{p^{e-1}}$ coincides with X. Thus in both cases $|G^{p^{e-1}}| \leq p$, contrary to our assumption. Thus we have $|G/\Omega_{e-1}(G) : (G/\Omega_{e-1}(G))'| \geq p^2$, and this, together with (3.2), yields that $\Phi(G)\Omega_{e-1}(G) = \Phi(G)$, i.e. that $\Omega_{e-1}(G) \subseteq \Phi(G)$. This proves the claim.

Since $p \geq 5$, the elementary abelian group $G/\Phi(G)$ is a Beauville group. Let us see that every Beauville structure of $G/\Phi(G)$ lifts to a Beauville structure of G. If we use the bar notation in $G/\Phi(G)$, it suffices to show that, given two elements $x, y \in G \smallsetminus \Phi(G)$, the condition $\langle \overline{x} \rangle \cap \langle \overline{y} \rangle = \overline{1}$ implies that $\langle x \rangle \cap \langle y \rangle = 1$. Observe that x and y are of order p^e, since $\Omega_{e-1}(G) \subseteq \Phi(G)$.

Case 1: We first assume that (3.1) holds in G. If $\langle x \rangle \cap \langle y \rangle \neq 1$ then $\langle x^{p^{e-1}} \rangle = \langle y^{p^{e-1}} \rangle$, and consequently $x^{p^{e-1}} = y^{ip^{e-1}}$ for some integer i not divisible by p. According to (3.1), we have $xy^{-i} \in \Omega_{e-1}(G)$ and consequently $\langle \overline{x} \rangle = \langle \overline{y} \rangle$, which is a contradiction.

Case 2: We next assume that G is potent. Notice that a maximal subgroup M of G is power abelian, according to Theorem 3.1.19, and hence $|M : M^{p^{e-1}}| = |\Omega_{e-1}(M)|$. Also, $\Omega_{e-1}(G) \leq \Phi(G) \leq M$ implies that $\Omega_{e-1}(M) = \Omega_{e-1}(G)$. Thus we have $|G : G^{p^{e-1}}| = |M : M^{p^{e-1}}|$, and so $|G^{p^{e-1}} : M^{p^{e-1}}| = p$. Let us see that for every $g \in G \smallsetminus M$, we have $g^{p^{e-1}} \in G^{p^{e-1}} \smallsetminus M^{p^{e-1}}$. If $g^{p^{e-1}} \in M^{p^{e-1}}$ then in the quotient $\overline{G} = G/M^{p^{e-1}}$, we have $\overline{g} \in \Omega_{e-1}(\overline{G})$, and this, together with $\overline{M} \leq \Omega_{e-1}(\overline{G})$, yields that $\overline{G} = \langle \overline{g}, \overline{M} \rangle \leq \Omega_{e-1}(\overline{G})$. Since $\overline{G}$ is also potent, the exponent of $\Omega_{e-1}(\overline{G})$ is at most p^{e-1}, and hence $\overline{G}^{p^{e-1}} = \overline{1}$, that is $G^{p^{e-1}} \leq M^{p^{e-1}}$. This contradicts the property that $|G^{p^{e-1}} : M^{p^{e-1}}| = p$.

Let $x \in M$ for some maximal subgroup M of G. If $\langle x \rangle \cap \langle y \rangle \neq 1$ then $\langle x^{p^{e-1}} \rangle = \langle y^{p^{e-1}} \rangle$, and so $x^{ip^{e-1}} = y^{p^{e-1}}$ for some i not divisible by p. This implies that $y^{p^{e-1}} \in M^{p^{e-1}}$, which is a contradiction, since $\langle \overline{x} \rangle \cap \langle \overline{y} \rangle = \overline{1}$ in $G/\Phi(G)$, we have $y \notin M$.

Thus we complete the proof of the first implication in the statement of the theorem.

Let us now prove the converse. Since $\Omega_{\{e-1\}}(G)$ is a subgroup of G and $\exp G = p^e$, it follows from Proposition 3.2.1 that we only need to prove that G has no Beauville structure if $p = 2$ or 3, provided that $|G^{p^{e-1}}| \geq p^2$. Observe that since we assume that $|G^{p^{e-1}}| \geq p^2$, we have $\Omega_{e-1}(G) \subseteq \Phi(G)$, as shown above. Hence all elements of $G \smallsetminus \Phi(G)$ are of order p^e. Also note that if G is potent and $p = 2$ or 3, then G is powerful p-group and consequently satisfies the condition (3.1). Thus it suffices to prove the result in case (i). We are going to show that if (3.1) holds in G, a Beauville structure of G induces, by passing to the quotient, a Beauville structure in G/G^p. However, if $p = 2$ then G/G^2 is abelian of order 4, and if $p = 3$ then G/G^3 is of order at most 3^3 by [47, 14.2.3]. Since there is no abelian Beauville 2-group and the smallest Beauville 3-group is of order 3^5, G/G^p does not have a Beauville structure in both cases.

So let us see that if (3.1) holds in G, then a Beauville structure of G is inherited by G/G^p. To this purpose, we see that, given $x, y \in G \smallsetminus \Phi(G)$, the condition $\langle x \rangle \cap \langle y \rangle = 1$ implies that $\langle \overline{x} \rangle \cap \langle \overline{y} \rangle = \overline{1}$ in G/G^p. Otherwise, we have $\langle \overline{x} \rangle = \langle \overline{y} \rangle$, and consequently $xy^{-i} \in G^p$ for some i not divisible by p. Since G^p is generated by $\{g^p \mid g \in G\} \subseteq \Omega_{\{e-1\}}(G)$, it follows that $(xy^{-i})^{p^{e-1}} = 1$. By (3.1), we have $x^{p^{e-1}} = y^{ip^{e-1}}$. Since x and y are of order p^e, this implies that $\langle x \rangle \cap \langle y \rangle \neq 1$, which is a contradiction. □

The following corollary is an immediate consequence of Theorem 3.2.2.

Corollary 3.2.3. *Let G be a finite p-group, and suppose that G belongs to one of the following families:*

(i) *Regular p-groups, and in particular groups of order at most p^p.*

(ii) *Potent p-groups, and in particular powerful p-groups.*

(iii) *Generalized p-central p-groups, and in particular p-central p-groups.*

Then G is a Beauville group if and only if $p \geq 5$ and $|G^{p^{e-1}}| \geq p^2$, where $\exp G = p^e$.

The next result shows that, under the hypothesis of Theorem 3.2.2, the condition $|G^{p^{e-1}}| \geq p^2$ can be easily determined if G has a reasonably good presentation.

Proposition 3.2.4. *Let $G = \langle a, b \rangle$ be a finite p-group of exponent p^e which is either semi-p^{e-1}-abelian or potent. Then $|G^{p^{e-1}}| \geq p^2$ if and only if $|\langle a^{p^{e-1}}, b^{p^{e-1}} \rangle| \geq p^2$.*

Proof. First of all, notice that at least one of a or b is of order p^e. Otherwise, $a, b \in \Omega_{e-1}(G) = \{g \in G \mid g^{p^{e-1}} = 1\}$. This implies that $G \leq \Omega_{e-1}(G)$, and hence $\exp G \leq p^{e-1}$, which is a contradiction.

It is clear that the condition $|\langle a^{p^{e-1}}, b^{p^{e-1}}\rangle| \geq p^2$ implies $|G^{p^{e-1}}| \geq p^2$. To prove the converse, suppose, to the contrary, that $|\langle a^{p^{e-1}}, b^{p^{e-1}}\rangle| = p$. Then we have one of the following cases:

(i) $a^{p^{e-1}} = 1$ or $b^{p^{e-1}} = 1$.

(ii) $a^{p^{e-1}} \neq 1$ and $b^{p^{e-1}} \neq 1$.

If (ii) holds, then $b^{p^{e-1}} = a^{ip^{e-1}}$ for some integer i not divisible by p. If G is semi-p^{e-1}-abelian, then it follows that $(ba^{-i})^{p^{e-1}} = 1$, and hence ba^{-i} can play the role of b in (i). If G is potent, then as in the proof of Theorem 3.2.2, the condition $b^{p^{e-1}} = a^{ip^{e-1}}$ implies that a and b lie in the same maximal subgroups, which is a contradiction. Thus in both cases, we may assume that $a^{p^{e-1}} \neq 1$ and $b^{p^{e-1}} = 1$.

We next show that $\Phi(G) \leq \Omega_{e-1}(G)$. Recall that $\Phi(G) = G'G^p$ and $G^p \leq \Omega_{e-1}(G)$. Thus we only need to see that $G' = \langle [a,b]^g \mid g \in G\rangle \leq \Omega_{e-1}(G)$. Since $[a,b] = (b^{-1})^a b \in \Omega_{e-1}(G)$ and $\Omega_{e-1}(G) \trianglelefteq G$, we have $G' \leq \Omega_{e-1}(G)$, and hence $\Phi(G) \leq \Omega_{e-1}(G)$. Indeed, $\Phi(G)$ is a proper subgroup of $\Omega_{e-1}(G)$, since $b \in \Omega_{e-1}(G) \smallsetminus \Phi(G)$. Thus we have $|G : \Omega_{e-1}(G)| = |\{g^{p^{e-1}} \mid g \in G\}| = p$. This implies that the subgroup $G^{p^{e-1}}$ coincides with the set $\{g^{p^{e-1}} \mid g \in G\}$, and consequently $|G^{p^{e-1}}| = p$, contrary to our assumption that $|G^{p^{e-1}}| \geq p^2$. □

Observe that the condition $|\langle a^{p^{e-1}}, b^{p^{e-1}}\rangle| \geq p^2$ is tantamount to the fact that the two subgroups $\langle a^{p^{e-1}}\rangle$ and $\langle b^{p^{e-1}}\rangle$ are different and non-trivial.

In [2], it was proved that if $p > 3$ then there are at least $p+8$ Beauville groups of order p^5. Then the authors conjecture that the two non-isomorphic groups of order p^5 under the names H_3 and H_4 in that paper are Beauville for $p \geq 5$ and, as a consequence, that there are exactly $p + 10$ Beauville groups of order p^5 for $p \geq 5$. This can be shown easily by using Proposition 3.2.4. Indeed, both H_3 and H_4 can be described in the form

$$G = \langle a, b, c \mid a^{p^2} = b^{p^2} = c^p = [b, c] = 1,\ [a, b] = c,\ [a, c] = b^{rp}\rangle,$$

where r is not divisible by p. Observe that $G = \langle a, b\rangle$. Since $\exp G = p^2$ and $\langle a^p\rangle \neq \langle b^p\rangle$ are non-trivial, and consequently G is a Beauville group.

For groups of class less than p (so in particular for groups of order at most p^p), we can further simplify the determination of whether the group is Beauville or not by using the Lazard Correspondence. Recall that the Lazard Correspondence uses the Baker-Campbell-Hausdorff formula to establish a one-to-one correspondence between finite p-groups of class less than p and nilpotent Lie rings of p-power order of class less than p (see [35, Section 10.2]). The underlying set for both the group and the Lie ring is the same, and it turns out that the nth power of an element in the group coincides with its nth multiple in the Lie ring. Thus if $G = \langle a, b \rangle$, we can check the conditions in Proposition 3.2.4 by working in the Lie ring instead of in the group, i.e. we have to check whether $\langle p^{e-1}a \rangle$ and $\langle p^{e-1}b \rangle$ are different and non-trivial. This is particularly interesting for p-groups of small order, since their classification relies in classifying first nilpotent Lie rings of the same order and then applying the Lazard correspondence. For example, this is the procedure followed in [45] and [46] to determine all groups of orders p^6 and p^7 for $p \geq 7$. By using the presentations of the nilpotent Lie rings of order p^6 provided in [51], we have obtained that the number of Beauville groups of order p^6 is

$$4p + 20 + 4\gcd(p-1, 3) + \gcd(p-1, 4)$$

for $p \geq 7$. Since the total number of 2-generator groups of order p^6 is

$$10p + 62 + 14\gcd(p-1, 3) + 7\gcd(p-1, 4) + 2\gcd(p-1, 5),$$

it follows that the ratio between the number of Beauville groups and the number of all 2-generator groups of order p^6 tends to $2/5$ as $p \to \infty$. Note that in [2], the authors could only say that this limit is smaller than 1, by finding $p-1$ non-Beauville 2-generator groups of order p^6.

As an illustration of our method, let us consider the following two nilpotent Lie rings of order p^6 taken from [51]:

$$L_1 = \langle a, b \mid p^2 a, pb - [b, a, a], p\text{-class } 3 \rangle$$

and

$$L_2 = \langle a, b \mid pa - [b, a, a, a], pb - [b, a, a, a], [b, a, a, b], \\ [b, a, b, b] + [b, a, a, a], p\text{-class } 4 \rangle.$$

Clearly, in both L_1 and L_2, the elements a and b are of order p^2, which is the exponent of the additive group of the Lie ring. In the first case, $\langle pa \rangle$ and $\langle pb \rangle$ are different subgroups, while in the second case they are equal. Thus L_1 gives rise to a Beauville group under the Lazard correspondence, while L_2 does not.

It would be equally possible to calculate the exact number of Beauville groups of order p^7, for $p \geq 7$, but we have not pursued that task.

As a final application of Theorem 3.2.2, we extend the characterization given in [49, Theorem 4] of split metacyclic Beauville p-groups to all metacyclic p-groups.

Corollary 3.2.5. *A metacyclic p-group G is a Beauville group if and only if $p \geq 5$ and G is a semidirect product of two cyclic groups of the same order.*

Proof. Let $G = \langle a, b \rangle$ with $\langle a \rangle \trianglelefteq G$. Assume first that p is odd, and let $\exp G = p^e$. Then G' is cyclic and G is regular by Theorem 3.1.2. Thus G is semi-p^{e-1}-abelian and then, by Proposition 3.2.4, G is a Beauville group if and only if $p \geq 5$ and the subgroups $\langle a^{p^{e-1}} \rangle$ and $\langle b^{p^{e-1}} \rangle$ are non-trivial and different. This means that $G = \langle b \rangle \ltimes \langle a \rangle$ is a semidirect product with a and b of the same order.

Now we consider the case $p = 2$. We have to prove that G is not a Beauville group. If $G' \leq G^4$ then G is powerful, and the result follows from Corollary 3.2.3. Thus we assume that G' is not contained in G^4, i.e. that $G' = \langle a^2 \rangle$. We claim that, for every set $\{x, y\}$ of generators, we have $bG' \subseteq \Sigma(x, y)$. This proves that G is not a Beauville group also in this case. Since G has only three maximal subgroups, we may assume that $x \in \langle b \rangle G^2 \smallsetminus G^2$. Since $G^2 = \langle b^2 \rangle G'$, we can write $x = b^i w$ with i odd and $w \in G'$. Then there is a power of x of the form $x^* = bw^*$, for some $w^* \in G'$. Now observe that

$$G' = \langle [x^*, a] \rangle = \{[x^*, a]^i \mid i \in \mathbb{N}\} = \{[x^*, a^i] \mid i \in \mathbb{N}\},$$

and consequently the conjugacy class of x^* equals $x^* G' = bG'$. This proves that bG' is contained in $\Sigma(x, y)$, as desired. □

We next show that the assumptions (i) or (ii) are essential in Theorem 3.2.2. Indeed, for a general finite p-group G, the condition that $|G^{p^{e-1}}| \geq p^2$ is neither sufficient nor necessary for G to be a Beauville group. We show this in Corollary 3.2.7, by using quotients of some infinite pro-p groups that we define now.

Let $k \geq 1$ be a fixed integer, and consider the ring of integers R of the cyclotomic field $\mathbb{Q}_p(\zeta)$, where $\mathbb{Q}_p$ is the field of p-adic numbers and ζ is a primitive p^kth root of unity. Then $R = \mathbb{Z}_p[\zeta]$ is a discrete valuation ring and a free $\mathbb{Z}_p$-module of rank $p^{k-1}(p-1)$. Also, the element $\zeta - 1$ is a uniformizer, and we have

$$(p) = (\zeta - 1)^{p^{k-1}(p-1)}. \tag{3.3}$$

Multiplication by ζ defines an automorphism of order p^k of the additive group of R, which can be used to construct a split extension of R by C_{p^k}. In order to avoid mixing additive and multiplicative notation, we consider a multiplicative copy A of R, via an isomorphism $\varphi : A \to R$. If $C = \langle t \rangle$ is a cyclic group of order p^k, then we define $P_k = C \ltimes A$, where the action of t on A corresponds under φ to multiplication by ζ, that is, $\varphi(a^t) = \zeta\varphi(a)$ for all $a \in A$. Observe that P_k is a 2-generator pro-p group, topologically generated by t and by $a_1 = \varphi^{-1}(1)$. Also, we have $P_k' = [A, t]$, which corresponds to the ideal $(\zeta - 1)$ of R under φ. More generally, the lower central series of P_k consists of the subgroups $[A, t, \ldots, t]$, and the action of C on A is uniserial. In particular, if $k = 1$ then we get the only infinite pro-p group of maximal class.

As we next see, the pro-p groups P_k are a source of infinitely many Beauville p-groups.

Theorem 3.2.6. *Let $p \geq 5$ be a prime and let $k \geq 1$ be an integer. If N is a normal subgroup of P_k of finite index and $N \leq A^p$, then the factor group P_k/N is a Beauville group.*

Proof. By [14, Theorem 1.17], N is open in P_k, and consequently, P_k/N is a 2-generator p-group. For every $a \in A$, we have

$$(ta)^{p^k} = t^{p^k} a^{\sum_{i=0}^{p^k-1} t^i}. \tag{3.4}$$

Since ζ is a primitive p^kth root of unity and $t^{p^k} = 1$, it follows that $(ta)^{p^k} = 1$. Now the image of ta in P_k/A is of order p^k, and consequently taN is of order p^k in P_k/N as well.

Let $a, b \in A$ and assume that the subgroups generated by taN and tbN have non-trivial intersection. Then these subgroups have the same p^{k-1}st power, and it readily follows that $(taN)^{p^{k-1}} = (tbN)^{p^{k-1}}$. By a calculation similar to (3.4), we get

$$a^{\sum_{i=0}^{p^{k-1}-1} t^i} \equiv b^{\sum_{i=0}^{p^{k-1}-1} t^i} \pmod{N},$$

and then the same congruence holds modulo A^p. It follows that

$$\Big(\sum_{i=0}^{p^{k-1}-1} \zeta^i \Big) (\varphi(a) - \varphi(b)) \equiv 0 \pmod{p} \tag{3.5}$$

in R. Now in the polynomial ring $\mathbb{F}_p[X]$ we have

$$\sum_{i=0}^{p^{k-1}-1} X^i = (X-1)^{p^{k-1}-1},$$

and consequently

$$\sum_{i=0}^{p^{k-1}-1} \zeta^i \equiv (\zeta - 1)^{p^{k-1}-1} \pmod{p}.$$

If we replace this into (3.5) and use (3.3), we get

$$\varphi(a) - \varphi(b) \in (\zeta - 1)^{p^k - 2p^{k-1} + 1}.$$

In particular, $\varphi(a) - \varphi(b) \in (\zeta - 1)$ or, what is the same, $a \equiv b \pmod{P_k'}$.

Now, by the previous paragraph, if $x, y \in \{t, ta_1, \ldots, ta_1^{p-1}\}$ and $x \neq y$, then $\langle xN \rangle \cap \langle yN \rangle = 1$. Since xN and yN are generators of P_k/N and $p \geq 5$, we conclude that P_k/N is a Beauville group. □

Corollary 3.2.7. *Let $p \geq 5$ be a prime. Then, for each of the implications in the criterion for Beauville groups given in Theorem 3.2.2, there exist infinitely many 2-generator p-groups (and even infinitely many p-groups of maximal class) for which the implication fails.*

Proof. Consider arbitrary integers $e > k \geq 1$, and let N be a normal subgroup of P_k such that $|A^{p^{e-1}} : N| = p$. By Theorem 3.2.6, $G = P_k/N$ is a Beauville group. In the proof of that theorem, we have seen that all elements of the form taN with $a \in A$ are of order p^k. It readily follows that every element of $P_k \smallsetminus A$ is of order at most p^k when passing to G. Thus $\exp G = p^e$ and $G^{p^{e-1}} = A^{p^{e-1}}/N$ is of order p. This shows that the 'only if' part of Theorem 3.2.2 fails for G.

Let us construct a family of groups for which the 'if' part fails. Take again $e > k \geq 1$, and consider now $N \trianglelefteq P_k$ lying between $A^{p^{e-1}}$ and A^{p^e}, and such that $|A^{p^{e-1}} : N| = p^m \geq p^2$. Let $L \trianglelefteq P_k$ be an intermediate subgroup between N and $A^{p^{e-1}}$ such that $|L : N| = p$. Thus $L/N \leq Z(P_k/N)$. Let us write $H = A/N$ and $Z = L/N$. By using the theory of cyclic extensions [54, Section 3.7], we can get a new group $G = \langle u, H \rangle$, where the action of u on H is again the one induced by multiplication by ζ, but $u^{p^k} \in Z \smallsetminus 1$. Observe that G is a 2-generator group. A calculation as in (3.4) shows that every $x \in uH$ is now of order p^{k+1}, and $\langle x^{p^k} \rangle = Z$. Also, all elements of $G \smallsetminus H$ are of order at most p^{k+1}. Then $\exp G = p^e$ and $|G^{p^{e-1}}| = p^m$. Now, any set $\{x, y\}$ of generators of G must contain an element, say x, outside the maximal subgroup $\langle u^p \rangle H$, and then a power of x will be in uH. Consequently, $Z \subseteq \Sigma(x, y)$ and G cannot be a Beauville group. □

We end this section by showing that it is not possible to find a variation of Theorem 3.2.2 which ensures the existence of Beauville structures in an arbitrary finite p-group, even if we strengthen the requirement on the size of $G^{p^{e-1}}$. Indeed, for every power of p there are non-Beauville p-groups for which the order of $G^{p^{e-1}}$ is exactly that power.

Corollary 3.2.8. *For every prime $p \geq 5$, and positive integer m, there exists a 2-generator p-group G such that:*

1. *If $\exp G = p^e$ then $|G^{p^{e-1}}| = p^m$.*
2. *G is not a Beauville p-group.*

Proof. Let $G = P_k/N$ be as in the second part of the proof of the last corollary. Since $\log_p |A^{p^{e-1}} : A^{p^e}| = p^{k-1}(p-1)$, we can make $|A^{p^{e-1}} : N|$ as large as we want by taking k big enough. This gives the desired groups. □

3.3 Beauville structures which are not inherited by the Frattini quotient

In the previous section, by Theorem 3.2.2, we prove that if G is a 2-generator finite p-group of exponent p^e satisfying condition (3.1) for every $x, y \in G$, then G is a

Beauville group if and only if $p \geq 5$ and $|G^{p^{e-1}}| \geq p^2$. Indeed, every lift of a Beauville structure in $G/\Phi(G)$ yields a Beauville structure of G.

In this section, we want to determine if there is a Beauville structure of G which does not reduce to a Beauville structure of $G/\Phi(G)$. To this purpose, we will concentrate on the index $|G : \Omega_{e-1}(G)|$.

Lemma 3.3.1. *Let G be a Beauville p-group of exponent p^e satisfying condition (3.1). If $|G : \Omega_{e-1}(G)| \leq p^3$, then every Beauville structure of G is inherited by $G/\Phi(G)$.*

Proof. First of all, notice that the conditions $|G^{p^{e-1}}| \geq p^2$ and (3.1) imply that $\Omega_{e-1}(G) \leq \Phi(G)$, as shown in the proof of Theorem 3.2.2. Thus we have $|G : \Omega_{e-1}(G)| = p^2$ or p^3.

We will see that every Beauville structure of G can be inherited by the quotient group $G/\Omega_{e-1}(G)$. To this purpose, we need to show that, given two elements $x, y \in G \smallsetminus \Phi(G)$, the condition $\langle x\rangle \cap \langle y\rangle = 1$ implies that $\langle \overline{x}\rangle \cap \langle \overline{y}\rangle = \overline{1}$ in $G/\Omega_{e-1}(G)$. Otherwise, we have $\langle \overline{x}\rangle = \langle \overline{y}\rangle$ in $G/\Omega_{e-1}(G)$, since $\exp G/\Omega_{e-1}(G) = p$. This implies that $xy^{-i} \in \Omega_{e-1}(G)$ for some i not divisible by p, and hence $(xy^{-i})^{p^{e-1}} = 1$. Then it follows from (3.1) that $x^{p^{e-1}} = y^{ip^{e-1}}$. Since x and y are of order p^e, we have $\langle x\rangle \cap \langle y\rangle \neq 1$, which is a contradiction.

If $|G/\Omega_{e-1}(G)| = p^2$ then $\Omega_{e-1}(G)$ coincides with $\Phi(G)$, and by the previous paragraph, we are done. If $|G/\Omega_{e-1}(G)| = p^3$ then the quotient group $G/\Omega_{e-1}(G)$ is extraspecial, since it is non-abelian. Recall that a p-group P is said to be extraspecial if $\Phi(P) = P' = Z(P)$ and $|Z(P)| = p$. If $x \in P \smallsetminus \Phi(P)$ then there exists $g \in P$ such that $[x, g] \neq 1$, and hence $P' = \langle [x, g]\rangle = \{[x, g^i] \mid i = 0, 1, \ldots, p-1\}$. Thus, the derived subgroup of an extraspecial group is covered by commutators of any element outside the Frattini subgroup.

Let $\{\overline{x_1}, \overline{y_1}\}$ and $\{\overline{x_2}, \overline{y_2}\}$ form a Beauville structure for $\overline{G} = G/\Omega_{e-1}(G)$. If we set $A = \{x_1, y_1, x_1y_1\}$ and $B = \{x_2, y_2, x_2y_2\}$, then the previous paragraph, together with $p \geq 5$, implies that a and b are linearly independent modulo $\Phi(\overline{G})$ for every $a \in A$ and $b \in B$. Thus, every Beauville structure of $G/\Omega_{e-1}(G)$ is inherited by the Frattini quotient $G/\Omega_{e-1}(G) \big/ \Phi(G/\Omega_{e-1}(G)) \cong G/\Phi(G)$. □

In order to prove Theorem 3.3.3, we need the following lemma.

