On the Invariant Rings of Modular Bireflection Groups with Applications of Macaulay's Double Annihilator Correspondence

Christopher Lee

SMSAS

University of Kent

This dissertation is submitted for the degree of

Doctor of Philosophy

September 2019

Acknowledgements

I would like to thank my supervisors Peter Fleischmann and Jim Shank. Peter, for the opportunity to pursue this PhD, and for his patience, guidance and time over the years. Jim, for going above and beyond his responsibilities to make sure I can complete this thesis. I thank the EPSRC and the University of Kent for funding this PhD, and the latter also for providing the environment to make this possible.

I would like to specially thank Claire Carter for being understanding and her pep talks for making sure I stay on track.

And lastly, a big thank you to my family, especially to my mum, for keeping me going, through both the best and worst of times.

Abstract

Let V be a faithful finite-dimensional representation of a finite group G over an odd prime field k, and $S = k[V]$, the symmetric algebra on the dual V^*. Chapter 2 shows how to find the invariant ring S^G when G is an abelian unipotent two-row group. The invariant rings are complete intersections.

Chapter 3 shows an algorithm that computes the Macaulay inverse for any homogenous S_+-primary irreducible ideal of S. It will also be shown that the Hilbert ideal of the invariant rings of the abelian two-row groups from chapter 2 are complete intersection ideals with inverse monomials as Macaulay inverses.

Table of contents

1 Introduction **1**

1.1 Invariant rings 5

1.2 Macaulay's double annihilator correspondence 10

2 Invariant rings of abelian two-row groups **15**

2.1 One-column-extended case 19

2.2 Totally one-extended case 27

2.3 Subgroups with two-dimensional invariant subspace 35

2.3.1 Blocks with unsaturated columns 38

2.3.2 Blocks with saturated columns 52

2.4 Two-extended narrow blocks 72

2.5 Two-extended wide blocks 80

2.6 Subgroups with one-dimensional invariant subspace 94

3 Computing Macaulay inverses **99**

3.1 A constructing algorithm 99

3.2 Nakajima groups 101

3.3 Two-row groups 102

3.4 A type-two exceptional group 107

Symbols **116**

References **118**

Chapter 1

Introduction

In modular invariant theory, the main object of interest is the invariant subring of a polynomial ring under the action of a finite group. This invariant ring is constructed as follows: Let k be a field of characteristic p, and V be a faithful finite-dimensional representation of a finite group G over k. Fix a basis $\{v_1, \cdots, v_n\}$ for V. Write $B := \{x_1, \cdots, x_n\}$ for the dual basis in V^*. The (left) G-action on V induces a (left) G-action on V^* given by $(\sigma(x))\, v = x \cdot (\sigma^{-1}(v))$ for all $\sigma \in G$, $x \in V^*$ and $v \in V$. This extends to a G-action on the polynomial ring $S := \mathrm{Sym}(V^*) = k[V]$ whose G-invariant ring is $S^G := \{f \in S : \sigma(f) = f\}$.

For a fixed representation V^* of G, elements $\sigma \in G$ will be described by $n \times n$ matrices, acting on V^* from the left, with respect to the basis B.

Example 1.0.1. [6, 4.2] Let $n = 4$. Let $\sigma_1, \sigma_2 \in \mathrm{GL}(V)$ where

$$\sigma_1 := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ \sigma_2 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

so that $\sigma_1(x_3) = x_3 + x_1$ and $\sigma_2(x_4) = x_4 + x_2$. Let $N = \langle \sigma_1, \sigma_2 \rangle$ and $G = \langle \sigma_1 \sigma_2 \rangle$.

Their invariant rings are

$$\begin{aligned} S^{\langle\sigma_1\rangle} &= k\left[x_1, \quad x_2, \quad x_3^p - x_1^{p-1}x_3, \quad x_4\right], \\ S^N &= k\left[x_1, \quad x_2, \quad x_3^p - x_1^{p-1}x_3, \quad x_4^p - x_2^{p-1}x_4\right], \\ \text{and } S^G &= k\left[x_1, \quad x_2, \quad x_3^p - x_1^{p-1}x_3, \quad x_4^p - x_2^{p-1}x_4, \quad x_1x_4 - x_2x_3\right]. \end{aligned}$$

The group G is called the double transvection group.

The main open question in modular invariant theory is the classification of groups $G \leq \mathrm{GL}(V)$ whose invariant ring S^G is a polynomial algebra over k. Or more generally, invariant rings that are complete intersections.

Definition 1.0.2. A k-algebra R of Krull dimension n is a *complete intersection* if there is a k-algebra epimorphism $k[X_1, \cdots, X_m] \twoheadrightarrow R$ from a polynomial ring such that the kernel is generated by $m - n$ homogeneous elements. The kernel (the relation ideal of R) is then called a *complete intersection ideal.* The k-algebra R is *polynomial* if the epimorphism can be chosen such that $m = n$.

If an invariant ring S^G is polynomial or a complete intersection, then G must, respectively, be a reflection or bireflection group [4, 1.5.3 and 1.5.4].

Definition 1.0.3. An element $\sigma \in \mathrm{GL}(V)$ is a *(pseudo-)reflection* if its invariant subspace $V^{\langle\sigma\rangle} \leq V$ has codimension at most 1. It is a *bireflection* if the codimension is at most 2. A group $G \leq \mathrm{GL}(V)$ is a *reflection* group if it can be generated by reflections. It is a *pure reflection* group if it contains only reflections. Similarly for *(pure) bireflection* groups.

In the non-modular case, that is p being coprime to $|G|$ or $p = 0$, the Shephard-Todd-Chevalley theorem says that the groups with polynomial invariant rings are in fact precisely the reflection groups [15, 7.4.1]. This need not be true when G is modular [4, 8.2.4]. But if $k = \mathbb{F}_p$, there is a characterisation using Nakajima groups.

Definition 1.0.4. Let G be upper-triangular with respect to B. Let G_i denote its *one-column* subgroups at column i. That is,

$$G_i := \{\sigma_i \in G : \sigma_i(x_j) = x_j \text{ for } j \neq i\} \leq G.$$

The group G is *Nakajima (with respect to B)* if $G = G_n \cdots G_1$. More generally, the *Nakajima overgroup* of G, denoted by $\mathrm{Nak}_B^+(G)$, is the smallest Nakajima group (with respect to B) that contains G. It can be found as

$$\mathrm{Nak}_B^+(G) := \left\langle \sigma \in \mathrm{GL}(V) : \begin{array}{l} \sigma(x_i) = \tau(x_i) \text{ for some } \tau \in G \text{ and} \\ \sigma(x_j) = x_j \text{ for } j \neq i, \text{ for some } 1 \leq i \leq n \end{array} \right\rangle.$$

Theorem 1.0.5. [4, 8.0.7] Let G be upper-triangular with respect to B. The group G is Nakajima if and only if $S^G = k[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n]$, where $\boldsymbol{N}_i$ is the *G-orbit product* of x_i, for $i = 1, \cdots, n$, defined as

$$\boldsymbol{N}_i := \boldsymbol{N}_i^G := \prod_{y \in Gx_i} y.$$

Let more generally G be a p-group, but over $k = \mathbb{F}_p$. Then G is Nakajima with respect to some basis if and only if S^G is polynomial, by theorem [13, 1.4].

When G is a bireflection group, much less is known about S^G, even when restricted to prime fields $k = \mathbb{F}_p$. However, there were recent progress on pure bireflection groups over $\mathbb{F}_p$ with p odd. It involved characterising the pure bireflection groups, and then identifying the groups known to have a complete intersection invariant ring. The pure bireflection group characterisation is as follows.

Theorem 1.0.6. [9, 1.5] Let p be odd. Every finite unipotent pure bireflection p-group is one of the following: (1) a two-row group; (2) a two-column group; (3) a hook group; (4) an exceptional group of type one; or (5) of type two. (In the paper referenced, groups act on V^* from the right. So two rows in the references become two columns in our matrices, and vice versa.)

Only two-row groups will be defined here, as the focus of this thesis. To define them, write $[\sigma, f] := [\sigma - 1](f)$, for $\sigma \in \mathrm{GL}(V)$ and $f \in S$.

Definition 1.0.7. A group $G \leq \mathrm{GL}(V)$ is *two-row* if $\dim_{\mathbb{F}_p}[G, V^*] \leq 2$. Define

$$E := \left\{ \sigma = \left(\begin{array}{cc|c} 1 & a_2 & \multirow{2}{*}{M} \\ 0 & 1 & \\ \hline \multicolumn{2}{c|}{0} & I_{(n-2)\times(n-2)} \end{array} \right) \in \mathrm{GL}(V) : a_2 \in k, M \in k^{2\times(n-2)} \right\}.$$

Then E is the maximal unipotent two-row group with respect to B such that $[E, V^*] = \langle x_1, x_2 \rangle_k$. Every two-row group is congruent to a subgroup of E.

From the characterisation list in theorem 1.0.6, removing groups that are known to have a complete intersection invariant ring produces the following theorem.

Theorem 1.0.8. [8, 1.0.5] Suppose $k = \mathbb{F}_p$ with p odd. Let G be a (finite unipotent) pure bireflection p-group. If S^G is not a complete intersection, then G is one of the following: (1) a non-abelian two-row group; (2) an abelian two-row group that is not a reflection group; (3) a two-column group; or (4) an abelian hook group with $[G, [G, V^*]] \neq 0$.

This thesis will show that abelian two-row groups also have complete intersection invariant rings (theorem 2.6.5), thereby removing them from the list. There are cases for which this is already known, such as the double transvection group and the following symmetric square representation.

Theorem 1.0.9. [3, 3.3] Let $n = 3$. Let $G := \langle \tau \rangle$ where

$$\tau = \begin{pmatrix} 1 & c & c^2 \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix},$$

for some $c \in k$. The invariant ring S^G is a complete intersection given by

$$S^G := k[\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3, f],$$
$$\text{where } f = x_2^2 - x_1 x_3.$$

1.1 Invariant rings

Chapter 2 will show that every abelian subgroup of E is congruent to one of two forms of two-row groups whose invariant rings will then be be found. By looking at the invariants that generate the invariant ring as a k-algebra, it will follow that the invariant rings are complete intersections.

One of the common ways to find invariant rings is to change the problem to finding the invariant ring of a different group.

Proposition 1.1.1. [4, 11.0.1] Let p be prime. Let $H \leq G$ be a maximal proper subgroup of index at most p. Let $\sigma \in G \setminus H$. Suppose there is some $f \in S^H$ such that $g := [\sigma - 1](f)$ is in S^G. If $[\sigma - 1]\left(S^H\right) \subseteq Sg$, then $S^H = S^G[f]$.

Suppose $k = \mathbb{F}_p$. If S^G is a complete intsersection, then so is S^H, by proposition [16, 3.1.1].

This proposition allows us to find S^H by finding instead S^G for some appropriate choices of σ and f. This is useful for two-row groups, since there is always a Nakajima overgroup with known invariants. The inheritance of complete intersection property makes this a desirable proposition to use. For finding the invariant f mentioned in the proposition, the following theorem can be used.

Theorem 1.1.2. [2, 4.4] Let $k = \mathbb{F}_p$. Let G be a p-group with a polynomial invariant ring. Let $H < G$ be a maximal subgroup and $\sigma \in G \setminus H$. Consider the one-column subgroups $H_l \leq G_l$ for $l = 1, \cdots, n$. Let $l_1 < \cdots < l_s$ be the columns with strict inclusion $H_{l_j} < G_{l_j}$. Pick $\sigma_j \in G_{l_j} \setminus H_{l_j}$ for $j = 1, \cdots, s$ such that $\sigma_1, \cdots, \sigma_s$ and σ all lie in the same coset of H in G. Define $X_j = \left[\sigma_j H_{l_j}, x_{l_j}\right]$ as commutators on the respective columns, and let $Y_j = \left(\bigcup_{i=1}^{s} X_i\right) \setminus X_j$. Then $S^H = S^G[f]$ where [1]

$$f = \sum_{j=1}^{s} \left(\prod_{g \in Y_j} g \right) \boldsymbol{N}_{l_j}^{H_{l_j}}.$$

[1]The original theorem statement uses $\prod_{\tau \in H_{l_j}} \tau\left(x_{l_j}\right)$ in place of the orbit product $\boldsymbol{N}_{l_j}^{H_{l_j}}$. But since H_{l_j} is a one-column group at column l_j, this product is the same as the orbit product.

By proposition [10, 9], this function f satisfies

$$[\sigma, f] = \operatorname*{lcm}_{j=1}^{s} \left[\sigma_j, \boldsymbol{N}_{l_j}^{H_j}\right] = \operatorname*{lcm}_{\tau \in G_i \setminus H_i, \forall i} [\tau, x_i],$$

in which the right-most expression ranges over all elements in $G_i \setminus H_i$ over all i. It is a product of elements of V^* that are distinct up to an $\mathbb{F}_p$-multiple.

The inclusion of the commutator subspace in a principal ideal that is necessary for using proposition 1.1.1 is not always possible. Failing that, one can look for a localisation of the invariant ring instead. Under certain conditions on the leading terms of known invariants, it may be possible to find a k-algebra generating set of S^G by using one of a localisation.

Let $\mathrm{LM}(f)$ denote the leading monomial of a polynomial $f \in S$ (with respect to some term order). And $\mathrm{LT}(f)$ for the leading term. Define the *grevlex* (graded reverse lexicographical) monomial ordering on $k[x_1, \cdots, x_n]$ parametrised by $x_1 < \cdots < x_n$ as follows: given two monomials $f = x_1^{e_1} \cdots x_n^{e_n}$ and $f' = x_1^{e_1'} \cdots x_n^{e_n'}$, we say that $f < f'$ if and only if (1) $\deg(f) < \deg(f')$; or (2) the degrees are equal but $(e_1, \cdots, e_n) > (e_1', \cdots, e_n')$ lexicographically.

Theorem 1.1.3. [3, 1.1 and 1.2] Suppose $n > 1$ and G is a finite upper-triangular p-group with respect to B. Use grevlex order $x_i < x_{i+1}$. Let $\mathcal{B} = \{f_1, \cdots, f_m\}$ be a set of G-invariants such that

(1) $f_1 = x_1$;

(2) $\mathrm{LM}(f_i) = x_i^{e_i}$ with $e_i \geq 1$ for $i = 1, \cdots, n$, so that S^G is integral over $k[\mathcal{B}]$;

(3) $\mathrm{LM}(f_i) \in k[x_2, \cdots, x_n]$ for $i \neq 1$;

(4) $k\left[\mathcal{B}, x_1^{-1}\right] = S^G\left[x_1^{-1}\right]$.

Applying SAGBI/divide-by-x, to be defined in algorithm 1.1.8, on $\mathcal{B}$ results in a SAGBI basis say $\mathcal{B}_l$ for S^G, and $S^G = k[\mathcal{B}_l]$.

Before going into the SAGBI/divide-by-x algorithm, consider the preconditions of the theorem, with the group being investigated in mind, namely the abelian two-row groups over $k = \mathbb{F}_p$. The groups are unipotent and an orbit product $\boldsymbol{N}_i$ always has $x_i^{e_i}$ as its leading term for some p-power e_i. So conditions (1) and (2) are always possible. The remaining two conditions are less simple. Condition (3) requires carefully choosing a basis together with invariants on a case by case basis. For condition (4), there is a helpful theorem for finding the localisation. Write $S[i]$ for the polynomial subring $k[x_j : 1 \leq j \leq i] \leq S$.

Theorem 1.1.4. [5, 2.4 and 2.3] Let $G \leq \mathrm{GL}(V)$ be a unipotent p-group. Let $f_1, \cdots, f_n$ be homogeneous G-invariants. If each f_i is in $S[i]^G$ and its degree in x_i is positive and minimial amongst invariants in $S[i]^G$, then

$$\begin{aligned} \mathrm{Quot}\left(S^G\right) &= \mathrm{Quot}\left(k\left[f_1, \cdots, f_n\right]\right), \\ \text{and } S^G\left[f^{-1}\right] &= k\left[f_1, \cdots, f_n, f^{-1}\right], \end{aligned}$$

for some $f \in S^G$. If, furthermore, g_i is the leading coefficient of f_i as a polynomial in x_i over $S[i-1]$ for $i = 1, \cdots, n$, then we can also write instead

$$S^G\left[g_i^{-1} : 1 \leq i \leq n\right] = k\left[f_i, g_i^{-1} : 1 \leq i \leq n\right].$$

For two-row groups, since G is unipotent so that $x_1 \in S^G$, if every g_i is a power of x_1, then it simplifies to $S^G\left[x_1^{-1}\right] = k\left[f_1, \cdots, f_n, x_1^{-1}\right]$. Making this possible is again a matter of carefully choosing the invariants.

Back to the SAGBI/divide-by-x algorithm. It attempts to compute a SAGBI basis for a k-algebra R using what is called subductions on a generating set $\mathcal{B}$.

Definition 1.1.5. Let $R \leq S$ be a k-subalgebra and $\mathcal{B} = \{f_1, \cdots, f_s\} \subseteq R$ for some s. Then $\mathcal{B}$ is a *SAGBI basis* for R if the leading term algebra of R can be generated by $\{\mathrm{LT}(f) : f \in \mathcal{B}\}$. It is a Subalgebra Analogue of Gröeber Bases for Ideals.

As the name suggests, a *subduction* over $\mathcal{B}$ is similar to reduction by an ideal $I = \sum_{h \in \mathcal{B}} Rh \trianglelefteq R$. Both of them finds a polynomial $g = f - h$ for some $h \in R$ such that $\mathrm{LT}(g)$ is smaller than every element in $\mathrm{LT}(\mathcal{B})$ with respect to a chosen monomial order. When reducing, $h \in I$. When subducting, $h \in k[\mathcal{B}]$ instead.

Algorithm 1.1.6. (Subduction algorithm [4, 5.1.6]).

(In) A polynomial $f \in S$ to subduct over a finite set $\mathcal{B} = \{f_1, \cdots, f_s\} \subset S$.

(Out) A polynomial $g \in S$, called a *subduction* of f over $\mathcal{B}$, such that

(a) $\mathrm{LT}\,(g)$ cannot be factorised over $\mathrm{LT}\,(\mathcal{B})$; and

(b) $g = f - h$, for some element $h \in k\,[\mathcal{B}]$.

(1) Set $g := f$ and $h = 0$.

(2) If $g = 0$ or if $\mathrm{LT}\,(g)$ cannot be factorised over $\{\mathrm{LT}\,(f_i)\}_{i=1}^{s}$, then done.

(3) Write $\mathrm{LT}\,(g) = c\prod_{i=1}^{s} \mathrm{LT}\,(f_i)^{e_i}$, for some $c \in k$ and $e_i \geq 0$. Set

$$h := h + c \cdot \prod_{i=1}^{s} f_i^{e_i} \text{ and } g := g - c \cdot \prod_{i=1}^{s} f_i^{e_i}.$$

Go to step (2).

If f is in R, then so is the output g, because h is. If furthermore g is non-zero, then its leading term does not lie in $k\,[\mathrm{LT}\,(f_i) : i = 1, \cdots, s]$ by construction, and g is a potential candidate to be added to $\mathcal{B}$ to form a SAGBI basis for R. The SAGBI/divide-by-x algorithm subducts tête-a-tête differences for potential candidates.

Definition 1.1.7. A *tête-a-tête* over $\mathcal{B}$ is a pair of distinct factorisation of a monomial in S using $\mathrm{LT}\,(f_1), \cdots, \mathrm{LT}\,(f_s)$ as factors. That is,

$$\prod_{i=1}^{s} \mathrm{LT}\,(f_i)^{e_i} = c\prod_{i=1}^{s} \mathrm{LT}\,(f_i)^{e_i'},$$

for some exponents $e_i, e_i' \geq 0$ and $c \in k$. The tête-a-tête is *trivial* if both $e_i \geq 1$ and $e_i' \geq 1$ hold at the same time for some i. The polynomial

$$\prod_{i=1}^{s} f_i^{e_i} - c\prod_{i=1}^{s} f_i^{e_i'}$$

is then called a *tête-a-tête difference.*

If $R = k\,[\mathcal{B}]$, then the set $\mathcal{B}$ is a SAGBI basis for R if and only if every tête-a-tête difference over $\mathcal{B}$ subducts to zero over $\mathcal{B}$. And to check that every tête-a-tête difference subducts to zero, it is sufficient to check the non-trivial tête-a-têtes. The SAGBI algorithm finds a SAGBI basis by adjoining to the set $\mathcal{B}$ non-zero subductions of non-trivial tête-a-tête differences until every tête-a-tête difference subducts to zereo.

Algorithm 1.1.8. (SAGBI [4, 5.1.7]/divide-by-x [3, after 1.1]). Assume $n > 1$ and use the grevlex order $x_i < x_{i+1}$. (The x refers to the smallest x_i. So x_1.)

(In) Let $\mathcal{B} = \{f_1, \cdots, f_m\} \subseteq S^G$ be a finite homogeneous set of invariants satisfying the precondition of theorem 1.1.3.

(Out) A sequence $(\mathcal{B} = \mathcal{B}_0, \mathcal{B}_1, \cdots)$ of sets of homogeneous invariants in S^G satisfying the chain condition $k[\mathcal{B}_0] \leq k[\mathcal{B}_1] \leq \cdots$ The sequence terminates, and the last subset in the sequence, that is $\mathcal{B}_i$ when the algorithm terminates, is a SAGBI basis for S^G.

(1) Set $i = 0$ and $\mathcal{B}_0 := \mathcal{B}$.

(2) Let $\overline{\mathcal{B}}$ be the set of non-trivial tête-a-tête differences over $\mathcal{B}_i$.

(3) Replace every element in $\overline{\mathcal{B}}$ by its subduction over $\mathcal{B}_i$.

(4) If $\overline{\mathcal{B}} = \{0\}$, then the sets constructed so far are the output, and done.

(5) Replace every f in $\overline{\mathcal{B}}$ by $x_1^{-\deg_{x_1}(\mathrm{LT}(f))} f$, so that the new f has a leading monomial with exponent 0 for x_1. (This is the "divide-by-x" part.)

(6) Set $\mathcal{B}_{i+1}$ to $\mathcal{B}_i \cup \overline{\mathcal{B}}$.

(7) For each $f \in \overline{\mathcal{B}}$ in any order, remove f from $\mathcal{B}_{i+1}$ if the subduction of f over $\mathcal{B}_{i+1} \setminus \{f\}$ is zero.

(8) Increase i by one and go to step (2).

We have some observations to step (7). It is an optional step. Any polynomial removed in this step is redundant in the resulting SAGBI basis. So this step reduces the number of unnecessary subductions in step (2) in further iterations. Furthermore, we can allow removal of elements in $\mathcal{B}_i$ in step (7). That is, we iterate through f in $\mathcal{B}_{i+1}$ instead of just $\overline{\mathcal{B}}$. Even though $\mathcal{B}_{i+1}$ may not contain $\mathcal{B}_i$ anymore after step (7), we still have $k[\mathcal{B}_i] \leq k[\mathcal{B}_{i+1}]$ by construction of $\mathcal{B}_{i+1}$, and the algorithm is still guaranteed to terminate using chain condition.

Another observation is to step (2). By skipping step (4) which is the only step with a termination condition, not all non-trivial tête-a-têtes need to be found in step (2). Any tête-a-tête missed will need to be checked by the next iteration of step (2) if the algorithm is to terminate, or the tête-a-tête becomes irrelevant because of removals in the new step (7). Together with the above observation on step (7), it means tête-a-tête differences can be added to and removed from the input set as we find new and redundant invariants. Sections 2.4 and 2.5 will make heavy use of this SAGBI/divide-by-x algorithm to find the invariant rings of certain abelian two-row groups that we will define as "blocks" in definition 2.3.1.

1.2 Macaulay's double annihilator correspondence

In order to classify groups G with polynomial invariant rings S^G, many conditions equivalent to S^G being polynomial were found. In the non-modular case, one such condition is on the coinvariant ring, defined as follows. The *Hilbert ideal* of the ring extension $S \geq S^G$ is the ideal $S_+^G S \trianglelefteq S$ generated by the homogeneous non-constant polynomials in S^G. Its corresponding fibre algebra $S_G := S/S_+^G S$ is called the *G-coinvariant ring.* The following always hold.

$$\begin{aligned} S^G \text{ is polynomial } &\implies S_G \text{ is a complete intersection} \\ &\implies S_G \text{ is a Poincaré-duality algebra, defined as follows.} \end{aligned}$$

Definition 1.2.1. [12, p. 1] Let $P = S/I$ for some homogeneous ideal $I \trianglelefteq S$. Write $P = \bigoplus_{i=0}^{\infty} P_i$ as a direct sum of its homogeneous components. The k-algebra P satisfies *Poincaré duality* of *formal dimension* (or *top degree*) t if

(1) $P_i = 0$ for $i > t$, so that it is Artinian;

(2) $\dim_k (P_t) = 1$; and

(3) For all $i = 0, \cdots, t$, the natural multiplication $P_i \otimes P_{t-i} \to P_t$ is non-

singular in the sense that, for each $f_i \in P_i$, we have $f_i = 0$ if and only $f_i \cdot P_{t-i} = 0$.

For the purpose of looking at coinvariant rings, S_G is a Poincaré-duality algebra if and only if the ideal $S_+^G S$ is S_+-primary irreducible [12, VI.3.2], where S_+ is the maximal homogeneous polynomial ideal $S_+ = \sum_{i=1}^n Sx_i \lhd S$.

When G is non-modular, S^G is polynomial if S_G satisfies Poincaré-duality [11, 3.8], giving converses. In the modular case, it is only conjectured that S_G is a complete intersection if it has Poincaré-duality [14, 8]. Or in terms of the Hilbert ideal, the conjecture is that $S_+^G S$ is a complete intersection ideal whenever it is irreducible. This relates invariant theory to a different open problem — the classification of Macaulay inverses for complete intersection ideals.

First, start with some structures for introducing Macaulay inverses. Let $S^{-1} := k\left[x_1^{-1}, \cdots, x_n^{-1}\right]$ be the inverse polynomial ring. Denote monomials by $x^{\boldsymbol{e}} := x_1^{e_1} \cdots x_n^{e_n}$ where $\boldsymbol{e} = (e_1, \cdots, e_n)$ is an n-tuple of integers. Write $|\boldsymbol{e}| = e_1 + \cdots + e_n$ for their degrees. The inverse polynomial ring S^{-1} can be equipped with a (left) S-module structure defined by

$$x^{\boldsymbol{e}} \cap x^{-\boldsymbol{f}} = \begin{cases} x^{-(\boldsymbol{f}-\boldsymbol{e})}, & \text{if } \boldsymbol{f}-\boldsymbol{e} \in \mathbb{Z}_{\geq 0}^n, \\ 0, & \text{otherwise,} \end{cases}$$

where $\boldsymbol{e}, \boldsymbol{f} \in \mathbb{Z}_{\geq 0}^n$. Using this action, it is possible to define the S-modules

$$\operatorname{Ann}_S(\gamma) := \{f \in S : f \cap \gamma = 0\} \text{ for each } \gamma \in S^{-1},$$
$$\text{and } \operatorname{Ann}_{S^{-1}}(I) := \left\{\gamma \in S^{-1} : f \cap \gamma = 0\right\} \text{ for each } I \trianglelefteq S.$$

And now for the Macaulay duality which defines the Macaulay inverses. Let $\mathcal{M}$ be the collection of all non-trivial homogeneous cyclic S-submodules of S^{-1}. Its elements are of the form $S \cdot \gamma$ for some non-zero homogeneous $\gamma \in S^{-1}$. Let $\mathcal{I}$ be the collection of all homogeneous S_+-primary irreducible ideals of S.

Theorem 1.2.2. [12, VI.1.2] There is a bijection

$$\begin{aligned} \mathcal{M} &\to \mathcal{I} \\ S \cdot \gamma &\mapsto \operatorname{Ann}_S(\gamma) \\ \operatorname{Ann}_{S^{-1}}(I) &\leftarrow\!\shortmid I, \end{aligned}$$

where $\gamma \in S^{-1}$ is non-zero and homogeneous.

This bijection is called Macaulay's double annihilator correspondence. If $S \cdot \gamma$ is the inverse image of some $I \in \mathcal{I}$ under this correspondence, then γ is called a *Macaulay inverse* for I, unique up to a k-multiple. This correspondence is a consequence of a similar bijection within the polynomial ring S itself.

Theorem 1.2.3. [12, I.2.1] Let $I \trianglelefteq S$ be a homogeneous S_+-primary ideal. Write, for the set of its over-ideals, $\operatorname{over}(I) = \{J \trianglelefteq S : I \trianglelefteq J\}$.

(1) The ideal I is irreducible if and only if the set $\operatorname{over}(I) \setminus \{I\}$ has a unique minimal when ordered by inclusion.

Suppose I is irreducible.

(2) There is an involution on $\operatorname{over}(I)$ given by

$$\begin{aligned} \Xi : \operatorname{over}(I) &\to \operatorname{over}(I) \\ \Xi(J) &= (I : J) \end{aligned}$$

(3) $J \in \operatorname{over}(I)$ is irreducible if and only if $\Xi(J) = I + Sf$ for some homogeneous polynomial $f \in S$.

Back to the open problem, which is classifying the inverse polynomials that correspond to complete intersection ideals under Macaulay's double annihilator correspondence. There have been few examples of Macaulay inverses of complete intersection ideals [7, 1]. There is a known algorithm [12, section VI.2], using what are called Catalecticant matrices, to compute $\operatorname{Ann}_S(\gamma)$ from a given non-zero homogeneous $\gamma \in S^{-1}$. This thesis introduces a converse, algorithm 3.1.2, to compute the Macaulay inverse when given $I \in \mathcal{I}$. By applying it to complete intersection ideals, many more examples can be found.

In terms of invariant theory, this means a non-zero homogeneous inverse polynomial can be assigned to every coinvariant ring that satisfies Poincaré duality. For example, we will show that Nakajima groups are assigned inverse monomials. The abelian two-row groups over $\mathbb{F}_p$ with p odd, with knowledge of their invariant rings to be found in chapter 2, also has inverse monomials as the Macaulay inverse for the Hilbert ideal of their invariant rings with respect to some basis. Consequently, they have complete intersection coinvariant rings.

Slightly more is true. It will be shown that, over $\mathbb{F}_p$, most of the abelian two-row groups in fact satisfy $S_+^G S = S_+^{\mathrm{Nak}_B^+(G)} S$ with respect to some basis B. It will use the property that $[G, V^*] \leq (V^*)^G$, which gives "nice"-ness of those groups in the following sense.

Definition 1.2.4. [8, 3.0.6], Let G be an upper triangular p-group (with respect to B). Then G is *nice* (with respect to B) if $\left[\mathrm{Nak}_B^+(G), \mathrm{Nak}_B^+(G)\right] \leq G$.

Lemma 1.2.5. [8, 3.0.16], If $[G, V^*] \leq (V^*)^G$, then G is nice.

Lemma 1.2.6. [8, 3.0.11], If G is nice, then $\boldsymbol{N}_i^G = \boldsymbol{N}_i^{\mathrm{Nak}_B^+(G)}$ for $i = 1, \cdots, n$.

There are some other pure bireflection groups that have this property that $S_+^G S = S_+^{\mathrm{Nak}_B^+(G)} S$ holds in some basis B. For example, the exceptional group of type two over $\mathbb{F}_p$ with p odd. We define such groups for odd p here. Set $n = 6$ and $p \neq 2$. Given $a, b, c \in k$, define

$$\omega_{a,b,c} := \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & a & -c & 0 \\ 0 & 1 & 0 & 0 & b & a \\ 0 & 0 & 1 & b & 0 & c \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \in \mathrm{GL}(V).$$

Let $\Omega := \{\omega_{a,b,c} : a, b, c \in k\}$. It forms a group using the following property.

Lemma 1.2.7. [8, 2.6.1] $w_{a,b,c}w_{a',b',c'} = w_{a+a',\ b+b',\ c+c'}$ for all $a, b, c, a', b', c' \in k$.

Definition 1.2.8. [8, 2.2.5 and 2.6.4]. Let p be odd. A group $G \leq \mathrm{GL}(V)$ is an *exceptional (pure bireflection) group of type two* if it is congruent to a subgroup of Ω that contains $\omega_{1,0,0}$, $\omega_{0,1,0}$ and $\omega_{0,0,c}$ for some non-zero $c \in k$.

If $k = \mathbb{F}_p$ with p odd, then $G = \Omega$ is the only exception group of type two and its invariant ring is known.

Theorem 1.2.9. [8, 6.2.3]. Let $k = \mathbb{F}_p$. Let $G = \langle \omega_{1,0,0}, \omega_{0,1,0}, \omega_{0,0,1} \rangle$. Then S^G is a complete intersection, generated as a k-algebra by $\boldsymbol{N}_1^G, \cdots, \boldsymbol{N}_6^G$, and

$$\begin{aligned} f_1 &:= \left(x_5^p - x_1^{p-1}x_5\right)\left(x_3^p - x_1^{p-1}x_3\right) - \left(x_4^p - x_1^{p-1}x_4\right)\left(x_2^p - x_1^{p-1}x_2\right), \\ f_2 &:= \left(x_5^p - x_1^{p-1}x_5\right)x_3 + \left(x_6^p - x_3^{p-1}x_6\right)x_1 \\ &\qquad - \left(x_2^p - x_3^{p-1}x_2\right)x_4 - \left(x_2^p - x_1^{p-1}x_2\right)x_4 - \left(x_4^p - x_2^{p-1}x_4\right)x_2 \end{aligned}$$

and $f_3 := x_1x_6 - x_2x_4 + x_3x_5$.

Using niceness, we can see that, over $\mathbb{F}_p$ with p odd, the exceptional group of type two has the same Hilbert ideal as that of its Nakajima overgroup with respect to the given basis. It will be shown that this is true for certain exceptional groups of type two over finite fields, also using niceness, giving hopes that this may hold for more pure bireflection groups.

Chapter 2

Invariant rings of abelian two-row groups

Let $k = \mathbb{F}_p$ with p odd.[1] Let $E \leq \mathrm{GL}(V)$ be the maximal unipotent two-row group with respect to B defined in 1.0.7. This chapter will find the invariant rings of all abelian subgroups of E up to a congruence and show that they are all complete intersections. The overall strategy is to decompose each subgroup $G \leq E$ in a way similar to a direct sum decomposition, so that finding the invariant rings of the components in the decomposition is sufficient for determining S^G.

Let $F \leq E$ be the abelian subgroup that fixes $\langle x_1, x_2 \rangle_k$. It consists of elements of E with a zero in entry $(1,2)$ of its matrix representation. The decomposition of subgroups of F will be into three components. Sections 2.1 and 2.2 will find the invariant ring of the first component. Section 2.3 will describe the whole decomposition using the first component as a starting point and then find the invariant ring of the second component. Sections 2.4 and 2.5 will deal with the third component. Section 2.6 will then find S^G for any remaining abelian subgroups $G \leq E$ and then summarise the findings of this chapter.

So most of this chapter will be on investigating the subgroups of F. We introduce some notations to make describing its elements easier.

Notation 2.0.1. Let $T(\sigma)$ denote the *tail matrix* of $\sigma \in F$ which is defined as

[1] Throughout this chapter, we will sometimes use $\mathbb{F}_p$ instead of k as appropriate, to highlight difficulties in generalising to larger base fields $k \neq \mathbb{F}_p$.

the sub-matrix of σ of rows $1, 2$ and columns $3, \cdots, n$. Tail matrices uniquely identify elements of F, so we write as short-hand

$$\sigma = [T(\sigma)] = \left[\begin{pmatrix} a_3 & a_4 & \cdots & a_n \\ b_3 & b_4 & \cdots & b_n \end{pmatrix}\right].$$

We refer to column $j-2$ of the tail matrix as column j (of σ), to be consistent with its column index in σ. If only columns say i to j are possibly non-zero, we also write, for brevity

$$\left[\begin{pmatrix} a_i & \cdots & a_j \\ b_i & \cdots & b_j \end{pmatrix}_j\right] = \left[\begin{pmatrix} 0 & \cdots & 0 & a_i & \cdots & a_j & 0 & \cdots & 0 \\ 0 & \cdots & 0 & b_i & \cdots & b_j & 0 & \cdots & 0 \end{pmatrix}\right].$$

For example, $\sigma = \left[\binom{a_j}{b_j}_j\right]$ is a one-column reflection at column j. If the non-zero columns are sparse, we use addition. For example, for $i < j$,

$$\left[\begin{pmatrix} a_i \\ b_i \end{pmatrix}_i + \begin{pmatrix} a_j \\ b_j \end{pmatrix}_j\right] = \left[\begin{pmatrix} a_i & 0 & \cdots & 0 & a_j \\ b_i & 0 & \cdots & 0 & b_j \end{pmatrix}_j\right] = \left[\begin{pmatrix} a_i \\ b_i \end{pmatrix}_i\right]\left[\begin{pmatrix} a_j \\ b_j \end{pmatrix}_j\right],$$

since products in F correspond to sums of tail matrices. Outside of matrices, we will also write as short-hand $\binom{a}{b} = ax_1 + bx_2$.

Using the correspondence of group operations, we can find a natural group isomorphism between the multiplicative group F and the additive group $T(F)$. The latter can be written as a direct sum say

$$T(F) = \left\{\begin{pmatrix} a_3 & \cdots & a_i \\ b_3 & \cdots & b_i \end{pmatrix} : a_j, b_j \in k\right\} \oplus \left\{\begin{pmatrix} a_{i+1} & \cdots & a_n \\ b_{i+1} & \cdots & b_n \end{pmatrix} : a_j, b_j \in k\right\}.$$

Each component of this direct sum corresponds to a subgroup of F. The aforementioned decomposition of F is based on this type of correspondence:

Notation 2.0.2. Let G' and G'' be unipotent two-row groups acting on k-vector spaces say $\langle x'_1, \cdots, x'_{n'}\rangle_k$ and $\langle x''_1, \cdots, x''_{n''}\rangle_k$ respectively of dimensions n' and n'' both at least three, such that G' fixes x'_1, x'_2 and G'' fixes x''_1, x''_2. Their product

$G' \times G''$ has a natural representation on the space $\langle x'_1, \cdots, x'_{n'},\ x''_1, \cdots, x''_{n''}\rangle_k$ of dimension $n' + n''$. By identifying x'_1 with x''_1 and x'_2 with x''_2, the action of $G' \times G''$ on the space $\langle x'_1, \cdots, x'_{n'},\ x''_3, \cdots, x''_{n''}\rangle_k$ can be seen as a subgroup of F with $n = n' + n'' - 2$. Write $G' \boxtimes G''$ for this subgroup.