Lemma 3.3.2. *Let G be a 2-generator p-group of order $p^n \geq p^4$. Then there exist $x \in G \smallsetminus \Phi(G)$ and $u \in \Phi(G) \smallsetminus \{[x,g] \mid g \in G\}$.*

Proof. Note that a p-group has maximal class if and only if it has an element with centralizer of order p^2 (see [30, III.14.23]). Thus if G is not a group of maximal class, then for any $x \in G \smallsetminus \Phi(G)$ we have $|C_G(x)| \geq p^3$. On the other hand, if G is a group of maximal class and we write $G_i = \gamma_i(G)$ for $i \geq 2$, then the subgroup $G_1 = C_G(G_2/G_4)$ is a maximal subgroup of G. In this case, for any $x \in G_1 \smallsetminus \Phi(G)$, we have $|C_G(x)| \geq p^3$. Thus in both cases we get

$$|\{[x,g] \mid g \in G\}| = |\operatorname{Cl}_G(x)| = |G : C_G(x)| \leq p^{n-3}.$$

Since $|\Phi(G)| = p^{n-2}$, there exists $u \in \Phi(G)$ such that $u \notin \{[x,g] \mid g \in G\}$. $\square$

Theorem 3.3.3. *Let G be a Beauville p-group of exponent p^e satisfying condition (3.1). Then G has a Beauville structure which is not inherited by $G/\Phi(G)$ if and only if $|G : \Omega_{e-1}(G)| \geq p^4$.*

Proof. One of the implications in the statement of the theorem follows directly from Lemma 3.3.1.

Let us now prove the converse. If we use the bar notation in $G/\Omega_{e-1}(G)$, then by Lemma 3.3.2, there exist $\overline{x} \in \overline{G} \smallsetminus \Phi(\overline{G})$ and $\overline{u} \in \Phi(\overline{G}) \smallsetminus \{[\overline{x}, \overline{g}] \mid \overline{g} \in \overline{G}\}$. Choose $y \in G$ such that $G = \langle x, y \rangle$. We claim that $\{x, y\}$ and $\{xu, xy^3\}$ form a Beauville structure for G. Clearly this Beauville structure cannot be inherited by $G/\Phi(G)$, since $\langle \overline{x} \rangle = \langle \overline{xu} \rangle$ in $G/\Phi(G)$.

Note that since G is a Beauville group satisfying (3.1), we have $p \geq 5$ and $|G^{p^{e-1}}| \geq p^2$. Also by the proof of Theorem 3.2.2, we have $\Omega_{e-1}(G) \leq \Phi(G)$. Let $A = \{x, y, xy\}$ and $B = \{xu, xy^3, xuxy^3\}$. If $a = x$ and $b = xy^3$ or $xuxy^3$ then $\langle \overline{a} \rangle \cap \langle \overline{b} \rangle = \overline{1}$ in the quotient $G/\Phi(G)$, since x and y are linearly independent modulo $\Phi(G)$. Thus if $\langle a^g \rangle \cap \langle b^h \rangle \neq 1$ for some $g, h \in G$, then we have $\langle (a^g)^{p^{e-1}} \rangle = \langle (b^h)^{p^{e-1}} \rangle$, and consequently $(a^g)^{p^{e-1}} = (b^h)^{jp^{e-1}}$ for some integer j not divisible by p. According to (3.1), we have $(a^g(b^h)^{-j})^{p^{e-1}} = 1$, that is $a^g(b^h)^{-j} \in \Omega_{e-1}(G)$. This implies that

$\langle \overline{a} \rangle = \langle \overline{b} \rangle$ in the quotient $G/\Phi(G)$, which is a contradiction. The same argument applies when $a = xy$ and $b \in B$. In the case $a = y$ and $b \in B$, again we have $\langle \overline{a} \rangle \cap \langle \overline{b} \rangle = \overline{1}$ in the quotient $G/\Phi(G)$, since x and y are linearly independent modulo $\Phi(G)$ and $p \geq 3$. Therefore, $\langle a^g \rangle \cap \langle b^h \rangle = 1$ for every $g, h \in G$, as shown above.

Thus we are only left with the case $a = x$ and $b = xu$. We need to prove that $\langle x \rangle^g \cap \langle xu \rangle = 1$ for any $g \in G$. If $\langle x \rangle^g \cap \langle xu \rangle \neq 1$ for some $g \in G$, then $\langle (x^g)^{p^{e-1}} \rangle = \langle (xu)^{p^{e-1}} \rangle$, and consequently $(x^g)^{jp^{e-1}} = (xu)^{p^{e-1}}$ for some integer j not divisible by p. According to (3.1), we have $(u^{-1}x^{-1}(x^g)^j)^{p^{e-1}} = 1$ and hence $\overline{xu} = (\overline{x^g})^j$ in $G/\Omega_{e-1}(G)$, which is a contradiction. Indeed, since $\overline{G} = G/\Omega_{e-1}(G)$ is a p-group, $\overline{x}$ is of order p and $\overline{u} \in \Phi(\overline{G}) \smallsetminus \{[\overline{x}, \overline{g}] \mid \overline{g} \in \overline{G}\}$, it follows from Lemma 2.3.2 that $\langle \overline{x} \rangle^{\overline{g}} \cap \langle \overline{xu} \rangle = \overline{1}$ for any $\overline{g} \in \overline{G}$. □

3.4 Characterization of regular Beauville groups without induced Beauville structures

Recall that, by Lemma 2.3.4, if G is a finite group and G/N has a Beauville structure with one of the generating sets satisfying $o(x) = o(xN)$, $o(y) = o(yN)$ and $o(xy) = o(xyN)$, then we can lift this Beauville structure in G/N to a Beauville structure of G. In this section, our aim is to characterize regular Beauville p-groups in which no Beauville structure of G can be obtained by using the property above.

First of all, we see that in such a group we have $|G^{p^{e-1}}| = p^2$. If we take a normal subgroup $N \leq G^{p^{e-1}}$ of order p, then $\exp G/N = p^e$. Also, since a quotient of a regular p-group is also regular, G/N is regular. If $|G^{p^{e-1}}| > p^2$ then we have $|(G/N)^{p^{e-1}}| = |G^{p^{e-1}}/N| \geq p^2$, and consequently G/N has a Beauville structure, by Theorem 3.2.2. Let $\{\overline{x_1}, \overline{y_1}\}$ and $\{\overline{x_2}, \overline{y_2}\}$ form a Beauville structure for G/N. Since $N \leq G^{p^{e-1}} \leq \Phi(G)$, this implies that $G = \langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle$. Notice that any element outside the Frattini subgroup has order p^e in both G and G/N. It then follows from Lemma 2.3.4 that $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G.

Thus the condition $|G^{p^{e-1}}| = p^2$ is necessary to guarantee that G has no Beauville structure with a triple such that $o(x) = o(xN)$, $o(y) = o(yN)$ and $o(xy) = o(xyN)$, but it is not a sufficient condition. We have the following example.

Example 3.4.1. Let G be a p-group splitting over A, i.e. $G = \langle b\rangle \ltimes A$, where $A = \langle a_1\rangle \times \langle a_2\rangle \cong C_{p^2} \times C_p$ and the action of $\langle b\rangle \cong C_{p^2}$ on A is given by $a_1^b = a_1a_2$ and $a_2^b = a_2$. Then $G = \langle a_1, b\rangle$ is of exponent p^2. Since $G' = \langle [a_1, b]^g \mid g \in G\rangle$ and $[a_1, b] = a_2 \in Z(G)$, this implies that G has class $2 < p$, and hence G is regular, by Theorem 3.1.2. Observe that since G is of class 2, for any two elements $x, y \in G$ we have $(xy)^p = x^py^p[y, x]^{\binom{p}{2}}$ by Lemma 2.2.21. In our case, since $\exp G' = p$, we have $(xy)^p = x^py^p$, and it follows that $G^p = \langle a_1^p, b^p\rangle$. Note that a_1^p and b^p commute, and consequently $|G^p| = p^2$. If $p \geq 5$ then by Proposition 3.2.4, G has a Beauville structure .

We now consider the quotient $G/\langle a_2\rangle$ which is of exponent p^2. Since $G/\langle a_2\rangle$ is abelian and $|(G/\langle a_2\rangle)^p| = p^2$, $G/\langle a_2\rangle$ is a Beauville group with a Beauville structure $\{\overline{a_1}, \overline{b}\}$ and $\{\overline{a_1^2b}, \overline{a_1^4b}\}$ if $p \geq 5$. Notice that any element outside the Frattini subgroup has order p^2 in both G and $G/\langle a_2\rangle$. Then by Lemma 2.3.4, the Beauville structure of $G/\langle a_2\rangle$ with $\{\overline{a_1}, \overline{b}\}$ as one of the generating sets can be lifted to a Beauville structure for G.

Theorem 3.4.2. *Let G be a regular Beauville p-group of exponent p^e. Then G has no Beauville structure obtained from a Beauville structure of a proper quotient G/N with one of the generating set satisfying $o(x) = o(xN)$, $o(y) = o(yN)$ and $o(xy) = o(xyN)$ if and only if $|G^{p^{e-1}}| = p^2$ and $\Omega_1(Z(G)) \leq G^{p^{e-1}}$.*

Proof. We already showed that in such a group we have $|G^{p^{e-1}}| = p^2$. We next show that the condition $\Omega_1(Z(G)) \leq G^{p^{e-1}}$ is also necessary. Otherwise, there exists $g \in \Omega_1(Z(G)) \smallsetminus G^{p^{e-1}}$. We now consider the normal subgroup $N = \langle g\rangle$ of order p. Since G/N is a regular p-group of exponent p^e and $|(G/N)^{p^{e-1}}| = p^2$, this implies that G/N is a Beauville group. Let $\{\overline{x_1}, \overline{y_1}\}$ and $\{\overline{x_2}, \overline{y_2}\}$ form a Beauville structure for G/N where $G = \langle x_1, y_1\rangle = \langle x_2, y_2\rangle$. Then by Lemma 2.3.4, this Beauville structure of G/N can be lifted to a Beauville structure for G, which is a contradiction. Thus we complete the proof of one of the implications in the statement of the theorem.

To prove the converse, we assume that $|G^{p^{e-1}}| = p^2$ and $\Omega_1(Z(G)) \leq G^{p^{e-1}}$. Suppose, on the contrary, that G has a Beauville structure which is obtained from a

Beauville structure of G/N with one of the generating sets satisfying $o(x) = o(xN)$, $o(y) = o(yN)$ and $o(xy) = o(xyN)$. It follows that the exponent of both G and G/N is p^e. Since G/N is a Beauville group, we have $|(G/N)^{p^{e-1}}| \geq p^2$, where

$$|(G/N)^{p^{e-1}}| = |G^{p^{e-1}}N/N| = \frac{|G^{p^{e-1}}|}{|G^{p^{e-1}} \cap N|} = \frac{p^2}{|G^{p^{e-1}} \cap N|}.$$

Thus we have $G^{p^{e-1}} \cap N = 1$, and this, together with $\Omega_1(Z(G)) \leq G^{p^{e-1}}$, yields that $\Omega_1(Z(G)) \cap N = 1$. Since N is a normal subgroup, there exists an element of order p inside $Z(G) \cap N$, and hence $\Omega_1(Z(G)) \cap N \neq 1$, which is a contradiction. □

CHAPTER 4

THIN p-GROUPS

This chapter is devoted to Beauville structures in thin p-groups. More precisely, we first focus on p-groups of maximal class in Section 4.2. We restrict ourselves to p-groups of maximal class that either are metabelian, or have a maximal subgroup of class ≤ 2. We next turn our attention to metabelian thin p-groups of class at least p in Section 4.3.

4.1 Preliminaries

In this section, we present some preliminaries for p-groups of maximal class and thin p-groups. The results can be found with detailed proofs in the given references. No originality is claimed in this section.

Definition 4.1.1. *Let G be a p-group of order $p^n \geq p^2$. Then G is said to be a **p-group of maximal class** if it has nilpotency class $n-1$.*

Theorem 4.1.2. [20, Theorem 3.5] *Let G be a p-group of maximal class of order p^n. Then*

(i) *We have $|G : G'| = p^2$ and $|\gamma_i(G) : \gamma_{i+1}(G)| = p$ for $2 \leq i \leq n-1$. Hence $|G : \gamma_i(G)| = p^i$ for $2 \leq i \leq n$.*

(ii) *Unless G is cyclic of order p^2, we have $\Phi(G) = G'$ and $d(G) = 2$.*

(iii) *The only normal subgroups of G are the $\gamma_i(G)$ and the maximal subgroups of G.*

(iv) *If $N \trianglelefteq G$ and $|G : N| \geq p^2$, then G/N is also a group of maximal class.*

(v) $Z_i(G) = \gamma_{n-i}(G)$ *for* $0 \leq i \leq n-1$.

Theorem 4.1.3. [30, Theorem III.11.9] *Let G be a non-abelian 2-group. Then the following are equivalent:*

(i) *G has maximal class.*

(ii) $|G/G'| = 4$.

(iii) *G is a dihedral group or semidihedral group or generalized quaternion group.*

Theorem 4.1.4. [30, Theorem III.14.23] *Let G be a p-group with $|G| = p^n \geq p^2$. Then G has maximal class if and only if there exists an element $x \in G$ such that*

$$|\{x^g \mid g \in G\}| = |G : C_G(x)| = p^{n-2}.$$

Since p-groups of order $\leq p^3$ are well-known, there is no loss of generality if we only deal with p-groups of maximal class of order $\geq p^4$.

Definition 4.1.5. *Let G be a p-group of maximal class of order $\geq p^4$. We define the characteristic subgroup G_1 of G by*

$$G_1 = C_G(G'/\gamma_4(G)).$$

In other words, G_1 is composed of the elements $x \in G$ such that $[x, G'] \leq G_4$.

Notation: For $2 \leq i \leq n$ we will write $G_i = \gamma_i(G)$.

Theorem 4.1.6. [30, Lemma III.14.4] *Let G be a p-group of maximal class. Then G_1 is a maximal subgroup of G.*

Definition 4.1.7. *Let G be a p-group of maximal class of order p^n. Then we define the* ***two-step centralizers*** $C_G(G_i/G_{i+2})$ *for* $1 \leq i \leq n-2$.

As happened with G_1, all two-step centralizers are characteristic and maximal in G. Since G_1/G_2 is cyclic, Lemma 2.2.5 implies that $[G_1, G_1] = [G_1, G_2] \leq G_4$. Therefore, we have that $C_G(G_1/G_3) = G_1$, and thus it is enough to consider the two-step centralizers for $2 \leq i \leq n-2$.

Theorem 4.1.8. [30, Theorem III.14.6] *Let G be a p-group of maximal class of order $p^n \geq p^5$. Then $G_1 = C_G(G_i/G_{i+2})$ for $2 \leq i \leq n-3$.*

Thus from the above theorem, there are at most two different two-step centralizers, namely G_1 and $C_G(G_{n-2})$.

Definition 4.1.9. *Let G be a p-group of maximal class of order p^n. Then G is said to be* ***exceptional*** *if $G_1 \neq C_G(G_{n-2})$.*

Theorem 4.1.10. [30, Theorem III.14.6] *If a p-group G of maximal class of order p^n is exceptional, then $p \geq 5$, n is even and $6 \leq n \leq p+1$.*

Thus if $|G| = p^n \geq p^{p+2}$ then G is not exceptional and hence $G_1 = C_G(G_{n-2})$.

Definition 4.1.11. *Let G be a p-group of maximal class of order p^n. An element $s \in G$ is called* ***uniform*** *if $s \notin G_1 \cup C_G(G_{n-2})$.*

Notice that all p-groups of maximal class have uniform elements, since a group cannot be the union of two proper subgroups.

Theorem 4.1.12. [30, Theorem III.14.13] *Let G be a p-group of maximal class and let s be a uniform element of G. Then the following properties hold:*

(i) $C_G(s) = \langle s \rangle Z(G)$.

(ii) $s^p \in Z(G)$ *and consequently* $o(s) \leq p^2$.

(iii) $|C_G(s)| = p^2$ *and the conjugates of s are exactly the elements in the coset sG'.*

Lemma 4.1.13. [20, Lemma 3.14] *Let G be p-group of maximal class of order p^n, and let s be a uniform element. If $1 \leq i \leq n-2$ and $x \in G_i \setminus G_{i+1}$, then $[s,x] \in G_{i+1} \setminus G_{i+2}$.*

Let G be a p-group of maximal class, and let s be a uniform element and $s_1 \in G_1 \setminus G_2$. We can define recursively $s_i = [s_{i-1}, s]$ for $i \geq 2$. It then follows from the above lemma that $s_i \in G_i \setminus G_{i+1}$, and hence $G_i = \langle s_i, G_{i+1} \rangle$ for all $1 \leq i \leq n-1$.

We next give the results regarding the power structure of a p-group of maximal class.

Theorem 4.1.14. [30, Theorem III.14.14] *Let G be a p-group of maximal class of order $p^n \leq p^{p+1}$. Then $\exp G/Z(G) = \exp G' = p$.*

Theorem 4.1.15. [20, Theorem 4.9] *Let G be a p-group of maximal class of order $p^n \geq p^{p+2}$. If $1 \leq i \leq n - p$ and $x \in G_i \smallsetminus G_{i+1}$, then $x^p \in G_{i+p-1} \smallsetminus G_{i+p}$.*

We now state the basic properties of thin p-groups which will be used in the proofs of the main results in Section 4.3.

Definition 4.1.16. *A non-cyclic p-group is said to be **thin** if every anti-chain in the lattice of its normal subgroups contains at most $p + 1$ elements. An **anti-chain** is a subset of the lattice such that any two elements in the subset are incomparable.*

An alternative definition of a thin p-group is as follows.

Definition 4.1.17. *A p-group G is **thin** if the following two conditions holds:*

(i) *For every normal subgroup N of G, we have $\gamma_{i+1}(G) \leq N \leq \gamma_i(G)$ for some i.*

(ii) *$|\gamma_i(G) : \gamma_{i+1}(G)| \leq p^2$ for all i.*

Clearly, if the two conditions in Definition 4.1.17 hold, then Definition 4.1.16 follows. Conversely, note that the only abelian thin p-groups are cyclic or elementary abelian of order p^2. Thus if G is not cyclic, then G/G' must be elementary abelian of order p^2 and of exponent p, and then the remaining factors of the lower central series are of order p or p^2. Hence the conditions (ii) holds. By the result in [12, page 281], every normal subgroup of a thin p-group is between two consecutive terms of the lower central series, and thus the condition (i) holds.

The lattice of normal subgroups of the non-cyclic abelian thin group is referred to as a **diamond**. Note that if G is a non-cyclic thin group, then G/G' is elementary abelian of order p^2, and this implies that G is 2-generator.

It is clear from Theorem 4.1.2 that p-groups of maximal class are thin. In the sequel, we will exclude p-groups of maximal class from our consideration of thin groups. Thus we assume $p > 2$, since $|G : G'| = 4$ implies that G is of maximal class by Theorem 4.1.3.

Lemma 4.1.18. [10, Lemma 2.1] *Let G be a thin p-group and $g \in \gamma_i(G) \smallsetminus \gamma_{i+1}(G)$. Then $\gamma_{i+1}(G) = [g, G]\gamma_{i+2}(G)$.*

Lemma 4.1.19. [10, Corollary 2.2] *The lower and upper central series of a thin p-group coincide.*

Lemma 4.1.20. [10, Lemma 1.3] *Let G be a finite p-group, p an odd prime. Then*

(i) *If G is a metabelian thin group, then $\gamma_3(G)/\gamma_4(G)$ is non-cyclic.*

(ii) *If G is thin, then $|G| \geq p^5$, $\mathrm{cl}(G) > 2$, and $G/\gamma_3(G)$ is of exponent p.*

Theorem 4.1.21. [10, Theorem A, Theorem 3.4] *Let G be a metabelian thin p-group. Then*

(i) *$\gamma_{p+1}(G)$ is cyclic and $\gamma_{p+2}(G) = 1$, and hence $\mathrm{cl}(G) \leq p + 1$.*

(ii) *The lattice of normal subgroups of G consists of a diamond on top, followed by a chain of length 1, at most $p - 2$ diamonds, plus possibly another chain of length 1. Hence $|G| \leq p^{2p}$.*

(iii) $\exp(G) \leq p^2$.

We next recall a commutator relation between the generators of G.

Theorem 4.1.22. [10, Theorem B] *Let G be a metabelian thin p-group. Then for every $x \in G \smallsetminus G'$ there corresponds an element y such that $G = \langle x, y \rangle$ and*

$$[y, x, x, x] \equiv [y, x, y, y]^h \pmod{\gamma_5(G)}. \tag{4.1}$$

where h is a quadratic non-residue modulo p.

The following two lemmas are more general results on p-groups.

Lemma 4.1.23. [42, Theorem 3] ***(Meier-Wunderli)*** *If G is a metabelian 2-generator p-group, then $G^p \geq \gamma_p(G)$.*

Lemma 4.1.24. [10, Lemma 1.2] *Let G be a p-group. If $G/\gamma_{i+1}(G)$ has exponent p, for $1 \leq i \leq p - 1$, then $\gamma_j(G)/\gamma_{j+i}(G)$ has exponent p.*

We now recall the power structure of a metabelian thin p-group.

Lemma 4.1.25. [10, Lemma 3.3] *Let G be a metabelian thin p-group, and let $g \in G \setminus \gamma_2(G)$. Assume that $g^p \in \gamma_i(G) \setminus \gamma_{i+1}(G)$. Then $\gamma_{i+1}(G)$ is cyclic, and $\mathrm{cl}(G) \leq i + 1$.*

Lemma 4.1.26. *Let G be a metabelian thin p-group, and l be the largest integer such that $G^p \leq \gamma_l(G)$. Then $3 \leq l \leq p$, $\gamma_{l+1}(G)$ is cyclic, $\gamma_{l+2}(G) = 1$ and $\gamma_2(G)^p \leq \gamma_{l+1}(G)$.*

Proof. By Lemma 4.1.20, $l \geq 3$. Moreover, if $G^p \leq \gamma_p(G)$, then by Lemma 4.1.23, we have $G^p = \gamma_p(G)$, and hence $l \leq p$. We now apply Lemma 4.1.24 to get $\gamma_2(G)^p \leq \gamma_{l+1}(G)$. Then there is an element $g \in G \setminus \gamma_2(G)$ with $g^p \in \gamma_l(G) \setminus \gamma_{l+1}(G)$, and by Lemma 4.1.25, $\gamma_{l+1}(G)$ is cyclic, and this implies that $\gamma_{l+2}(G) = 1$. □

The following corollary follows directly from Lemma 4.1.26.

Corollary 4.1.27. *Let G be a metabelian thin p-group. Then $|G^p| \leq p^3$.*

Lemma 4.1.28. *Let G be a metabelian thin p-group such that its lattice of normal subgroups ends with a chain. Then the order of G^p cannot be p^2.*

Proof. If G is of class $p + 1$, then $G^p = \gamma_p(G)$, and hence $|G^p| = p^3$. Thus we assume that $\mathrm{cl}(G) = c \leq p$. We claim that if M is a maximal subgroup of G, then it is regular. Since $|M : G'| = p$, we have $M' = [M, G'] \leq \gamma_3(G)$, and this implies that $\gamma_c(M) \leq \gamma_{c+1}(G) = 1$. Thus $\mathrm{cl}(M) < c \leq p$, and so M is regular.

Suppose, on the contrary, that $|G^p| = p^2$. Now consider the quotient group $\overline{G} = G/\gamma_c(G)$, which is regular. Then $|\overline{G}^p| = p$, and hence $|\overline{G} : \Omega_1(\overline{G})| = p$. Write $\Omega_1(\overline{G}) = M/\gamma_c(G)$ for some maximal subgroup M of G. Since $\overline{G}$ is regular, $\exp\ \Omega_1(\overline{G}) = p$. This implies that $M^p \leq \gamma_c(G)$, and so $|M^p| \leq p$. Then $|M : \Omega_1(M)| \leq p$ as M is regular. Since $\Omega_1(M) \trianglelefteq G$ and $|G : \Omega_1(M)| \leq p^2$, we get $G' \leq \Omega_1(M)$, where $\exp\ \Omega_1(M) = p$. Thus $\exp\ G' = p$.

On the other hand, if M is an arbitrary maximal subgroup of G, we have $G' \leq M$ and since $\exp G' = p$, we get $G' \leq \Omega_1(M) \leq M$. Then $|M^p| = |M : \Omega_1(M)| \leq p$. Since G is thin, this implies that $M^p \leq \gamma_c(G)$ for any maximal subgroup M. But $G^p = \langle M^p \mid M \text{ maximal in } G\rangle \leq \gamma_c(G)$, and hence $|G^p| \leq p$, which is a contradiction. □

4.2 p-Groups of maximal class

In this section, our aim is to determine Beauville structures in p-groups of maximal class which either are metabelian or satisfy $\operatorname{cl}(G_1) \leq 2$.

We begin with a lemma concerning p-groups of maximal class of order $\leq p^p$.

Lemma 4.2.1. *Let G be a p-group of maximal class of order at most p^p. Then G is a Beauville group if and only if $p \geq 5$ and $\exp G = p$.*

Proof. By Theorem 4.1.14, we have $\exp G/Z(G) = p$. Thus $|G^p| \leq p$ and $\exp G = p$ or p^2. Since $|G| \leq p^p$, it then follows from Theorem 3.1.2 that G is regular. Then Corollary 3.2.3 implies that G is a Beauville group if and only if $p \geq 5$ and $\exp G = p$. □

Theorem 4.2.2. *If $p = 2$ or 3, then no p-group of maximal class is a Beauville group.*

Proof. Let G be a p-group of maximal class for $p = 2$ or 3. Since $p < 5$, G is not exceptional by Theorem 4.1.10. Thus all elements of $G \smallsetminus G_1$ are uniform. By way of contradiction, suppose that $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G. Since G has $p + 1 \leq 4$ maximal subgroups, at least one of the elements in both triples $\{x_1, y_1, x_1y_1\}$ and $\{x_2, y_2, x_2y_2\}$, say x_1 and x_2, fall in the same maximal subgroup different from G_1. Hence $x_2 = x_1^i g$ for some $g \in G'$ and for some integer i not divisible by p. Since x_1^i is uniform, this implies that x_2 and x_1^i are conjugate, by Theorem 4.1.12, and this is a contradiction. □

Theorem 4.2.3. *Let G be a p-group of maximal class, and let M be a maximal subgroup of G. Then all elements in $M \smallsetminus G'$ have the same order.*

Proof. We deal separately with the cases $|G| = p^n \geq p^{p+2}$ and $\leq p^{p+1}$. If $|G| \geq p^{p+2}$ then all elements in $G \smallsetminus G_1$ are uniform elements. Thus if $M \neq G_1$ then all elements in $M \smallsetminus G'$ are conjugate to powers of a fixed element in $M \smallsetminus G'$, and hence they have the same order. If $M = G_1$ then by Theorem 4.1.15, all elements in $G_1 \smallsetminus G'$ have order $p^{\lceil \frac{n-1}{p-1} \rceil}$.

Thus we assume that $|G| \leq p^{p+1}$. Let $x \in M \smallsetminus G'$ and $y \in G'$. Then by the Hall-Petrescu formula, we have

$$(xy)^p = x^p y^p c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} \dots c_p,$$

where $c_i \in \gamma_i(\langle x, y\rangle) \leq \gamma_{i+1}(G)$ for $2 \leq i \leq p$. By Theorem 4.1.14, $\exp G' = p$, and this, together with $\gamma_{p+1}(G) = 1$, implies that $(xy)^p = x^p$. □

In the sequel, we assume that G has order $p^n \geq p^{p+1}$. We choose an element $s_1 \in G_1 \smallsetminus G'$ and a uniform element s. Since $G/G' \cong C_p \times C_p$, each pair of elements in $S = \{s_1, ss_1^i \mid 0 \leq i \leq p-1\}$ are linearly independent modulo G'. Also, note that all elements of $\langle ss_1^i\rangle G' \smallsetminus G'$ have the same order, by Theorem 4.2.3.

In order to determine Beauville structures in G, it is fundamental to control the orders of elements outside G_1. To this purpose, we need to know the order of each ss_1^i for $0 \leq i \leq p-1$. However, it is not always easy to determine these orders in an arbitrary p-group of maximal class. Thus we will restrict our attention to a p-group of maximal class G such that either G' is abelian, that is G is metabelian, or $\mathrm{cl}(G_1) \leq 2$. Note that a large number of p-groups of maximal class have one of these two properties, as follows from the construction procedures describe in [43] for metabelian groups and in [38] for the groups with G_1 of class 2.

Lemma 4.2.4. *Let G be a p-group of maximal class of order $\geq p^{p+1}$. Suppose that G satisfies one of the following:*

(i) *All elements of $G \smallsetminus G_1$ are of order p^2.*

(ii) *There exists $s \in G \smallsetminus G_1$ such that $o(s) = p$ and all elements outside $G_1 \cup \langle s, G'\rangle$ are of order p^2.*

Then G is not a Beauville group.

Proof. Suppose that, on the contrary, $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G. Then without loss of generality, we can assume that x_1 and x_2 are of order p^2. It then follows that $\langle x_1^p\rangle = \langle x_2^p\rangle = Z(G)$, which is a contradiction. □

As a consequence of Lemma 4.2.4, if we want G to be a Beauville group, it is necessary for G to have at least two maximal subgroups other than G_1 such that all elements in those maximal subgroups outside G' have order p.

We proceed to determine pth powers of ss_1^i. We deal separately with two cases: G is metabelian, or $\mathrm{cl}(G_1) \leq 2$. We begin by analyzing metabelian p-groups of maximal class. In this case, we rely on the following result of Miech.

Lemma 4.2.5. [43, Lemma 8] *Let G be a metabelian p-group of maximal class of order $p^n \geq p^{p+1}$, where p is odd, and let s be a uniform element. Suppose that $[G_1, G_2] = G_{n-k}$ and $[s_1, s_2] = s_{n-k}^{a(n-k)} \dots s_{n-1}^{a(n-1)}$. Then for $0 \leq i \leq p-1$*

$$(ss_1^i)^p = s^p \big(s_1^p s_2^{\binom{p}{2}} \dots s_p^{\binom{p}{p}}\big)^i s_{n-1}^{\psi i^2},$$

where

$$\psi = \begin{cases} a(n-k) & \textit{if} \quad k = p-2, \\ 0 & \textit{if} \quad k \leq p-3. \end{cases}$$

Lemma 4.2.6. *Let G be a metabelian p-group of maximal class of order $p^n \geq p^{p+1}$, where p is odd, and let s be a uniform element and s_1 be an element in $G_1 \smallsetminus G'$. Suppose that $o(s) = o(ss_1) = p$ and $(ss_1^2)^p = s_{n-1}^{\lambda}$. Then for $1 \leq i \leq p-1$*

$$(ss_1^i)^p = s_{n-1}^{\lambda\binom{i}{2}}.$$

Proof. For the proof, we use Lemma 4.2.5. If we call $a = s_1^p s_2^{\binom{p}{2}} \dots s_p^{\binom{p}{p}}$ and $b = s_{n-1}^{\psi}$, then

$$(ss_1^i)^p = a^i b^{i^2} \quad \text{for} \quad 1 \leq i \leq p-1.$$

Since $a, b \in Z(G)$, we have $(ss_1^2)^p = (ab)^2 b^2 = (ss_1)^{2p} b^2 = b^2$. Note that $(ss_1)^p = 1$ implies $a = b^{-1}$, and thus $(ss_1^i)^p = b^{i^2-i} = (b^2)^{\binom{i}{2}} = s_{n-1}^{\lambda\binom{i}{2}}$. □

We next deal with the case $\mathrm{cl}(G_1) \leq 2$. For this purpose we need another result of Miech.

Theorem 4.2.7. [44, Theorem 4] *Let G be a group generated by x and y, $G_2 = G'$, and $G_1 = \langle y, G_2 \rangle$. Let $\sigma_0 = y$ and $\sigma_{i+1} = [\sigma_i, x]$ for $i \geq 0$. Then for any nonnegative integer n*

$$(xy)^n \equiv x^p y^p \sigma_1^{\binom{n}{2}} \dots \sigma_{n-1}^{\binom{n}{n}} Q_n \pmod{\gamma_3(G_1)},$$

where

$$Q_n = \prod_{k=1}^{n-1}\prod_{l=0}^{k-1}[\sigma_k, \sigma_k]^{B(n,k,l)}, \tag{4.2}$$

for a nonnegative integer $B(n,k,l)$ depending on n, k and l.

Lemma 4.2.8. *Let G be a p-group of maximal class such that $\mathrm{cl}(G_1) \leq 2$, where p is odd, and let s be a uniform element. Suppose that $o(s) = o(ss_1) = p$ and $(ss_1^2)^p = s_{n-1}^{\lambda}$. Then for $1 \leq i \leq p-1$*

$$(ss_1^i)^p = s_{n-1}^{\lambda\binom{i}{2}}.$$

Proof. To prove the lemma, we will apply Theorem 4.2.7. We set $\sigma_{i,0} = s_1^i$ and $\sigma_{i,k} = [s_1^i, s, \overset{k}{\ldots}, s]$ for $k \geq 1$. Set $Q_{i,p} = \prod_{k=1}^{p-1}\prod_{l=0}^{k-1}[\sigma_{i,k}, \sigma_{i,l}]^{B(p,k,l)}$.

First of all, by using induction on k, we will show that $\sigma_{i,k} = s_{k+1}^i t_k^{\binom{i}{2}}$ for some $t_k \in [G_1, G_1]$. Now $\sigma_{i,1} = [s_1^i, s] = s_1^{-i}(s_i^s)^i = s_1^{-i}(s_1s_2)^i$, and since $\mathrm{cl}(G_1) \leq 2$ we have $(s_1s_2)^i = s_1^i s_2^i [s_2, s_1]^{\binom{i}{2}}$, thus $\sigma_{i,1} = s_2^i[s_2, s_1]^{\binom{i}{2}}$. We assume that for $k \geq 2$, $\sigma_{i,k-1} = s_k^i t_{k-1}^{\binom{i}{2}}$. Then we have $\sigma_{i,k} = [s_k^i, s][t_{k-1}^{\binom{i}{2}}, s]$. Notice that for any $x \in [G_1, G_1] \leq Z(G_1)$, $[x^n, s] = [x, s]^n$ for $n \in \mathbb{Z}$. It then follows that $\sigma_{i,k} = [s_k^i, s][t_{k-1}, s]^{\binom{i}{2}}$. Now $[s_k^i, s] = s_k^{-i}(s_k^s)^i = s_k^{-i}(s_ks_{k+1})^i$. Again since $\mathrm{cl}(G_1) \leq 2$, this implies that $(s_ks_{k+1})^i = s_k^i s_{k+1}^i [s_{k+1}, s_k]^{\binom{i}{2}}$, and thus $\sigma_{i,k} = s_{k+1}^i([s_{k+1}, s_k][t_{k-1}, s])^{\binom{i}{2}}$. We call $t_k = [s_{k+1}, s_k][t_{k-1}, s] \in [G_1, G_1]$, and the induction is complete.

Since $t_k \in Z(G_1)$, by Theorem 4.2.7, we get

$$(ss_1^i)^p = s_1^{ip} s_2^{i\binom{p}{2}} \ldots s_p^i \big(t_1^{\binom{p}{2}} t_2^{\binom{p}{3}} \ldots t_{p-1}^{\binom{p}{p}}\big)^{\binom{i}{2}} Q_{i,p}.$$

Also, note that since $\mathrm{cl}(G_1) \leq 2$, for any $x, y \in G_1$ and $m, n \in \mathbb{Z}$ we have $[x^m, y^n] = [x, y]^{mn}$, and this, together with $x^i y^i = (xy)^i [x, y]^{\binom{i}{2}}$ yields that

$$(ss_1^i)^p = \big(s_1^p s_2^{\binom{p}{2}} \ldots s_p\big)^i \Big(\prod_{j=1}^{p-1}\prod_{k=j+1}^{p}[s_j, s_k]^{\binom{p}{j}\binom{p}{k}} \big(t_1^{\binom{p}{2}} t_2^{\binom{p}{3}} \ldots t_{p-1}^{\binom{p}{p}}\big)\Big)^{\binom{i}{2}} Q_{i,p}.$$

On the other hand, $[\sigma_{i,k}, \sigma_{i,l}] = [s_{k+1}^i t_k^{\binom{i}{2}}, s_{l+1}^i t_l^{\binom{i}{2}}] = [s_{k+1}^i, s_{l+1}^i] = [s_{k+1}, s_{l+1}]^{i^2}$, and this implies that $Q_{i,p} = Q_{1,p}^{i^2}$, by (4.2). If we call $\mu = \frac{-|G|+1}{2}$ and

$$A = \prod_{j=1}^{p-1}\prod_{k=j+1}^{p}[s_j, s_k]^{\binom{p}{j}\binom{p}{k}} \big(t_1^{\binom{p}{2}} t_2^{\binom{p}{3}} \ldots t_{p-1}^{\binom{p}{p}}\big),$$

then

$$\begin{aligned}(ss_1^i)^p &= \left(s_1^p s_2^{\binom{p}{2}} \dots s_p\right)^i A^{\mu(i^2-i)} Q_{1,p}^{i^2}\\ &= \left(s_1^p s_2^{\binom{p}{2}} \dots s_p A^{-\mu}\right)^i \left(A^{\mu} Q_{1,p}\right)^{i^2},\end{aligned}$$

where the last equality follows from the fact that $A \in [G_1, G_1] \leq Z(G_1)$.

For simplicity, let us call $a = s_1^p s_2^{\binom{p}{2}} \dots s_p A^{-\mu}$ and $b = A^{\mu} Q_{1,p}$. Then $(ss_1^i)^p = a^i b^{i^2}$ for $1 \leq i \leq p-1$. Since $b \in [G_1, G_1]$, a and b commute, and thus we have $(ss_1^2)^p = (ab)^2 b^2 = (ss_1)^{2p} b^2 = b^2$. Consequently, by using the same argument as in the proof of Lemma 4.2.6, we get

$$(ss_1^i)^p = s_{n-1}^{\lambda\binom{i}{2}} \quad \text{for} \quad 1 \leq i \leq p-1,$$

as desired. □

We are now ready to state the main results of this section.

Theorem 4.2.9. *Let G be a p-group of maximal class of order $p^n \geq p^{p+1}$, where p is odd, such that either G is metabelian or $\mathrm{cl}(G_1) \leq 2$. Suppose that G is not as in Lemma 4.2.4. Then one of the following holds:*

(i) *All elements of $G \setminus G_1$ are of order p.*

(ii) *There exist a uniform element s and $s_1 \in G_1 \setminus G'$ such that $o(s) = o(ss_1) = p$ and all elements outside $G_1 \cup \langle s, G' \rangle \cup \langle ss_1, G' \rangle$ are of order p^2.*

Proof. Since G does not satisfy the conditions in Lemma 4.2.4, there exist a uniform element s and an element $s_1 \in G_1 \setminus G_2$ such that $o(s) = o(ss_1) = p$. Then by Lemma 4.2.6 and Lemma 4.2.8, we have

$$(ss_1^i)^p = s_{n-1}^{\lambda\binom{i}{2}} \quad \text{for} \quad 1 \leq i \leq p-1,$$

where $(ss_1^2)^p = s_{n-1}^{\lambda}$.

Observe that $o(ss_1^i) = p$ if and only if

$$\lambda(i-1) \equiv 0 \pmod{p}. \tag{4.3}$$

If $\lambda \equiv 0 \pmod{p}$ then (4.3) holds for all i, that is $o(ss_1^i) = p$ for $1 \leq i \leq p-1$, and hence we get (i). Otherwise, $i = 1$ is the unique solution for (4.3), and thus (ii) holds. This completes the proof. □

We are now ready to determine Beauville structures in G.

Theorem 4.2.10. *Let G be as in Theorem 4.2.9. Then G is a Beauville group if and only if $p \geq 5$ and one of the following two cases holds:*

1. *(i) holds.*
2. *(ii) holds, and either $n \neq k(p-1)+2$ with $k \geq 1$, or $n = p+1$ and $\exp G_1 = p$.*

Proof. By Theorem 4.2.2, G can only be a Beauville group if $p \geq 5$. Let us first show that if $p \geq 5$ and (i) holds, then G is a Beauville group. Since $p \geq 5$, $G/\Phi(G) \cong C_p \times C_p$ is a Beauville group. We will see that every Beauville structure of $G/\Phi(G)$ lifts to a Beauville structure of G. To this purpose, it suffices to show that, given $x, y \in G \setminus \Phi(G)$, the condition $\langle \overline{x} \rangle \cap \langle \overline{y} \rangle = \overline{1}$ implies that $\langle x \rangle \cap \langle y \rangle = 1$, where we use the bar notation in $G/\Phi(G)$. Observe that since $\langle \overline{x} \rangle \cap \langle \overline{y} \rangle = \overline{1}$, at least one of x and y, say x, is of order p. Thus if $\langle x \rangle \cap \langle y \rangle \neq 1$ then $\langle x \rangle \subseteq \langle y \rangle$ and this implies that $\langle \overline{x} \rangle = \langle \overline{y} \rangle$, which is a contradiction.

We next show that if $p \geq 5$, (ii) holds and $|G| = p^n \geq p^{p+2}$ with $n \neq k(p-1)+2$ for $k \geq 1$, then G is a Beauville group. We claim that $\{s, s_1\}$ and $\{ss_1^2, ss_1^4\}$ form a Beauville structure for G.

Let $X = \{s, s_1, ss_1\}$ and $Y = \{ss_1^2, ss_1^4, ss_1^2ss_1^4\}$, where each $y \in Y$ is of order p^2. We need to show that
$$\langle x^g \rangle \cap \langle y^h \rangle = 1, \tag{4.4}$$
for all $x \in X$, $y \in Y$ and $g, h \in G$. Observe that x^g and y^h lie in different maximal subgroups of G in every case, since s and s_1 are linearly independent modulo $\Phi(G)$ and $p \geq 5$. Assume first that $x = s$ or ss_1, which are of order p. If (4.4) does not hold, then $\langle x^g \rangle \subseteq \langle y^h \rangle$, and consequently $\langle x\Phi(G) \rangle = \langle y\Phi(G) \rangle$, which is a contradiction. Thus we assume that $x = s_1$. By Theorem 4.1.15, we have $o(s_1) = p^e$ for some $e \geq 2$. If (4.4) does not hold, then $\langle (x^{p^{e-1}})^g \rangle = \langle (y^p)^h \rangle$, and consequently $\langle x^{p^{e-1}} \rangle = G_{n-1}$,

which is a contradiction. Indeed, since $n \neq k(p-1)+2$, $x^{p^{e-1}}$ can not lie in G_{n-1}, by Theorem 4.1.15.

Now we assume that (ii) holds, $|G| = p^{p+1}$ and $\exp G_1 = p$. We claim that $\{s, s_1\}$ and $\{ss_1^2, ss_1^4\}$ form a Beauville structure for G. If $X = \{s, s_1, ss_1\}$ and $Y = \{ss_1^2, ss_1^4, ss_1^2ss_1^4\}$ then all elements in X are of order p. Then clearly for all $x \in X$, $y \in Y$, and $g, h \in G$ we have $\langle x^g \rangle \cap \langle y^h \rangle = 1$. Otherwise, $\langle x\Phi(G) \rangle = \langle y\Phi(G) \rangle$, which is a contradiction.

Thus we complete the proof of one implication of the theorem. For the converse, let us first see that if (ii) holds and $n = k(p-1)+2$ for some $k \geq 2$, then G cannot be a Beauville group. Suppose that, on the contrary, $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G. Let $A = \{x_1, y_1, x_1y_1\}$ and $B = \{x_2, y_2, x_2y_2\}$. If there exist $a \in A$ and $b \in B$ which are uniform elements of order p^2, then $\langle a^p \rangle = \langle b^p \rangle = Z(G)$. Thus we may assume that $x_1 \in G_1$ and y_1 and x_1y_1 are uniform elements of order p. It then follows from Theorem 4.1.15 that $x_1^{p^k} \in G_{k(p-1)+1} \smallsetminus G_{k(p-1)+2}$, i.e. $1 \neq x_1^{p^k} \in Z(G)$. On the other hand, since the conjugates of any uniform element s are exactly the elements in the coset sG', there cannot be a uniform element of order p in B. Thus there exists $b \in B$ which is uniform of order p^2, and hence $\langle b^p \rangle = \langle x_1^{p^k} \rangle = Z(G)$, which is a contradiction.

Finally, we need to show that if (ii) holds, $|G| = p^{p+1}$ and $\exp G_1 = p^2$, then G has no Beauville structure. The proof is quite similar to the proof of Lemma 4.2.4, thus we skip the proof. □

4.3 Metabelian thin p-groups

In this section, we study Beauville structures in metabelian thin p-groups. By Theorem 4.1.21, we know that metabelian thin p-groups have class at most $p+1$. If the class is less than p, then by Theorem 3.1.2, the group is regular, and hence Theorem 3.2.2 can be used to determine Beauville structures. Thus we focus on metabelian thin p-groups of class p or $p+1$.

We start with determining which metabelian thin 3-groups are Beauville groups.

Remark 4.3.1. Recall that the computer algebra system GAP has a library called `SmallGroup`. This library gives access to all groups of certain "small" orders. The groups are sorted by their orders and they are listed up to isomorphism.

Theorem 4.3.2. *Let G be a metabelian thin 3-group. Then G is a Beauville group if and only if it is isomorphic to one of* `SmallGroup`$(3^5, 3)$*,* `SmallGroup`$(3^6, 34)$*, or* `SmallGroup`$(3^6, 37)$*.*

Proof. Since $|G| \leq 3^6$ by Theorem 4.1.21 and the smallest Beauville 3-group is of order 3^5, the order of G can only be 3^5 or 3^6. Let us first assume that $|G| = 3^5$. We know that the only Beauville 3-group of order 3^5 is $S =$ `SmallGroup`$(3^5, 3)$, and hence G is a Beauville group if and only if $G \cong S$. We will see in Theorem 5.2.8 that S is isomorphic to the quotient group $\mathcal{N}/\mathcal{N}_6$ of the Nottingham group over $\mathbb{F}_3$ and this quotient group is a metabelian thin p-group.

We next assume that $|G| = 3^6$. It has been shown in [2] that there are only three Beauville 3-groups of order 3^6, namely $S =$ `SmallGroup`$(3^6, n)$ for $n = 34, 37, 40$. However, if $n = 40$ then $|Z(S)| = 9$ and $|\gamma_4(S)| = 3$. This implies that $Z(S) \neq \gamma_4(S)$, and thus S is not thin. On the other hand, if $n = 34$ or 37 then by using the computer algebra system GAP, we can see that every normal subgroup of S lies between two consecutive terms of the lower central series of S and $|\gamma_i(S) : \gamma_{i+1}(S)| \leq 3^2$ for all $1 \leq i \leq 4$, and S' is abelian. Thus S is a metabelian thin 3-group. Consequently, G is a Beauville group if and only if $G \cong S$ for $n = 34$ or 37. □

Thus we assume that $p \geq 5$. Let G be a metabelian thin p-group with $\mathrm{cl}(G) = p$ or $p + 1$. Then we have three cases:

(i) $\mathrm{cl}(G) = p + 1$.

(ii) $\mathrm{cl}(G) = p$ and $|\gamma_p(G)| = p^2$.

(iii) $\mathrm{cl}(G) = p$ and $|\gamma_p(G)| = p$.

In the first two cases, we have $G^p \leq \gamma_p(G)$, by Lemma 4.1.26. It then follows from Lemma 4.1.23 that $G^p = \gamma_p(G)$. Also we have $\gamma_2(G)^p \leq \gamma_{p+1}(G)$. On the other hand, in the last case if l is the largest integer satisfying $G^p \leq \gamma_l(G)$, then $l = p-1$ or p and hence $\gamma_p(G) \leq G^p \leq \gamma_{p-1}(G)$.

Our first step is to calculate the pth powers of $x^t y$ modulo $\gamma_{p+1}(G)$ for all $0 \leq t \leq p-1$ if $G = \langle x, y \rangle$ and $\gamma_2(G)^p \leq \gamma_{p+1}(G)$. To this purpose, we need the following lemma.