Lemma 2.0.3. The invariant ring of $G' \boxtimes G''$ is

$$\begin{aligned} & k\left[x'_1, \cdots, x'_{n'},\ x''_3, \cdots, x''_{n''}\right]^{G' \boxtimes G''} \\ &= k\left[x'_1, \cdots, x'_{n'}\right]^{G'} \otimes_{k\left[x'_1, x'_2\right]} k\left[x'_1, x'_2, x''_3, \cdots, x''_{n''}\right]^{G''}. \end{aligned}$$

Proof. Let $S = k\left[x'_1, \cdots, x'_{n'}, x''_3, \cdots, x''_{n''}\right]$. Identifying x'_1 with x''_1 and x'_2 with x''_2 gives $S^{G' \boxtimes G''} = S^{G' \times G''} = \left(S^{G'}\right)^{G''}$. Since G' acts trivially on $\langle x''_1, \cdots, x''_{n''}\rangle_k$,

$$\begin{aligned} \left(S^{G'}\right)^{G''} &= \left(k\left[x'_1, \cdots, x'_{n'}\right]^{G'}\left[x''_3, \cdots, x''_{n''}\right]\right)^{G''} \\ &= \left(k\left[x'_1, \cdots, x'_{n}\right]^{G'} \otimes_{k\left[x'_1, x'_2\right]} k\left[x'_1, x'_2, x''_3, \cdots, x''_{n''}\right]\right)^{G''}. \end{aligned}$$

And since G'' acts trivially on $k\left[x'_1, \cdots, x'_{n'}\right]$, the right-hand side expands to the tensor product in the lemma, as required. □

By decomposing a group $G \leq F$ into a $\boxtimes$-product, we can reduce the problem of finding S^G into finding the invariants of smaller groups. Given a group G, including when $G = F$, define a subgroup chain $1 = G[2] \leq \cdots \leq G[n] = G$ by

$$\begin{aligned} G[i] &:= \{\sigma \in G : \sigma \text{ fixes } x_j \in B \text{ for } j > i\} \\ &= \left\{ \left[\begin{pmatrix} * & \cdots & \overbrace{*}^{\text{Column } i} & 0 & \cdots & 0 \\ * & \cdots & * & 0 & \cdots & 0 \end{pmatrix} \right] \in G \right\} \text{ if } G \leq F. \end{aligned}$$

The way we split a group $G \leq F$ into a $\boxtimes$-product will be to find a basis of V^* with respect to which $G = \langle G[m_0], G'\rangle$ for some subgroup $G' \leq G$ that fixes $x_1, \cdots, x_{m_0}$ for some i. With this, we can write $G = G[m_0] \boxtimes G'$, in which we naturally restrict the action of $G[m_0]$ to $\langle x_1, \cdots, x_{m_0}\rangle_k$ and of G' to $\langle x_1, x_2,\ x_{m_0+1}, \cdots, x_n\rangle_k$.

To build the subgroup chain, we will find $\sigma_i, \tau_i \in G$ such that $G[i] = \langle G[i-1], \sigma_i, \tau_i \rangle$, usually in increasing order of $i = 3, \cdots, n$. Two elements (both possibly trivial) for each i will be sufficient because of the following lemma.

Lemma 2.0.4. Let $i = 3, \cdots, n$. Then $[G[i] : G[i-1]] = 1$, p or p^2.

Proof. Since G is a p-group, $[G[i] : G[i-1]]$ is a p-power. Suppose it is p^3. Then $G[i] = \langle G[i-1], \sigma, \sigma', \sigma'' \rangle$, for some $\sigma, \sigma', \sigma'' \notin G[i-1]$. Consider their actions on x_i. Write $\sigma = \left[\begin{pmatrix} \cdots c_i \\ \cdots d_i \end{pmatrix}_i \right]$ and $\sigma' = \left[\begin{pmatrix} \cdots c'_i \\ \cdots d'_i \end{pmatrix}_i \right]$, and similarly for σ''. We have three elements $\begin{pmatrix} c_i \\ d_i \end{pmatrix}$, $\begin{pmatrix} c'_i \\ d'_i \end{pmatrix}$ and $\begin{pmatrix} c''_i \\ d''_i \end{pmatrix}$ of a k-vector space $\langle x_1, x_2 \rangle_k$ of dimension two. They form a k-linearly dependent set, with a relation say

$$\begin{pmatrix} c''_i \\ d''_i \end{pmatrix} + e \begin{pmatrix} c_i \\ d_i \end{pmatrix} + e' \begin{pmatrix} c'_i \\ d'_i \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

for some $e, e' \in k$. But then $\sigma'' \sigma^e (\sigma')^{e'} \in G[i-1]$, and $G[i] = \langle G[i-1], \sigma, \sigma' \rangle$. Since F is elementary abelian, the subgroup index is at most p^2. $\square$

We let $G \leq F$, for most of this chapter up to section 2.5, and will find S^G up to a congruence. We assume that $n > 2$ to have $F \neq 1$. The group satisfies $(V^*)^G \geq \langle x_1, x_2 \rangle_k$. We will assume that $(V^*)^G = \langle x_1, x_2 \rangle_k$. If the inclusion happens to be strict instead, then we can assume that $(V^*)^G = \langle x_1, x_2, \ x_{n-i}, \ldots x_n \rangle_k$, for some i, by using a suitable change of basis that fixes $\langle x_1, x_2 \rangle_k$. The group F is stable under this change of basis in the following sense.

Definition 2.0.5. Fix two bases B, B' of V^*. Let $\rho_B : G \to \mathrm{GL}_n(k)$ denote the representation of G with respect to B. A change of basis from B to B' is

1. *G-stable* if $\rho_B(G) = \rho_{B'}(G)$;

2. *G-fixed* if $\rho_B(g) = \rho_{B'}(g)$ for all $g \in G$.

Note 2.0.6. In this chapter, unless specified otherwise, assume all changes of basis, fixes $\langle x_1, x_2 \rangle$, leaving $[F, V^*]$ unchanged. This includes changes of basis that fixes only $G[2] = 1$.

So with an F-stable change of basis, G remains two row, fixing $\langle x_1, x_2 \rangle$. And to determine the invariant ring S^G, it is sufficient to find $S[n-i-1]^G$, where $\langle x_1, \cdots, x_{n-i-1} \rangle_k^G = \langle x_1, x_2 \rangle_k$. So from here, assume $(V^*)^G = \langle x_1, x_2 \rangle_k$.

The above properties on changes of basis will be used mostly with subgroups $G[i] \leq G$. As we pick σ_i and τ_i for each i to form a chain of subgroups, changes of basis that we apply may also change the matrix entries of σ_j and τ_j with $j < i$ that were already chosen. This may interfere with our aim of finding a $\boxtimes$-product representation for G. So the definitions will be used to emphasise when they do not.

Note that $G[i]$-fixing is weaker than fixing the basis elements $\{x_1, \cdots, x_i\}$ of B. For example, consider the group

$$G = \left\langle \sigma_3 = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_3 \right], \sigma_4 = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_4 \right] \right\rangle$$

with $n = 4$, and the change of basis replacing x_3 by $x_3 + x_4$. This change of basis from B to $B' = \{x_1, x_2, x_3 + x_4, x_4\}$ fixes $G[3] = \langle \sigma_3 \rangle$, since σ_3 fixes x_4, and so $\rho_B(\sigma_3) = \rho_{B'}(\sigma_3)$. In the proofs to follow, this type of replacement of basis elements will be common. And after a replacement, the basis element $x_3 \in B$ will then refer to the old "$x_3 + x_4$".

The condition G'-stable is weaker than G'-fixing still because

$$\rho_{B'}(\sigma_4) = \left[\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right] \neq \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_4 \right] = \rho_B(\sigma_4).$$

So the change of basis from B to B' is not G-fixed. However, we can see that it is G-stable since $\rho_B(\sigma_3\sigma_4) = \left[\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \right]$ and G is a group.

2.1 One-column-extended case

Let $I = I(G) \leq G$ be the subgroup generated by reflections in G. Define

$$H = H(G) := C_G\left((V^*)^I \right) := \left\{ \sigma \in G : \left[\sigma, (V^*)^I \right] = 0 \right\}.$$

It is also the maximal subgroup $H \leq G$ such that $(V^*)^H = (V^*)^I$. This section focuses on finding S^G when $G = H$. Define $m = m(G) := n - \dim (V^*)^{I(G)} + 2$. We have $m(G) = m(H) = m(I)$, and $G = H$ is also equivalent to $m = n$. This characterisation will be used in a later section.

Wu had showed in theorem [16, 3.2.1] how to find S^G when $G = I$ holds. The method for finding invariant rings in this section and the next two will be based on a key argument in his theorem. It allows us to reduce the problem of finding S^G to one of finding $S^{\langle G,\rho\rangle}$ where ρ is a reflection, usually one-column.

Lemma 2.1.1. Let $\rho \in F \setminus G$ be a reflection. Suppose, for every non-trivial $y \in \langle x_1, x_2\rangle_k$, there is a reflection θ in the coset ρG such that $[\theta, V^*] = \langle y\rangle_{\mathbb{F}_p}$. Then there is an invariant $f \in S^G$ of degree $p+1$ such that $S^G = S^{\langle G,\rho\rangle}[f]$ and f is in the ideal $Sx_1 + Sx_2$. If $S^{\langle G,\rho\rangle}$ is a complete intersection, then so is S^G.

Proof. Since F is elementary abelian, $G < \langle G, \rho\rangle$ is a maximal subgroup and we can apply proposition 1.1.1: if there is an $f \in S^G$ such that $[\rho, f] \in S^{\langle G,\rho\rangle}$ and $\left[\rho, S^G\right]$ is a subset of the ideal $S \cdot [\rho, f]$, then $S^G = S^{\langle G,\rho\rangle}[f]$, and S^G is a complete intersection if $S^{\langle G,\rho\rangle}$ is. So it is sufficient to find such an f, if it is of degree $p+1$ and is in $Sx_1 + Sx_2$.

Since F is elementary abelian, let $\overline{G} < F$ be a maximal subgroup containing G but not ρ. Since S^F is polynomial, we can use theorem 1.1.2: there is a non-trivial invariant $f \in S^{\overline{G}}$ given by

$$f = \sum_j \left(\prod_{g \in Y_j} g\right) \boldsymbol{N}_j^{\overline{G}_j},$$

where the sum is over the indices $j = 3, \cdots, n$ satisfying $\overline{G}_j < F_j$ and so $\left|\overline{G}_j\right| = p$, and where Y_j is a set of degree 1-commutators in $[F, V^*] = \langle x_1, x_2\rangle_k$.

Now we check the conditions for applying proposition 1.1.1: both $[\rho, f] \in S^{\langle G,\rho\rangle}$ and $\left[\rho, S^G\right] \subseteq S \cdot [\rho, f]$. Theorem 1.1.2 says that $[\rho, f]$ is a product of elements of $\left[\overline{G}, V^*\right]$ distinct up to a $\mathbb{F}_p$-multiple. Since $\left[\overline{G}, V^*\right] = \langle x_1, x_2\rangle_{\mathbb{F}_p}$,

$$[\rho, f] \in k[x_1, x_2] \subseteq S^F \subseteq S^{\langle G,\rho\rangle}.$$

For the other condition, note that the possible distinct factors are the $p+1$ elements x_1 and $x_2+\lambda x_1$ with $\lambda \in \mathbb{F}_p$, whence $[\rho, f]$ divides $x_1 \prod_{\lambda \in k}(x_2+\lambda x_1)$. If we can show that these $p+1$ elements all divide $[\rho, g]$ in S for all $g \in S^G$, then $[\rho, f]$ would also divide $[\rho, g]$ in S, whence $\left[\rho, S^G\right] \subseteq S \cdot [\rho, f]$ follows.

Pick any $y = \langle x_1, x_2 \rangle_k$. The premise of this lemma says that there is some $\theta \in \rho G$ satisfying, for every monomial $x_1^{e_1} \cdots x_n^{e_n} \in S$,

$$[\theta - 1]\left(x_1^{e_1} \cdots x_n^{e_n}\right) = \left(x_1 + \lambda_1 y\right)^{e_1} \cdots \left(x_n^{e_n} + \lambda_n y\right)^{e_n} - x_1^{e_1} \cdots x_n^{e_n},$$

for some $\lambda_1, \cdots, \lambda_n \in k$. This shows y that divides $[\theta, g]$. And since $[\rho, g] = [\theta, g]$ for all $\theta \in \rho G$, we have y dividing $[\rho, g]$ as well as required.

It remains to check the degree of f and whether f is in the ideal $Sx_1 + Sx_2$. Set $g = f$ to see that $x_1 \prod_{\lambda \in k}(x_2 + \lambda x_1)$ divides $[\rho, f]$. But we also found above that $[\rho, f]$ divides the product. So the two are in fact equal. In particular, the degree of f must be $p+1$. Consider the form of f above where it was defined as a sum indexed by j. The sum cannot be empty. The orbit product $\boldsymbol{N}_j^{\overline{G}_j}$ in each term of the sum has degree p. This means we must have a non-trivial product $\prod_{g \in Y_j} g \in \langle x_1, x_2 \rangle_k$ for each j, whence $f \in Sx_1 + Sx_2$. $\square$

If lemma 2.1.1 can be applied in such a way that $\left[\overline{G}, x_n\right] = \left[\overline{G}_n, x_n\right]$ where $\overline{G} = \langle G, \rho \rangle$, then we can further simply the problem.

Lemma 2.1.2. Let $\sigma_n = \left[\binom{1}{0}_n\right]$ and $\rho = \left[\binom{0}{1}_n\right]$. If $G = \langle G[n-1], \sigma_n \rangle$, or $\langle G[n-1], \sigma_n, \rho \rangle$ then $S^G = S[n-1]^G\left[\boldsymbol{N}_n^G\right]$.

Proof. This is a special case of lemma 2.0.3 with $G = G[n-1] \boxtimes G_n$. $\square$

So lemma 2.1.1 can change the problem of finding $S[n]^G$ to $S[n]^{\langle G, \rho \rangle}$ and then lemma 2.1.2 can change it to $S[n-1]^G$. This suggests that it may be possible to find S^G by induction on n if we can ensure that G contains a one-column reflection at column n, or more generally at each column $3, \cdots, n$, giving an easy choice of ρ for applying lemma 2.1.1 repeatedly. We show that our condition $G = H$ allows for exactly this.

Lemma 2.1.3. Suppose $G = H$. Fix $i = 3, \cdots, n$. After any choice of (G_2-fixing) changes of basis, there is still a reflection in $G \setminus G[i-1]$,

Proof. By definitions, the groups have the same invariant spaces

$$(V^*)^I = (V^*)^H = (V^*)^G = \langle x_1, x_2 \rangle .$$

This means there is an element in I that does not fix x_i. Since I is a reflection group, one of them must a reflection, whence a reflection in $G \setminus G[i-1]$. $\square$

The following shows how to turn the reflection into a one-column.

Lemma 2.1.4. Suppose $G = H$. Pick $i = 3, \cdots, n$. Suppose there is some reflection $\sigma \in G \setminus G[i-1]$. Using a $G[i-1]$-fixing change of basis, there is a one-column $\sigma_i \in G \setminus G[i-1]$, of the form either

$$\sigma_i = \left[\begin{pmatrix} 1 \\ b_i \end{pmatrix}_i \right] \text{ or } \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_i \right],$$

where $b_i \in k$.

Proof. Columns of a reflection are k-linear multiples of each other. So write

$$\sigma = \left[\begin{pmatrix} \lambda_3 a_i & \cdots & \lambda_n a_i \\ \lambda_3 b_i & \cdots & \lambda_n b_i \end{pmatrix} \right],$$

for some pair $a_i, b_i \in k$ not both zero (since $\sigma \neq 1$), and for some $\lambda_3, \cdots, \lambda_n \in k$, with $\lambda_i, \cdots, \lambda_n$ not all zero (since $\sigma \notin G[i-1]$).

Reorder $x_i, \cdots, x_n$ in B to assume $\lambda_i \neq 0$. This fixes $G[i-1]$ since $G[i-1]$ fixes these basis elements. By renaming the matrix entries, assume $\lambda_i = 1$ so that

$$\sigma = \left[\begin{pmatrix} \lambda_3 a_i & \cdots & a_i & \cdots & \lambda_n a_i \\ \lambda_3 b_i & \cdots & b_i & \cdots & \lambda_n b_i \end{pmatrix} \right].$$

To make σ one-column, replace each x_j in B by $x_j - \lambda_j x_i$, for columns

$j = 3, \cdots, \widehat{i}, \cdots, n$. The effect of this is as follows: Before the change of basis,

$$\sigma : x_j - \lambda_j x_i \mapsto \left(x_j + \begin{pmatrix} \lambda_j a_i \\ \lambda_j b_i \end{pmatrix} \right) - \lambda_j \left(x_i + \begin{pmatrix} a_i \\ b_i \end{pmatrix} \right) = x_j - \lambda_j x_i.$$

This means σ acts trivially on the new basis vectors and becomes one-column, giving $\sigma = \left[\left(\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right)_i \right]$. This fixes $G[i-1]$ since $G[i-1]$ fixes x_i.

And now to pick σ_i of the required form, we proceed as follows. If $a_i \neq 0$, then pick $\sigma^{a_i^{-1}} = \left(\begin{smallmatrix} 1 \\ a_i^{-1} b_i \end{smallmatrix}\right)$. If $a_i = 0$, then $b_i \neq 0$ and pick $\sigma^{b_i^{-1}} = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. □

The proof of this lemma exemplifies the arguments that will be used to find σ_i and τ_i of specific forms to find a ⊠-product in this chapter. There will not be any explicit checks on their effects anymore, as they are all similar.

To complete a generating set for G, we will find $\tau_3, \cdots, \tau_n$ as well. They will be in specific forms to make our induction proof easier.

Lemma 2.1.5. Fix $i = 3, \cdots, n$. Let $\sigma_j = \left[\left(\begin{smallmatrix} a_j \\ b_j \end{smallmatrix}\right)_j \right]$ with either $a_j = 1$ or $\left(\begin{smallmatrix} a_j \\ b_j \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$, for $j = 3, \cdots, i$, by using lemma 2.1.4 or otherwise.

(1) If $G[i] = G' := \langle G[i-1], \sigma_i \rangle$, then set $\tau_i = 1$.

(2) If $G[i] > G'$, then $G[i] = \langle G', \tau_i \rangle$ for some $\tau_i \in G \setminus G'$. Using a $G[i-1]$-fixing and G'-stable change of basis, we can choose τ_i to be of the form

$$\tau_i = \left[\begin{pmatrix} \lambda_{i,3} a_i & \cdots & \lambda_{i,i-1} a_i & a_i' & 0 & \cdots \\ \lambda_{i,3} b_i & \cdots & \lambda_{i,i-1} b_i & b_i' & 0 & \cdots \end{pmatrix} \right]$$

$$\text{where } \begin{pmatrix} a_i' \\ b_i' \end{pmatrix} = \begin{cases} \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right), & \text{if } a_i = 1, \\ \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), & \text{if } a_i = 0, \end{cases}$$

and where $\lambda_{i,j} \in k$ is zero whenever $\left(\begin{smallmatrix} a_j \\ b_j \end{smallmatrix}\right) = \left(\begin{smallmatrix} a_i \\ b_i \end{smallmatrix}\right)$.