Lemma 4.3.3. [43, Lemma 6] *Let G be a metabelian p-group and $x, y \in G$. Set $\sigma_1 = y$ and $\sigma_i = [\sigma_{i-1}, x]$ for $i \geq 2$. Then*

$$(xy)^p = x^p y^p \sigma_2^{\binom{p}{2}} \dots \sigma_p^{\binom{p}{p}} z,$$

where

$$z = \prod_{i=1}^{p-1} \prod_{j=1}^{p-1} [\sigma_{i+1}, \sigma_1, \overset{j}{\dots} \sigma_1]^{C(i,j)},$$

and

$$C(i,j) = \sum_{k=1}^{p-1} \binom{k}{i} \binom{k}{j}.$$

Lemma 4.3.4. *Let G be a metabelian thin p-group such that $\gamma_2(G)^p \leq \gamma_{p+1}(G)$. If x and y are the generators of G satisfying (4.1), then for all $0 \leq t \leq p-1$*

$$(x^t y)^p \equiv (x^p)^t y^p [y, x,_{p-2} y]^{\frac{-2t}{1-ht^2}} [y, x,_{p-3} y, x]^{\frac{2t^2}{1-ht^2}} \pmod{\gamma_{p+1}(G)}. \tag{4.5}$$

Proof. By Lemma 4.3.3, we have

$$(x^t y)^p = (x^p)^t y^p [y, x^t]^{\binom{p}{2}} \dots [y,_{p-1} x^t]^{\binom{p}{p}} \prod_{i=1}^{p-1} \prod_{j=1}^{p-1} [y,_i x^t,_j y]^{C(i,j)}.$$

Since $\gamma_2(G)^p \leq \gamma_{p+1}(G)$, it then follows that

$$(x^t y)^p \equiv (x^p)^t y^p [y,_{p-1} x^t] \prod_{\substack{1 \leq i,j \\ i+j \leq p-1}} [y,_i x^t,_j y]^{C(i,j)} \pmod{\gamma_{p+1}(G)}.$$

Note that for $i + j > 0$, $C(i,j)$ is the coefficient of $u^i v^j$ in $\sum_{k=0}^{p-1} (1+u)^k (1+v)^k$, where

$$\begin{aligned} \sum_{k=0}^{p-1} (1+u)^k (1+v)^k = \sum_{k=0}^{p-1} ((1+u)(1+v))^k &= \frac{(1+u+v+uv)^p - 1}{u+v+uv} \\ &\equiv \frac{(1+u+v+uv-1)^p}{u+v+uv} \pmod{p} \\ &\equiv \big((u+v) + uv\big)^{p-1} \pmod{p}. \end{aligned}$$

In the previous expression the monomials of total degree less than p appear only in $(u+v)^{p-1} \equiv \sum_{r=0}^{p-1}(-1)^r u^r v^{p-r-1} \pmod{p}$, and hence

$$C(i,j) \equiv \begin{cases} 0 \pmod{p} & \text{if } i+j < p-1, \\ (-1)^i \pmod{p} & \text{if } i+j = p-1. \end{cases}$$

Thus the condition $\gamma_2(G)^p \leq \gamma_{p+1}(G)$ implies that

$$(x^t y)^p \equiv (x^p)^t y^p \prod_{i=1}^{p-1} [y,_i x^t,_{p-i-1} y]^{(-1)^i} \pmod{\gamma_{p+1}(G)}.$$

On the other hand, notice that for $1 \leq t \leq p-1$

$$[y, x^t, x^t, x^t] \equiv [y, x, x, x]^{t^3} \pmod{\gamma_5(G)},$$

since commutators of length 4 are multilinear modulo $\gamma_5(G)$. Then by (4.1), we have

$$[y, x, x, x]^{t^3} \equiv [y, x, y, y]^{ht^3} \pmod{\gamma_5(G)}.$$

Again by multilinearity of commutators, we get

$$[y, x, y, y]^{ht^3} \equiv [y, x^t, y, y]^{ht^2} \pmod{\gamma_5(G)},$$

and hence

$$[y, x^t, x^t, x^t] \equiv [y, x^t, y, y]^{ht^2} \pmod{\gamma_5(G)}. \tag{4.6}$$

Since G is metabelian, for every $a, b \in G$ and $c \in G'$ we have $[c, a, b] = [c, b, a]$. Thus we have $[y, x^t, x^t, y] = [y, x^t, y, x^t]$. Then this equality, together with (4.6), yields that

$$[y,_i x^t,_{p-i-1} y]^{(-1)^i} \equiv \begin{cases} [y, x^t,_{p-2} y]^{-(ht^2)^{s-1}} \pmod{\gamma_{p+1}(G)} & \text{if } i = 2s-1\ , \\ [y, x^t,_{p-3} y, x^t]^{(ht^2)^{s-1}} \pmod{\gamma_{p+1}(G)} & \text{if } i = 2s\ , \end{cases}$$

and hence

$$(x^t y)^p \equiv (x^p)^t y^p \left([y, x,_{p-2} y]^{-t} [y, x,_{p-3} y, x]^{t^2} \right)^{\sum_{s=1}^{(p-1)/2} (ht^2)^{s-1}} \pmod{\gamma_{p+1}(G)}.$$

Note that since h is a quadratic non-residue, we have $h^{\frac{p-1}{2}} = -1$. Thus

$$\sum_{s=1}^{(p-1)/2} (ht^2)^{s-1} = \frac{1-(ht^2)^{\frac{p-1}{2}}}{1-ht^2} = \frac{2}{1-ht^2}.$$

Consequently, we get

$$(x^t y)^p \equiv (x^p)^t y^p [y, x,_{p-2} y]^{\frac{-2t}{1-ht^2}} [y, x,_{p-3} y, x]^{\frac{2t^2}{1-ht^2}} \pmod{\gamma_{p+1}(G)},$$

for $0 \leq t \leq p-1$, as desired. □

Lemma 4.3.5. *Let G be a metabelian thin p-group such that $|\gamma_p(G)| \geq p^2$ and let x and y be the generators of G satisfying (4.1). Then for every $t_0 \in \{0, 1 \ldots, p-1\}$ there exist at most three distinct $t \in \{0, 1 \ldots, p-1\}$ such that*

$$\langle (x^{t_0} y)^p \rangle \equiv \langle (x^t y)^p \rangle \pmod{\gamma_{p+1}(G)}. \tag{4.7}$$

Proof. Since $|\gamma_p(G)| \geq p^2$, we have $G^p = \gamma_p(G)$, by Lemma 4.1.26, this implies $\gamma_2(G)^p \leq \gamma_{p+1}(G)$. Also $|\gamma_p(G) : \gamma_{p+1}(G)| = p^2$. Notice that, as a consequence of Lemma 4.1.18, $l = [y, x,_{p-2} y]$ and $m = [y, x,_{p-3} y, x]$ are linearly independent modulo $\gamma_{p+1}(G)$, and hence (l, m) is a basis of $\gamma_p(G)$ modulo $\gamma_{p+1}(G)$. If we set $x^p \equiv l^\alpha m^\beta \pmod{\gamma_{p+1}(G)}$ and $y^p \equiv l^\gamma m^\delta \pmod{\gamma_{p+1}(G)}$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{F}_p$, then by (4.5), we have

$$(x^t y)^p \equiv l^{\gamma + \alpha t - \frac{2t}{1-ht^2}} \; m^{\delta + \beta t + \frac{2t^2}{1-ht^2}} \pmod{\gamma_{p+1}(G)}. \tag{4.8}$$

Observe that as rational functions in t, neither $f(t) = \gamma + \alpha t - \frac{2t}{1-ht^2}$ nor $g(t) = \delta + \beta t + \frac{2t^2}{1-ht^2}$ are zero.

We now fix $t_0 \in \{0, 1 \ldots, p-1\}$. Then (4.7) holds if and only if there exists $\lambda \in \mathbb{F}_p^*$ such that

$$f(t) = \lambda f(t_0) \quad \text{and} \quad g(t) = \lambda g(t_0).$$

If $f(t_0) = 0$ or $g(t_0) = 0$, then we have $f(t) = 0$ or $g(t) = 0$, that is $(1 - ht^2)(\gamma + \alpha t) - 2t = 0$ or $(1 - ht^2)(\delta + \beta t) + 2t^2 = 0$. Otherwise, we have $\frac{f(t)}{f(t_0)} = \frac{g(t)}{g(t_0)}$. Then $g(t_0) f(t) - f(t_0) g(t) = 0$, that is

$$g(t_0)\big((1 - ht^2)(\gamma + \alpha t) - 2t\big) - f(t_0)\big((1 - ht^2)(\delta + \beta t) + 2t^2\big) = 0,$$

which is a polynomial in t of degree ≤ 3. Thus in every case, there are at most three distinct $t \in \{0, 1 \ldots, p-1\}$ such that $\langle (x^{t_0} y)^p \rangle \equiv \langle (x^t y)^p \rangle \pmod{\gamma_{p+1}(G)}$. □

Lemma 4.3.6. *Let G be a metabelian thin p-group such that $\gamma_2(G)^p \leq \gamma_{p+1}(G)$. If M is a maximal subgroup of G and $a, b \in M \setminus G'$, then $\langle a \rangle^p \equiv \langle b \rangle^p \pmod{\gamma_{p+1}(G)}$.*

Proof. If we write $b = a^i c$ for some $c \in G'$ and for some integer i not divisible by p, then by the Hall-Petrescu collection formula, Theorem 2.2.20, we have

$$(a^i c)^p = a^{pi} c^p c_2^{\binom{p}{2}} c_3^{\binom{p}{3}} \dots c_p^{\binom{p}{p}},$$

where $c_j \in \gamma_j(\langle a, c\rangle) \leq \gamma_{j+1}(G)$. Thus $(a^i c)^p \equiv a^{pi} \pmod{\gamma_{p+1}(G)}$, and hence $\langle a\rangle^p \equiv \langle b\rangle^p \pmod{\gamma_{p+1}(G)}$. □

Remark 4.3.7. If we replace x with x^*, where $x^* \in G \setminus G'$ is not a power of x, there exists a corresponding y^* satisfying (4.1). Then $x \in \langle (x^*)^{t_0} y^*, G'\rangle \setminus G'$ for some $0 \leq t_0 \leq p-1$, and according to Lemma 4.3.6, we have $\langle x^p\rangle \equiv \langle ((x^*)^{t_0} y^*)^p\rangle \pmod{\gamma_{p+1}(G)}$. It then follows from Lemma 4.3.5 that there exist at most three distinct $t \in \{0, 1 \dots, p-1\}$ such that $\langle x^p\rangle \equiv \langle (x^t y)^p\rangle \pmod{\gamma_{p+1}(G)}$.

The following corollary is an immediate consequence of Lemma 4.3.5 and Lemma 4.3.6.

Corollary 4.3.8. *Let G be a metabelian thin p-group such that $|\gamma_p(G)| \geq p^2$. If M is a maximal subgroup of G, then there exist at most two maximal subgroups M_1, M_2 different from M such that $M^p \equiv M_1^p \equiv M_2^p \pmod{\gamma_{p+1}(G)}$.*

Before we present the main results, we need the following two remarks.

Remark 4.3.9. Let G be a finite 2-generator p-group. Then we can always find elements $x, y \in G \setminus \Phi(G)$ such that x, y and xy fall into the given three maximal subgroups of G. Let M_1, M_2 and M_3 be three maximal subgroups of G. Choose $x \in M_1 \setminus \Phi(G)$ and $y \in M_2 \setminus \Phi(G)$. Since each element in the set $\{xy^j \mid 1 \leq j \leq p-1\}$ falls into different maximal subgroups, there exists $1 \leq j \leq p-1$ such that $xy^j \in M_3 \setminus \Phi(G)$. Thus if we put $x* = x$ and $y* = y^j$, then elements in the triple $\{x^*, y^*, x^*y^*\}$ fall into the given three maximal subgroups.

Remark 4.3.10. At the end of this section we give a method to construct metabelian thin p-groups. By using this construction and the computer algebra system GAP, we can see that there is no metabelian thin 5-group of class 5 such that $|\gamma_5(G)| = 5^2$ and 5th powers of maximal subgroups coincide in pairs.

We are now ready to give the main results of this section.

Theorem 4.3.11. *Let G be a metabelian thin p-group with $\mathrm{cl}(G) = p$ such that $|\gamma_p(G)| = p^2$, where $p \geq 5$. Then G has a Beauville structure in which one of the two triples has all elements of order p^2.*

Proof. We divide our proof into three cases depending on the number of maximal subgroups whose pth powers coincide, and in every case, we take into account Corollary 4.3.8 and Remark 4.3.9.

Case 1**:** Assume that there is a 1-1 correspondence between maximal subgroups M_i of exponent p^2 and M_i^p. Choose a set of generators $\{x_1, y_1\}$ such that $o(x_1) = o(y_1) = o(x_1y_1) = p^2$.

Case 2**:** Assume that there exist three maximal subgroups of exponent p^2 such that their pth power subgroups coincide. Then choose a set of generators $\{x_1, y_1\}$ such that x_1, y_1 and x_1y_1 fall into those maximal subgroups.

In both Case 1 and 2, since $p \geq 5$, we can choose another set of generators $\{x_2, y_2\}$ so that each pair of elements in $\{x_i, y_i, x_iy_i \mid i = 1, 2\}$ is linearly independent modulo G' by Remark 4.3.9.

Case 3**:** Assume that we are not in the first two cases. Then there exist two maximal subgroups M_1, M_2 of exponent p^2 such that $M_1^p = M_2^p$ and $M^p \neq M_1^p$ for all other maximal subgroups M.

Let us first deal with $p \geq 7$. We start by choosing a set of generators $\{x_1, y_1\}$ where $x_1 \in M_1$ and $y_1 \in M_2$ are such that $o(x_1y_1) = p^2$, say $x_1y_1 \in M_3$. Then there might be a maximal subgroup M_4 such that $M_3^p = M_4^p$ (note that there is no other $i \neq 3, 4$ satisfying $M_i^p = M_3^p$, otherwise we are in Case 2). Since $p \geq 7$, we can choose another set of generators $\{x_2, y_2\}$ so that $x_2, y_2, x_2y_2 \notin M_4$ and each pair of elements in $\{x_i, y_i, x_iy_i \mid i = 1, 2\}$ is linearly independent modulo G', by Remark 4.3.9.

If $p = 5$ then by Remark 4.3.10, 5th powers of maximal subgroups do not coincide in pairs. Thus in Case 3, there exists a maximal subgroup, say M_3, of exponent 5^2, where all other M^5 are different from M_3^5. Then choose sets of generators $\{x_1, y_1\}$ and $\{x_2, y_2\}$ so that $x_1 \in M_1$, $y_1 \in M_2$ and $x_1y_1 \in M_3$ and each pair of elements in $\{x_i, y_i, x_iy_i \mid i = 1, 2\}$ is linearly independent modulo G'.

We claim that, in every case, $\{x_1, y_1\}$ and $\{x_2, y_2\}$ form a Beauville structure for G. If $A = \{x_1, y_1, x_1y_1\}$ and $B = \{x_2, y_2, x_2y_2\}$, then we need to show that

$$\langle a^g \rangle \cap \langle b^h \rangle = 1, \tag{4.9}$$

for all $a \in A$, $b \in B$ and $g, h \in G$. Note that $o(a) = p^2$ for every $a \in A$. Assume first that $o(b) = p$. If $\langle a^g \rangle \cap \langle b^h \rangle \neq 1$ for some $g, h \in G$, then $\langle b^h \rangle \subseteq \langle a^g \rangle$, and hence $\langle aG' \rangle = \langle bG' \rangle$, which is a contradiction, since a and b are linearly independent modulo G'. Thus we assume that $o(b) = p^2$. If (4.9) does not hold, then $\langle (a^g)^p \rangle = \langle (b^h)^p \rangle$, which contradicts the choice of b. □

We next deal with the case $\mathrm{cl}(G) = p + 1$.

Theorem 4.3.12. *Let G be a metabelian thin p-group with $\mathrm{cl}(G) = p + 1$, where $p \geq 5$. Then G has a Beauville structure.*

Proof. By Theorem 4.3.11, $\overline{G} = G/\gamma_{p+1}(G)$ has a Beauville structure in which one of the two triples has all elements of order p^2, i.e. they have the same order in both G and $\overline{G}$. Then we can apply Lemma 2.3.4 and thus G is a Beauville group. □

We next analyze the case $\mathrm{cl}(G) = p$ and $|\gamma_p(G)| = p$. Observe that in this case $p \geq 5$, otherwise G is of maximal class. Recall that we have $\gamma_p(G) \leq G^p \leq \gamma_{p-1}(G)$, and thus there are two possibilities:

(i) $G^p = \gamma_{p-1}(G)$,

(ii) $G^p = \gamma_p(G)$.

Observe that G^p cannot be a proper subgroup of $\gamma_{p-1}(G)$ of order p^2, by Lemma 4.1.28.

Theorem 4.3.13. *Let G be a group in case (i). Then G has a Beauville structure .*

Proof. First of all, notice that there exists a pair of generators a and b of G such that a^p and b^p are linearly independent modulo $\gamma_p(G)$. By the Hall-Petrescu formula, we have

$$(a^t b)^p = a^{tp} b^p c_2^{\binom{p}{2}} \dots c_p^{\binom{p}{p}},$$

where $c_j \in \gamma_j(\langle a^t, b\rangle)$. Since $\gamma_2(G)^p \leq \gamma_p(G)$, by Lemma 4.1.26, we get

$$(a^t b)^p \equiv a^{tp} b^p \pmod{\gamma_p(G)}$$

for $1 \leq t \leq p-1$. Observe that, similarly to Lemma 4.3.6, for every maximal subgroup M, $m \in M$ and $c \in G'$, we have $(mc)^p \equiv m^p \pmod{\gamma_p(G)}$. It then follows that the power subgroups M^p are all different modulo $\gamma_p(G)$.

On the other hand, since $\overline{G} = G/\gamma_p(G)$ is of class $p-1$, it is a regular p-group such that $|\overline{G}^p| = p^2$. According to Theorem 3.2.2, $\overline{G}$ is a Beauville group since $p \geq 5$. From the observation above, all elements outside G' are of order p^2 in both G and $\overline{G}$. Then we can apply Lemma 2.3.4 to conclude that G is a Beauville group. □

Theorem 4.3.14. *Let G be a group in case (ii). Then G has a Beauville structure if and only if it has at least three maximal subgroups of exponent p.*

Proof. If the number of maximal subgroups of exponent p is less than three, then $\Omega_1(G)$ is contained in the union of at most two maximal subgroups. Since $|G^p| = p$, it then follows from Proposition 3.2.1 that G has no Beauville structure.

On the other hand, if at least three maximal subgroups have exponent p, then according to Lemma 2.3.5, G is a Beauville group. □

We continue this section with the construction of metabelian thin p-groups. As a consequence, we will see that if $\mathrm{cl}(G) = p$ and $|\gamma_p(G)| = p$, then both cases (i) and (ii) are possible.

A partial ordering can be introduced on the set of non-cyclic metabelian thin p-groups by saying that G *strictly dominates* H if H is isomorphic to a proper quotient of G. Then in this poset, G is said to be an *ancestor* if it is not strictly dominated by any thin group. This means that all metabelian thin p-groups are quotients of ancestors.

We will give the construction of all ancestors of order at least p^7 for $p > 3$, which is given in [10].

Construction 4.3.15. Let $M = \langle c_0, c_{l-1}, u_i, v_i, 1 \leq i \leq l-2\rangle$ be an additively written abelian group where $l \leq p$, with relations

$$pc_{l-1} = pu_i = pv_i = 0, \;\; pc_0 = \lambda c_{l-1},$$

for some λ. Here c_{l-1} is allowed to be zero, and in this case, M is elementary abelian of order p^{2l-3}. Otherwise, M has order p^{2l-2}, and is elementary abelian for $\lambda = 0$ and of type $(p^2, p, \dots, p)$ otherwise.

We next define two endomorphisms Y and X of M by

$$Y(c_0) = v_1, \;\; Y(c_{l-1}) = 0,$$
$$Y(u_i) = u_{i+1}, \;\; Y(v_i) = v_{i+1}, \quad \text{for } i < l-2,$$
$$Y(u_{l-2}) = \mu c_{l-1}, \;\; Y(v_{l-2}) = \nu c_{l-1},$$

for some μ and ν, that can be both zero only for $c_{l-1} = 0$, and

$$X(c_0) = u_1, \;\; X(c_{l-1}) = 0,$$
$$X(u_i) = kv_{i+1} + Y^{i-1}(w), \;\; X(v_i) = u_{i+1}, \quad \text{for } i < l-2,$$
$$X(u_{l-2}) = k\nu c_{l-1}, \;\; X(v_{l-2}) = \mu c_{l-1},$$

where k is a non-square modulo p, and w is a fixed element in

$$\langle u_3, v_3, \dots, u_{l-2}, v_{l-2}, c_{l-1} \rangle.$$

Then it is easy to see that X and Y commute, and $X^l = Y^l = 0$. Thus $x = 1 + X$ and $y = 1 + Y$ are commuting automorphisms of M, and since $l \leq p$, they have order p.

Let A be the commutative ring of endomorphisms of M generated by x and y, and let I be the ideal of A generated by X and Y. Then M is a cyclic A-module, generated by c_0. By checking the action on c_0, it is easy to see that

$$X^2 = kY^2 + \varphi, \quad \text{for some } \varphi \in I^3,$$
$$\mu XY^{l-2} = \nu Y^{l-1},$$

where $w = \varphi(c_0)$.

Let α, β, γ and δ be integers so that the endomorphisms

$$\phi \equiv \alpha XY^{l-3} + \beta Y^{l-2} \pmod{I^{l-1}} \;\text{ and}$$
$$\psi \equiv \gamma XY^{l-3} + \delta Y^{l-2} \pmod{I^{l-1}}$$

satisfy the following relations:

$$X\phi = 0, \;\; Y\psi = 0, \;\; -X\psi = N(y), \;\; Y\phi = N(x),$$

where the norm $N(z)$ of an element of A is defined as

$$\begin{aligned} N(z) &= 1 + z + \cdots + z^{p-1} \\ &= p + \binom{p}{2}(z-1) + \cdots + \binom{p}{i}(z-1)^{i-1} + \cdots + (z-1)^{p-1}. \end{aligned}$$

We can now construct a metabelian thin p-group. Note that M is abelian, and x and y are commuting automorphisms of M of order p. Set

$$\begin{gathered} m_1 = \alpha u_{l-2} + \beta v_{l-2}, \\ m_2 = \gamma u_{l-2} + \delta v_{l-2}, \\ m_{1,2} = -c_0, \text{ and } m_{2,1} = c_0. \end{gathered}$$

Then we have

$$(y-1)(m_1) = Y(m_1) = (\alpha\mu + \beta\nu)c_{l-1},$$

and

$$(1 + x + \cdots + x^{p-1})(m_{2,1}) = N(x)(c_0) = Y\phi(c_0) = (\alpha\mu + \beta\nu)c_{l-1}.$$

Also

$$(x-1)(m_2) = X(m_2) = (\gamma k\nu + \delta\mu)c_{l-1},$$

and

$$(1 + y + \cdots + y^{p-1})(m_{1,2}) = N(y)(-c_0) = X\psi(c_0) = (\gamma k\nu + \delta\mu)c_{l-1}.$$

Thus by using Theorem 2.2.26, we can construct a metabelian p-group $G = \langle a, b\rangle$ as an extension of M by an elementary abelian group of order p^2 where

$$\begin{gathered} [a,b] = c_0, \\ m^a = x(m), \;\; m^b = y(m) \text{ for all } m \in M, \\ a^p = \phi(c_0), \;\; b^p = \psi(c_0). \end{gathered}$$

By [10, pages 170,171], such a group G will be thin. Then according to Theorem 4.1 in [10], the resulting group G has exponent p^2 and we have the following:

1. If we want G to have order p^{2l-1} and $\mathrm{cl}(G) = l$, then we can choose freely α, β, γ and δ which are not all zero unless $l = p$. In this case, we have $\exp G' = p$.

2. For $l < p$, if we want G to have order p^{2l} and $\mathrm{cl}(G) = l + 1$, then

$$\alpha = s, \;\; \beta = kt, \;\; \gamma = -t, \;\; \delta = -s,$$

for s, t not both zero. In this case, we have

$$\lambda = s^2 - kt^2, \;\; \mu = s, \;\; \nu = -t,$$

and $\exp G' = p^2$.

We next use the construction to show that there exists a group as in case (i) in page 62 , that is, $\mathrm{cl}(G) = p$, $|\gamma_p(G)| = p$ and $G^p = \gamma_{p-1}(G)$. Let us take $l = p - 1$, $t = 0$ and $s = 1$, then by the construction, we have $\lambda = 1$, $\mu = 1$, $\nu = 0$ and

$$\begin{aligned} \phi &\equiv XY^{p-4} \pmod{I^{p-2}} \\ \psi &\equiv -Y^{p-3} \pmod{I^{p-2}}. \end{aligned}$$

Hence $a^p = [a, b, a, b, \overset{p-4}{\ldots}, b]$ and $b^p = [a, b, \overset{p-2}{\ldots}, b]$. By Lemma 4.1.18, a^p and b^p are linearly independent modulo $\gamma_p(G)$. Then $\gamma_{p-1}(G) = \langle a^p, b^p \rangle \gamma_p(G) = \langle a^p, b^p, c_0^p \rangle \leq G^p$. Thus $G^p = \gamma_{p-1}(G)$.

We continue this section by showing groups as in Theorem 4.3.14 exist. We first observe that there is a metabelian thin p-group G of class p and $\gamma_p(G) \cong C_p \times C_p$ in which there are three maximal subgroups whose pth powers coincide in a non-trivial subgroup and all maximal subgroups have exponent p^2.

Recall that by the proof of Lemma 4.3.5, we have

$$(x^t y)^p \equiv l^{\gamma + \alpha t - \frac{2t}{1-ht^2}} \;\; m^{\delta + \beta t + \frac{2t^2}{1-ht^2}} \pmod{\gamma_{p+1}(G)},$$

where (l, m) is a basis of $\gamma_p(G)$ modulo $\gamma_{p+1}(G)$. By the construction, we can freely choose α, β, γ and δ. Our aim is to choose γ and α so that $\gamma + \alpha t - \frac{2t}{1-ht^2} = 0$ has three different solutions. Now $\gamma + \alpha t - \frac{2t}{1-ht^2} = 0$ if and only if

$$-\alpha h t^3 - \gamma h t^2 + (\alpha - 2)t + \gamma = 0. \tag{4.10}$$

If we take $\gamma = 0$, then (4.10) holds if and only if either $t = 0$ or $-\alpha h t^2 + (\alpha - 2) = 0$, that is $t^2 = \frac{\alpha - 2}{\alpha} h^{-1}$.

Notice that the map

$$\begin{aligned} \mathbb{F}_p \smallsetminus \{0\} &\longrightarrow \mathbb{F}_p \smallsetminus \{1\} \\ \alpha &\longmapsto 1 - \frac{2}{\alpha} \end{aligned}$$

is a bijection. Let us take a quadratic non-residue $j \in \mathbb{F}_p \smallsetminus \{1\}$, then there exists $\alpha \in \mathbb{F}_p \smallsetminus \{0\}$ such that $j = 1 - \frac{2}{\alpha}$. Thus we have $t^2 = jh^{-1}$, for some $t \neq 0$, since jh^{-1} is a non-zero quadratic residue. Therefore, there are two different non-zero solutions of (4.10), say t_1 and t_2, and consequently $y^p, (x^{t_1}y)^p, (x^{t_2}y)^p \in \langle m \rangle$.

We next choose β and δ so that all maximal subgroups have exponent p^2. Observe that

$$\delta + \beta t + \frac{2t^2}{1 - ht^2} = 0 \quad \text{if and only if} \quad -\beta h t^3 + (2 - \delta h)t^2 + \beta t + \delta = 0.$$

If we choose $\beta = 0$ and $\delta = 2h^{-1}$, then since $2h^{-1} \neq 0$, we have no solution in t. Thus, if $\gamma = \beta = 0$, $\delta = 2h^{-1}$ and $\alpha \in \mathbb{F}_p \smallsetminus \{0\}$ is such that $j = 1 - \frac{2}{\alpha}$ is a quadratic non-residue, then by (4.8) and Lemma 4.3.6, all maximal subgroups have exponent p^2 and there are three maximal subgroups whose pth powers coincide.

Set $\overline{G} = G/\langle m \rangle$, then $\overline{G}$ is a group as in case (ii) with three maximal subgroups of exponent p.

On the other hand, since $\gamma_p(G)$ has $p+1$ maximal subgroups and $\langle y^p \rangle = \langle (x^{t_1}y)^p \rangle = \langle (x^{t_2}y)^p \rangle$, there exists a maximal subgroup N of $\gamma_p(G)$ which does not coincide with the pth power of any maximal subgroup of G. Hence $\overline{G} = G/N$ is a group as in case (ii) in which all maximal subgroups are of exponent p^2.

CHAPTER 5

QUOTIENTS OF THE NOTTINGHAM GROUP

In this chapter, we state the main result on quotients of the Nottingham group. We determine which quotients of the Nottingham group over $\mathbb{F}_p$ are Beauville groups, for an odd prime p. As a consequence, we give the first explicit infinite family of Beauville 3-groups, and we show that there are Beauville 3-groups of order 3^n for every $n \geq 5$. Before moving on to the results we give the definition of the Nottingham group and some properties in Section 5.1. These properties play a significant role in proving the main theorems of this chapter.