Proof. Suppose $G' < G[i]$ strictly. Pick any $\tau \in G[i] \setminus G'$. Write

$$\tau = \left[\begin{pmatrix} c_3 & \cdots & c_i & 0 & \cdots \\ d_3 & \cdots & d_i & 0 & \cdots \end{pmatrix} \right],$$

for some pairs $c_j, d_j \in k$ not all zeroes. If column i is $\binom{c_i}{d_i} = e\binom{a_i}{b_i}$ for some $e \in \mathbb{F}_p$, then $\tau\sigma_i^{-e}$ fixes x_i, and $\tau\sigma_i^{-e} \in G[i-1]$, contradicting the definition of τ. So instead $\binom{a_i}{b_i}$ and $\binom{c_i}{d_i}$ must span $\langle x_1, x_2\rangle_k$ over $\mathbb{F}_p$. Write $\binom{a'_i}{b'_i}$ defined in the lemma as a $\mathbb{F}_p$-linear multiple of them, say

$$\begin{pmatrix} a'_i \\ b'_i \end{pmatrix} = e\begin{pmatrix} a_i \\ b_i \end{pmatrix} + e'\begin{pmatrix} c_i \\ d_i \end{pmatrix},$$

for some $e, e' \in k$ with $e' \neq 0$. Replace τ by $\sigma_i^e \tau^{e'}$ to assume $\binom{c_i}{d_i} = \binom{a'_i}{b'_i}$.

If $i = 3$, then τ is one-column. Assume $i > 3$. Consider the columns $\binom{c_j}{d_j}$, in decreasing order $j = i-1, \cdots, 3$. Suppose $\binom{a_j}{b_j} = \binom{a_i}{b_i}$. We want $\lambda_{i,j} = 0$. The pair $\binom{a_j}{b_j} = \binom{a_i}{b_i}$ and $\binom{c_i}{d_i}$ spans $\langle x_1, x_2\rangle_k$ over $\mathbb{F}_p$, as mentioned above. Write column j as

$$\begin{pmatrix} c_j \\ d_j \end{pmatrix} = e\begin{pmatrix} a_j \\ b_j \end{pmatrix} + \lambda\begin{pmatrix} c_i \\ d_i \end{pmatrix},$$

for some $e, \lambda \in k$. Replace τ by $\tau\sigma_j^{-e}$ to assume that $\binom{c_j}{d_j} = \lambda\binom{c_i}{d_i}$. Now, replace x_j in B by $x_j - \lambda x_i$. This fixes $G[i-1]$ and gives $\lambda = 0$, as necessary for τ. However, this does not leave the one-column σ_i unchanged. It becomes:

$$\sigma_i = \begin{array}{c} \begin{array}{cccccc} & \overbrace{}^{\text{Column } j} & & & & \end{array} \\ \left[\begin{pmatrix} \cdots & -\lambda a_i & \cdots & a_i & 0 & \cdots \\ \cdots & -\lambda' b_i & \cdots & b_i & 0 & \cdots \end{pmatrix}\right] \end{array}.$$

To mitigate this, since $\binom{a_j}{b_j} = \binom{a_i}{b_i}$, replace σ_i by $\sigma_i\sigma_j^{-e'}$.

Suppose instead that $\binom{a_j}{b_j} \neq \binom{a_i}{b_i}$. Since a_i and a_j can only be 0 or 1, the pair $\binom{a_j}{b_j}$ and $\binom{a_i}{b_i}$ spans $\langle x_1, x_2\rangle_k$ over k. So, we can write column j of τ as

$$\begin{pmatrix} c_j \\ d_j \end{pmatrix} = e\begin{pmatrix} a_j \\ b_j \end{pmatrix} + \lambda_{i,j}\begin{pmatrix} a_i \\ b_i \end{pmatrix},$$

for some $e, \lambda_{i,j} \in k$. Replace τ by $\tau\sigma_j^{-e}$ to assume $\binom{c_j}{d_j} = \lambda_{i,j}\binom{a_i}{b_i}$. $\square$

We can now prove the main result of this section. As mentioned before, we will use the matrix forms of σ_i and τ_i, as specified in lemmas 2.1.4 and 2.1.5

respectively, to find an overgroup chain of G that remain in F, the maximal two-row group fixing $\langle x_1, x_2\rangle_k$.

Proposition 2.1.6. Suppose $G = H$. Then S^G is a complete intersection. Up to a change of basis of V^*, we have $S^G = k\left[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n, f_3, \cdots, f_n\right]$, for some $f_3, \cdots, f_n \in Sx_1 + Sx_2$ that are either zero or of degree $p+1$.

Proof. Proceed by induction on n. Pick $\sigma_3, \cdots, \sigma_n \in G$ and $\tau_3, \cdots, \tau_n \in G$ as in lemmas 2.1.4 and 2.1.5. Since σ_n is one-column, if τ_n is also one-column or trivial, then apply lemma 2.1.2 to get

$$S^G = S\left[n-1\right]^G\left[\boldsymbol{N}_n^G\right].$$

In this case, set $f_n = 0$, and we are done by inductive hypothesis on $S\left[n-1\right]^G$. This applies to the base case $n = 3$, which is Nakajima.

Suppose instead that τ_n is not one-column. Lemma 2.1.5 says that we have

$$\tau_n = \left[\begin{pmatrix} \lambda_{n,3}a_n & \cdots & \lambda_{n,n-1}a_n & a_n' \\ \lambda_{n,3}b_n & \cdots & \lambda_{n,n-1}b_n & b_n' \end{pmatrix}\right],$$

and $\lambda_{n,i}$ is non-zero for some i. Let $\rho \in F\setminus G$ be the one-column reflection where $\left[\rho, x_n\right] = \left[\tau_n, x_n\right] = \binom{a_n'}{b_n'}$. Note that $\rho^{-1}\tau_n \in F\left[n-1\right]$. Expand

$$\langle G, \rho\rangle = \langle G\left[n-1\right], \sigma_n, \tau_n, \rho\rangle = \left\langle G\left[n-1\right], \rho^{-1}\tau_n, \sigma_n, \rho\right\rangle,$$

where $\langle \sigma_n, \rho\rangle$ is one-column at column n, and the actions of the groups $\langle G, \rho\rangle$ and $G' := \langle G\left[n-1\right], \rho^{-1}\tau_n\rangle$ on $S\left[n-1\right]$ are the same. By lemma 2.1.2,

$$S^{\langle G,\rho\rangle} = S\left[n-1\right]^{\langle G,\rho\rangle}\left[\boldsymbol{N}_n^G\right] = S\left[n-1\right]^{G'}\left[\boldsymbol{N}_n^G\right].$$

Now apply induction hypothesis to $S\left[n-1\right]^{G'}$. Its precondition $H\left(G'\right) = G'$ needs to be checked. The group G' fixes x_n since $\rho^{-1}\tau_n$ does. It contains one-column reflections $\sigma_3, \cdots, \sigma_{n-1}$ at columns $3, \cdots, n-1$ respectively. Since taking invariant subspace reverses inclusions of groups, write

$$\begin{gathered}\langle\sigma_3,\cdots,\sigma_{n-1}\rangle\le I\left(G'\right)\le H\left(G'\right)\le G'\\ \langle x_1,x_2,x_n\rangle=\left(V^*\right)^{\langle\sigma_3,\cdots,\sigma_{n-1}\rangle}\ge\left(V^*\right)^{I(G')}\ge\left(V^*\right)^{H(G')}\ge\left(V^*\right)^{G'}=\langle x_1,x_2,x_n\rangle.\end{gathered}$$

This shows that $H\left(G'\right)=G'$. Apply induction hypothesis on $S\left[n-1\right]^{G'}$: with a change of basis of $\langle x_1,\cdots,x_{n-1}\rangle_k$, we have a complete intersection

$$S^{\langle G,\rho\rangle}=k\left[\boldsymbol{N}_1^{G'},\cdots,\boldsymbol{N}_{n-1}^{G'},f_3,\cdots,f_{n-1}\right]\left[\boldsymbol{N}_n^G\right],$$

where $\boldsymbol{N}_i^{G'}=\boldsymbol{N}_i^G$ for $i=1,\cdots,n-1$ by definition of G'. The above matrix form of τ_n still stands after this change of basis since columns $3,\cdots,n-1$ of τ_n are k-multiples of each other. The one-columns σ_n and ρ are also unaffected.

If lemma 2.1.1 can be applied as well, then we have, for some $f_n\in S^G$,

$$S^G=S^{\langle G,\rho\rangle}\left[f_n\right]=k\left[\boldsymbol{N}_1,\cdots,\boldsymbol{N}_{n-1},f_3,\cdots,f_{n-1}\right]\left[\boldsymbol{N}_n,f_n\right].$$

To show that the pre-condition of that lemma can be satisfied, pick any non-trivial $y\in\langle x_1,x_2\rangle_k$. We show there is a reflection $\theta\in\rho G$ such that $[\theta,V^*]=\langle y\rangle_k$. It is sufficient to check the $p+1$ choices of y unique up to a k-multiple.

Write $\sigma_n=\left[\binom{a_n}{b_n}_n\right]$. We get p distinct choices using the one-columns

$$\theta=\rho\sigma_n^e=\left[\begin{pmatrix}a'_n+ea_n\\ b'_n+eb_n\end{pmatrix}_n\right]\in\rho G$$

for $e\in\mathbb{F}_p$ then provide p distinct choices. The last remaining choice to check is $y=[\sigma_n,x_n]=\binom{a_n}{b_n}$. Since one of $\lambda_{n,i}$ is non-zero, setting

$$\theta=\rho\tau_n^{-1}=\left[\begin{pmatrix}-\lambda_{n,3}a_n&\cdots&-\lambda_{n,n-1}a_n&0\\ -\lambda_{n,3}b_n&\cdots&-\lambda_{n,n-1}b_n&0\end{pmatrix}\right]\in\rho G$$

would suffice for the choice $y=\binom{a_n}{b_n}$. So lemma 2.1.1 can be applied. The lemma gives the inclusion $f_n\in Sx_1+Sx_2$ and its degree. And since $S^{\langle G,\rho\rangle}$ is a complete intersection, the lemma says that $S^G = S^{\langle G,\rho\rangle}[f_n]$ is as well. $\square$

The following example illustrates how to use the proof of the proposition. The invariant f in lemma 2.1.1 was chosen to be the one constructed in theorem 1.1.2. However, in practise, any choice of f that satisfies the precondition for the given ρ can be used in its place.

Example 2.1.7. Set $n = 4$. Let $G = \langle \sigma_3, \sigma_4, \tau_4 \rangle$ where

$$\sigma_3 = \left[\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right], \sigma_4 = \left[\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right] \text{ and } \tau_4 = \left[\begin{pmatrix} 1 & 0 \\ 0 & b' \end{pmatrix}\right],$$

Suppose $b' \neq 0$. Then

$$S^G = k[\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3, \boldsymbol{N}_4, f_4],$$
$$\text{where } f_4 = [\tau_4, x_3]\,\boldsymbol{N}_3^{\langle\tau_4\rangle} - (b')^{-1}[\tau_4, x_4]\,\boldsymbol{N}_4^{\langle\tau_4\rangle}.$$

Proof. We check that there is a one-column reflection for each column $i > 2$, namely σ_3 and σ_4. This ensures that we have $G = H(G)$. Since $[\tau_4, x_4] = \binom{0}{b'}$ is not an $\mathbb{F}_p$-multiple of $[\sigma_4, x_4] = \binom{1}{0}$, we pick $\rho = \left[\binom{0}{b'}_4\right]$. The invariant given expands as

$$f_4 = x_2 \prod_{\lambda\in k}(x_3 + \lambda x_2) - (b')^{-1} x_1 \prod_{\lambda\in k}(x_4 + \lambda x_1).$$

It satisfies $[\rho, f_4] = -x_1 \prod_{\lambda\in k}(x_2 + \lambda x_1)$. And so we have $S^G = S^{\overline{G}}[f_4]$, where $\overline{G} = \langle \sigma_3, \sigma_4, \tau_4, \rho \rangle$ is Nakajima. $\square$

2.2 Totally one-extended case

In this section, we will find S^G for groups $G \leq F$ that will be called *totally one-extended*, to be defined below in 2.2.2. In particular, this includes some groups that do not satisfy $G = H$, or equivalently some groups that satisfy $n > m$.

Proposition 2.1.6 relied on being able to construct one-column reflections σ_i

at each column $3, \cdots, n$ as specified in lemma 2.1.4. When $G \neq H$, this is not possible by definition. However it is still true that $G[i] = \langle G[i-1], \sigma_i, \tau_i \rangle$ for some $\sigma_i, \tau_i \in G[i]$, using $[G[i] : G[i-1]] \leq p^2$ from lemma 2.0.4.

Similar techniques as in the previous section will be used to choose $\sigma_3, \cdots, \sigma_n$ and $\tau_3, \cdots, \tau_n$ in G with helpful matrix forms, to provide natural choices of reflection ρ for applying lemma 2.1.1. It will again change the problem of finding S^G to $S^{\overline{G}}$, where $\overline{G} = \langle G, \rho \rangle$, and then to $S[n-1]^{\overline{G}}$ using lemma 2.1.2. By ensuring that $m\left(\overline{G}[n-1]\right) \geq m(G)$, we can use induction on $n - m$.

The first step is to describe the form for each σ_i. Pick $i = 3, \cdots, n$. Let $\sigma \in G \setminus G[i-1]$, say $\sigma = \left[\left(\begin{smallmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{smallmatrix}\right)\right]$. Since $\sigma \notin G[i-1]$, the columns $\left(\begin{smallmatrix} c_j \\ d_j \end{smallmatrix}\right)$ for $j \geq i$ cannot all be zeroes, and must span over $\mathbb{F}_p$ a subspace of $\langle x_1, x_2 \rangle_k$ of dimension either one or two. These two possible dimensions correspond to two possible forms for σ, and will be referred to by the following names.

Definition 2.2.1. We say σ *one-extends (over) column i-1* if the dimension is 1. Otherwise, it *two-extends column i-1.* As a short-hand referencing subscripts, given $\sigma_i \in G \setminus G[i-1]$, we simply say that σ_i *j-extends* (over column $i - j$).

As examples, every non-trivial element one-extends some column and reflections do not two-extend any columns. A double transvection say $\sigma_4 = \left[\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_4\right]$ both one-extends and two-extends at the same time, so these properties may not give much extra insight to an element itself. The terminology essentially describes, in terms of matrix entries, whether an element $\sigma \in G$ acts as a non-trivial reflection or as a double transvection on the space $\langle x_1, x_2, \; x_{i-1}, \cdots, x_n \rangle_k$. What is important is the existence of elements of G one-extending a given column. That is, whether there are any non-trivial reflections on the aforementioned subspace.

Definition 2.2.2. We say that G *one-extends column* $i-1$ if there is some $\sigma_i \in G \setminus G[i-1]$ that one-extends (column $i-1$). Otherwise, it *two-extends column* $i-1$. We say that G is *totally one-extended (with respect to B)* if $G[i]$ one-extends column $i-1$, or equivalently $G[i] \neq G[i-1]$, for $i = 3, \cdots, n$, This section focuses on the totally one-extended case. Note that, in such cases, there must be at least one non-trivial reflection, since an element in F that one-extends column 2 is a reflection. So $m \geq 3$. And $n \geq 4$ if $G > H$. Now, we build on top of the one-column requirements for σ_i from lemma 2.1.4.

Lemma 2.2.3. Fix $i = 3, \cdots, n$. Suppose G one-extends column $i-1$. Using a $G[i-1]$-fixing change of basis, there is some $\sigma_i \in G[i] \setminus G[i-1]$ such that

(1) If $i = 3$, then $\sigma_3 = \left[\binom{1}{b_3}_3\right]$ or $\left[\binom{0}{1}_3\right]$ for some b_3.

(2) If $i \geq 4$, then σ_i is in one of the following two forms with entries in k:

$$\sigma_i = \left[\begin{pmatrix} 0 & \cdots & 0 & 1 \\ d_{i,3} & \cdots & d_{i,i-1} & b_i \end{pmatrix}_i\right] \text{ or } \left[\begin{pmatrix} c_{i,3} & \cdots & c_{i,i-1} & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}_i\right].$$

(3) If $i \leq m$, assume that σ_i is one-column by lemma 2.1.4.

(4) If $i \geq m+1$, then each of columns $j = 3, \cdots, i-1$ of σ_i can be chosen such that $\binom{c_{i,j}}{d_{i,j}} = \binom{0}{0}$ whenever there is some $\sigma_j \in G[j] \setminus G[j-1]$ also of the above form (but with $i = j$) such that $[\sigma_j, x_j] \neq [\sigma_i, x_i]$.

Proof. Pick any non-trivial $\sigma_i = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{pmatrix}\right] \in G$ that one-extends column $i-1$. Assume $i > m$ so that σ_i is not a reflection, otherwise lemma 2.1.4 suffices. Since columns $i, \cdots, n$ are k-multiples of each other (when non-zero), by using the same changes of basis and replacements on these columns as in the one-column case in lemma 2.1.4 assume that either

$$\sigma_i = \left[\begin{pmatrix} c_{i,3} & \cdots & c_{i,i-1} & 1 & 0 & \cdots \\ d_{i,3} & \cdots & d_{i,i-1} & b_i & 0 & \cdots \end{pmatrix}\right] \text{ or } \left[\begin{pmatrix} c_{i,3} & \cdots & c_{i,i-1} & 0 & 0 & \cdots \\ d_{i,3} & \cdots & d_{i,i-1} & 1 & 0 & \cdots \end{pmatrix}\right].$$

Consider the columns $\binom{c_{i,j}}{d_{i,j}}$, in decreasing order $j = i-1, \cdots, 3$. Write either

$$\begin{pmatrix} c_{i,j} \\ d_{i,j} \end{pmatrix} = \lambda_j \begin{pmatrix} 1 \\ b_i \end{pmatrix} + \mu_j \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} c_{i,j} \\ d_{i,j} \end{pmatrix} = \lambda_j \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \mu_j \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

for some $\lambda_j, \mu_j \in k$. Replace x_j in B by $x_j - \lambda_j x_i$ to get the basic required form:

$$\sigma_i = \left[\begin{pmatrix} \cdots & 0 & \cdots & 1 & 0 & \cdots \\ \cdots & \mu_j & \cdots & b_i & 0 & \cdots \end{pmatrix}\right] \text{ or } \left[\begin{pmatrix} \cdots & \mu_j & \cdots & 0 & 0 & \cdots \\ \cdots & 0 & \cdots & 1 & 0 & \cdots \end{pmatrix}\right].$$

For the extra condition of having zeroes in part (4), fix $j = 3, \cdots, i-1$. Suppose there is some $\sigma_j \in G[j] \setminus G[j-1]$ also of the form specified in this lemma with $[\sigma_j, x_j] \neq [\sigma_i, x_i]$. Write $\binom{a_j}{b_j} := [\sigma_j, x_j]$ and $\binom{a_i}{b_i} = [\sigma_i, x_i]$. Since a_j and a_i are both either 0 or 1, the pairs $\binom{a_j}{b_j}$ and $\binom{a_i}{b_i}$ span $\langle x_1, x_2 \rangle_k$ over $\mathbb{F}_p$. So we can write

$$\begin{pmatrix} c_{i,j} \\ d_{i,j} \end{pmatrix} + e \begin{pmatrix} a_j \\ b_j \end{pmatrix} = \lambda \begin{pmatrix} a_i \\ b_i \end{pmatrix},$$

for some $e, \lambda \in \mathbb{F}_p$. Replace σ_i by $\sigma_i \sigma_j^e$ to assume that $e = 0$. Replace x_j in B by $x_j - \lambda x_i$ to assume that $\lambda = 0$ as well, and giving $\binom{c_{i,j}}{d_{i,j}} = \binom{0}{0}$. □

We will construct τ_i for $i = 4, \cdots, n$ as well. This will be similar to the $G = H$ case as in lemma 2.1.5. However, as in lemma 2.2.3, we will add some extra conditions for having columns of zeroes depending on whether $[\sigma_j, x_j] \neq [\sigma_i, x_i]$, to make our induction later on easier.