5.1 Preliminaries

In this section, we present some preliminaries for the Nottingham group. The proof of the results can be found in the given references.

The Nottingham group was first introduced by D. Johnson [33] as a group of formal power series under substitution.

Definition 5.1.1. *Let $\mathbb{F}_q$ be a finite field. The Nottingham group over $\mathbb{F}_q$, denoted by $\mathcal{N}(\mathbb{F}_q)$, is defined to be the group of formal power series of the form*

$$f = t(1 + \sum_{k=1}^{\infty} \alpha_k t^k) \in \mathbb{F}_q[[t]]$$

under formal substitution: given $g \in \mathcal{N}(\mathbb{F}_q)$, set $fg = g(1 + \sum_{k=1}^{\infty} \alpha_k g^k)$.

Equivalently, the Nottingham group may be described as follows:

Definition 5.1.2. *The Nottingham group over $\mathbb{F}_q$ is the topological group of normalized automorphisms of the ring $\mathbb{F}_q[[t]]$ of formal power series :*

$$\mathcal{N}(\mathbb{F}_q) = \{f \in \operatorname{Aut}(\mathbb{F}_q[[t]]) \mid f(t) = t + \sum_{i \geq 2} \alpha_i t^i\}.$$

The group operation is composition and given $g \in \mathcal{N}(\mathbb{F}_q)$, we set $fg = f \circ g$.

Throughout this chapter, we shall write $\mathcal{N}$ for $\mathcal{N}(\mathbb{F}_q)$ and the elements of $\mathcal{N}$ will be thought of as automorphisms of $\mathbb{F}_q[[t]]$.

We next define a chain of subgroups $\mathcal{N}_k$ $(k \geq 1)$ of $\mathcal{N}$ by

$$\mathcal{N}_k = \{f \in \operatorname{Aut}(\mathbb{F}_q[[t]]) \mid f(t) = t + \sum_{i \geq k+1} \alpha_i t^i\}.$$

Each $\mathcal{N}_k$ is an open normal subgroup of $\mathcal{N}$ and $|\mathcal{N}_k : \mathcal{N}_{k+1}| = q$. It can be seen that $\mathcal{N} \cong \varprojlim(\mathcal{N}/\mathcal{N}_k)$. Thus if q is a power of p, then $\mathcal{N}$ is a pro-p group. Indeed, it is a finitely generated pro-p group.

We now state some results regarding the generators of the Nottingham group. For this purpose, we introduce the following specific elements.

Definition 5.1.3. *For $i \in \mathbb{N}$ with $i \not\equiv 0 \pmod{p}$ and $\lambda \in \mathbb{F}_q$, we define $f_i[\lambda] \in \mathcal{N}$ by*

$$f_i[\lambda] \colon t \longmapsto t(1 - \lambda t^i)^{-1/i}.$$

Then $f_i[\lambda] \in \mathcal{N}_i$ (see [36], page 41).

Proposition 5.1.4. [36, Proposition 1.2] *The set $\{f_i[\lambda] \mid i \in \mathbb{N}$ with $i \not\equiv 0 \pmod{p}, \lambda \in \mathbb{F}_q^*\}$ is a complete set of representatives for the conjugacy classes of the elements of order p in $\mathcal{N}$.*

Definition 5.1.5. *For $i \geq 1$ and $\lambda \in \mathbb{F}_q$, we define $e_i[\lambda] \in \mathcal{N}_i$ by*

$$e_i[\lambda] \colon t \longmapsto t(1 + \lambda t^i).$$

Let $\mathbb{F}_q$ be a field with odd characteristic. If $\mathbb{F}_q$ is additively generated by $\{\lambda_1, \lambda_2, \ldots, \lambda_e\}$, then $\mathcal{N}$ is topologically generated by $2e$ elements, that is

$$\mathcal{N} = \overline{\langle e_1[\lambda_j], e_2[\lambda_j] \mid 1 \leq j \leq e \rangle}.$$

Lemma 5.1.6. [11, Remark 3(ii)] *Let $\mathcal{N}$ be the Nottingham group over $\mathbb{F}_p$, for an odd prime p. Then $\mathcal{N}$ can be generated by two elements of order p, namely $f_1[1]$ and $f_2[1]$.*

Definition 5.1.7. *If $1 \neq f \in \mathcal{N}$ then there is an integer $k \geq 1$ such that $f \in \mathcal{N}_k \setminus \mathcal{N}_{k+1}$. We call k the **depth** of f and denote it by $D(f)$. Also, we define the depth of the identity to be ∞.*

Proposition 5.1.8. [11, Proposition 1] *Let f, $g \in \mathcal{N}$ with $D(f) = k$ and $D(g) = \ell$. Then*

$$\begin{aligned} D([f,g]) &= k + \ell \quad \textit{if} \quad k \not\equiv \ell \pmod{p}, \\ D([f,g]) &> k + \ell \quad \textit{if} \quad k \equiv \ell \pmod{p}. \end{aligned}$$

Theorem 5.1.9. [11, Theorem 2] *For $p \neq 2$,*

$$[\mathcal{N}_k, \mathcal{N}_\ell] = \begin{cases} \mathcal{N}_{k+\ell}, & \textit{if} \quad k \not\equiv \ell \pmod{p}, \\ \mathcal{N}_{k+\ell+1}, & \textit{if} \quad k \equiv \ell \pmod{p}. \end{cases}$$

The following can be easily deduced from Theorem 5.1.9 for $p \neq 2$.

(i) The derived series of $\mathcal{N}$ is given by $\mathcal{N}^{(i)} = \mathcal{N}_{2^{i+1}-1}$ for $i \geq 0$, and $|\mathcal{N} : \mathcal{N}^{(i)}| = q^{2^{i+1}-2}$.

(ii) The lower central series of $\mathcal{N}$ is given by $\gamma_i(\mathcal{N}) = \mathcal{N}_{r_i}$, where $r_i = i + 1 + \lfloor \frac{i-2}{p-1} \rfloor$.

Thus if $\mathcal{N}$ is the Nottingham group over $\mathbb{F}_p$, for an odd prime p, then $|\gamma_i(\mathcal{N}) : \gamma_{i+1}(\mathcal{N})| \leq p^2$ and the equality holds if and only if $i = k(p-1) + 1$ for some $k \geq 0$. In other words, we have '**diamonds**' of order p^2 in the lower central series which correspond to the quotients $\mathcal{N}_{kp+1}/\mathcal{N}_{kp+3}$.

Theorem 5.1.10. [37, Theorem 1.3] *Let $\mathcal{N}$ be the Nottingham group over $\mathbb{F}_q$ of characteristic $p \neq 2$. Then for every $1 \neq \mathcal{W} \trianglelefteq \mathcal{N}$, there exists $k \in \mathbb{N}$ such that one of the following holds:*

(i) $\mathcal{N}_{k+1} \leq \mathcal{W} \leq \mathcal{N}_k$ *where* $k \not\equiv 1 \pmod{p}$.

(ii) $\mathcal{N}_{k+2} \leq \mathcal{W} \leq \mathcal{N}_k$ *where* $k \equiv 1 \pmod{p}$.

Thus every non-trivial normal subgroup of $\mathcal{N}$ is of finite index.

In particular, if $\mathcal{N}$ is the Nottingham group over $\mathbb{F}_p$, for an odd prime p, then every non-trivial normal subgroup of $\mathcal{N}$ is either a term of the chain $\{\mathcal{N}_k\}$ or one of the $p+1$ intermediate subgroups in a diamond corresponding to $\mathcal{N}_{kp+1}/\mathcal{N}_{kp+3}$. Thus the Nottingham group over $\mathbb{F}_p$ is an example of thin infinite pro-p group.

Lemma 5.1.11. [11, Lemma 1] *If $D(f) = k$ then*

$$\begin{aligned} D(f^p) &= kp \quad \textit{if} \quad k \equiv 0 \pmod{p}, \\ D(f^p) &> kp \quad \textit{if} \quad k \not\equiv 0 \pmod{p}. \end{aligned}$$

Theorem 5.1.12. [11, Theorem 6] *If $p \neq 2$ then*

$$\mathcal{N}_k^p = \overline{\mathcal{N}_k^p} = \mathcal{N}_{kp+\overline{k}},$$

where $k \equiv \overline{k} \pmod{p}$ and $0 \leq \overline{k} \leq p-1$.

Notation: We write z_m for the number $p^m + p^{m-1} + \cdots + p + 2$ for every $m \geq 1$ and we put $z_0 = 2$.

The following theorem implies that p^mth powers of elements of the Nottingham group are contained in $\mathcal{N}_{z_m - 1}$.

Theorem 5.1.13. [53, Theorem 6] *Let z_m be as defined above and $p \neq 2$. Then for every $m \geq 1$ and $k < z_m$, the exponent of $\mathcal{N}/\mathcal{N}_k$ is at most p^m.*

We next mention how we can calculate the p^mth powers of elements of the Nottingham group. For any $f \in \mathcal{N}$, we can form a matrix M where $M_{i,j}$ is the coefficient of t^j in the power series $f(t^i)$, which is the image of t^i under f. Then we have the following lemma.

Lemma 5.1.14. [53, Lemma 5] *Let $f \in \mathcal{N}$, and let M be the matrix associated to f. Then for every $r \geq 1$, the coefficient of t^n in the series $f^{p^r}(t)$ is*

$$\sum_{\mathbf{i}=(i_0,\ldots,i_\ell)} M_{i_0,i_1} M_{i_1,i_2} \ldots M_{i_{\ell-1},i_\ell}, \tag{5.1}$$

where $\ell = p^r$ and the tuples $\mathbf{i} = (i_0, \ldots, i_\ell)$ in the sum are taken so that $1 = i_0 < i_1 < i_2 < \cdots < i_{\ell-1} < i_\ell = n$.

We finally state a result regarding the centralizers of elements of order p with depth k of the Nottingham group.

Theorem 5.1.15. [36, page 42] *Let f be an element of $\mathcal{N}$ of order p with $D(f) = k$. Then for every $\ell \in k + 1 + p\mathbb{N}$ we have*

$$C_{\mathcal{N}/\mathcal{N}_\ell}(f\mathcal{N}_\ell) = C_{\mathcal{N}}(f)\mathcal{N}_{\ell-k}/\mathcal{N}_\ell.$$

5.2 Main result

In this section, we analyse quotients of the Nottingham group over the field $\mathbb{F}_p$, for an odd prime p. Before proving the main result, we require Theorems 5.2.6 and 5.2.8. It should be noted that Lemma 5.2.2 is crucial to determine Beauville structures in the quotients of the Nottingham group.

Before proving the following two lemmas, we first observe that for every $k \geq 1$, we have

$$f \equiv g \pmod{\mathcal{N}_k} \quad \text{if and only if} \quad f(t) \equiv g(t) \pmod{t^{k+1}}. \tag{5.2}$$

Indeed, $f \equiv g \pmod{\mathcal{N}_k}$ implies that there exists $h \in \mathcal{N}_k$ such that $f = hg$. Let h be given by $h(t) = t + \sum_{i\geq k+1} a_i t^i$. Then

$$f(t) = h(g(t)) = g(t) + \sum_{i\geq k+1} a_i g(t)^i \equiv g(t) \pmod{t^{k+1}}.$$

Conversely, let us assume that $f(t) \equiv g(t) \pmod{t^{k+1}}$, that is $f(t) = g(t) + \sum_{i\geq k+1} a_i t^i$. Since $g \in \mathcal{N}$, there exists $g^{-1} \in \mathcal{N}$ such that $g^{-1}(g(t)) = t$. Let h be given by $h(t) = t + \sum_{i\geq k+1} a_i g^{-1}(t)^i$. Then $h \in \mathcal{N}_k$, and $h(g(t)) = g(t) + \sum_{i\geq k+1} a_i g^{-1}(g(t))^i = g(t) + \sum_{i\geq k+1} a_i t^i = f(t)$. Thus $f = hg$, and hence $f \equiv g \pmod{\mathcal{N}_k}$.

Our approach to prove the main result is based on the analysis of the quotients of the form $\mathcal{N}/\mathcal{N}_{z_m+1}$ for every $m \geq 1$. To this purpose, the important point is to control the p^mth powers of elements outside $\mathcal{N}'$ modulo $\mathcal{N}_{z_m+1}$ since they are potential generators of that quotient group.

Lemma 5.2.1. *Let $f \in \mathcal{N}_{z_k-1}$ and $g \in \mathcal{N}_{z_k+1}$, where $k \geq 0$. Then, for every $\ell \geq 1$ we have*

$$(fg)^{p^\ell} \equiv f^{p^\ell} \pmod{\mathcal{N}_{z_{k+\ell}+1}}.$$

Proof. According to Theorem 2.2.20, we have

$$(fg)^{p^\ell} = f^{p^\ell} g^{p^\ell} c_2^{\binom{p^\ell}{2}} c_3^{\binom{p^\ell}{3}} \dots c_{p-1}^{\binom{p^\ell}{p-1}} \dots c_{p^\ell}, \tag{5.3}$$

where $c_i \in \gamma_i(\langle f, g\rangle)$ for every $2 \leq i \leq p^\ell$. Since $g \in \mathcal{N}_{z_k+1}$, it then follows from Theorem 5.1.12 that

$$g^{p^\ell} \in \mathcal{N}_{z_k+1}^{p^\ell} \leq \mathcal{N}_{p^\ell(z_k+1)} \leq \mathcal{N}_{z_{k+\ell}+1}.$$

On the other hand, let $1 \leq i \leq p^\ell$, and choose r such that $p^r \leq i < p^{r+1}$. Then the binomial coefficient $\binom{p^\ell}{i}$ is divisible by $p^{\ell-r}$, by Corollary 2.2.24. Since $p^r \leq i < p^{r+1}$, we have $c_i \in \gamma_{p^r}(\langle f, g\rangle)$, where

$$\gamma_{p^r}(\langle f, g\rangle) \leq [\mathcal{N}_{z_k+1}, \mathcal{N}_{z_k-1}, \overset{p^r-1}{\dots}, \mathcal{N}_{z_k-1}] = \mathcal{N}_{2+p^r(z_k-1)+\frac{p^r-1}{p-1}}.$$

The equality follows immediately from Theorem 5.1.9. Since

$$2 + p^r(z_k - 1) + \frac{p^r - 1}{p - 1} = z_{r+k} + 1,$$

we get

$$c_i^{\binom{p^\ell}{i}} \in \mathcal{N}_{z_{r+k}+1}^{p^{\ell-r}} \leq \mathcal{N}_{p^{\ell-r}(z_{r+k}+1)} \leq \mathcal{N}_{z_{k+\ell}+1},$$

by using Theorem 5.1.12. Thus we conclude from (5.3) that $(fg)^{p^\ell} \equiv f^{p^\ell} \pmod{\mathcal{N}_{z_{k+\ell}+1}}$.

□

As a consequence of Lemma 5.2.1, if we want to know p^mth powers of all elements outside $\mathcal{N}'$ in the quotient $\mathcal{N}/\mathcal{N}_{z_m+1}$, it is enough to calculate the p^mth power of one element in $\mathcal{M} \smallsetminus \mathcal{N}'$ for every maximal subgroup $\mathcal{M}$ of $\mathcal{N}$.

We note that $\Phi(\mathcal{N}) = \mathcal{N}_3$, by Remark 3 in [11] and hence $\mathcal{N}/\Phi(\mathcal{N}) \cong C_p \times C_p$. Thus $\mathcal{N}$ has $p + 1$ maximal subgroups. These maximal subgroups are $\mathcal{N}_2$, together with the subgroups $\mathcal{M}_\lambda = \langle f_\lambda, \mathcal{N}'\rangle$ for all $\lambda \in \mathbb{F}_p$, where the element f_λ is given by $f_\lambda(t) = t + t^2 + \lambda t^3$.

We recall from Proposition 5.1.4 that the elements a and b given by $a(t) = t(1 - t)^{-1}$ and $b(t) = t(1-2t)^{-1/2}$ are both of order p. Indeed, $a(t) = t(1-t)^{-1} = t(\sum_{i=0}^{\infty} t^i) \equiv t+t^2+t^3 \pmod{t^4}$. Then by (5.2) we have $a \equiv f_1 \pmod{\mathcal{N}_3}$. Thus $\mathcal{M}_1 = \langle a, \mathcal{N}'\rangle$. Also $\mathcal{N}_2 = \langle b, \mathcal{N}'\rangle$. By Lemma 5.2.1, we conclude that all elements in $\mathcal{M}_1 \smallsetminus \mathcal{N}'$ and $\mathcal{N}_2 \smallsetminus \mathcal{N}'$ have order at most p^m in the quotient group $\mathcal{N}/\mathcal{N}_{z_m+1}$. On the other hand, we will see that all elements in $\mathcal{M}_\lambda \setminus \mathcal{N}'$ with $\lambda \neq 1$ have order p^{m+1} in $\mathcal{N}/\mathcal{N}_{z_m+1}$. To this purpose, we need to calculate $f_\lambda^{p^m}$ modulo $\mathcal{N}_{z_m+1}$. The following lemma is crucial for the calculation of $f_\lambda^{p^m}$.

Lemma 5.2.2. *Let $f \in \mathcal{N}$ be defined via*

$$f(t) \equiv t + \lambda t^{z_{m-1}} + \mu t^{z_{m-1}+1} \pmod{t^{z_{m-1}+2}},$$

where $m \geq 1$. Then

$$f^p(t) \equiv \begin{cases} t + \lambda^{p-1}(\lambda^2-\mu)t^{z_1} - \lambda^{p-2}(\lambda^2-\mu)^2 t^{z_1+1} \pmod{t^{z_1+2}}, & \textit{if} \quad m = 1, \\ t - \lambda^{p-1}\mu t^{z_m} - \lambda^{p-2}\mu^2 t^{z_m+1} \pmod{t^{z_m+2}}, & \textit{if} \quad m > 1. \end{cases} \tag{5.4}$$

Proof. By Lemma 5.2.1 and (5.2), we may assume that $f(t) = t+\lambda t^{z_{m-1}}+\mu t^{z_{m-1}+1}$. Since $f \in \mathcal{N}_{z_{m-1}-1}$, it follows from Theorem 5.1.12 that $f^p \in \mathcal{N}_{z_{m-1}-1}^p = \mathcal{N}_{z_m-1}$. Thus for every $2 \leq i \leq z_m - 1$, the coefficient of t^i in $f^p(t)$ is zero. For the proof we rely on Lemma 5.1.14. According to the definition of the matrix M, we have

$$f(t^i) = t^i + \sum_{j\geq 1} M_{i,i+j} t^{i+j}.$$

By expanding the ith power in

$$f(t^i) = f(t)^i = (t + t^{z_{m-1}}(\lambda+\mu t))^i = \sum_{s=0}^{i} \binom{i}{s} t^{i-s}(t^{z_{m-1}}(\lambda+\mu t))^s, \tag{5.5}$$

we obtain the following values of $M_{i,i+j}$ for $1 \leq j \leq z_{m-1}+1$: if $m > 1$ we have

$$M_{i,i+j} = \begin{cases} \lambda i, & \text{if } j = z_{m-1}-1, \\ \mu i, & \text{if } j = z_{m-1}, \\ 0, & \text{if } 1 \leq j < z_{m-1}-1 \text{ or } j = z_{m-1}+1, \end{cases} \tag{5.6}$$

and if $m = 1$ then

$$M_{i,i+j} = \begin{cases} \lambda i, & \text{if } j = 1, \\ \lambda^2\binom{i}{2} + \mu i, & \text{if } j = 2, \\ 2\lambda\mu\binom{i}{2} + \lambda^3\binom{i}{3}, & \text{if } j = 3. \end{cases} \tag{5.7}$$

We deduce from (5.6) that if there is a non-zero term in the sum (5.1) corresponding to a tuple $\mathbf{i} = (i_0, \ldots, i_p)$, then we must have $i_{j+1} \geq i_j + z_{m-1} - 1$ for every $j = 0, \ldots, p-1$. Thus $i_j \geq j(z_{m-1}-1)+1$ for every $j = 0, \ldots, p$.

Let us first assume that $m > 1$. We start by calculating the coefficient α of t^{z_m} in $f^p(t)$. Since $i_p = z_m = p(z_{m-1} - 1) + 2$, for some $k \in \{1, \dots, p\}$ we must have $i_j = j(z_{m-1} - 1) + 1$ for $j = 0, \dots, k-1$ and $i_j = j(z_{m-1} - 1) + 2$ for $j = k, \dots, p$. For simplicity we write $q_j = j(z_{m-1} - 1) + 1$. Then

$$\alpha = \sum_{k=1}^{p} \alpha_k,$$

where

$$\alpha_k = \Big(\prod_{i=1}^{k-1} M_{q_{i-1},q_i}\Big) M_{q_{k-1},q_k+1} \Big(\prod_{i=k+1}^{p} M_{q_{i-1}+1,q_i+1}\Big).$$

By (5.6) we have

$$M_{q_{j-1},q_j} = \lambda q_{j-1} = \lambda j, \quad \text{for } j = 1, \dots, k-1,$$
$$M_{q_{k-1},q_k+1} = \mu q_{k-1} = \mu k,$$

and

$$M_{q_{j-1}+1,q_j+1} = \lambda(q_{j-1} + 1) = \lambda(j+1), \quad \text{for } j = k+1, \dots, p.$$

Thus

$$\alpha_k = \lambda^{p-1}\mu\, k!(k+2)\dots(p+1).$$

Since α_k contains the factor p unless $k = p-1$, we get

$$\alpha = \lambda^{p-1}\mu(p-1)! = -\lambda^{p-1}\mu.$$

We next calculate the coefficient β of t^{z_m+1} in $f(t^p)$. Since $i_p = z_m + 1 = p(z_{m-1} - 1) + 3$, β must be a product of factors of the form M_{i_{j-1},i_j}, where $i_j - i_{j-1} = z_{m-1} - 1$ except for two values k and ℓ for which $i_k - i_{k-1} = i_\ell - i_{\ell-1} = z_{m-1}$, or one value r for which $i_r - i_{r-1} = z_{m-1} + 1$. The latter case gives a zero product, since $M_{i,i+z_{m-1}+1} = 0$ by (5.6), and hence

$$\beta = \sum_{1 \le k < \ell \le p} \beta_{k,\ell},$$

where

$$\beta_{k,l} = \Big(\prod_{i=1}^{k-1} M_{q_{i-1},q_i}\Big) M_{q_{k-1},q_k+1} \Big(\prod_{i=k+1}^{\ell-1} M_{q_{i-1}+1,q_i+1}\Big)$$
$$M_{q_{\ell-1}+1,q_\ell+2} \Big(\prod_{i=\ell+1}^{p} M_{q_{i-1}+2,q_i+2}\Big).$$

By (5.6), we have

$$\beta_{k,\ell} = \lambda^{p-2}\mu^2 \prod_{\substack{i=1 \\ i\neq k+1,\,\ell+2}}^{p+2} i,$$

which is 0 unless $k = p-1$ and $\ell = p$, or $1 \leq k \leq p-3$ and $\ell = p-2$. Consequently

$$\beta = \lambda^{p-2}\mu^2\Big((p-1)!(p+1) + \sum_{k=1}^{p-3} \frac{(p-1)!(p+1)(p+2)}{k+1}\Big) = -\lambda^{p-2}\mu^2,$$

where the last equality follows from Theorem 2.2.22. This completes the proof when $m > 1$.

Let us now assume that $m = 1$. We first calculate the coefficient α of t^{z_1} in $f^p(t)$. Similar to the case $m > 1$, we have

$$\alpha = \sum_{k=1}^{p} \alpha_k,$$

where

$$\alpha_k = \Big(\prod_{i=1}^{k-1} M_{q_{i-1},q_i}\Big)\, M_{q_{k-1},q_k+1}\,\Big(\prod_{i=k+1}^{p} M_{q_{i-1}+1,q_i+1}\Big).$$

Then by (5.7),

$$\alpha_k = \lambda^{p-1}\Big(\lambda^2\binom{k}{2} + \mu k\Big)\,(k-1)!(k+2)\ldots(p+1).$$

Since α_k is 0 unless $k = p-1$, we finally get

$$\alpha = \lambda^{p-1}(-\lambda^2 + \mu)(p-1)!(p+1) = \lambda^{p-1}(\lambda^2 - \mu).$$

The coefficient β of t^{z_1+1} in $f^p(t)$ can be obtained in a similar way. In that case, we have

$$\beta = \sum_{1\leq k<\ell\leq p} \beta_{k,\ell} + \sum_{r=1}^{p} \beta_r$$

where $\beta_{k,\ell}$ is as defined above, and

$$\beta_r = \Big(\prod_{i=1}^{r-1} M_{q_{i-1},q_i}\Big)\, M_{q_{r-1},q_r+2}\,\Big(\prod_{i=r+1}^{p} M_{q_{i-1}+2,q_i+2}\Big).$$

By (5.7), we have

$$\beta_{k,\ell} = \lambda^{p-2}\Big(\lambda^2\binom{k}{2} + \mu k\Big)\Big(\lambda^2\binom{\ell+1}{2} + \mu(\ell+1)\Big) \prod_{\substack{i=1 \\ i\neq k,\,k+1,\,\ell+1,\,\ell+2}}^{p+2} i,$$

which is 0 unless $k = p - 1$ and $\ell = p$, or $1 \leq k \leq p - 3$ and $\ell = p - 2$. Thus

$$\begin{aligned}\sum_{1 \leq k < \ell \leq p} \beta_{k,\ell} = \lambda^{p-2}\mu(-\lambda^2 + \mu)(p-1)!(p+1)& \\ + \lambda^{p-2}(\lambda^2 - \mu)\sum_{k=1}^{p-3} \frac{(p-1)!(p+1)(p+2)\left(\lambda^2\binom{k}{2} + \mu k\right)}{k(k+1)}& \\ = \lambda^{p-2}(\lambda^2 - \mu)(-3\lambda^2 + \mu),&\end{aligned}$$

where the last equality follows from Theorem 2.2.22. On the other hand,

$$\beta_r = \lambda^{p-1}\left(2\lambda\mu\binom{r}{2} + \lambda^3\binom{r}{3}\right)(r-1)!(r+3)\dots(p+2).$$

We now consider separately $p = 3$ and $p \geq 5$. Let us first assume that $p \geq 5$. Then β_r is 0 unless $r = p - 1$ or $p - 2$. Thus

$$\begin{aligned}\sum_{r=1}^{p} \beta_r &= \lambda^{p-1}\left(2\lambda\mu\binom{p-1}{2} + \lambda^3\binom{p-1}{3}\right)(p-2)!(p+2) \\ &+ \lambda^{p-1}\left(2\lambda\mu\binom{p-2}{2} + \lambda^3\binom{p-2}{3}\right)(p-3)!(p+1)(p+2) \\ &= 2\lambda^{p-1}(2\lambda\mu - \lambda^3) - \lambda^{p-1}(6\lambda\mu - 4\lambda^3) \\ &= 2\lambda^p(\lambda^2 - \mu).\end{aligned}$$

If $p = 3$ then

$$\sum_{r=1}^{3} \beta_r = \beta_2 + \beta_3 = 10\lambda^3\mu + 2\lambda^5 = 2\lambda^3(\lambda^2 - \mu).$$

Thus in both cases we get the same result, namely $\sum_{r=1}^{p} \beta_r = 2\lambda^p(\lambda^2 - \mu)$. Consequently

$$\beta = \lambda^{p-2}(\lambda^2 - \mu)(-3\lambda^2 + \mu) + 2\lambda^p(\lambda^2 - \mu) = -\lambda^{p-2}(\lambda^2 - \mu)^2,$$

as desired. This completes the proof. □

Corollary 5.2.3. *For every $\lambda \in \mathbb{F}_p$ and $m \geq 1$, we have*

$$f_\lambda^{p^m}(t) \equiv t + (1-\lambda)^m t^{z_m} - (1-\lambda)^{m+1} t^{z_m+1} \pmod{t^{z_m+2}}.$$

Proof. To prove the corollary, we use induction on m. By Lemma 5.2.2, we have

$$f_\lambda^p(t) \equiv t + (1-\lambda)t^{z_1} - (1-\lambda)^2 t^{z_1+1} \pmod{t^{z_1+2}}.$$

We now assume that the result holds for $m-1$ for some $m \geq 2$. That is,

$$f_\lambda^{p^{m-1}}(t) \equiv t + (1-\lambda)^{m-1} t^{z_{m-1}} - (1-\lambda)^m t^{z_{m-1}+1} \pmod{t^{z_{m-1}+2}}.$$

Then Lemma 5.2.2 implies that the coefficient of t^{z_m} in $f_\lambda^{p^m}(t)$ is

$$(1-\lambda)^{(p-1)(m-1)}(1-\lambda)^m = (1-\lambda)^{p(m-1)+1} = (1-\lambda)^m,$$

and the coefficient of t^{z_m+1} in $f_\lambda^{p^m}(t)$ is

$$-(1-\lambda)^{(p-2)(m-1)}(1-\lambda)^{2m} = -(1-\lambda)^{p(m-1)+2} = -(1-\lambda)^{m+1}.$$

The last equalities follow from the fact that for every $\lambda \in \mathbb{F}_p$, $\lambda^p = \lambda$. This completes the proof. □

We next consider a quotient $G = \mathcal{N}/\mathcal{N}_{z_m+1}$ of the Nottingham group, for a fixed $m \geq 1$. We will use the following notation: for every $1 \leq k \leq z_m + 1$, $N_k = \mathcal{N}_k/\mathcal{N}_{z_m+1}$, and for every $\lambda \in \mathbb{F}_p$, $M_\lambda = \mathcal{M}_\lambda/\mathcal{N}_{z_m+1}$.

Corollary 5.2.4. *If $G = \mathcal{N}/\mathcal{N}_{z_m+1}$ then for $\lambda \in \mathbb{F}_p$, $\lambda \neq 1$, the power subgroups $M_\lambda^{p^m}$ are all different and of order p, contained in N_{z_m-1}. In particular, all elements of $M_\lambda \smallsetminus G'$ are of order p^{m+1} for $\lambda \neq 1$.*

Proof. We know that $M_\lambda^{p^m}$ is the image of $\mathcal{M}_\lambda^{p^m}$ in G. Lemma 5.2.1 yields that for every $\lambda \in \mathbb{F}_p$, $\lambda \neq 1$, $M_\lambda^{p^m}$ is equal to the image of $\langle f_\lambda^{p^m} \rangle$ in G, and hence by Corollary 5.2.3, $M_\lambda^{p^m}$ is of order p. Thus for every $\lambda \neq 1$, we have $1 = N_{z_m+1} < M_\lambda^{p^m} < N_{z_m-1}$. Furthermore, since f_λ is of order p^{m+1} in G for $\lambda \neq 1$, it follows from Lemma 5.2.1 that all elements of $M_\lambda \smallsetminus G'$ are of order p^{m+1} for $\lambda \neq 1$.

It remains to show that $M_\lambda^{p^m}$ are all different for $\lambda \neq 1$. If $M_{\lambda_1}^{p^m} = M_{\lambda_2}^{p^m}$ for some $\lambda_1, \lambda_2 \in \mathbb{F}_p$, $\lambda_1, \lambda_2 \neq 1$, then $\langle f_{\lambda_1}^{p^m} \rangle \equiv \langle f_{\lambda_2}^{p^m} \rangle \pmod{\mathcal{N}_{z_m+1}}$. Then (5.2) implies that $f_{\lambda_1}^{ip^m}(t) \equiv f_{\lambda_2}^{p^m}(t) \pmod{t^{z_m+2}}$ for some integer i not divisible by p. Observe that since $f_{\lambda_1}^{p^m}(t) \equiv t + (1-\lambda_1)^m t^{z_m} - (1-\lambda_1)^{m+1} t^{z_m+1} \pmod{t^{z_m+2}}$, by Corollary 5.2.3, we have

$$f_{\lambda_1}^{2p^m}(t) = (f_{\lambda_1}^{p^m} \circ f_{\lambda_1}^{p^m})(t) \equiv t + 2(1-\lambda_1)^m t^{z_m} - 2(1-\lambda_1)^{m+1} t^{z_m+1} \pmod{t^{z_m+2}}.$$

Then inductively we get

$$f_{\lambda_1}^{ip^m}(t) \equiv t + i(1-\lambda_1)^m t^{z_m} - i(1-\lambda_1)^{m+1} t^{z_m+1} \pmod{t^{z_m+2}}.$$

Hence $\langle f_{\lambda_1}^{p^m}\rangle \equiv \langle f_{\lambda_2}^{p^m}\rangle \pmod{\mathcal{N}_{z_m+1}}$ if and only if

$$i(1-\lambda_1)^m = (1-\lambda_2)^m, \text{ and } i(1-\lambda_1)^{m+1} = (1-\lambda_2)^{m+1}.$$

This clearly forces $\lambda_1 = \lambda_2$. Thus $M_\lambda^{p^m}$ are all different for every $\lambda \in \mathbb{F}_p$, $\lambda \neq 1$. □

We now begin to determine which quotients of the Nottingham group are Beauville groups. We first consider the quotients of the form $\mathcal{N}/\mathcal{N}_k$. We deal separately with the cases $p > 3$ and $p = 3$. On the other hand, the following lemma holds in both cases $p > 3$ and $p = 3$.

Lemma 5.2.5. *$\mathcal{N}/\mathcal{N}_{z_m}$ is not a Beauville group for every $m \geq 1$.*

Proof. By Lemma 5.2.1 and by Corollary 5.2.3, all elements in $\mathcal{M}_\lambda/\mathcal{N}_{z_m} \smallsetminus \mathcal{N}'/\mathcal{N}_{z_m}$ are of order p^{m+1} for $\lambda \neq 1$. Since $\exp \mathcal{N}/\mathcal{N}_{z_m} = p^{m+1}$, it then follows that condition (i) of Proposition 3.2.1 is fulfilled. On the other hand, by Theorem 5.1.12, we have $\mathcal{N}^{p^m} \leq \mathcal{N}_{z_m-1}$, and so $(\mathcal{N}/\mathcal{N}_{z_m})^{p^m} \leq \mathcal{N}_{z_m-1}/\mathcal{N}_{z_m}$. This, togehter with $|\mathcal{N}_{z_m-1}/\mathcal{N}_{z_m}| = p$, yields that $(\mathcal{N}/\mathcal{N}_{z_m})^{p^m}$ has order p. Thus also condition (ii) of Proposition 3.2.1 holds, and we conclude that $\mathcal{N}/\mathcal{N}_{z_m}$ is not a Beauville group. □

Theorem 5.2.6. *If $p \geq 5$ then a quotient $\mathcal{N}/\mathcal{N}_k$ is a Beauville group if and only if $k \geq 3$ and $k \neq z_m$ for all $m \geq 1$.*

Proof. First of all, note that by Lemma 5.2.5, $\mathcal{N}/\mathcal{N}_{z_m}$ is not a Beauville group for $m \geq 1$. On the other hand, if $k = 2$ then $\mathcal{N}/\mathcal{N}_2 \cong C_p$ which is not a Beauville group. This completes the proof of one implication in the statement of the theorem.

Let us now prove the converse. We begin by proving that $G = \mathcal{N}/\mathcal{N}_{z_m+1}$ is a Beauville group for all $m \geq 1$. Let u and v be the images in G of the automorphisms a and b which were defined after Lemma 5.2.1. Then $\{u, v\}$ and $\{uv^2, uv^4\}$ are both systems of generators of G, and we claim that they yield a Beauville structure for G. If $X = \{u, v, uv\}$ and $Y = \{uv^2, uv^4, uv^2uv^4\}$, we have to see that

$$\langle x^g\rangle \cap \langle y^h\rangle = 1 \tag{5.8}$$

for all $x \in X$, $y \in Y$, and $g, h \in G$. Observe that $\langle x\Phi(G)\rangle$ and $\langle y\Phi(G)\rangle$ have trivial intersection for every $x \in X$ and $y \in Y$, since a and b are linearly independent modulo $\Phi(G)$ and $p \geq 5$. As a consequence, x^g and y^h lie in different maximal subgroups of G in every case.

Assume first that $x = u$ or v, which are elements of order p. It then follows from Lemma 2.3.1 that

$$\Big(\bigcup_{g \in G} \langle x \rangle^g\Big) \bigcap \Big(\bigcup_{g \in G} \langle y \rangle^g\Big) = 1,$$

for every $y \in Y$.

We next assume that $x = uv$. Now, uv and all elements $y \in Y$ lie in $M_\lambda \smallsetminus G'$ for some $\lambda \in \mathbb{F}_p$, $\lambda \neq 1$, and so they are all of order p^{m+1}, by Corollary 5.2.4. If (5.8) does not hold, then

$$\langle (x^g)^{p^m} \rangle = \langle (y^h)^{p^m} \rangle$$

and, again by Corollary 5.2.4, $x^g, y^h \in M_\lambda$ for some λ. This is a contradiction, and we thus complete the proof that G is a Beauville group.

Let us now consider a general quotient $\mathcal{N}/\mathcal{N}_k$ with $k \geq 3$ and $k \neq z_m$ for all $m \geq 1$. Then either $3 \leq k \leq p+1$ or $z_m + 1 \leq k \leq z_{m+1} - 1$ for some $m \geq 1$. In the former case, $\exp \mathcal{N}/\mathcal{N}_k = p$. Since $p \geq 5$, it implies that $\mathcal{N}/\mathcal{N}_k$ is a Beauville group by Corollary 2.1.14. In the latter case, we claim that the Beauville structure of $\mathcal{N}/\mathcal{N}_{z_m+1}$ shown in the previous paragraph can be inherited by a quotient $\mathcal{N}/\mathcal{N}_k$ for $z_m + 1 \leq k \leq z_{m+1} - 1$. One of the generating sets in the Beauville structure of $\mathcal{N}/\mathcal{N}_{z_m+1}$ is $\{a\mathcal{N}_{z_m+1}, b\mathcal{N}_{z_m+1}\}$. By Corollary 5.2.4, we have $(ab)^{p^m} \in \mathcal{N}_{z_m-1} \smallsetminus \mathcal{N}_{z_m+1}$ and $(ab)^{p^{m+1}} \in \mathcal{N}_{z_{m+1}-1} \leq \mathcal{N}_k$, thus $o(ab\mathcal{N}_k) = p^{m+1}$. Since also $o(a\mathcal{N}_k) = o(b\mathcal{N}_k) = p$, we can apply Lemma 2.3.4, and hence $\mathcal{N}/\mathcal{N}_k$ is a Beauville group. □

Next we show a similar result for $p = 3$. To this purpose, we need the following lemma.

Lemma 5.2.7. *Let $p = 3$ and $m \geq 1$, and put $G = \mathcal{N}/\mathcal{N}_{z_m+1}$ and $N_k = \mathcal{N}_k/\mathcal{N}_{z_m+1}$ for all $k \geq 1$. If u and v are the images of a and b in G, respectively, then*

$$\{[u, g] \mid g \in G\} \cap N_{z_m-1} = [u, N_{z_m-2}],$$

$$\{[v, g] \mid g \in G\} \cap N_{z_m-1} = N_{z_m},$$

and both of order p.

Proof. By Theorem 5.1.9, G is a finite nilpotent group of class $2z_{m-1} - 1$ since $\gamma_{2z_{m-1}}(G) = N_{z_m+1} = 1$ and $\gamma_{2z_{m-1}-1}(G) = N_{z_m-1} \neq 1$. Let $N_{z_m-2}/N_{z_m-1} = \langle \overline{w} \rangle$, for some $w \in N_{z_m-2}$. Then

$$\begin{aligned} \gamma_{2z_{m-1}-1}(G) = N_{z_m-1} &= \langle [u,w],[v,w] \rangle = \langle [u,w] \rangle \times \langle [v,w] \rangle \\ &= [u, N_{z_m-2}] \times [v, N_{z_m-2}] = [u, N_{z_m-2}] \times N_{z_m}. \end{aligned}$$

Observe that $[v, N_{z_m-2}] = N_{z_m}$, because $b \in \mathcal{N}_2 \smallsetminus \mathcal{N}_3$ and $[\mathcal{N}_2, \mathcal{N}_{z_m-2}] = \mathcal{N}_{z_m}$.

Then $[u, N_{z_m-2}]$ has order p. We first show that $\{[u,g] \mid g \in G\} \cap N_{z_m-1} = [u, N_{z_m-2}]$. By Lemma 2.3.3, we have $\{[u,g] \mid g \in G\} \cap N_{z_m-1}$ is a subgroup of N_{z_m-1} since $N_{z_m-1} \leq Z(G)$. It is clear that $[u, N_{z_m-2}] \leq \{[u,g] \mid g \in G\} \cap N_{z_m-1}$. We argue by contradiction, and suppose that $[u, N_{z_m-2}]$ is proper, that is

$$[u, N_{z_m-2}] \lneqq \{[u,g] \mid g \in G\} \cap N_{z_m-1} \leq N_{z_m-1}.$$

Then, since N_{z_m-1} is of order p^2, we get $\{[u,g] \mid g \in G\} \cap N_{z_m-1} = N_{z_m-1}$. Thus there exists $g \in G$ such that $1 \neq [u,g] \in N_{z_m}$. Since $a \in \mathcal{N}_1 \smallsetminus \mathcal{N}_2$ is of order p, Theorem 5.1.15 yields

$$C_{\mathcal{N}/\mathcal{N}_{z_m}}(a\mathcal{N}_{z_m}) = C_{\mathcal{N}}(a)\mathcal{N}_{z_m-1}/\mathcal{N}_{z_m}.$$

Thus we can write $g = ch$, with $[u,c] = 1$ and $h \in N_{z_m-1}$. It follows that $[u,g] = [u,ch] = [u,h][u,c]^h = [u,h] \in [G, N_{z_m-1}] = 1$, since N_{z_m-1} is central in G, which is a contradiction.

We next prove the result for the element v. Let $[v,g] \in N_{z_m-1}$ for some $g \in G$. Since $b \in \mathcal{N}_2 \smallsetminus \mathcal{N}_3$ is of order p, again by Theorem 5.1.15, we have

$$C_{\mathcal{N}/\mathcal{N}_{z_m-2}}(b\mathcal{N}_{z_m-2}) = C_{\mathcal{N}}(b)\mathcal{N}_{z_m-4}/\mathcal{N}_{z_m-2}.$$

Thus we can write $g = ch$ with $[v,c] = 1$ and $h \in N_{z_m-4}$, and consequently $[v,g] = [v,ch] = [v,h][v,c]^h = [v,h]$. Now, if $D(h) = z_m - 4$, then by Proposition 5.1.8 $D([v,h]) = z_m - 2$, that is $[v,h] \in N_{z_m-2} \smallsetminus N_{z_m-1}$, which is not true. Thus $h \in N_{z_m-3}$

and hence we conclude that $[v, g] \in [N_2, N_{z_m-3}] = N_{z_m}$. Since N_{z_m} has order p, we get $\{[v, g] \mid g \in G\} \cap N_{z_m-1} = N_{z_m}$, as desired.

□

Theorem 5.2.8. *If $p = 3$ then a quotient $\mathcal{N}/\mathcal{N}_k$ is a Beauville group if and only if $k \geq 6$ and $k \neq z_m$ for all $m \geq 1$.*

Proof. Since the smallest Beauville 3-group is of order 3^5, the quotient $\mathcal{N}/\mathcal{N}_k$ can only be a Beauville 3-group if $k \geq 6$; note that 6 is the same as z_1+1 in this case. Now, by arguing as in the proof of Theorem 5.2.6, it suffices to see that $G = \mathcal{N}/\mathcal{N}_{z_m+1}$ is a Beauville group for every $m \geq 1$.

Let u and v be the images of a and b in G, respectively. By Lemma 5.2.7, there exist $w, z \in N_{z_m-1}$ such that $w \notin \{[u, g] \mid g \in G\}$ and $z \notin \{[v, g] \mid g \in G\}$. Observe that w and z are central elements of order p in G. We claim that $\{u, v\}$ and $\{(uw)^{-1}, vz\}$ form a Beauville structure in G. Let $X = \{u, v, uv\}$ and $Y = \{(uw)^{-1}, vz, u^{-1}vw^{-1}z\}$. Assume first that $x \in X$ is of order p, and let $y \in Y$. If $\langle x\Phi(G)\rangle \neq \langle y\Phi(G)\rangle$ in $G/\Phi(G)$, then by Lemma 2.3.1, $\langle x\rangle^g \cap \langle y\rangle^h = 1$ for every $g, h \in G$. Otherwise, we are in one of the following two cases: $x = u$ and $y = (uw)^{-1}$, or $x = v$ and $y = vz$. Then the condition $\langle x\rangle^g \cap \langle y\rangle^h = 1$ follows by Lemma 2.3.2.

We now assume that $x = uv$. Again applying Lemma 2.3.1, we get $\langle x\rangle^g \cap \langle y\rangle^h = 1$ where $y = (uw)^{-1}$ or $y = vz$, which is of order p. Thus we are only left with the case when $x = uv$ and $y = u^{-1}vw^{-1}z$. Now x and y lie in two different maximal subgroups which are different from M_1 and N_2. By Corollary 5.2.4, both x and y are of order p^{m+1} and $\langle x^{p^m}\rangle \neq \langle y^{p^m}\rangle$. Since $x^{p^m}, y^{p^m} \in N_{z_m-1}$ are central in G, it follows that $\langle x\rangle^g \cap \langle y\rangle^h = 1$ for all $g, h \in G$ also in this case. This completes the proof that G is a Beauville group. □

By Theorems 5.2.6 and 5.2.8, we determine which quotients of the Nottingham group of the form $\mathcal{N}/\mathcal{N}_k$ are Beauville groups. We next analyse the case of quotients of the form $\mathcal{N}/\mathcal{W}$, where $\mathcal{W}$ is an intermediate subgroup in a diamond $\mathcal{N}_{kp+1}/\mathcal{N}_{kp+3}$.

It is clear that $\mathcal{N}_{z_m-1}/\mathcal{N}_{z_m+1}$ is a diamond for all $m \geq 0$. We refer to these as

distinguished diamonds.

Theorem 5.2.9. *Let $\mathcal{W}$ be an intermediate subgroup in a diamond of the Nottingham group which is not distinguished. Then $\mathcal{N}/\mathcal{W}$ is a Beauville group.*

Proof. Let $\mathcal{N}_{kp+3} < \mathcal{W} < \mathcal{N}_{kp+1}$, where $\mathcal{N}_{kp+1}/\mathcal{N}_{kp+3}$ is not distinguished. We choose m such that $z_m + 1 < kp + 3 < z_{m+1} + 1$. By Theorems 5.2.6 and 5.2.8, $\mathcal{N}/\mathcal{N}_{z_m+1}$ has a Beauville structure whose first set of generators is $\{a\mathcal{N}_{z_m+1}, b\mathcal{N}_{z_m+1}\}$. Now a and b are both of order p modulo $\mathcal{W}$ and modulo $\mathcal{N}_{z_m+1}$. Since $(ab)^{p^m} \in \mathcal{N}_{z_m-1} \setminus \mathcal{N}_{z_m}$ and $(ab)^{p^{m+1}} \in \mathcal{N}_{z_{m+1}-1}$ by Corollary 5.2.4, ab has the same order modulo $\mathcal{W}$ and $\mathcal{N}_{z_m+1}$, namely p^{m+1}. Hence $\mathcal{N}/\mathcal{W}$ is a Beauville group by Lemma 2.3.4. □

Theorem 5.2.10. (Main Theorem) *Let $\mathcal{N}$ be the Nottingham group over $\mathbb{F}_p$, where p is an odd prime, and let $\mathcal{W}$ be a normal subgroup of $\mathcal{N}$ of index $\geq p^2$ or p^5, according as $p > 3$ or $p = 3$. Then $\mathcal{N}/\mathcal{W}$ is a Beauville group if and only if $\mathcal{W} \neq \mathcal{N}_{z_m}, \langle e, \mathcal{N}_{z_m+1}\rangle$, where e is the automorphism given by $e(t) = t + t^{z_m}$ for all $m \geq 1$ or $m \geq 2$, according as $p > 3$ or $p = 3$.*

Proof. It remains to deal with the case of quotients of the form $\mathcal{N}/\mathcal{W}$, where $\mathcal{W}$ is an intermediate subgroup in a distinguished diamond $\mathcal{N}_{z_m-1}/\mathcal{N}_{z_m+1}$ for some $m \geq 1$ or $m \geq 2$, according as $p > 3$ or $p = 3$. The $p + 1$ intermediate subgroups between $\mathcal{N}_{z_m+1}$ and $\mathcal{N}_{z_m-1}$ are $\mathcal{N}_{z_m}$ and the subgroups $\mathcal{W}_\alpha = \langle e_\alpha, \mathcal{N}_{z_m+1}\rangle$, where $\alpha \in \mathbb{F}_p$ and $e_\alpha(t) = t + t^{z_m} + \alpha t^{z_m+1}$.

We already know that $\mathcal{N}/\mathcal{N}_{z_m}$ is not a Beauville group by Lemma 5.2.5. By using the same argument we show that neither $\mathcal{N}/\mathcal{W}_0$ is a Beauville group. By Corollary 5.2.4, we know that all elements in $\mathcal{M}_\lambda/\mathcal{W}_0 \setminus \mathcal{N}'/\mathcal{W}_0$ are of order p^{m+1} for $\lambda \neq 1$, and hence $\exp \mathcal{N}/\mathcal{W}_0 = p^{m+1}$. Then $\Omega_{\{m\}}(\mathcal{N}/\mathcal{W}_0)$ is contained in two maximal subgroups, which are $\mathcal{M}_1/\mathcal{W}_0$ and $\mathcal{N}_2/\mathcal{W}_0$. On the other hand, since $\mathcal{N}^{p^m} \leq \mathcal{N}_{z_m-1}$ we have $(\mathcal{N}/\mathcal{W}_0)^{p^m} = \mathcal{N}^{p^m}\mathcal{W}_0/\mathcal{W}_0 \leq \mathcal{N}_{z_m-1}/\mathcal{W}_0$, and so $(\mathcal{N}/\mathcal{W}_0)^{p^m}$ is of order p. Thus $\mathcal{N}/\mathcal{W}_0$ is not a Beauville group by Proposition 3.2.1.

Thus we may assume that $\mathcal{W} = \mathcal{W}_\alpha$ for some $\alpha \neq 0$. If we define f_λ as above by means of $f_\lambda(t) = t + t^2 + \lambda t^3$, then by Corollary 5.2.3 we have

$$f_{1+\alpha}^{p^m}(t) \equiv t + (-\alpha)^m t^{z_m} - (-\alpha)^{m+1} t^{z_m+1} \pmod{t^{z_m+2}},$$

and hence

$$f_{1+\alpha}^{p^m} \equiv e_\alpha^{(-\alpha)^m} \pmod{\mathcal{N}_{z_m+1}}.$$

Consequently, $\mathcal{W}_\alpha = \langle f_{1+\alpha}^{p^m}, \mathcal{N}_{z_m+1}\rangle$. We next observe that $f_{1+\alpha} \equiv ab^\alpha \pmod{\mathcal{N}_3}$. Since $a(t) \equiv t + t^2 + t^3 \pmod{t^4}$, and $b(t) \equiv t + t^3 \pmod{t^4}$, we have $ab^\alpha(t) \equiv t + t^2 + (1+\alpha)t^3 \pmod{t^4}$, and (5.2) implies that $f_{1+\alpha} \equiv ab^\alpha \pmod{\mathcal{N}_3}$. Then Lemma 5.2.1 yields that

$$f_{1+\alpha}^{p^m} \equiv (ab^\alpha)^{p^m} \pmod{\mathcal{N}_{z_m+1}}.$$

Hence $\mathcal{W}_\alpha = \langle (ab^\alpha)^{p^m}, \mathcal{N}_{z_m+1}\rangle$. In particular, the order of ab^α modulo $\mathcal{W}_\alpha$ is p^m.