Lemma 2.2.4. Assume that $H = G[m]$. Fix $i = m+1, \cdots, n$. Suppose G one-extends column $i-1$ and there are $\sigma_j \in G[j] \setminus G[j-1]$ for $j = 3, \cdots, i$ as constructed in lemma 2.2.3, so that $[\sigma_j, x_j] = \binom{1}{b_j}$ or $\binom{0}{1}$ for some b_j. Suppose also that $[G[i] : G[i-1]] = p^2$, which allows the assumption that $b_i = 0$. So,

$$\sigma_i = \left[\begin{pmatrix} 0 & \cdots & 0 & 1 \\ d_{i,3} & \cdots & d_{i,i-1} & 0 \end{pmatrix}_i\right]$$

Using a $G[i-1]$-stable change of basis, there is some τ_i of the form

$$\tau_i = \left[\begin{pmatrix} c'_{i,3} & \cdots & c'_{i,i-1} & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}_i\right] \in G[i] \setminus G[i-1].$$

The change of basis can be chosen such that σ_i still has the above form with possibly different values of $d_{i,3}, \cdots, d_{i,i-1}$, and satisfies part (4) of lemma 2.2.3.

Proof. Since $[G[i] : G[i-1]] = p^2$, for each $\binom{a'_i}{b'_i} \neq \binom{0}{0}$, there is some $\tau_i \in G[i] \setminus G[i-1]$ such that $[\tau_i, x_i] = \binom{a'_i}{b'_i}$. So we can pick

$$\tau_i = \left[\begin{pmatrix} c'_{i,3} & \cdots & c'_{i,i-1} & 0 \\ d'_{i,3} & \cdots & d'_{i,i-1} & 1 \end{pmatrix}_i \right].$$

The proof will be much the same as that of lemma 2.1.5. Consider columns $\binom{c'_{i,j}}{d'_{i,j}}$ in decreasing order $j = i-1, \cdots, 3$. If $[G[j] : G[j-1]] = p^2$ also, then $G[j] = \langle G[j-1], \sigma_j, \tau_j \rangle$ for some τ_j, and it is clear that we can replace τ_i by $\tau_i \sigma_j^e \tau_j^{e'}$ for some $e, e' \in \mathbb{F}_p$ to assume that $[\tau_i, x_j] = \binom{0}{0}$.

Assume instead that $[G[j] : G[j-1]] = p$. Write $\binom{a_j}{b_j} := [\sigma_j, x_j]$. If $\binom{a_j}{b_j} \neq \binom{1}{0}$, then $b_j \neq 0$ and we can replace τ_i by $\tau_i \sigma_j^e$ where $e = -b_j^{-1} d'_{i,j}$ (reusing variable e) to assume that $d'_{i,j} = 0$ as needed.

Suppose instead that $\binom{a_j}{b_j} = \binom{1}{0}$. Then we can replace τ_i by $\tau_i \sigma_j^e$ where $e = -a_j^{-1} c'_{i,j}$ to assume that $c'_{i,j} = 0$. Since $\binom{a_i}{b_i} = \binom{1}{0}$, we can replace x_j in B by $x_j - d'_{i,j} x_i$ to assume $d'_{i,j} = 0$ as well. This change of basis fixes $G[i-1]$ and changes τ_i to act trivially on x_j, but modifies σ_i to becomes

$$\sigma_i = \left[\begin{pmatrix} 0 & \cdots & 0 & 1 \\ d_{i,3} & \cdots & d_{i,i-1} & 0 \end{pmatrix}_i + \begin{pmatrix} -d'_{i,j} \\ 0 \end{pmatrix}_j \right].$$

To mitigate this, replace σ_i by $\sigma_i \sigma_j^{d'_{i,j}}$. Since $[\sigma_i, x_i] = [\sigma_j, x_j]$, this preserves the property of σ_i having columns of zeroes from part (4) of lemma 2.2.3. □

We will now use the specified forms of σ_i and τ_i to find S^G.

Proposition 2.2.5. Suppose G is totally one-extended. Then S^G is a complete intersection. Up to a change of basis of V^*, we have

$$S^G = k[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n, f_3, \cdots, f_{2n-m}],$$

for some $f_3, \cdots, f_{2n-m} \in Sx_1 + Sx_2$ that are either trivial or of degree $p+1$.

Proof. This proof will use induction on $n-m$, on the hypothesis that the proposition holds. The base case $n = m$ is $G = H$, proved in lemma 2.1.6.

Assume that $n > m > 3$. Begin by specifying the forms of $\sigma_3, \cdots, \sigma_n$. Consider the subgroup $H < G$. Since $(V^*)^H$ has dimension $n-m+2$ over k, using a change of basis, assume that H fixes x_1, x_2 and $x_{m+1}, \cdots, x_n$. By applying lemma 2.1.4 to H on the subspace $\langle x_1, \cdots, x_m \rangle_k$, assume there are one-column reflections $\sigma_i = \left[\binom{a_i}{b_i}_i\right]$ for $3 \leq i \leq m$, so that $H = G[m]$. For the remaing elements, use lemmas 2.2.3 and 2.2.4 to find non-reflections $\sigma_{m+1}, \cdots, \sigma_n$ and $\tau_{m+1}, \cdots, \tau_n$ that one-extend or are trivial. Write $\binom{a_i}{b_i} = [\sigma_i, x_i]$ for $i = 3, \cdots, n$.

Lemma 2.2.3 says that each σ_i is of the form, for $i \geq 4$,

$$\sigma_i = \left[\begin{pmatrix} \lambda_{i,3}c_i & \cdots & \lambda_{i,i-1}c_i & a_i \\ \lambda_{i,3}d_i & \cdots & \lambda_{i,i-1}d_i & b_i \end{pmatrix}_i\right],$$

where $\binom{c_i}{d_i} = \binom{0}{1}$ or $\binom{1}{0}$ depending on whether $\binom{a_i}{b_i} = \binom{1}{b_i}$ or $\binom{0}{1}$ respectively, and where $\lambda_{i,j}$ is non-zero only if $\binom{a_j}{b_j} = \binom{a_i}{b_i}$. For $i \geq m+1$, we also have at least one $\lambda_{i,j}$ being non-zero. Note that the pair $\binom{c_i}{d_i}$ and $\binom{a_i}{b_i}$ spans $\langle x_1, x_2 \rangle_k$.

Define the reflection $\rho := \left[\binom{a_n}{b_n}_n\right]$ and overgroup $\overline{G} := \langle G, \rho \rangle$. We will use lemma 2.1.1 to obtain $S^G = S^{\overline{G}}[f_{2n-m}]$ for some f_{2n-m}. We need to check the pre-condition of that lemma: given any non-trivial $y \in \langle x_1, x_2 \rangle_k$, there is some $\theta \in \rho G$ such that $[\theta, V^*] = \langle y \rangle_k$. If $y \in \left\langle \binom{a_n}{b_n} \right\rangle_{\mathbb{F}_p}$, then $\theta = \rho$ sufficies. Suppose $y \notin \left\langle \binom{a_n}{b_n} \right\rangle_{\mathbb{F}_p}$. Then the pair $\binom{c}{d} := y$ and $\binom{a_n}{b_n}$ spans $\langle x_1, x_2 \rangle_k$. Set $\theta = \rho\sigma_n^{-1}$. Then

$$\theta = \left[\begin{pmatrix} -\lambda_{n,3}c_n & \cdots & -\lambda_{n,n-1}c_n & 0 \\ -\lambda_{n,3}d_n & \cdots & -\lambda_{n,n-1}d_n & 0 \end{pmatrix}\right],$$

not all columns zeroes. It has columns consisting of k-multiples of $\binom{c_n}{d_n}$ on the left. Its columns to the right, currently at least one, are k-multiples of $\binom{c}{d}$. It satisfies the following form: for some minimal $i \geq 3$,

$$\theta = \left[\left(\begin{array}{cc|ccc} \cdots & \mu_{i-1}c_n & \mu_i c & \cdots & \mu_n c \\ \cdots & \mu_{i-1}d_n & \mu_i d & \cdots & \mu_n d \end{array}\right)\right],$$

not all columns are zeroes, but each μ_j is non-zero only if $\binom{a_j}{b_j} = \binom{a_n}{b_n}$, mimicking the condition from the definition of σ_i. Note that $\mu_{i-1} \neq 0$ if $i \geq 4$ by minimality of i. The aim is to reduce i until $i = 3$, at which point $[\theta, V^*] = \langle y \rangle_k$ holds, as required by the pre-condition.

Fix $i \geq 4$. Write, for some $e, \lambda \in k$,

$$\mu_{i-1}\begin{pmatrix} c_n \\ d_n \end{pmatrix} + e\begin{pmatrix} a_{i-1} \\ b_{i-1} \end{pmatrix} = \lambda\begin{pmatrix} c \\ d \end{pmatrix}.$$

Replace θ by $\theta\sigma_{i-1}^e$. This replacement does three things. Firstly, column $i-1$ becomes a k-multiple of $\binom{c}{d}$, effectively decreasing i for the new θ. Secondly, this leaves μ_j unchanged for columns $j \geq i$, since σ_{i-1} fixes such columns.

The last columns to account for are columns $3 \leq j \leq i-2$. By definition of θ, since $\mu_{i-1} \neq 0$, we have $\binom{a_{i-1}}{b_{i-1}} = \binom{a_n}{b_n}$. By definition of σ_{i-1} from lemma 2.2.3, we have $\binom{c_{i-1}}{d_{i-1}} = \binom{c_n}{d_n}$ as well. This ensures every column j remains a multiple of $\binom{c_n}{d_n}$ with the non-zero condition intact. This can be repeated until $i = 3$.

We now have $S^G = S^{\overline{G}}[f_{2n-m}]$ for some $f_{2n-m} \in S^G$ by lemma 2.1.1. The next step depends on the subgroup index $[G : G[n-1]]$ which can be p or p^2. Suppose the easier case $G = \langle G[n-1], \sigma_n \rangle$ holds. Then we have

$$\overline{G} = \langle G[n-1], \sigma_n, \rho \rangle = \left\langle G[n-1], \sigma_n\rho^{-1}, \rho \right\rangle = \left\langle G[n-1], \sigma_n\rho^{-1} \right\rangle \boxtimes \langle \rho \rangle,$$

since $\overline{G}[n-1] = \langle G[n-1], \sigma_n\rho^{-1} \rangle$ and $\langle \rho \rangle$ is one-column at column n. By lemma 2.1.2, we have $S^{\overline{G}} = S[n-1]^{\overline{G}}\left[\boldsymbol{N}_n^{\langle \rho \rangle}\right]$. To find $S[n-1]^{\overline{G}}$, note that $I(G) \leq I(\overline{G})$, and so $m(\overline{G}) \geq m(G)$, And since $\overline{G}[n-1]$ has a smaller value of "n" and so of "$n-m$", induction hypothesis can be applied to $\overline{G}[n-1]$. The induction step then follows for the case $[G : G[n-1]] = p$.

Assume instead that $[G : G[n-1]] = p^2$, and for convenience $b_n = 0$. By lemma 2.2.4, we can also assume that

$$\tau_i = \left[\begin{pmatrix} c'_{i,3} & \cdots & c'_{i,i-1} & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}_i \right].$$

Define the reflection $\rho' = \left[\binom{0}{1}_n\right]$ and overgroup $\overline{\overline{G}} = \langle \overline{G}, \rho' \rangle$. We use lemma 2.1.1 once more to obtain $S^{\overline{G}} = S^{\overline{\overline{G}}}[f_{2n-m-1}]$ for some f_{2n-m-1}. Its precondition is easier this time. If $y \notin \left\langle \binom{1}{0} \right\rangle_k$, since $\rho = \left[\binom{1}{0}_n\right] \in \overline{G}$, we can then pick $\theta = \rho'\rho^e = \left[\binom{e}{1}_n\right]$ for some e. If $y \in \left\langle \binom{1}{0} \right\rangle_k$, then $\theta = \rho\tau_i^{-1}$ suffices.

As in the index p case, we have

$$\begin{aligned} \overline{\overline{G}} &= \left\langle G[n-1], \sigma_n\rho^{-1}, \tau_n(\rho')^{-1}, \rho, \rho' \right\rangle \\ &= \left\langle G[n-1], \sigma_n\rho^{-1}, \tau_n(\rho')^{-1} \right\rangle \boxtimes \langle \rho, \rho' \rangle, \end{aligned}$$

and, by lemma 2.1.2, we have $S^{\overline{\overline{G}}} = S[n-1]^{\overline{\overline{G}}}\left[\boldsymbol{N}_n^{\langle \rho, \rho' \rangle}\right]$. Apply induction hypothesis on $\overline{\overline{G}}[n-1]$, then the induction step and the proposition follow. □

The proof above relies on the totally-one-extended property in order to show how to find and use the invariants $f_i \in S^G$ and each of their corresponding elements θ appended to G. When finding invariants, by using theorem 1.1.2 or otherwise, these choices are usually known, and we can apply lemma 2.1.1 directly, as shown in the following example.

Example 2.2.6. Let $n \geq 4$. Let $G = \langle \sigma_i \in F : i = 3, \cdots, n \rangle$, where $\sigma_3 = \left[\binom{1}{0}_3\right]$, and $\sigma_i = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i\right]$ for $i = 4, \cdots, n$. Then $S^G = k[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n, f_4, \cdots, f_n]$,

$$\begin{aligned} \text{where } f_i &= x_1 \prod_{\lambda \in k} (x_{i-1} + \lambda x_1) + x_2 \prod_{\mu \in k} (x_i + \mu x_2) \\ &= x_1 x_{i-1}^p - x_1^p x_{i-1} + x_2 x_i^p - x_2^p x_i, \text{ for } 4 \leq i \leq n-1; \\ \text{and } f_n &= x_1 \prod_{\lambda \in k} (x_{n-1} + \lambda x_1) - x_n \prod_{\lambda \in k} (x_2 + \lambda x_1) \\ &= x_1 x_{n-1}^p - x_1^p x_{n-1} - x_2^p x_n + x_1^{p-1} x_2 x_n. \end{aligned}$$

Proof. Consider induction on n. The base case is $n = 4$. Let $\theta = \left[\binom{0}{1}_3\right]$. Since

$[\theta, f_4] = x_1 \prod_{\lambda \in k} (x_2 + \lambda x_1)$, lemma 2.1.1 gives $S^G = S^{\langle G, \theta \rangle} [f_4]$. The over-group

$$\langle G, \theta \rangle = \left\langle \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_3 \right], \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_4 \right], \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_3 \right] \right\rangle$$

is Nakajima, so $S^G = k [\boldsymbol{N}_1, \cdots, \boldsymbol{N}_4, f_4]$, giving the base case.

The inductive step is similar. Suppose $n \geq 5$. Pick $\theta = \left[\binom{0}{1}_3 \right]$, to have $S^G = S^{\overline{G}} [f_4]$ as before, where $\overline{G} := \langle G, \theta \rangle$, Since $\overline{G}$ contains both $\left[\binom{0}{1}_3 \right]$ and $\left[\binom{1}{0}_3 \right]$. lemma 2.1.2 can be applied to ignore column 3 instead of n, giving

$$S^{\overline{G}} = k [x_1, \cdots, \widehat{x_3}, \cdots, x_n]^{\overline{G}} \left[\boldsymbol{N}_3^{\overline{G}} \right].$$

But the invariant ring without column 3 is case $n-1$. By induction hypothesis.

$$k [x_1, \cdots, \widehat{x_3}, \cdots, x_n]^{\overline{G}} = k \left[\boldsymbol{N}_4^{\overline{G}}, \cdots, \boldsymbol{N}_n^{\overline{G}}, f_5, \cdots, f_n \right].$$

Adjoining $\boldsymbol{N}_3^{\overline{G}}$ and and f_4 gives the required from, since the norms of $\overline{G}$ and of G are the same, completing the proof. □

2.3 Subgroups with two-dimensional invariant subspace

Not all groups $G \leq F$ are totally one-extended. In the extreme case, there are groups with no non-trivial reflections ($m = 2$). In this section, we will show that every subgroup $G \leq F$ can be written as a $\boxtimes$-product of three components. The first is a totally one-extended group whose invariant ring was just found in proposition 2.2.5. We will find the invariant ring of the second component in proposition 2.3.26. The third will be left to sections 2.4 and 2.5.

The double transvection group $G = \left\langle \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right]_4 \right\rangle$ is the simplest example of a subgroup of F with no non-trivial reflections. More generally, every "block" is a group with no non-trivial reflections.

Definition 2.3.1. Given columns $i_1 \geq 2$ and $i_2 \geq i_1 + 2$, define the subgroup

$$F^{\langle i_1, i_2 \rangle} := \left\langle \sigma_i := \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i \right] : i = i_1 + 2, \cdots, i_2 \right\rangle \leq F.$$

We will call $F^{\langle i_1, i_2 \rangle}$ a *(two-row) block* of *width* $i_2 - i_1$. We will also refer to columns $i_1 + 1, \cdots, i_2$ as the *columns of block* $F^{\langle i_1, i_2 \rangle}$.

For example, blocks of width 2 are double transvection groups. For blocks with greater widths, by aligning columns instead of using subscripts, the elements $\sigma_{i_1+2}, \cdots, \sigma_{i_2}$ can be visualised as

$$\begin{array}{ccccccc}
\text{Column:} & i_1+1 & i_1+2 & \cdots & i_2-2 & i_2-1 & i_2 \\
 & \multicolumn{2}{c}{\left[\begin{pmatrix} 0 & \qquad 1 \\ 1 & \qquad 0 \end{pmatrix}\right]} & \cdots & \multicolumn{2}{c}{\left[\begin{pmatrix} 0 & \qquad 1 \\ 1 & \qquad 0 \end{pmatrix}\right]} & \\
 & & \multicolumn{2}{c}{\left[\begin{pmatrix} 0 & \qquad 1 \\ 1 & \qquad 0 \end{pmatrix}\right]} & \cdots & \multicolumn{2}{c}{\left[\begin{pmatrix} 0 & \qquad 1 \\ 1 & \qquad 0 \end{pmatrix}\right]}
\end{array}$$

We go back to the claim about reflections.

Lemma 2.3.2. There are no non-trivial reflections in a block $F^{\langle 2, n \rangle}$, for $n \geq 4$.

Proof. Consider induction on the block width $n - 2$. The base case of width 2 is the double transvection group. For the induction step, suppose $n \geq 5$. Let σ be a reflection in the block. Write $\sigma = \sigma_4^{e_4} \cdots \sigma_n^{e_n}$, for some $e_4, \cdots, e_n$. Note that σ has $\binom{0}{e_4}$ in column 3, and of $\binom{e_n}{0}$ in column n. Since σ is a reflection, one of the two columns must be zero. That is, $e_3 = 0$ or $e_n = 0$, and σ can be considered as an element of either $F^{\langle 3, n \rangle}$ or $F^{\langle 2, n-1 \rangle}$. Since these blocks have a smaller width, induction hypothesis then forces $\sigma = 1$, as required. $\square$

These blocks are important because we will find them in every group $G \leq F$ that is not totally one-extended. If G is not totally one-extended, then it can be generated by a totally one-extended subgroup $G[m_0] \leq G$, and some blocks whose columns are disjoint from each other such that together includes every columns $m_0 + 1, \cdots, n$, and some elements τ_{m_j} in specific forms.

Proposition 2.3.3. Suppose $G[m_0] < G$ is a totally one-extended subgroup such that G does not one-extend $G[m_0]$. Up to a $G[m_0]$-fixing change of basis,

$$G = \left\langle G[m_0], F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle}, \tau_{m_j} : 1 \leq j \leq l' \right\rangle,$$

for some $m_0 < m_1 < \cdots < m_l = n$ with $l \geq 1$, and for some $0 \leq l' \leq l$, where each τ_{m_j} is of the from

$$\tau_{m_j} := \left[\begin{pmatrix} 0 & \cdots & 0 \\ \underbrace{*}_{\text{Column } m_0+1} & \cdots & \underbrace{*}_{\text{Column } m_j} \end{pmatrix}_{m_j} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_{j-1}+1} \right], \text{ for } 1 \leq j \leq l'.$$

That is, the element τ_{m_j} has $\left(\begin{smallmatrix} 1 & 0 & \cdots & 0 \\ * & * & \cdots & * \end{smallmatrix}\right)$ in the columns of block $F^{\langle m_{j-1}, m_j\rangle}$, and has $\left(\begin{smallmatrix} 0 & \cdots & 0 \\ * & \cdots & * \end{smallmatrix}\right)$ in the columns of blocks to the left of $F^{\langle m_{j-1}, m_j\rangle}$ if any. Note that, when $l' = 0$, there are no τ_{m_j} in the generating set of G described above.

If proposition 2.3.3 holds, by noting that every τ_{m_j} fixes $x_1, \cdots, x_{m_0}$ and $x_{m_{l'}}, \cdots, x_n$, we can rewrite G as a $\boxtimes$-product of three two-row groups. Roughly,

$$G = G[m_0] \boxtimes \left\langle F^{\langle *,* \rangle}, \tau_* : 1 \leq j \leq l' \right\rangle \boxtimes \left(F^{\langle 2,* \rangle} \boxtimes \cdots \boxtimes F^{\langle 2,* \rangle} \right),$$

giving us the three components we want to decompose to.

Most of this section is dedicataed to proving proposition 2.3.3. The strategy will be to find suitable matrix forms for σ_i, τ_i that generate G as before. The first step is to find a totally one-extended subgroup $G[m_0] \leq G$ that is a maximal amongst such subgroups. Recall that an element $\sigma \in G$ one-extends column $i-1$ if and only if it acts as a non-trivial reflection on the subsapce $\langle x_1, x_2,\ x_i, \cdots, x_n\rangle \leq V^*$. So, in increasing order of i, starting at $i = 3$, pick $\sigma_i \in G$ that one-extends column $i-1$ using that criteria, until there are none. Each σ_i can be made into an element of $G[i]$ using lemmas 2.1.4 or 2.2.3, depending on whether σ_i is a reflection on V^* or not. When an appropriate σ_i cannot be found, then the subgroup $G[i-1]$ found so far is the required maximal. Let $G[m_0] \leq G$ be the constructed maximal, with $m_0 \leq n$.

Lemma 2.3.4. This maximal $G[m_0]$ is in fact unique. In particular, we can define $m_0 := m_0(G)$ as the maximal column number such that $G[m_0]$ is totally one-extended.

Proof. Suppose there is another maximal generated by $\sigma'_3, \cdots, \sigma'_{m'_0} \in G$ for some $m'_0 \leq n$, with respect to another basis say $B' = \{x'_1, \cdots, x'_n\}$ of V^*, with $x'_1 = x_1$ and $x'_2 = x_2$. For a contradiction, suppose the maximals are different. We stay with the basis B. There is some $\sigma'_i \notin G[m_0]$ minimal in i. By minimality, $\sigma'_j \in G[m_0]$ for $3 \leq j \leq i-1$. Since they are products of $\sigma_3, \cdots, \sigma_{m_0}$, there is an inclusion of subspaces

$$\left\langle x_1, x_2, x'_j : 3 \leq j \leq i-1 \right\rangle_k < \langle x_1, x_2, x_j : 3 \leq j \leq m_0 \rangle_k .$$

On the other hand, by maximality of m_0, we must have σ'_i two-extending column m_0. Using the above inclusion of subspaces, apply a change of basis to the bigger space to one beginning with $\left\{x'_1, \cdots, x'_{i-1}\right\}$. Under this new basis, σ'_i still two-extends column m_0, whence also column $i-1$. This contradicts the definition of σ'_i that it one-extends column $i-1$ with respect to B'. □

With this, it is possible to assume G does not one-extend column m_0. If $m_0 = n$, then G is itself totally one-extended, and is a known case. And it is not possible to have $m_0 = n-1$, since $G = G[n]$ then one-extends column $n-1$.

2.3.1 Blocks with unsaturated columns

In this section, from here on, assume $m_0 \leq n-2$. The second step is to start building the blocks $F^{\langle *,* \rangle}$ as given in proposition 2.3.3. In this subsection, we deal with the case where we only need to find the blocks, corresponding to having $l' = 0$ in proposition 2.3.3. We do this by assuming that $[G[i] : G[i-1]] \leq p$ for $i = m_0+1, \cdots, n$, leaving the subgroup index p^2 case to subsection 2.3.2. This means we always have $G[i] = \langle G[i-1], \sigma_i \rangle$ for some σ_i. With our aim of constructing blocks in mind, we will try to pick $\sigma_i = \left[\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_i\right]$ or $\sigma_i = 1$.

For fixed $i \geq m_0+1$, if G does not one-extend $G[i-1]$ as is the case for

$i = m_0 + 1$, we are forced to pick $\sigma_i = 1$ by definition. Lemma 2.3.5 will show that we can then pick $\sigma_{i+1} = \left[\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_{i+1}\right]$, essentially starting a new block.

When G does one-extend $G\,[i-1]$, we will first assume that $m_0 = 2$ by ignoring columns $3 \leq j \leq m_0$, and that $G\,[i-1]$ is already generated by blocks, We will show that, under these assumptions, $G\,[i]$ can be generated by the same blocks as $G\,[i-1]$, but with the width of one of the blocks increased by one. The basic strategy will be treat $G\,[i]$ based on the number of blocks used to generate $G\,[i-1]$. Lemma 2.3.8 treats the case with one block. Lemma 2.3.9 for two blocks, and generalised to more than two in lemma 2.3.10.

If $m_0 \geq 3$, because the process described above ignored columns $3 \leq j \leq m_0$, the elements $\sigma_{m_0+1}, \cdots, \sigma_n$ found may take any values in those columns. We will show how to make those columns zeroes in lemma 2.3.11 and then summarise our construction of this subsection in lemma 2.3.13.

We note that the lemmas will qualify their changes of basis as being $G\,[i]$-fixing or $G\,[i]$-stable, as defined in 2.0.5. This will be relevant later.

To begin, we consider the case when G does not one-extend $G\,[i]$, in which we can only pick $\sigma_i = 1$. We immediately pick σ_{i+1} of the required form.

Lemma 2.3.5. *Fix $i = 4, \cdots, n$. Pick any $\sigma_i \in G \setminus G\,[i-2]$ that two-extends column $i-2$. With a $G\,[i-2]$-fixing change of basis, we can assume that $\sigma_i = \left[\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_i\right]$.*

Proof. This mimics the one-column case. Write $\sigma_i = \left[\left(\begin{smallmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{smallmatrix}\right)\right]$. In the basis B, rearrange $x_i, \cdots, x_n$ so that columns $\left(\begin{smallmatrix} c_i \\ d_i \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} c_{i+1} \\ d_{i+1} \end{smallmatrix}\right)$ span $\langle x_1, x_2 \rangle_k$. Write

$$
\begin{pmatrix} 0 \\ 1 \end{pmatrix} = e \begin{pmatrix} c_i \\ d_i \end{pmatrix} + e' \begin{pmatrix} c_{i+1} \\ d_{i+1} \end{pmatrix}
$$
$$
\begin{pmatrix} 1 \\ 0 \end{pmatrix} = e'' \begin{pmatrix} c_i \\ d_i \end{pmatrix} + e''' \begin{pmatrix} c_{i+1} \\ d_{i+1} \end{pmatrix},
$$

for some $e, e', e'', e''' \in k$. Replace x_i and x_{i+1} in B by $ex_i + e'x_{i+1}$ and $e''x_i + e'''x_{i+1}$ respectively, to assume that $\left(\begin{smallmatrix} c_i \\ d_i \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} c_{i+1} \\ d_{i+1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. For the remaining columns $j = 3, \cdots, \widehat{i}, \widehat{i+1}, \cdots, n$, replace each x_j in B by $x_j - d_jx_i - c_jx_{i+1}$ to make them zeroes. This gives the required form. $\square$

This is how a new block begins, forced by not being able to choose σ_i that one-extends when G does not one-extend column $i-1$. In contrast, when G does one-extend column $i-1$, our choice of σ_i will be chosen such that the width of some existing block in $G[i-1]$ will increase by one. We start with the case when there is just one block found so far.

Lemma 2.3.6. Suppose G has no non-trivial reflections, $n \geq 5$,

$$G[n-1] := \left\langle \sigma_i := \left[\begin{pmatrix} 0 & 1 \\ 1 & b_i \end{pmatrix}_i \right] : i = 4, \cdots, n-1 \right\rangle$$

for some $b_i \in k$, and $G = \langle G[n-1], \sigma_n \rangle$ for some $\sigma_n \in G \setminus G[n-1]$. With a $G[n-1]$-fixing change of basis, we can assume that

$$\sigma_n = \left[\begin{pmatrix} 0 & 1 \\ 1 & b_n \end{pmatrix}_n \right] \text{ or } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_3 + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_n \right],$$

for some $b_n \in k$, such that $[\sigma_n, x_n] \in \langle [\sigma, x_n] \rangle_k$.

Proof. Write $\sigma = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{pmatrix} \right]$, where $\binom{c_n}{d_n} \neq \binom{0}{0}$. Depending on whether $c_n \neq 0$, assume $\binom{c_n}{d_n} = \binom{1}{d_n}$ or $\binom{0}{1}$. Let $\rho_i = \left[\binom{c_n}{d_n}_i \right]$ for $i = 3, \cdots, n-1$. We want to show that the set consisting of these new one-columns ρ_i, the double transvections σ_i from $G[n-1]$ and one extra element in $F[n-1]$:

$$\left\{ \rho_3, \cdots, \rho_{n-1}, \sigma_4, \cdots, \sigma_{n-1}, \sigma \cdot \left[\begin{pmatrix} -c_n \\ -d_n \end{pmatrix}_n \right] = \left[\begin{pmatrix} c_3 & \cdots & c_{n-1} \\ d_3 & \cdots & d_{n-1} \end{pmatrix}_{n-1} \right] \right\}$$

forms a basis of $F[n-1]$. Suppose it is not a basis. Then

$$\sigma_4^{e_4} \cdots \sigma_{n-1}^{e_{n-1}} \cdot \rho_3^{e'_3} \cdots \rho_{n-1}^{e'_{n-1}} = \sigma \cdot \left[\begin{pmatrix} -c_n \\ -d_n \end{pmatrix}_n \right].$$

for some $e_4, \cdots, e_{n-1}, e'_3, \cdots, e'_{n-1} \in \mathbb{F}_p$. This rearranges to

$$\sigma^{-1} \cdot \sigma_4^{e_4} \cdots \sigma_{n-1}^{e_{n-1}} = \left[\begin{pmatrix} -c_n \\ -d_n \end{pmatrix}_n \right] \cdot \cdot \rho_3^{-e'_3} \cdots \rho_{n-1}^{-e'_{n-1}}.$$

The right-hand side has a k-multiple of $\binom{c_n}{d_n}$ in every column, and so is a reflection. The left-hand side is an element of G, so this reflection must be trivial, contradicting the definition of σ.

So we can assume that the aforementioned set is a basis for $F[n-1]$. Pick any $\theta \in F[n-1] \setminus G$. It will describe the action of σ_n on $S[n-1]$. There are $e_4, \cdots, e_{n-1}, e'_3, \cdots, e'_{n-1}, e \in \mathbb{F}_p$ (different from before) such that

$$\theta = \sigma_4^{e_4} \cdots \sigma_{n-1}^{e_{n-1}} \cdot \rho_3^{e'_3} \cdots \rho_{n-1}^{e'_{n-1}} \left(\sigma \cdot \left[\begin{pmatrix} -c_n \\ -d_n \end{pmatrix}_n\right]\right)^e$$

In the basis B, replace each x_i for $i = 3, \cdots, n-1$ by $x_i - e'_i e^{-1} x_n$. Amongst the factors of θ as written, this affects only the last. This change is compensated in the equation by having $e'_3 = \cdots = e'_{n-1} = 0$, to give

$$\theta = \sigma_4^{e_4} \cdots \sigma_{n-1}^{e_{n-1}} \left(\sigma \cdot \left[\begin{pmatrix} -c_n \\ -d_n \end{pmatrix}_n\right]\right)^e$$
$$\theta \cdot \left[\begin{pmatrix} ec_n \\ ed_n \end{pmatrix}_n\right] = \sigma_4^{e_4} \cdots \sigma_{n-1}^{e_{n-1}} \cdot \sigma^e \in G$$

Set σ_n to be the value in the last line. Since $\theta \notin G$, we must have $e \neq 0$. Replace x_n in the basis B by $e^{-1}x_n$ to get $\sigma_n = \theta \cdot \left[\begin{pmatrix} c_n \\ d_n \end{pmatrix}_n\right]$.

If $c_n = 0$, pick $\theta = \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_3\right]$. Else, pick $\theta = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_{n-1}\right]$ to get $\sigma_n = \left[\begin{pmatrix} 0 & 1 \\ 1 & d_n \end{pmatrix}_n\right]$. ☐

By reordering the basis B and relabeling b_i in the lemma as necessary, we can assume that the group G in lemma 2.3.6 is

$$G = \left\langle \left[\begin{pmatrix} 0 & 1 \\ 1 & b_i \end{pmatrix}_i\right] : i = 4, \cdots, n \right\rangle.$$

This is almost a block. The next lemma will show how to change each b_i to zero.

Lemma 2.3.7. Let $n \geq 4$. Let $G = \left\langle \sigma_i := \left[\begin{pmatrix} 0 & 1 \\ 1 & b_i \end{pmatrix}_i\right] : 4 \leq i \leq n \right\rangle$, with $b_i \in k$. With a change of basis, we can assume that $b_4 = \cdots = b_n = 0$.

Proof. If $n = 4$, then G is the double-transvection group, and done. So assume that $n > 4$. Apply the change of basis in B replacing x_n by $x_n - b_n x_{n-1}$. Then

1. σ_n becomes $\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_n\right]$ as necessary;
2. σ_{n-1} becomes $\left[\begin{pmatrix} 0 & 1 & -b_n \\ 1 & b_{n-1} & -b_{n-1}b_n \end{pmatrix}_n\right]$; and

3. σ_j is left unchanged if $j \neq n$ and $j \neq n-1$.

Replace σ_{n-1} by $\sigma_{n-1}\sigma_n^{b_n} = \left[\begin{pmatrix} 0 & 1 & 0 \\ 1 & b_{n-1}+b_n & -b_{n-1}b_n \end{pmatrix}\right]$. Then the following holds with $i = n-1$ in the current basis of V^*.

1. $\sigma_j = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_j\right]$ are of the required forms for $j > i$;
2. $\sigma_i = \left[\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & b'_i & b'_{i+1} & \cdots & b'_n \end{pmatrix}_n\right]$, for some $b'_i, \cdots, b'_n \in k$; and
3. $\sigma_j = \left[\begin{pmatrix} 0 & 1 \\ 1 & b_j \end{pmatrix}_j\right]$ are unchanged for $j < i$.

Suppose these three conditions are true for some $n > i \geq 4$. Noting that σ_j has zeroes in column $i-1$ unless $j = i$ which has $\binom{0}{1}$, and $j = i-1$ which has $\binom{1}{b_{i-1}}$ if $i > 4$, apply the change of basis replacing x_j by $x_j - b'_j x_{i-1}$ for $j = i, \cdots, n$.

1. σ_i becomes $\left[\left(\begin{array}{cc|c} 0 & 0 & 1 \\ 0 & 1 & 0 \end{array}\right)_i\right]$ as necessary;
2. σ_{i-1} becomes $\left[\left(\begin{array}{cc|ccc} 0 & 1 & -b'_i \cdot 1 & \cdots & -b'_n \cdot 1 \\ 1 & b_{i-1} & -b'_i b_{i-1} & \cdots & -b'_n b_{i-1} \end{array}\right)_n\right]$ if $i > 4$; and
3. σ_j is left unchanged if $j \neq i$ and $j \neq i-1$.

If $i = 4$, then done. Otherwise, replacing σ_{i-1} with $\sigma_{i-1}\sigma_i^{b'_i} \cdots \sigma_n^{b'_n}$, to satisfy the above three conditions for the case $i-1$. Apply the same steps again. Since i is decreased by one each time, it must eventually reach $i = 4$, and done. $\square$

We put the last two lemmas together.

Lemma 2.3.8. Let $n \geq 5$. Suppose G has no non-trivial reflections with $G[n-1] = F^{\langle 2,n-1 \rangle}$ and $[G : G[n-1]] = p$. With a change of basis, we can assume that $G = F^{\langle 2,n \rangle}$.

Proof. By lemma 2.3.6, with a change of basis, we can write $G = \langle G[n-1], \sigma_n \rangle$, where $\sigma_n = \left[\begin{pmatrix} 0 & 1 \\ 1 & b_n \end{pmatrix}_n\right]$ or $\left[\binom{1}{0}_3 + \binom{0}{1}_n\right]$, for some $b_n \in k$. In the first case, by lemma 2.3.7, using a change of basis, we can assume that $b_n = 0$, giving $G = \left\langle F^{\langle 2,n-1 \rangle}, \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_n\right] \right\rangle = F^{\langle 2,n \rangle}$. In the latter case, reordering the basis B, by moving x_n to before x_3, also gives $G = \left\langle \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_4\right], F^{\langle 3,n \rangle} \right\rangle = F^{\langle 2,n \rangle}$, as required. $\square$

The lemma showed how to extend one block repeatedly. Now consider the case with two blocks. Here, more care is needed around changes of basis.