Now, since $m \geq 1$ if $p > 3$ and $m \geq 2$ if $p = 3$, $\mathcal{N}/\mathcal{N}_{z_{m-1}+1}$ has a Beauville structure with $\{a\mathcal{N}_{z_{m-1}+1}, b\mathcal{N}_{z_{m-1}+1}\}$ as one of the generating sets. In a similar way, we can prove that $\mathcal{N}/\mathcal{N}_{z_{m-1}+1}$ has a Beauville structure whose first set of generators is $\{a\mathcal{N}_{z_{m-1}+1}, b^\alpha\mathcal{N}_{z_{m-1}+1}\}$.

Let u and v be the images of a and b in $G = \mathcal{N}/\mathcal{N}_{z_{m-1}+1}$, respectively. If $p = 3$, then $\{u, v^2\}$ and $\{uw, vz\}$ also form a Beauville structure for G. The proof is essentially the same as the proof of Theorem 5.2.8.

If $p > 3$, then for $1 \leq \alpha \leq p-3$ the set of generators $\{u, v^\alpha\}$ and $\{uv^{1+\alpha}, uv^{p-1}\}$ form a Beauville structure for G. If $\alpha = p-2$, then $\{u, v^\alpha\}$ and $\{uv^2, uv^{p-4}\}$ form a Beauville structure for G, and finally if $\alpha = p-1$, then $\{u, v^\alpha\}$ and $\{uv, uv^3\}$ form a Beauville structure for G. The proofs are essentially the same as the proof of Theorem 5.2.6.

Then we have $o(a\mathcal{N}_{z_{m-1}+1}) = o(a\mathcal{W}_\alpha) = p$, $o(b\mathcal{N}_{z_{m-1}+1}) = o(b\mathcal{W}_\alpha) = p$ and $o(ab^\alpha\mathcal{N}_{z_{m-1}+1}) = o(ab^\alpha\mathcal{W}_\alpha) = p^m$, and consequently we can apply Lemma 2.3.4 to conclude that $\mathcal{N}/\mathcal{W}_\alpha$ has a Beauville structure. □

We close the chapter by showing that condition (i) in Proposition 3.2.1 cannot be relaxed. More specifically, given a 2-generator finite p-group G of exponent p^e in which $\Omega_{\{e-1\}}(G)$ is contained in the union of three maximal subgroups and $|G^{p^{e-1}}| = p$, it may well happen that G is a Beauville group. To this end, consider an intermediate subgroup $\mathcal{N}_{z_m+1} < \mathcal{W} < \mathcal{N}_{z_m-1}$ in a distinguished diamond of the Nottingham group, where $m \geq 1$ or $m \geq 2$, according as $p > 3$ or $p = 3$. If $\mathcal{W} \neq \mathcal{N}_{z_m}, \langle e, \mathcal{N}_{z_m+1} \rangle$ then $G = \mathcal{N}/\mathcal{W}$ is a Beauville group by Theorem 5.2.10. Also, as indicated in the proof of that theorem, we have $\mathcal{W} = \langle (ab^{\alpha})^{p^m}, \mathcal{N}_{z_m+1} \rangle$ for some $\alpha \neq 0$ in $\mathbb{F}_p$. It then follows from Corollary 5.2.4 that $\exp G = p^{m+1}$ and that $\Omega_{\{m\}}(G)$ is contained in the three maximal subgroups of G that contain the images of a, b and ab^{α}.

CHAPTER 6

p-CENTRAL QUOTIENTS OF FREE GROUPS AND FREE PRODUCTS

In this chapter, we prove a conjecture of Boston that if $p \geq 5$, all p-central quotients of the free group on two generators and of the free product of two cyclic groups of order p are Beauville groups. In the case of the free product, we also determine Beauville structures in p-central quotients when $p = 3$. As a consequence, we give an infinite family of Beauville 3-groups. We next compare these examples with the Beauville quotients of the Nottingham group over $\mathbb{F}_3$ given in Chapter 5, and we show that the two infinite families only coincide at the group of order 3^5.

6.1 Preliminaries

In this section, we briefly recall the definition and some properties of p-central quotients. Also we present some preliminaries regarding free groups and free products of groups.

Definition 6.1.1. *For any group G, the normal series*

$$G = \lambda_1(G) \geq \lambda_2(G) \geq \cdots \geq \lambda_n(G) \geq \ldots$$

*given by $\lambda_n(G) = [\lambda_{n-1}(G), G]\lambda_{n-1}(G)^p$ for $n > 1$ is called the **p-central series** of G. Then a quotient group $G/\lambda_n(G)$ is said to be a **p-central quotient** of G.*

Theorem 6.1.2. [31, Definition 1.4, Theorem 1.5] *Let G be a group. Then*

(i) $\lambda_n(G) = \gamma_1(G)^{p^{n-1}}\gamma_2(G)^{p^{n-2}} \ldots \gamma_{n-1}(G)^p\gamma_n(G)$.

(ii) $[\lambda_m(G), \lambda_n(G)] \leq \lambda_{m+n}(G)$.

(iii) $\lambda_n(G)^{p^i} \leq \lambda_{n+i}(G)$.

Theorem 6.1.3. [29, Theorem 9.14] *If G is a d-generator group, then $G/\lambda_2(G)$ is elementary abelian of order at most p^d. If G is a finite p-group, then $\lambda_2(G) = \Phi(G)$.*

Lemma 6.1.4. [29, Lemma 9.15] *If θ is a homomorphism of G, then $\theta(\lambda_i(G)) = \lambda_i(\theta(G))$. Consequently, each term of the p-central series is a characteristic subgroup of G. Also, if $N \trianglelefteq G$ then $\lambda_i(G/N) = \lambda_i(G)N/N$.*

Theorem 6.1.5. [29, Lemma 9.20] *If $G/\lambda_2(G)$ is generated by the images of $g_1, g_2, \ldots, g_n$, then $\lambda_2(G)/\lambda_3(G)$ is generated by the images of g_i^p for $1 \leq i \leq d$ and $[g_i, g_j]$ for $1 \leq i < j \leq d$. More generally, for $k > 1$, let S be a subset of* G *which generates G modulo $\lambda_2(G)$, and let T generate $\lambda_k(G)$ modulo $\lambda_{k+1}(G)$. Then $\lambda_{k+1}(G)$ is generated modulo $\lambda_{k+2}(G)$ by $[s,t]$ for $s \in S$, $t \in T$ and t^p for $t \in T$.*

Theorem 6.1.6. [31, Theorem 1.8] *Let G be a group. Then any element of $\lambda_n(G)$ can be written in the form*

$$a_1^{p^{n-1}} a_2^{p^{n-2}} \ldots a_n \quad \textit{for some} \quad a_i \in \gamma_i(G).$$

The following lemma states a special case of the Hall-Petrescu formula.

Lemma 6.1.7. [31, Lemma 1.1] *Let G be a group, $x, y \in G$ and let p be an odd prime. Then for $n \geq 3$*

$$(xy)^{p^{n-2}} \equiv x^{p^{n-2}} y^{p^{n-2}} \pmod{\gamma_2(G)^{p^{n-2}} \prod_{r=1}^{n-2} \gamma_{p^r}(G)^{p^{n-2-r}}}.$$

Lemma 6.1.8. *Let G be a group and $x, y \in G$. For $n \geq 2$, we have*

$$(xy)^{p^{n-2}} \equiv x^{p^{n-2}} y^{p^{n-2}} \pmod{\lambda_n(G)}.$$

Proof. By Lemma 6.1.7, we have

$$(xy)^{p^{n-2}} \equiv x^{p^{n-2}} y^{p^{n-2}} \pmod{\gamma_2(G)^{p^{n-2}} \prod_{r=1}^{n-2} \gamma_{p^r}(G)^{p^{n-2-r}}}. \tag{6.1}$$

Now the result follows, since by Theorem 6.1.2, $\gamma_2(G)^{p^{n-2}} \leq \lambda_n(G)$ and for $1 \leq r \leq n-2$ we have

$$\gamma_{p^r}(G)^{p^{n-2-r}} \leq \lambda_{p^r+n-2-r}(G) \leq \lambda_n(G).$$

Note that the last inclusion holds, since p is odd. □

Note that if $y \in \lambda_2(G)$ in Lemma 6.1.8, then

$$(xy)^{p^{n-2}} \equiv x^{p^{n-2}} \pmod{\lambda_n(G)}. \tag{6.2}$$

Lemma 6.1.9. *Let G be a group such that $\exp G/G' = p$. Then for all $n > 1$, $\lambda_n(G) = \gamma_n(G)$.*

Proof. Since $\exp G/G' = p$, we have $G^p \leq G'$, and hence $\lambda_2(G) = G'$. Now assume that the result holds for $n \geq 2$, that is, $\lambda_n(G) = \gamma_n(G)$. Then $\lambda_{n+1}(G) = \gamma_{n+1}(G)\gamma_n(G)^p$. Since $\exp \gamma_i(G)/\gamma_{i+1}(G) \mid \exp G/G' = p$ for all $i \geq 1$, this implies that $\gamma_n(G)^p \leq \gamma_{n+1}(G)$, and hence $\lambda_n(G) = \gamma_n(G)$. □

We next give the definition of free groups.

Definition 6.1.10. ***(Universal property of the free groups)*** *A group F is said to be* ***free*** *on a nonempty set S if there is a function $\phi : S \longrightarrow F$ such that if G is any group and $\theta : S \longrightarrow G$ is any function, then there exists a unique homomorphism $f : F \longrightarrow G$ such that $\theta = f \circ \phi$.*

Theorem 6.1.11. [47, Theorem 2.1.5] *If G is any group and S is a subset of G that generates G, then G is a homomorphic image of the free group on the set S.*

Definition 6.1.12. *Let S be an arbitary set. A* ***word*** *in S is a finite sequence of elements which we write as $w = y_1 y_2 \ldots y_n$, where $y_i \in S$. Consider $S^{-1} = \{s^{-1} \mid s \in S\}$ where s^{-1} is just a formal expression, and set $S^{\pm 1} = S \cup S^{-1}$. An expression of the type $w = s_{i_1}^{\epsilon_1} \ldots s_{i_n}^{\epsilon_n}$ ($s_{i_j} \in S, \epsilon_j \in \{1, -1\}$) is called* ***group word*** *in S. A group word $w = y_1 \ldots y_n$ is called* ***reduced*** *if w does not contain a subword of the type yy^{-1} for $y \in S^{\pm 1}$.*

The following is an alternative definition of free groups that uses reduced words.

Definition 6.1.13. *A group F is called a* ***free group*** *if there exits a generating set S of F such that every non-empty reduced group word in S defines a non-trivial element of F. If this is the case, F is said to be* ***freely generated*** *by S, and the generating set S is called a* ***basis*** *for F.*

The following theorem will be essential in Section 6.2.

Theorem 6.1.14. [41, Problem 2, Section 2.2] *Let $F = \langle x, y \rangle$ be the free group on two generators. Then an element $w = x^{n_1}y^{m_1} \dots x^{n_k}y^{m_k}$ for $n_i, m_i \in \mathbb{Z}$ belongs to F' if and only if the exponent sum of both letters is zero, that is $\sum_{i=1}^{k} n_i = \sum_{i=1}^{k} m_i = 0$.*

Proof. Consider the abelianization F/F' of the free group F. This is the free abelian group on $\{x, y\}$. Then $w = x^{n_1}y^{m_1} \dots x^{n_k}y^{m_k} \in F'$ if and only if it is the empty word in the free abelian group, and this happen if and only if $\sum_{i=1}^{k} n_i = \sum_{i=1}^{k} m_i = 0$. □

We now present some results regarding the free product of groups. Also, we will see later that free groups are free products of inifinite cyclic groups.

Definition 6.1.15. *A group G is said to be* ***free product*** *of its subgroups G_α if the subgroups G_α generate G, that is if every element g of G is the product of a finite number of elements of G_α*

$$g = g_1g_2 \dots g_n \quad g_i \in G_{\alpha_i}, \quad i = 1, 2 \dots, n, \tag{6.3}$$

and if every $1 \neq g \in G$ has a unique representation in the form 6.3 subject to the condition that $g_i \neq 1$ and no two adjacent elements are in the same subgroup G_α.

We can also speak of a free product of an arbitrary collection of groups.

Let an arbitrary set of groups $\{G_\alpha\}_{\alpha \in \Lambda}$ be given. A **word** is an ordered system of elements $w = g_1g_2 \dots g_n$, where $n \geq 1$, every g_i is an element other than the identity element of G_{α_i}, and two adjacent elements g_i and g_{i+1} belong to different groups G_{α_i}. The case $n = 0$ corresponds to the **empty word**.

If $w' = g'_1g'_2 \dots g'_m$ is another word, then we can define the product of w and w' in the following way:

Let $g'_1 = g_n^{-1},\ g'_2 = g_{n-1}^{-1}, \dots, g'_i = g_{n-i+1}^{-1}$ for $0 \leq i \leq \min(m, n)$, but $g'_{i+1} \neq g_{n-i}^{-1}$. If the elements g'_{i+1} and g_{n-i} belong to different groups G_α, then

$$ww' = g_1g_2 \dots g_{n-i}g'_{i+1}g'_{i+2} \dots g'_m,$$

but if g'_{i+1} and g_{n-i} lie in the same group G_α and $g_{n-i}g'_{i+1} = h$, then

$$ww' = g_1g_2 \dots g_{n-i-1}hg'_{i+2} \dots g'_m.$$

In other words, to obtain the product of w by w' we write down w and w' in juxtaposition and then carry out the necessary cancellations and contractions.

The empty world plays the role of the unit element in the multiplication of words. Thus the inverse of w is

$$w^{-1} = g_n^{-1} g_{n-1}^{-1} \cdots g_2^{-1} g_1^{-1}.$$

Then the set of all the words defined above form a group G, and this group is the free product of its subgroups $\overline{G}_\alpha$, where $\overline{G}_\alpha$ are isomorphic to the given groups G_α.

Definition 6.1.16. *If G is a free product of the set of groups $\{G_\alpha\}_{\alpha\in\Lambda}$, then the G_α are called the* ***free factors*** *of G.*

The free product G will be written $G = \mathrm{Fr}_{\alpha\in\Lambda} G_\alpha$. If Λ is a finite set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, then the free product G is written $G = G_{\alpha_1} * G_{\alpha_2} * \cdots * G_{\alpha_n}$.

Remark 6.1.17. [48, Theorem 11.52] Every non-trivial element of the free product $G = \mathrm{Fr}_{\alpha\in\Lambda} G_\alpha$ can be written uniquely in the form

$$g = g_1 g_2 \cdots g_n,$$

where each g_i is a non-trivial element of some G_{α_i}, and consecutive terms lie in different groups. This is called the **normal form** of g.

The definition of a free product can also be put into another form that uses generators and relations.

Theorem 6.1.18. [48, Theorem 11.53] *Let $\{G_\alpha \mid \alpha \in \Lambda\}$ be the nonempty set of groups. Suppose that $G_\alpha = \langle S_\alpha \mid R_\alpha\rangle$ are the presentations for G_α, where S_α is a set of generators and R_α is a set of defining relations in these generators. Then*

$$\mathrm{Fr}_{\alpha\in\Lambda} G_\alpha = \langle \cup_{\alpha\in\Lambda} S_\alpha \mid \cup_{\alpha\in\Lambda} R_\alpha\rangle.$$

The following is another approach to the concept of a free product.

Definition 6.1.19. [47, page 167] *Let $\{G_\alpha \mid \alpha \in \Lambda\}$ be a nonempty set of groups. The* ***free product*** *of the G_α is a group G for which there exist homomorphisms $\iota_\alpha : G_\alpha \longrightarrow G$ with the property that for any group H and any family of homomorphisms $\psi_\alpha : G_\alpha \longrightarrow H$ there exists a unique homomorphism $\psi : G \longrightarrow H$ such that $\psi_\alpha = \psi \circ \iota_\alpha$.*

Lemma 6.1.20. [48, Lemma 11.49] *If G is a free product of $\{G_\alpha \mid \alpha \in \Lambda\}$, then the homomorphisms ι_α are injections.*

Theorem 6.1.21. [47, Theorem 6.2.2] *For every nonempty set of groups $\{G_\alpha \mid \alpha \in \Lambda\}$ there corresponds a free product.*

The following theorem shows the uniqueness of the free product.

Theorem 6.1.22. [48, Theorem 11.50] *Let $\{G_\alpha \mid \alpha \in \Lambda\}$ be a set of groups. If each G_1 and G_2 are the free product of the G_α, then $G_1 \cong G_2$.*

Lemma 6.1.23. [48, Example 11.9] *A free group F is a free product of infinite cyclic groups.*

Proof. If X is a basis of F, then $\langle x \rangle$ is infinite cyclic group for each $x \in X$. We define $\iota_x : \langle x \rangle \longrightarrow F$ to be the inclusion. If H is a group, then a function $f : X \longrightarrow H$ determines a family of homomorphisms $\psi_x : \langle x \rangle \longrightarrow H$, namely $x^n \mapsto f(x)^n$. And the unique homomorphism $\psi : F \longrightarrow H$ which extends the function f clearly extends each of the homomorphisms ψ_x, that is $\psi \circ \iota_x = \psi_x$ for all $x \in X$. □

We will need the following lemma in Section 6.2.

Lemma 6.1.24. [47, Example 6.2.II] *The free product of two groups of order 2 is an infinite dihedral group.*

Proof. Let $G = \langle a \rangle * \langle b \rangle$ where $o(a) = o(b) = 2$. Write $c = ab$. Then we have $G = \langle a, c \rangle$ and $c^a = c^{-1}$. Thus G is an image of an infinite dihedral group D_∞. Observe that c has infinite order, since $c, c^2, c^3, \ldots$ are distinct elements by uniqueness of the normal form. On the other hand, since a proper image of D_∞ is finite, we have $G \cong D_\infty$. □

6.2 Main results

In this section, we give the main results of this chapter, namely we prove Boston's conjectures about Beauville structures in p-central quotients of the free group on two generators and of the free product of two cyclic groups of order p. We first deal with the free group case.

Let $F = \langle x, y\rangle$ be the free group on two generators. Notice that $\Phi(F/\lambda_n(F))$ for $n \geq 2$ coincides with $\lambda_2(F)/\lambda_n(F)$, and thus elements outside $\lambda_2(F)$ are potential generators in $F/\lambda_n(F)$. In order to determine Beauville structures in the quotients $F/\lambda_n(F)$, it is fundamental to control p^{n-2}nd powers of elements outside $\lambda_2(F)$ in these quotients groups.

Before we proceed to prove the main result for the free group we need to introduce two lemmas.

Lemma 6.2.1. *Let $F = \langle x, y\rangle$ be the free group on two generators. Then $x^{p^{n-2}}$ and $y^{p^{n-2}}$ are linearly independent modulo $\lambda_n(F)$ for $n \geq 2$.*

Proof. We argue by way of contradiction. Suppose that $y^{ip^{n-2}} \equiv x^{p^{n-2}} \pmod{\lambda_n(F)}$. It follows from Theorem 6.1.6 that $x^{-p^{n-2}}y^{ip^{n-2}} = a_1^{p^{n-1}}a_2^{p^{n-2}}\dots a_n$ for some $a_j \in \gamma_j(F)$, and then we have $y^{-ip^{n-2}}x^{p^{n-2}}a_1^{p^{n-1}} \in \gamma_2(F)$. Write $a_1 = x^k y^l z$ for some $z \in \gamma_2(F)$ and some $k, l \in \mathbb{Z}$. Then

$$a_1^{p^{n-1}} = (x^k y^l z)^{p^{n-1}} \equiv x^{kp^{n-1}}y^{lp^{n-1}} \pmod{\gamma_2(F)}.$$

Thus $y^{-ip^{n-2}}x^{p^{n-2}}a_1^{p^{n-1}} \in \gamma_2(F)$ if and only if $y^{-ip^{n-2}}x^{p^{n-2}(1+kp)}y^{lp^{n-1}} \in \gamma_2(F)$, and this happens if and only if $y^{p^{n-2}(lp-i)}x^{p^{n-2}(1+kp)} \in \gamma_2(F)$. On the other hand, by Theorem 6.1.14, an element of the free group F belongs to $\gamma_2(F)$ if and only if the exponent sum of both generators is zero. Hence we get $p^{n-2}(1 + kp) = 0$, which is a contradiction. □

As a consequence of Lemma 6.2.1, x and y have order p^{n-1} modulo $\lambda_n(F)$.

By (6.2), if we want to know p^{n-2}nd powers of all elements outside $\lambda_2(F)$ in $F/\lambda_n(F)$, it is enough to know the power of each element in the set $\{y, xy^i \mid 0 \leq i \leq p-1\}$. Also, by Lemma 6.1.8, we have

$$(xy^i)^{p^{n-2}} \equiv x^{p^{n-2}}y^{ip^{n-2}} \pmod{\lambda_n(F)} \quad \text{for} \quad 1 \leq i \leq p-1,$$

and since $x^{p^{n-2}}$ and $y^{p^{n-2}}$ are linearly independent modulo $\lambda_n(F)$ by Lemma 6.2.1, the following lemma is straightforward.

Lemma 6.2.2. *If $G = F/\lambda_n(F)$, the power subgroups $M^{p^{n-2}}$ are all different and of order p in $\lambda_{n-1}(F)/\lambda_n(F)$, as M runs over the $p+1$ maximal subgroups of G. In particular, all elements in $G \setminus \Phi(G)$ are of order p^{n-1}.*

We are now ready to prove the main result regarding the free group on two generators.

Theorem 6.2.3. *A p-central quotient $F/\lambda_n(F)$ is a Beauville group if and only if $p \geq 5$ and $n \geq 2$.*

Proof. For simplicity let us call G the quotient group $F/\lambda_n(F)$. We first show that if $p = 2$ or 3, then G is not a Beauville group. By way of contradiction, suppose that $\{u_1, v_1\}$ and $\{u_2, v_2\}$ form a Beauville structure for G. Since G has $p + 1 \leq 4$ maximal subgroups, and there are 6 elements in the union of two triples $\{u_1, v_1, u_1v_1\}$ and $\{u_2, v_2, u_2v_2\}$ we may assume that u_1 and u_2 are in the same maximal subgroup. Then by (6.2), we have $\langle u_1^{p^{n-2}} \rangle = \langle u_2^{p^{n-2}} \rangle$, which is a contradiction.

Thus we assume that $p \geq 5$. First of all, notice that if $n = 2$, $G \cong C_p \times C_p$ is a Beauville group, by Catanese's criterion. So we will deal with the case $n \geq 3$. Let u and v be the images in G of x and y, respectively. We claim that $\{u, v\}$ and $\{uv^2, uv^4\}$ form a Beauville structure for G. If $A = \{u, v, uv\}$ and $B = \{uv^2, uv^4, uv^2uv^4\}$, we need to show that

$$\langle a^g \rangle \cap \langle b^h \rangle = 1, \tag{6.4}$$

for all $a \in A$, $b \in B$, and $g, h \in G$. Observe that a^g and b^h lie in different maximal subgroups of G in every case, since u and v are linearly independent modulo $\Phi(G)$ and $p \geq 5$.

Now, all elements $a \in A$ and $b \in B$ are of order p^{n-1}, by Lemma 6.2.2. If (6.4) does not hold, then

$$\langle (a^g)^{p^{n-2}} \rangle = \langle (b^h)^{p^{n-2}} \rangle,$$

and again by Lemma 6.2.2, a^g and b^h lie in the same maximal subgroup of G, which is a contradiction. We thus complete the proof that G is a Beauville group. □

We next turn our attention to the free product of two cyclic groups of order p.

Let $F = \langle x, y \mid x^p, y^p \rangle$ be the free product of two cyclic groups of order p. Notice that since F/F' has exponent p, we have $\lambda_n(F) = \gamma_n(F)$ for all $n \geq 1$, by Lemma 6.1.9.

We start with a general lemma.

Lemma 6.2.4. *Let $\psi\colon G_1 \to G_2$ be a group homomorphism, let $x_1, y_1 \in G_1$ and $x_2 = \psi(x_1)$, $y_2 = \psi(y_1)$. If $o(x_1) = o(x_2)$ then the condition $\langle x_2^{\psi(g)} \rangle \cap \langle y_2^{\psi(h)} \rangle = 1$ implies that $\langle x_1^g \rangle \cap \langle y_1^h \rangle = 1$ for $g, h \in G_1$.*

Proof. We argue by way of contradiction. Suppose that $1 \neq z_1 \in \langle x_1^g \rangle \cap \langle y_1^h \rangle$. Then $\psi(z_1) \in \langle x_2^{\psi(g)} \rangle \cap \langle y_2^{\psi(h)} \rangle = 1$, and hence $z_1 \in \operatorname{Ker} \psi$. Since $o(x_1) = o(\psi(x_1))$, it follows that $\langle x_1^g \rangle \cap \operatorname{Ker} \psi = 1$, thus $z_1 = 1$, a contradiction. □

Recall that if a p-group G is regular, then $\Omega_i(G) = \{x \in G \mid x^{p^i} = 1\}$, by Theorem 3.1.3. Thus any p-group G of class $< p$ satisfies $\exp \Omega_i(G) \leq p^i$, since it is regular. On the other hand, if a group G is not regular, we cannot guarantee that $\exp \Omega_i(G) \leq p^i$. However, we can still find a bound for the exponent of $\Omega_i(G)$, which is related with the class of G.

Lemma 6.2.5. [15, Theorem A] *Let G be a p-group. Then for every $i, k \geq 1$, the condition $\gamma_{k(p-1)+1}(G) = 1$ implies that*

$$\exp \Omega_i(G) \leq p^{i+k-1}.$$

A key ingredient of the proof of the main theorem will be based on p-groups of maximal class with some specific properties. Let $G = \langle s \rangle \ltimes A$ where s is of order p and $A \cong \mathbb{Z}_p^{p-1}$. The action of s on A is via θ, where θ is defined by the companion matrix of the pth cyclotomic polynomial $x^{p-1} + \cdots + x + 1$. Then G is the only infinite pro-p group of maximal class. Since $s^p = 1$ and $\theta^{p-1} + \cdots + \theta + 1$ annihilates A, this implies that for every $a \in A$,

$$(sa)^p = s^p a^{s^{p-1} + \cdots + s + 1} = 1.$$

Thus all elements in $G \smallsetminus A$ are of order p. An alternative construction of G can be given by using the ring of cyclotomic integers (see Example 7.4.14 [39]).

Let P be a finite quotient of G of order p^n for $n \geq 3$. Let us call P_1 the abelian maximal subgroup of P and $P_i = [P_1, P, \overset{i-1}{\ldots}, P] = \gamma_i(P)$ for $i \geq 2$. Then by Lemma 6.1.9, we have $\lambda_i(P) = \gamma_i(P)$ for all $1 \leq i \leq n$. Also we have the following.

Lemma 6.2.6. *Let P be as given above. Then every element in $P_i \smallsetminus P_{i+1}$ is of order $p^{\lceil \frac{n-i}{p-1} \rceil}$, and hence* $\exp P_i = p^{\lceil \frac{n-i}{p-1} \rceil}$.

Proof. Let x be an element in $P_i \smallsetminus P_{i+1}$. We will use reverse induction on i to show that $o(x) = p^{\lceil \frac{n-i}{p-1} \rceil}$. If $i = n-1$ then $o(x) = p^{\lceil \frac{n-(n-1)}{p-1} \rceil}$. Now assume that the result holds for all $j \geq i+1$. Let us take a uniform element s in P. Then $(sx)^p = 1$ because every element outside P_1 is of order p. Since P_1 is abelian, we have

$$1 = (sx)^p = s^p x^p [x,s]^{\binom{p}{2}} [x,s,s]^{\binom{p}{3}} \ldots [x, s, \overset{p-1}{\ldots}, s]^{\binom{p}{p}}.$$

As $s^p = 1$, we get

$$x^p = ([x,s]^{\binom{p}{2}} [x,s,s]^{\binom{p}{3}} \ldots [x, s, \overset{p-1}{\ldots}, s]^{\binom{p}{p}})^{-1}.$$

Then by Lemma 4.1.13, $[x, s, \overset{k}{\ldots}, s] \in P_{i+k} \smallsetminus P_{i+k+1}$ for all $1 \leq k \leq p-1$. By the reverse induction, we know that $P_j^p \leq P_{j+p-1}$ for all $j \geq i+1$. This implies that

$$x^p \in P_{i+p-1} \smallsetminus P_{i+p}. \tag{6.5}$$

Then again by the reverse induction, $o(x^p) = p^{\lceil \frac{n-i-p+1}{p-1} \rceil}$ and thus $o(x) = p^{\lceil \frac{n-i}{p-1} \rceil}$, as desired. □

Now we can begin to determine which p-central quotients of F are Beauville groups. We first assume that $p = 2$.

Lemma 6.2.7. *Let F be the free product of two groups of order 2. Then no p-central quotient of F is a Beauville group.*

Proof. The free product F of two cyclic groups of order 2 is the infinite dihedral group D_∞ by Lemma 6.1.24. Then by Theorem 2.1.7, no finite quotient of F is a Beauville group. □

In the remainder, we consider the case where p is an odd prime.

Lemma 6.2.8. *Let $G = F/\lambda_n(F)$ for $n \geq 2$. If u and v are the images of x and y in G, then for any $i, j \not\equiv 0 \pmod{p}$ all elements in the coset $u^i v^j \Phi(G)$ have order $p^{\left\lceil \frac{n-1}{p-1} \right\rceil}$.*

Proof. Let P be the p-group of maximal class of order p^n which is mentioned above and let $s \in P \smallsetminus P_1$ and $s_1 \in P_1 \smallsetminus P'$. Note that all elements in $P \smallsetminus P_1$ are of order p. Then by the universal property of the free product and since $i, j \not\equiv 0 \pmod{p}$, we can define a homomorphism $\psi : F \longrightarrow P$ such that $\psi(x^i) = s^{-1}$ and $\psi(y^j) = ss_1$. Since $\lambda_n(P) = 1$, if we call u and v the images of x and y in G, respectively, then the map

$$\begin{aligned} \overline{\psi} \colon G &\longrightarrow P \\ u^i &\longmapsto s^{-1} \\ v^j &\longmapsto ss_1, \end{aligned}$$

is well-defined and an epimorphism. Set $k = \left\lceil \frac{n-1}{p-1} \right\rceil$. Since $\overline{\psi}$ is an epimorphism, we have $\overline{\psi}(u^i v^j \Phi(G)) = \overline{\psi}(u^i v^j)\Phi(P) = s_1\Phi(P)$, where every element in the coset $s_1\Phi(P)$ has the same order as s_1, namely p^k. Then for every $g \in u^i v^j \Phi(G)$, we have $o(g) \geq o(s_1) = p^k$. On the other hand, $\gamma_{k(p-1)+1}(G) \leq \gamma_n(G) = 1$. Then by Lemma 6.2.5, together with $\Omega_1(G) = G$, we get $\exp G \leq p^k$. Consequently $o(g) = p^k$. □

We deal separately with the cases $p \geq 5$ and $p = 3$.

Theorem 6.2.9. *If $p \geq 5$ then the p-central quotient $F/\lambda_n(F)$ is a Beauville group for every $n \geq 2$.*

Proof. For simplicity let us call G the quotient group $F/\lambda_n(F)$. If $n = 2$ then $G \cong C_p \times C_p$ is a Beauville group, by Catanese's criterion. Thus we assume that $n \geq 3$.

Let u and v be the images of x and y in G, respectively. We claim that $\{u, v\}$ and $\{uv^2, uv^4\}$ form a Beauville structure for G. Let $A = \{u, v, uv\}$ and $B = \{uv^2, uv^4, uv^2uv^4\}$. Assume first that $a = u$ or v, which are elements of order p, and $b \in B$. If $\langle a^g \rangle \cap \langle b^h \rangle \neq 1$ for some $g, h \in G$, then $\langle a^g \rangle \subseteq \langle b^h \rangle$, and hence $\langle a\Phi(G) \rangle = \langle b\Phi(G) \rangle$, which is a contradiction since $p \geq 5$. Next we assume that $a = uv$. Let $\overline{\psi}$ be the homomorphism in the proof of Lemma 6.2.8. Since $p \geq 5$, for every $b \in B$ we have $\overline{\psi}(b) \in P \setminus P_1$, which is of order p. Thus for all $g, h \in G$ we have $\langle s_1^{\overline{\psi}(g)} \rangle \cap \langle \overline{\psi}(b)^{\overline{\psi}(h)} \rangle = 1$. Since $o(uv) = o(s_1)$, it then follows from Lemma 6.2.4 that $\langle a^g \rangle \cap \langle b^h \rangle = 1$. This completes the proof. $\square$

In order to deal with the prime 3, we need Lemma 2.3.2 and the following lemma.

Lemma 6.2.10. *Let G be a p-group which is not of maximal class such that $d(G) = 2$. Then for every $x \in G$ there exists $t \in \Phi(G) \setminus \{[x, g] \mid g \in G\}$.*

Proof. Note that a p-group has maximal class if and only if it has an element with centralizer of order p^2, by Theorem 4.1.4. Thus for every $x \in G$ we have $|C_G(x)| \geq p^3$, and hence

$$|\{[x, g] \mid g \in G\}| = |\operatorname{Cl}_G(x)| = |G : C_G(x)| \leq p^{n-3}.$$

Since $d(G) = 2$, we have $|\Phi(G)| = p^{n-2}$. Then there exists $t \in \Phi(G)$ such that $t \notin \{[x, g] \mid g \in G\}$. $\square$

Theorem 6.2.11. *Let $p = 3$. Then the following hold.*

(i) *The p-central quotient $F/\lambda_n(F)$ is a Beauville group if and only if $n \geq 4$.*

(ii) *The series $\{\lambda_n(F)\}_{n \geq 4}$ can be refined to a normal series of F such that two consecutive terms of the series have index p and for every term N of the series F/N is a Beauville group.*

Proof. Since the smallest Beauville 3-group is of order 3^5, the quotient $F/\lambda_n(F)$ can only be a Beauville group if $n \geq 4$. We first assume that $n = 4$. Now consider the group

$$H = \langle a, b, c, d, e \mid a^3 = b^3 = c^3 = d^3 = e^3 = 1, [b, a] = c, [c, a] = d, [c, b] = e \rangle,$$

where we have omitted all commutators between generators which are trivial. This is the smallest Beauville 3-group. Since $\lambda_4(H) = 1$, $F/\lambda_4(F)$ maps onto H. On the other hand, since $\lambda_i(F) = \gamma_i(F)$ for all $i \geq 1$ and $|\gamma_2(F) : \gamma_3(F)| = 3$, it is clear that $|F/\lambda_4(F)| \leq 3^5$ and so $F/\lambda_4(F) \cong H$. Consequently, $F/\lambda_4(F)$ is a Beauville group. Thus we assume that $n \geq 5$.

Now let us call G the quotient group $F/\lambda_n(F)$. Consider the map $\overline{\psi}\colon G \longrightarrow P$ defined in the proof of Lemma 6.2.8. Since $\overline{\psi}$ is an epimorphism, $\overline{\psi}(\lambda_{n-1}(G)) = \lambda_{n-1}(P)$. As a consequence, the subgroup $\operatorname{Ker}\overline{\psi} \cap \lambda_{n-1}(G)$ has index 3 in $\lambda_{n-1}(G)$, since $\lambda_{n-1}(P)$ is of order 3 . Choose an arbitrary normal subgroup N of F such that $\lambda_n(F) \leq N < \lambda_{n-1}(F)$ and $N/\lambda_n(F) \leq \operatorname{Ker}\overline{\psi}$. Then $\overline{\psi}$ induces an epimorphism $\widetilde{\psi}$ from F/N to P.

We will see that $L = F/N$ is a Beauville group, which simultaneously proves (i) and (ii). Let u and v be the images of x and y in L, respectively. Set $k = \lceil \frac{n-1}{2} \rceil$. Then $o(uv) \leq o(xy\lambda_n(F)) = 3^k$. On the other hand, since $\widetilde{\psi}(uv) = s_1$, we have $o(uv) \geq o(s_1) = 3^k$, and consequently we get $o(uv) = 3^k$ in L. Since $F/\lambda_4(F) \cong H$ is not of maximal class, L is not of maximal class. Thus, by Lemma 6.2.10, there exist $z, t \in \Phi(L)$ such that $z \notin \{[u,l] \mid l \in L\}$ and $t \notin \{[v,l] \mid l \in L\}$. We claim that $\{u, v\}$ and $\{(uz)^{-1}, vt\}$ form a Beauville structure for L. Let $A = \{u, v, uv\}$ and $B = \{(uz)^{-1}, vt, (uz)^{-1}vt\}$.

If $a = u$, which is of order 3, and $b = vt$ or $(uz)^{-1}vt$, then we get $\langle a^g \rangle \cap \langle b^h \rangle = 1$ for every $g, h \in L$, as in the proof of Theorem 6.2.9. When $a = v$ and $b = (uz)^{-1}$ or $(uz)^{-1}vt$, the same argument applies. If we are in one of the following cases: $a = u$ and $b = (uz)^{-1}$, or $a = v$ and $b = vt$, then the condition $\langle a^g \rangle \cap \langle b^h \rangle = 1$ follows from Lemma 2.3.2.

It remains to check the case when $a = uv$ and $b \in B$. For every $b \in B$, we have $\widetilde{\psi}(b) \in P \smallsetminus P_1$, which has order 3. Since $o(uv) = o(s_1)$, the condition $\langle a^g \rangle \cap \langle b^h \rangle = 1$ follows from Lemma 6.2.4, as in the proof of Theorem 6.2.9. This completes the proof. □

Thus the quotients in Theorem 6.2.11 constitute an infinite family of Beauville 3-groups of order 3^n for all $n \geq 5$.

Observe that if $p = 3$ then $o(uv) = o((uz)^{-1}vt) = p^k$, where $k = \left\lceil \frac{n-1}{p-1} \right\rceil$, by Lemma 6.2.8. Also if $p \geq 5$ then every element $b \in B$ in the proof of Theorem 6.2.9 has order p^k. Thus the signatures of the triples in the Beauville structures arising from Theorems 6.2.9 and 6.2.11 are unbounded as n goes to infinity. Consequently these examples are different from those of Stix and Vdovina given in page 9 , since in their examples the signatures of one of the triples of the Beauville structures take a constant value.

We finish this section by comparing the infinite family of Beauville 3-groups in Theorem 6.2.11 with the ones given in Chapter 5 by considering quotients of the Nottingham group over $\mathbb{F}_3$. Recall that by Theorem 5.2.8, $\mathcal{N}/\mathcal{N}_k$ is a Beauville group if and only if $k \geq 6$ and $k \neq z_m$ for all $m \geq 1$. Furthermore, by Theorems 5.2.9 and 5.2.10, for $i \geq 1$ there exists a normal subgroup $\mathcal{W}$ between $\mathcal{N}_{ip+3}$ and $\mathcal{N}_{ip+1}$ such that $\mathcal{N}/\mathcal{W}$ is a Beauville group. This gives quotients of $\mathcal{N}$ which are Beauville groups of every order 3^n with $n \geq 5$.

We will show that these two infinite families of Beauville 3-groups only coincide at the group of order 3^5.

Theorem 6.2.12. *Let $N \neq \gamma_4(F)$ be a normal subgroup of F such that F/N is a Beauville group. Then F/N is not isomorphic to any quotient of $\mathcal{N}$ which is a Beauville group. On the other hand, $F/\gamma_4(F)$ is isomorphic to $\mathcal{N}/\gamma_4(\mathcal{N})$.*

Proof. Since there is only one Beauville group of order 3^5, $F/\gamma_4(F)$ is necessarily isomorphic to $\mathcal{N}/\gamma_4(\mathcal{N})$. Now suppose that $F/N \cong \mathcal{N}/\mathcal{W}$ where $\gamma_n(F) \leq N < \gamma_{n-1}(F)$ for $n \geq 5$ and F/N is a Beauville group. Since F/N is of class $n-1$ and $\mathcal{W}$ lies between two consecutive terms of the lower central series, we have $\gamma_n(\mathcal{N}) \leq \mathcal{W} < \gamma_{n-1}(\mathcal{N})$. Note that if $n = 5$ then $\gamma_5(\mathcal{N}) \leq \mathcal{W} < \gamma_4(\mathcal{N})$, where $\gamma_5(\mathcal{N}) = \mathcal{N}_7$ and $\gamma_4(\mathcal{N}) = \mathcal{N}_6$, by Theorem 5.1.9. Thus in this case, we have $\mathcal{W} = \gamma_5(\mathcal{N})$. If $n > 5$ then $\mathcal{W} \leq \gamma_5(\mathcal{N})$. Consequently the isomorphism $F/N \cong \mathcal{N}/\mathcal{W}$ implies that $F/\gamma_5(F)N \cong \mathcal{N}/\gamma_5(\mathcal{N})$. We next show that this is not possible.

Recall that $\gamma_2(\mathcal{N}) = \mathcal{N}_3$ and by Theorem 5.1.12, $\mathcal{N}_3^3 = \mathcal{N}_9$. Then exponent of $\gamma_2(\mathcal{N}/\gamma_5(\mathcal{N}))$ is 3. On the other hand, as in the proof of Theorem 6.2.11, there is an epimorphism from $F/\gamma_5(F)N$ to a p-group of maximal class P of order 3^5 with $\exp P' = 3^2$. Thus $\mathcal{N}/\gamma_5(\mathcal{N})$ cannot be isomorphic to $F/\gamma_5(F)N$. □

REFERENCES

[1] T. M. Apostol. *Introduction to Analytic Number Theory*. Springer, 1976.

[2] N. Barker, N. Boston, and B. Fairbairn. A note on Beauville p-groups. *Experiment. Math.*, 21:298–306, 2012.

[3] N. Barker, N. Boston, N. Peyerimhoff, and A. Vdovina. An infinite family of 2-groups with mixed Beauville structures. *Int. Math. Res. Notices*, 11:3598–3618, 2015.

[4] I. Bauer, F. Catanese, and F. Grunewald. Beauville surfaces without real structures I. In *Geometric Methods in Algebra and Number Theory*, volume 235, pages 1–42. Progr. Math., Birkhäuser Boston, 2005.

[5] I. Bauer, F. Catanese, and F. Grunewald. Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory. *Mediterr. J. Math.*, 3:121–146, 2006.

[6] A. Beauville. Surfaces algébriques complexes, Astérisque. *Soc. Math. France, Paris*, 54, 1978.

[7] H. U. Besche, B. Eick, and E. A. O'Brien. The groups of order at most 2000. *Electron. Research Announc. Amer. Math. Soc.*, 7:1–4, 2001.

[8] H. U. Besche, B. Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[9] N. Boston. A survey of Beauville p-groups. In *Beauville Surfaces and Groups*, volume 123, pages 35–40. Springer Proceedings in Mathematics & Statistics, 2015.

[10] R. Brandl, A. Caranti, and C. M. Scoppola. Metabelian thin p-groups. *Quart. J. Math. Oxford*, 43:157–173, 1992.

[11] R. Camina. The Nottingham Group. In *New Horizons in Pro-p Groups*, volume 184, pages 205–221. Birkhäuser Boston, Cambridge, MA, 2000.

[12] A. Caranti, S. Mattarei, M. F. Newman, and C. M. Scoppola. Thin groups of prime-power order and thin Lie algebras. *Q. J. Math.*, 47(3):279–296, 1996.

[13] F. Catanese. Fibred surfaces, varieties isogenous to a product and related moduli spaces. *Amer. J. Math.*, 122:1–44, 2000.

[14] J. D. Dixon, M. P. F. Du Sautoy, A. Mann, and D. Segal. *Analytic Pro-p Groups*. Cambridge University Press, second edition, 1999.

[15] T. E. Easterfield. The orders of products and commutators in prime power groups. *Proc. Cambridge Phil. Soc.*, 36:14–26, 1940.

[16] M. Erickson. *Pearls of Discrete Mathematics*. CRC Press, 2010.

[17] B. Fairbairn. Recent work on Beauville surfaces, structures and groups. In *Groups St Andrews 2013*, volume 422, pages 225–241. London Mathematical Society Lecture Note Series, 2015.

[18] B. Fairbairn, K. Magaard, and C. Parker. Corrigendum: Generation of finite quasisimple groups with an application to groups acting on Beauville surfaces. *Proc. Lond. Math. Soc.*, 107(3):1220, 2013.

[19] B. Fairbairn, K. Magaard, and C. Parker. Generation of finite quasisimple groups with an application to groups acting on Beauville surfaces. *Proc. Lond. Math. Soc.*, 107(3):744–798, 2013.

[20] G. A. Fernández-Alcober. An introduction to finite p-groups: regular p-groups and groups of maximal class. *Math. Contemp.*, 20:155–226, 2001.

[21] G. A. Fernández-Alcober. Omega subgroups of powerful p-groups. *Israel J. Math.*, 162:75–79, 2007.

[22] Y. Fuertes and G. González-Diez. On Beauville structures on the groups S_n and A_n. *Math. Z.*, 264(4):959–968, 2010.

[23] Y. Fuertes and G. A. Jones. Beauville surfaces and finite groups. *J. Algebra*, 340:13–27, 2011.

[24] S. Garion, M. Larsen, and A. Lubotzky. Beauville surfaces and finite simple groups. *J. Reine Angew. Math.*, 666:225–243, 2012.

[25] G. González-Diez and A. Jaikin-Zapirain. The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces,. *Proc. Lond. Math. Soc.*, 111:775–796, 2015.

[26] J. González-Sánchez and A. Jaikin-Zapirain. On the structure of normal subgroups of potent p-groups. *J. Algebra*, 276:193–209, 2004.

[27] J. González-Sánchez and T. Weigel. Finite p-central groups of height k. *Israel J. Math.*, 181:125–143, 2011.

[28] R. Guralnick and G. Malle. Simple groups admit Beauville structures. *J. London Math. Soc.*, 85:649–721, 2012.

[29] D. F. Holt, B. Eick, and E. A. O'brien. *Handbook of Computational Group Theory*. Chapman & Hall/CRC Press.

[30] B. Huppert. *Endliche Gruppen, I.* Springer, 1967.

[31] B. Huppert and N. Blackburn. *Finite Groups II.* Springer-Verlag, 1982.

[32] I. M. Isaacs. *Finite Group Theory*, volume 92. Am. Math. Soc, 2008.

[33] D. L. Johnson. The group of formal power series under substitution. *J. Austral. Math. Soc.*, 45:296–302, 1988.

[34] G. Jones. Beauville surfaces and groups: a survey. In *Rigidity and Symmetry*, volume 70, pages 205–225. Springer, 2014.

[35] E. I. Khukhro. *p-Automorphisms of Finite p-Groups.* Cambridge University Press, 1998.

[36] B. Klopsch. Automorphisms of the Nottingham group. *J. Algebra*, 223:37–56, 2000.

[37] B. Klopsch. Normal subgroups in substitution groups of formal power series. *J. Algebra*, 228:91–106, 2000.

[38] C. R. Leedham-Green and S. McKay. On p-groups of maximal class II. *Q. J. Math*, 29(2):175–186, 1978.

[39] C. R. Leedham-Green and S. McKay. *The Structure of Groups of Prime Power Order*. Oxford University Press, 2002.

[40] A. Lubotzky and A. Mann. Powerful p-groups. I. Finite groups. *J. Algebra*, 105:484–505, 1987.

[41] W. Mangus, A. Karrass, and D. Solitar. *Combinatorial Group Theory: Presentations of groups in terms of generators and relations*. Dover Publications, Inc., second edition, 1976.

[42] H. Meier-Wunderli. Metabelsche Gruppen. *Comment. Math. Helv*, 25:1–10, 1951.

[43] R. J. Miech. Metabelian p-groups of maximal class. *Trans. Amer. Math. Soc.*, 151:331–373, 1970.

[44] R. J. Miech. Counting commutators. *Trans. Amer. Math. Soc.*, 189:49–61, 1974.

[45] M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee. Groups and nilpotent lie rings whose order is the sixth power of a prime. *J. Algebra*, 278:383–401, 2004.

[46] E. A. O'Brien and M. R. Vaughan-Lee. The groups with order p^7 for odd prime p. *J. Algebra*, 292:243–258, 2005.

[47] D. J. S. Robinson. *A Course in the Theory of Groups*. Springer, second edition, 1996.

[48] J. J. Rotman. *An Introduction to the Theory of Groups*. Springer, fourth edition, 1995.

[49] J. Stix and A. Vdovina. Series of p-groups with Beauville structure. *Monatsh. Math.*, 2015. doi:10.1007/s00605-015-0805-9, arXiv:1405.3872 [math.GR].

[50] M. Suzuki. *Group Theory II*. Springer, 1986.

[51] M. R. Vaughan-Lee. Nilpotent lie ring of order p^6, 2002. `http://www.math.auckland.ac.nz\penalty-\@M/~{}obrien/research/p7/p6.pdf`.

[52] M. Y. Xu. A class of semi-p-abelian p-groups. *Kexue Tongbao*, 27(2):142–146, 1982.

[53] I. O. York. The exponent of certain finite p-groups. *Proc. Edinb. Math. Soc. (2)*, 33:483–490, 1990.

[54] H. Zassenhaus. *The Theory of Groups*. Chelsea Publishing Company, 1958.

CURRICULUM VITAE

PERSONAL INFORMATION

Name, Surname: Şükran Gül

Nationality: Turkish (TC)

Date and Place of Birth: January 3, 1989, Isparta

Marital Status: Single

E-mail: gsukran@metu.edu.tr

EDUCATION

Degree	Institution	Year of Graduation
Minor	METU, Computer Engineering	2013
B.S.	METU, Mathematics	2012
High School	Milli Piyango Anatolian High School	2007

WORK EXPERIENCE

Year	Place	Enrollment
2012-2016	METU, Department of Mathematics	Research Assistant

FOREIGN LANGUAGES

English (fluent), Spanish (elementary)

AWARDS AND SCHOLARSHIPS

- 2012-2016, TÜBİTAK 2211-Domestic Doctorate Fellowship
- 2015 February- August, TÜBİTAK 2214/A-International Research Fellowship for Doctorate Students
- 2014, METU Graduate Courses Performance Award

- B.S. in Mathematics with high honors, METU, 2012
- 2009-2012, Scholarship of İstanbul Middle East Technical University Alumni Association

ACADEMIC VISITS

- University of the Basque Country, Bilbao, Spain
  June-July-September 2016
  February 2015- February 2016
  June-July 2014
  June-July 2013
- University of L'Aquila, L'Aquila, Italy
  November 2015

The visits were supported by TÜBİTAK, the Spanish Government, grant MTM2014-53810-C2-2-P, the Basque Government, grant IT974-16, and ERC Grant PCG-336983.

POSTER PRESENTATIONS

- Beauville structures in finite p-groups, April 2016, 4th Cemal Koç Algebra Days, Ankara, Turkey
- Beauville structures in p-central quotients, March 2016, Ischia Group Theory, Naples, Italy

CONFERENCE TALKS

- Beauville structures in finite p-groups, September 2016, XI Encuentro en Teoría de Grupos, Barcelona, Spain
- New results on Beauville p-groups, June 2015, Groups and Their Actions, Bedlewo, Poland
- Beauville structures in powerful p-groups and regular p-groups, July 2014, First Joint International Meeting RSME-SCM-SEMA-SIMAI-UM, Bilbao, Spain

PUBLICATIONS

- G.A. Fernández-Alcober and Ş. Gül, Beauville structures in finite p-groups, *Journal of Algebra (2016)*, doi:10.1016/j.jalgebra.2016.11.007, `arXiv:1507.02942v2 [math.GR]`.
- G.A. Fernández-Alcober, N. Gavioli, Ş. Gül and C. M. Scoppola, Beauville thin p-groups, in preparation.
- Ş. Gül, Beauville structures in p-central quotients, *J. Group Theory (2016)*, doi:10.1515/jgth-2016-0031, `arXiv:1604.06031 [math.GR]`.
- Ş. Gül, A note on strongly real Beauville p-groups, `arXiv:1607.08907 [math.GR]`.