Lemma 2.3.9. Suppose G has no non-trivial reflections, $G\,[n-1]$ consists of two blocks say $G\,[n-1] = \left\langle F^{\langle 2,m_1\rangle}, F^{\langle m_1,m_2\rangle}\right\rangle$ with $m_2 = n-1$, and that $[G : G\,[n-1]] = p$. With a $G\,[n-1]$-stable change of basis, we can assume that $G = \langle G\,[n-1]\,, \sigma_n\rangle$, where

$$\sigma_n = \left[\begin{pmatrix}0\\1\end{pmatrix}_{m_j} + \begin{pmatrix}1\\b_n\end{pmatrix}_n\right] \text{ or } \left[\begin{pmatrix}1\\0\end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix}0\\1\end{pmatrix}_n\right],$$

with $j = 1$ or 2 and $b_n \in k$.

Proof. Pick any $\sigma_n \in G\,[n] \setminus G\,[n-1]$. Write $\sigma_n = \left[\begin{pmatrix} a_3 & \cdots & a_n \\ b_3 & \cdots & b_n\end{pmatrix}\right]$. We will change σ_n to the required form. Visually, we have

$$G = \langle \sigma_i : i = 4, \cdots, m_1 \text{ and } i = m_1+2, \cdots, n\rangle\,,$$

for some $4 \le m_1$ and $m_1 + 2 \le m_2 = n-1$, and where

$$\begin{array}{rl}
\text{Column} & \begin{array}{ccccc|ccc|c} 3 & & \cdots & & m_1 & m_1+1 & \cdots & m_2 & n \end{array}\\
\sigma_4 = & \left[\left(\begin{array}{ccccc|ccc|c} 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \end{array}\right)\right]\\
\vdots & \qquad\quad \ddots \qquad\qquad\qquad\quad \vdots \qquad\qquad\quad \vdots\\
\sigma_{m_1} = & \left[\left(\begin{array}{ccccc|ccc|c} 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 & 0 \end{array}\right)\right]\\
\sigma_{m_1+2} = & \left[\left(\begin{array}{ccc|ccccc|c} 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 & 0 \end{array}\right)\right]\\
\vdots & \qquad\quad \vdots \qquad\qquad\qquad\quad \ddots \qquad\qquad\quad \vdots\\
\sigma_{m_2} = & \left[\left(\begin{array}{ccc|ccccc|c} 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \end{array}\right)\right]\\
\sigma_n = & \left[\left(\begin{array}{ccc|ccc|c} a_3 & \cdots & a_{m_1} & a_{m_1+1} & \cdots & a_{m_2} & a_n \\ b_3 & \cdots & b_{m_1} & b_{m_1+1} & \cdots & b_{m_2} & b_n \end{array}\right)\right]
\end{array}$$

We first eliminate some known cases. Since σ_n cannot be a reflection, it must have at least two non-zero columns. In particular, it is not possible for $a_i = b_i = 0$ for all $i = 3, \cdots, m_2$. If σ_n has zeroes in all columns of either blocks $F^{\langle 2,m_1\rangle}$ or $F^{\langle m_1,m_2\rangle}$, then, by ignoring those columns, we are in the situation of one-extending columns m_2 or m_1 respectively, and the lemma follows from applying lemma 2.3.6.

So from here, we assume instead that σ_n has a non-zero column amongst columns $3, \cdots, m_1$, one amongst columns $m_1+1, \cdots, m_2$, and in column n. Consider the action of G on the subspace $\langle x_1, \cdots, x_{m_1},\ x_n\rangle$. It is described by $\left\langle F^{\langle 2,m_1\rangle}, \sigma_n\right\rangle$, where σ_n one-extends column m_1 in the subspace. Since σ_n does not act trivially on the subspace, apply lemma 2.3.6 on this subspace: with a $F^{\langle 2,m_1\rangle}$-fixing change of basis, we can assume that

$$\begin{aligned}
\sigma_n &= \left[\left(\begin{array}{cccc|ccc|c} 0 & \cdots & 0 & 0 & a_{m_1+1} & \cdots & a_{m_2} & 1 \\ 0 & \cdots & 0 & 1 & b_{m_1+1} & \cdots & b_{m_2} & b_n \end{array}\right)\right] \\
\text{or } \sigma_n &= \left[\left(\begin{array}{cccc|ccc|c} 1 & 0 & \cdots & 0 & a_{m_1+1} & \cdots & a_{m_2} & 0 \\ 0 & 0 & \cdots & 0 & b_{m_1+1} & \cdots & b_{m_2} & 1 \end{array}\right)\right]
\end{aligned}$$

depending on whether $a_n \neq 0$. Similarly, by considering the action of G on the subspace $\langle x_1, x_2,\ x_{m_1+1}, \cdots, x_n\rangle$, we can assume

$$\begin{aligned}
\sigma_n &= \left[\left(\begin{array}{ccc|ccc|c} \cdots & 0 & 0 & \cdots & 0 & 0 & 1 \\ \cdots & 0 & 1 & \cdots & 0 & 1 & b_n \end{array}\right)\right] \\
\text{or } \sigma_n &= \left[\left(\begin{array}{ccc|ccc|c} 1 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{array}\right)\right].
\end{aligned}$$

We will focus on the first case with $\binom{a_n}{b_n} = \binom{1}{b_n}$. The $a_n = 0$ case is analogous. By noting the linear dependence of the columns of σ_n, we can see that it is not possible to make σ_n have all zeroes in the columns of one of the blocks without involving the columns of the other block. So we will search for a change of basis that stablises the other block. We want to subtract the columns of second block $F^{\langle m_1,m_2\rangle}$ from the columns of the first block $F^{\langle m_0,m_1\rangle}$, in a way that $\binom{0}{1}$ in column m_1 of σ_n would be changed to zeroes using $\binom{0}{1}$ in column m_2. Let w_1 and w_2 denote the width of the two blocks. Assume that $w_1 \geq w_2$ (by swapping the two blocks if necessary and then undo-ing this swap later). Apply the change of basis replacing x_{m_1-i} by $x_{m_1-i} - x_{m_2-i}$, for $i = 0, \cdots, w_2 - 1$. This fixes $G[m_1]$. And certainly, σ_n becomes $\left[\left(\begin{smallmatrix} 0 & 1 \\ 1 & b_n \end{smallmatrix}\right)_n\right]$. However, it also affects the elements $\sigma_i = \left[\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)_i\right]$ of the second block for $i = m_1 + 2, \cdots, m_2$, They become

$$\sigma_i = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{i-w_2} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i\right].$$

Replacing σ_i by $\sigma_i \sigma_{i-w_2}^{-1}$ reverses the effect. Since $\sigma_{i-w_2} \in G[n-1]$, this change of basis is $G[n-1]$-stable, as required by the lemma.

In the case of $a_n = 0$, the change of basis replaces x_{2+i} by $x_{2+i} - x_{m_1+i}$ for $i = 1, \cdots, w_2$. And σ_i is replaced by $\sigma_i \sigma_{i-w_1}^{-1}$, also for $i = m_1 + 2, \cdots, m_1 + w_2$, where w_1 is the width of the first block. $\square$

In lemma 2.3.9, the reader may note that lemma 2.3.7 can be applied to force $b_n = 0$, or a reordering of basis, to recover the form of two blocks. However, this uses a change of basis that may not be $G[n-1]$-stable, which later lemmas will depend on. So the lemma had, and many of later ones will have, two cases.

Next we generalise to more than two blocks.

Lemma 2.3.10. Suppose G has no non-trivial reflections, $G[n-1]$ is generated by blocks, and $[G : G[n-1]] = p$. That is,

$$G[n-1] = \left\langle F^{\langle 2,m_1\rangle}, \cdots, F^{\langle m_{l-1},m_l\rangle}\right\rangle$$
$$G = \langle G[n-1], \sigma_n\rangle,$$

for some $2 = m_0 < m_1 < \cdots < m_l = n-1$, $l \geq 1$, and $\sigma_n \in G \setminus G[n-1]$. Suppose the width of the blocks from left to right are non-increasing. With a

$G\left[n-1\right]$-stable change of basis, we can assume that

$$\sigma_n = \left[\begin{pmatrix}0\\1\end{pmatrix}_{m_j} + \begin{pmatrix}1\\b_n\end{pmatrix}_n\right] \text{ or } \left[\begin{pmatrix}1\\0\end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix}0\\1\end{pmatrix}_n\right],$$

for some $1 \leq j \leq l$ and $b_n \in k$.

Proof. If $l = 1$, then this reduces to lemma 2.3.8. For larger l, proceed by induction. The base case $l = 2$ is lemma 2.3.9.

Suppose $l \geq 3$. Pick $\sigma \in G \setminus G\left[n-1\right]$ so that $G = \left\langle G\left[n-1\right], \sigma\right\rangle$. It cannot have all zeroes in every column $3, \cdots, n-1$, otherwise it is a reflection. In fact, assume that σ has at least one non-zero entry in the columns of each block $F^{\langle m_{j-1}, m_j\rangle}$, for $1 \leq l$. If this is not true and σ has zeroes in the columns of say block $F^{\langle m_{j-1}, m_j\rangle}$ then we can restrict out attention to the subspace

$$\left\langle x_1, \cdots, x_{m_{j-1}},\ x_{m_j+1}, \cdots, x_n \right\rangle.$$

The action of G on such a subspace is described by a subgroup $G' < G$ with one less block, namely the same blocks and σ but without $F^{\langle m_{j-1}, m_j\rangle}$. Since the block $F^{\langle m_{j-1}, m_j\rangle}$ fixes this subspace and G' fixes $\left\langle x_{m_{j-1}+1}, \cdots, x_{m_j}\right\rangle$, we have $G = G' \boxtimes F^{\langle 2, 2+m_j-m_{j-1}\rangle}$, up to a reordering of basis. By induction hypothesis, the subgroup G' satisfies the lemma. Undo-ing the basis reordering shows that the original group G also satisfies the lemma.

Suppose the assumption on non-zero entries in σ is true. In particular, σ has non-zero entries in at least one column of each of the right-most two blocks $F^{\langle m_{l-2}, m_{l-1}\rangle}$ and $F^{\langle m_{l-1}, m_l\rangle}$. Restrict our attention to the subspace corresponding to the columns of these two blocks and σ. That is, the subspace

$$\left\langle x_1, x_2,\ x_{m_{l-2}+1}, \cdots, x_n \right\rangle.$$

The action of G on this subspace is described by the subgroup $G' = \langle G'', \sigma\rangle$, where $G'' = \left\langle F^{\langle m_{l-2}, m_{l-1}\rangle}, F^{\langle m_{l-1}, m_l\rangle}\right\rangle$. Use induction hypothesis on the $l = 2$ case on the space: with a G''-stable change of basis of the subspace, we can now assume that σ fixes the columns of one of the two blocks in G''. With this, G now fails the assumption on non-zero entries, in which case we know it satisfies the lemma. So this completes the induction step and the proof. $\square$

It remains to consider the columns $3 \leq j \leq m_0$ of each σ_i. The aim is to show that the columns are all zeroes. This is approached by considering a basis similar to lemma 2.3.6. However, instead of a space that increases horizontally with block width, the space will be visualised vertically instead.

Lemma 2.3.11. Suppose $n \geq 6$ and $3 \leq m_0 \leq n-3$, and

$$G\left[n-1\right] = \left\langle G\left[m_0\right], F^{\langle m_0, n-1\rangle}\right\rangle$$
$$G = \left\langle G\left[n-1\right], \sigma_n\right\rangle,$$

for some $\sigma_n \in G \setminus G\left[n-1\right]$. With a $G\left[m_0\right]$-fixing and $G\left[n-1\right]$-stable change of basis, we can assume that

$$\sigma_n = \left[\begin{pmatrix} 0 & 1 \\ 1 & b_n \end{pmatrix}_n\right] \text{ or } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_0+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_n\right],$$

for some $b_n \in k$.

Proof. Write $\sigma_n = \left[\begin{pmatrix} c_3 & \cdots & c_{n-1} & a_n \\ d_3 & \cdots & d_{n-1} & b_n \end{pmatrix}\right]$. Consider the action of G on the subspace $\langle x_1, x_2, \ x_{m_0+1}, \cdots, x_n\rangle$. It can be described by $\left\langle F^{\langle m_0, n-1\rangle}, \sigma_n\right\rangle$. By lemma 2.3.8, using a $G\left[m_0\right]$-fixing and $G\left[n-1\right]$-stable change of basis, we can assume either

$$\sigma_n = \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} \\ d_3 & \cdots & d_{m_0} \end{pmatrix}_{m_0} + \begin{pmatrix} 0 & 1 \\ 1 & b_n \end{pmatrix}_n\right] \text{ or } \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} & 1 \\ d_3 & \cdots & d_{m_0} & 0 \end{pmatrix}_{m_0+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_n\right].$$

We will focus on the case $a_n = 1$ in entry $(1, n)$. The $a_n = 0$ case is analogous.

Align the columns of $\sigma_{m_0+2}, \cdots, \sigma_n$ as below.

$$\begin{array}{rl}
\text{Column} & \qquad 3 \qquad \cdots \qquad m_0 \qquad\qquad\qquad \cdots \qquad\quad n \\
\sigma_{m_0+2} = & \left[\left(\begin{array}{ccc|ccccc} 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \end{array}\right)\right] \\
\vdots & \qquad\quad \vdots \qquad\qquad\qquad\qquad \ddots \\
\sigma_{n-1} = & \left[\left(\begin{array}{ccc|ccccc} 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 1 & 0 & 0 \end{array}\right)\right] \\
\sigma_n = & \left[\left(\begin{array}{ccc|ccccc} c_3 & \cdots & c_{m_0} & 0 & \cdots & 0 & 0 & 1 \\ d_3 & \cdots & d_{m_0} & 0 & \cdots & 0 & 1 & b_n \end{array}\right)\right]
\end{array} \tag{2.1}$$

The matrix entries on the right can been seen as a large matrix of dimension $2(n - m_0 - 1) \times (n - 2)$. Let u_j denote column $j-2$ of this matrix. For example, $u_{m_0+1} = (0, 1, 0, 0, \cdots)^T$ with subscripts as labelled on the columns.

We will construct a basis for the column vector space $k^{2(n-m_0-1)}$ and use it to force $u_{m_0}, \cdots, u_3$ to be zeroes in that order. Let i be the largest of $j = m_0, \cdots, 3$ such that u_j contains non-zero entries. We allow $u_3, \cdots, u_i$ to contain any values, and not just the above form, as long as u_i is not all zeroes.

Let $\binom{a_i}{b_i} = [\sigma_i, x_i]$, where $\sigma_i \in G[m_0]$ is as constructed in lemma 2.2.3. (We only use the fact that $\sigma_i \in G[i] \setminus G[i-1]$.) Define

$$\begin{array}{rclccccl}
u'_{m_0+2} & = & (& a_i, b_i, & 0, 0, & \cdots, & 0, 0 &)^T \\
u'_{m_0+3} & = & (& 0, 0, & a_i, b_i, & \cdots, & 0, 0 &)^T \\
\vdots & = & & & & \ddots & & \\
u'_n & = & (& 0, 0, & 0, 0, & \cdots, & a_i, b_i &)^T
\end{array}$$

The set to consider for a basis consists of these new elements and some columns to the right of the big matrix:

$$\begin{array}{rl}
& \left\{u'_{m_0+2}, \cdots, u'_n,\ u_{m_0+1}, \cdots, u_{n-1}\right\}, \text{ if } a_i = 1; \\
\text{and} & \left\{u'_{m_0+2}, \cdots, u'_n,\ u_{m_0+2}, \cdots, u_n\right\}, \text{ if } a_i = 0.
\end{array}$$

Consider the span of this set for the case $a_i = 1$. Note that if the span contains the first three of the following, then it must also contain the fourth.

$$\begin{array}{rcllllll} u''_j & := & (& \cdots, & 0,1, & 0,0 & \cdots &)^T \\ u'_j & = & (& \cdots, & a_i,b_i, & 0,0 & \cdots &)^T \\ u_j & = & (& \cdots, & 1,0, & 0,1 & \cdots &)^T \\ u''_{j+1} & := & (& \cdots, & 0,0, & 0,1 & \cdots &)^T \end{array}$$

Start with $j = m_0 + 2$. Since the first vector $u''_{m_0+2} = u_{m_0+1}$ is in the span, the fourth vector u''_{m_0+3} is as well. So the case $j = m_0 + 3$ can be applied. Repeat until $j = n - 1$ to get u''_n in the space. Putting these together, the span contains

$$\begin{aligned} &\left\{u'_{m_0+2}, \cdots, u'_n,\ u''_{m_0+2}, \cdots, u''_n\right\}, \\ \text{where } &u'_j = (\cdots,\ 1,b_i,\ 0,0,\ \cdots) \\ \text{and } &u''_j = (\cdots,\ 0,1,\ 0,0,\ \cdots) \ \text{ in appropriate columns,} \end{aligned}$$

and it is clear that this spans $k^{2(n-m_0-1)}$.

The case $a_i = 0$ is similar. The four vectors to use are, starting with $j = n$,

$$\begin{array}{rcllllll} u''_j & := & (& \cdots, & 0,0, & 1,0 & \cdots &)^T \\ u'_j & = & (& \cdots, & 0,0, & a_i,b_i & \cdots &)^T \\ u_{j-1} & = & (& \cdots, & 1,0, & 0,1 & \cdots &)^T \\ u''_{j-1} & := & (& \cdots, & 1,0, & 0,0 & \cdots &)^T. \end{array}$$

Ending with $j = m_0 + 3$ gives also the set $\left\{u'_j, u''_j\right\}_{j=m_0+2}^{n}$ that spans $k^{2(n-m_0-1)}$. In both cases, this shows that our original set is a basis.

We now use this basis to make column u_i of the big matrix zero. Write (putting the two cases together for simplicity)

$$u_i = \left(u'_{m_0+2}\right)^{e'_{m_0+2}} + \cdots + \left(u'_n\right)^{e'_n} + u_{m_0+1}^{e_{m_0+1}} + \cdots + u_n^{e_n},$$

for some $e'_{m_0+2}, \cdots, e'_n, e_{m_0+1}, \cdots, e_n \in \mathbb{F}_p$. Since each u_j on the right end represents column j of the big matrix, replacing x_i in B by

$$x_i - e_{m_0+1}x_{m_0+1} - \cdots - e_n x_n$$

allows us to assume that

$$\begin{aligned} u_i &= \left(u'_{m_0+2}\right)^{e'_{m_0+2}} + \cdots + \left(u'_n\right)^{e'_n} \\ &= \left(\ e'_{m_0+2}a_i,\ e'_{m_0+2}b_i,\ \cdots,\ e'_n a_i,\ e'_n b_i\ \right)^T. \end{aligned}$$

That is, each of $\sigma_{m_0+2}, \cdots, \sigma_n$ has a k-multiple of $\binom{a_i}{b_i}$ in column i.

To make these columns zeroes, since $[\sigma_i, x_i] = \binom{a_i}{b_i}$, replace σ_j by $\sigma_j \sigma_i^{-e'_j}$ for $j = m_0 + 2, \cdots, n$. This turns u_i into a column of zeroes, thereby reducing the value of i. When $u_j = 0$ for $j = m_0, \cdots, 3$, we have the required form for $\sigma_{m_0+2}, \cdots, \sigma_n$.

Note, at no point, $\sigma_3, \cdots, \sigma_{m_0}$ was changed, and the changes of basis applied fix them. Note also $\sigma_{m_0+2}, \cdots, \sigma_n$ were multipled by elements of $G[m_0]$ and in particular not by σ_n. So the overall changes of basis were $G[n-1]$-stable. $\square$

Combining the last two lemmas together gives the most general case possible without breaking the assumption $[G[i] : G[i-1]] \le p$ for $m_0 + 1 \le i \le n$.

Lemma 2.3.12. Let $G \le F$. Suppose $n \ge 6$ and $3 \le m_0 \le n-3$, and

$$\begin{aligned} G[n-1] &= \left\langle G[m_0], F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle} \right\rangle \\ G &= \langle G[n-1], \sigma_n \rangle, \end{aligned}$$

for some $2 = m_0 < m_1 < \cdots < m_l = n-1$, $l \ge 1$, and $\sigma_n \in G \setminus G[n-1]$. Suppose the width of the blocks from left to right are non-increasing. With a $G[m_0]$-fixing and $G[n-1]$-stable change of basis, we can assume that

$$\sigma_n = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_{m_j} + \begin{pmatrix} 1 \\ b_n \end{pmatrix}_n \right] \text{ or } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_n \right],$$

for some $1 \le j \le l$ and $b_n \in k$.

Proof. If $l = 1$, then this is just lemma 2.3.11. Suppose $l \geq 2$. Consider the action of G on the subspace $\langle x_1, x_2,\ x_{m_0+1}, \cdots, x_n\rangle$. It is described by the subgroup $G' = \langle G'', \sigma_n\rangle$ where $G'' = \left\langle F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle}\right\rangle$. Apply lemma 2.3.10: with a G''-stable change of basis, we can assume that

$$\sigma_n = \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} \\ d_3 & \cdots & d_{m_0}\end{pmatrix}_{m_0} + \begin{pmatrix}0\\1\end{pmatrix}_{m_j} + \begin{pmatrix}1\\b_n\end{pmatrix}_n\right]$$
$$\text{or } \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} \\ d_3 & \cdots & d_{m_0}\end{pmatrix}_{m_0} + \begin{pmatrix}1\\0\end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix}0\\1\end{pmatrix}_n\right].$$

for some $1 \leq j \leq l$ and $b_n \in k$. The change of basis also fixes $G[m_0]$ since it is not involved in the subspace.

And now, σ_n only has non-zero entries in possibly columns $3, \cdots, m_0$ and columns of a single block $F^{\langle m_{j-1}, m_j\rangle}$. This time, consider the action of G on the subspace $\left\langle x_1, x_2,\ x_{m_{j-1}+1}, \cdots, m_j\right\rangle$. It is described by $G[m_0]$ and $F^{\langle m_{j-1}, m_j\rangle}$. Apply lemma 2.3.11: with a $G[m_0]$-fixing and $\left\langle G[m_0], F^{\langle m_{j-1}, m_j\rangle}\right\rangle$-stable change of basis, we can assume that σ_n has zeroes in columns $3, \cdots, m_0$. This gives σ_n the required form. Note that the change of basis is $G[n-1]$-stable since the other blocks are not involved in the subspace. This completes the proof. □

We put everything in this subsection together.

Lemma 2.3.13. Let $G \leq F$. Suppose $[G[i] : G[i-1]] \leq p$ for $m_0 + 1 \leq i \leq n$. Up to a change of basis, we can assume that

$$G = \left\langle G[m_0], F^{\langle m_{j-1}, m_j\rangle} : 1 \leq j \leq l\right\rangle.$$

for some $2 \leq m_0 < \cdots < m_l = n$, $l \geq 0$,

Proof. We will prove by induction on $G[i]$ satisfying the lemma, though some values of i will be skipped, as a consequence of $[G[i] : G[i-1]] = 1$. The base case is $i = m_0$, which does satisfy the lemma with $l = 0$.

For the induction step, fix $i = m_0, \cdots, n-1$. Suppose $G[i]$ satisfies this lemma. If $G[i+1] = G[i]$, applying lemma 2.3.5 creates a new block, to get

$$G[i+2] = \left\langle G[i], F^{\langle m_l, m_{l+1} \rangle} \right\rangle.$$

Assume instead $G[i+1] > G[i]$ is strict. Using the premise on subgroup index, $G[i+1] = \langle G[i], \sigma_{i+1} \rangle$ for some $\sigma_{i+1} \in G \setminus G[i]$. Applying lemma 2.3.12 shows that

$$\sigma_{i+1} = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_{m_j} + \begin{pmatrix} 1 \\ b_{i+1} \end{pmatrix}_{i+1} \right] \text{ or } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{i+1} \right],$$

for some $1 \le j \le n$ and $b_n \in k$. The blocks and basis can be reordered so that $j = l$. In the first form of σ_{i+1}, we can force $b_{i+1} = 0$ using a change of basis with lemma 2.3.7. In the second form, reorder the basis moving x_{i+1} to before $x_{m_{j-1}+1}$. In both cases, $\left\langle F^{\langle m_{j-1}, m_j \rangle}, \sigma_n \right\rangle$ turns into a block using a change of basis. This gives the required form, completing the induction step and proof. □

2.3.2 Blocks with saturated columns

In this subsection, we will finish proving proposition 2.3.3 which describes a general form for two-row groups. We will then find the invariant rings of some groups of the form $\left\langle F^{\langle *,* \rangle}, \tau_* \right\rangle$ in proposition 2.3.26.

For proving the general form, this subsection considers the remaining case when we find that $[G[i], G[i-1]] = p^2$ for some $i = m_0 + 1, \cdots, n$. The aim is to find non-trivial $\sigma_i, \tau_i \in G$ such that $G[i] = \langle G[i-1], \sigma_i, \tau_i \rangle$. We will find some non-trivial $\tau_i \in G$ for some such i, and its interaction with the rest of the group will be investigated. To start, we introduce a terminology to distinguish them with the case discussed in the last subsection.

Notation 2.3.14. Write $w_j := m_j - m_{j-1}$ for the width of a block $F^{\langle m_{j-1}, m_j \rangle}$.

The block itself has order $p^{w_j - 1}$, and so $[G[m_j] : G[m_{j-1}]] \ge p^{w_j - 1}$.

Definition 2.3.15. The columns of a block $F^{\langle m_{j-1}, m_j \rangle}$ are *saturated* in G if

$$[G\,[m_j] : G\,[m_{j-1}]] = p^{w_j}.$$

It is saturated in the following sense. If $[G\,[m_j] : G\,[m_{j-1}]] \geq p^{w_j+1}$, then G one-extends column m_{j-1}, using the lemma to follow.

Lemma 2.3.16. Let $G \leq F$ be a group of order p^{n-2} with no non-trivial reflections. Let $G' = \left\langle \rho_i := \left[\binom{a}{b}_i \right] : i = 3, \cdots, n \right\rangle$ with $\binom{a}{b} \neq \binom{0}{0}$. Then $F = \langle G, G' \rangle$. As a corollary, every subgroup of F of order at least p^{n-1} contains a reflection.

Proof. For a contradiction, suppose $\langle G, G' \rangle < F$ is strict. The group G can be generated by some $n-2$ elements $\sigma_3, \cdots, \sigma_n$ with no redundancies. So

$$\langle G, G' \rangle = \langle \sigma_3, \cdots, \sigma_n, \rho_3, \cdots, \rho_n \rangle,$$

with $2n-4$ elements listed on the right, exactly necessary for a basis of F. Since $\langle G, G' \rangle < F$, there must be non-trivial relations amongst these elements. Write

$$\begin{aligned} \sigma_3^{e_3} \cdots \sigma_n^{e_n} \cdot \rho_3^{e_3'} \cdots \rho_n^{e_n'} &= 1 \\ \rho_3^{e_3'} \cdots \rho_n^{e_n'} &= \sigma_3^{-e_3} \cdots \sigma_n^{-e_n} \in G, \end{aligned}$$

for some $e_3, \cdots, e_n, e_3', \cdots, e_n' \in \mathbb{F}_p$ not all zeroes. The product of ρ_i on the left-hand side is a reflection, since every column of the product is a $\mathbb{F}_p$-multiple of $\binom{a}{b}$. That means the product is trivial, as the only reflection in G. Since $\rho_3, \cdots \rho_n$ are one-columns with non-zero entries in different columns, their exponents $e_3', \cdots, e_n'$ must be zeroes. So the other exponents $e_1, \cdots e_{n-1}$ cannot all be zeroes by definition. But since $\sigma_3, \cdots, \sigma_{n-1}$ have no redundancies by definition, the product in the right-hand side cannot be trivial, leading to a contradiction.

For the corollary part, let $\overline{G} \leq F$ be a subgroup of order p^{n-1}. Assume that it does not contain any non-trivial reflections, and that it contains G, as some subgroup of order p^{n-2}. Take $\sigma \in \overline{G} \setminus G$. Using the basis of F found above,

$$\sigma = \sigma_3^{e_3} \cdots \sigma_n^{e_n} \cdot \rho_3^{e'_3} \cdots \rho_n^{e'_n}$$
$$\rho_3^{-e'_3} \cdots \rho_n^{-e'_n} = \sigma^{-1} \cdot \sigma_3^{e_3} \cdots \sigma_n^{e_n} \in \overline{G},$$

for some (different) $e_3, \cdots, e_n, e'_3, \cdots, e'_n \in \mathbb{F}_p$. If $\overline{G}$ has no non-trivial reflections, then the left-hand side is 1. This time, it leads to $\sigma = \sigma_3^{e_3} \cdots e_n^{e_n} \in G$, contradicting its definition. So every subgroup of F of order at least p^{n-1} must contain a subgroup of order p^{n-1} which in turn must contain a reflection. $\square$

This suggests that at most one non-trivial τ_j can be expected for each block in G, for otherwise G one-extends the last column of a previous block, and we could increase its width instead of starting a new block. This partially explains the choice of τ_{m_j} in proposition 2.3.3.

We now construct lemmas for proving proposition 2.3.3. As in the case with blocks with unsaturated columns in the last subsection, proceed by investigating a small set of columns at a time. It will be done in some form of induction. So a few useful lemmas will be shown first, to be used in induction steps.

The simplest situation not considered so far is when the group $G \leq F$ contains a block $F^{\langle 2,n\rangle}$, but has $\left[G : F^{\langle 2,n\rangle}\right] = p$. This is when τ_n becomes necessary.

Lemma 2.3.17. Let $n \geq 4$. Suppose G has no non-trivial reflections, $G = \left\langle F^{\langle 2,n\rangle}, \tau_n \right\rangle$ and $[G : G[n-1]] = p^2$. Without any changes of basis, we can assume that τ_n has the form required by proposition 2.3.3. That is,

$$\tau_n = \left[\begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_n \end{pmatrix}\right],$$

for some $d_3, \cdots, d_n \in k$. Not all choices of d_i are possible. In particular, $d_n \neq 0$, whence $[G : G[n-1]] = p^2$ remains true.

Proof. Write $\sigma_i = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i\right]$. Pick any $\tau \in G \setminus F^{\langle 2,n\rangle}$. Write $\tau = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{pmatrix}\right]$. Replace τ by $\tau\sigma_4^{-c_4} \cdots \sigma_n^{-c_n}$ to force $c_4 = \cdots = c_n = 0$. Note that $c_3 \neq 0$, else τ is now a reflection. Set τ_n to $\tau^{c_3^{-1}}$.

It remains to show that $d_n \neq 0$. If it is zero, then G contains

$$\tau_n \sigma_4^{-d_3} \cdots \sigma_n^{-d_{n-1}} = \left[\begin{pmatrix} 1 & -d_3 & \cdots & -d_{n-1} \\ 0 & 0 & \cdots & 0 \end{pmatrix} \right],$$

which is a non-trivial reflection — a contradiction. So $d_n \neq 0$ must hold. $\square$

In order to use induction, we look into how a group G that does not contain any non-trivial reflection may one-extend column $n-1$, when $G[n-1]$ contains two blocks say $F^{\langle 2,m_1 \rangle}$ and $F^{\langle m_1,n-1 \rangle}$. The subgroup index $[G : G[n-1]]$ can be p or p^2 and each of the two blocks may or may not have saturated columns, giving a total of eight cases to consider.

Start with the subgroup index p cases first. We will show that G can either be generated by two blocks as well, or G can be made in a single block. Lemma 2.3.9 considered the case where neither of the blocks have saturated columns. We consider next the cases where the second block $F^{\langle m_1,n-1 \rangle}$ has saturated columns.

Lemma 2.3.18. Let $n \geq 5$. Suppose G one-extends column $n-1$, and that $G[n-1] = \left\langle F^{\langle 2,n-1 \rangle}, \tau_{n-1} \right\rangle$ is a block with saturated columns as in lemma 2.3.17. There is a reflection σ in G, or equivalently G one-extends column 2. Using a $G[n-1]$-fixed change of basis, σ can be made into a one-column at column n.

Proof. Write $G[n-1] = \left\langle \sigma_i = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i \right], \tau_{n-1} : i = 4, \cdots, n-1 \right\rangle$. Pick any $\tau \in G \setminus G[n-1]$, say $\tau = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{pmatrix} \right]$. We want to apply lemma 2.3.16.

Define $\rho_i = \left[\begin{pmatrix} c_n \\ d_n \end{pmatrix}_i \right]$. Since $G[n-1]$ is a group of order p^{n-3} with no non-trivial reflections, the lemma says that the set $\{\sigma_4, \cdots, \sigma_{n-1}, \tau_{n-1}, \rho_3, \cdots, \rho_{n-1}\}$

forms a basis for $F[n-1]$. Using this basis, write

$$\left[\begin{pmatrix} c_3 & \cdots & c_{n-1} \\ d_3 & \cdots & d_{n-1} \end{pmatrix}_{n-1}\right] = \sigma_4^{e_4}\cdots\sigma_{n-1}^{e_{n-1}}\tau_{n-1}^{e}\rho_3^{e'_3}\cdots\rho_{n-1}^{e'_{n-1}}$$

$$\left[\begin{pmatrix} c_3 & \cdots & c_{n-1} \\ d_3 & \cdots & d_{n-1} \end{pmatrix}_{n-1}\right]\sigma_4^{-e_4}\cdots\sigma_{n-1}^{-e_{n-1}}\tau_{n-1}^{-e} = \rho_3^{e'_3}\cdots\rho_{n-1}^{e'_{n-1}}$$

$$= \left[\begin{pmatrix} e'_3c_n & \cdots & e'_{n-1}c_n \\ e'_3d_n & \cdots & e'_{n-1}d_n \end{pmatrix}_{n-1}\right],$$

for some $e_i, e, e'_i \in \mathbb{F}_p$. This shows that $\sigma := \tau\sigma_4^{-e_4}\cdots\sigma_{n-1}^{-e_{n-1}}\tau_{n-1}^{-e} \in G$ has a $\mathbb{F}_p$-multiple of $\binom{c_n}{d_n}$ in every column, say $\sigma = \left[\begin{pmatrix} \lambda_3c_n & \cdots & \lambda_nc_n \\ \lambda_3d_n & \cdots & \lambda_nd_n \end{pmatrix}\right]$ with $\lambda_n = 1$, whence a reflection.

To make σ one-column, replace x_i in B by $x_i - \lambda_i x_n$ for $i = 3, \cdots, n-1$. □

Using lemma 2.3.18, if the second block $F^{\langle m_1, n-1\rangle}$ has saturated columns, since σ from the lemma is one-column at column n, we can rearrange the basis B by moving x_n to before the columns of the second block, to have σ be a one-column in column $m_1 + 1$. If the first block does not have saturated columns, then we can apply lemma 2.3.8 to increase its width. If it does have saturated columns, use lemma 2.3.18 again to see that G one-extends column $m_0 = 2$, which is not possible.

For our investigation into $[G : G[n-1]] = p$, the remaining subcase is where the first block $F^{\langle 2, m_1\rangle}$ has saturated columns but the second block does not.

Lemma 2.3.19. Suppose G has no non-trivial reflections, $n \geq 7$,

$$G[n-1] = \left\langle F^{\langle 2,m_1\rangle}, \tau_{m_1}, F^{\langle m_1,n-1\rangle}\right\rangle$$
$$G = \langle G[n-1], \sigma_n\rangle$$

for some $4 \leq m_1 \leq n-3$, τ_{m_1} as described in lemma 2.3.17, and where $\sigma_n \in$

$G \setminus G[n-1]$. Using a $G[n-1]$-fixing change of basis, we can assume

$$\sigma_n = \left[\begin{pmatrix} 0 & 1 \\ 1 & b_n \end{pmatrix}_n\right] \text{ or } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_1+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_n\right],$$

The change of basis preserves column n of σ_n up to a k-multiple.

Proof. Note that σ_n cannot one-extend column m_1 by lemma 2.3.18, and it must have a non-zero entry in the columns of $F^{\langle m_1, n-1\rangle}$. Consider the action of G on the subspace $\langle x_{m_1+1}, \cdots, x_n\rangle$. It acts as $\left\langle F^{\langle m_1, n-1\rangle}, \sigma_n\right\rangle$. Using lemma 2.3.6, which uses a $F^{\langle m_1, n-1\rangle}$-fixing change of basis, we can assume that

$$\begin{aligned} \sigma = & \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} & 0 & \cdots & 0 & 1 \\ d_3 & \cdots & d_{m_0} & 0 & \cdots & 1 & b_n \end{pmatrix}\right] \\ \text{or} & \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} & 0 & 0 & \cdots & 0 \\ d_3 & \cdots & d_{m_0} & 1 & 0 & \cdots & 1 \end{pmatrix}\right]. \end{aligned}$$

The same steps as in lemma 2.3.18 are applicable. We consider the first form of σ; the other form is analogous. Define $\rho_i = \left[\begin{pmatrix} 1 \\ b_n \end{pmatrix}_i\right]$ (or $\left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_i\right]$ depending on the form of σ). The set

$$\{\sigma_4, \cdots, \sigma_{m_0}, \tau_{m_1}, \rho_3, \cdots, \rho_{m_0}\}$$

is a basis for $F[m_0]$ by lemma 2.3.16. Using this basis, by replacing σ with $\sigma\sigma_4^{e_4}\cdots\sigma_{m_0}^{e_{m_0}}\tau_{m_1}^{e}$ for some appropriately chosen exponents, we can assume that columns $3, \cdots, m_0$ of σ are k-multiples of $\binom{1}{b_n}$ (or $\binom{0}{1}$) Now apply the change of basis replacing x_i in B by $x_i - c_i x_n$ (or $x_i - d_i x_n$), for $i = 3, \cdots, m_0$. This forces columns $3, \cdots, m_0$ of σ to be zeroes, completing the proof. $\square$

This completes all cases with $[G : G[n-1]] = p$. We put them together.

Lemma 2.3.20. Suppose $G = \langle G[n-1], \sigma_n\rangle$ and $G[n-1]$ satisfies 2.3.3. So,

$$G[n-1] = \left\langle G[m_0], F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle}, \tau_{m_j} : 1 \le j \le l'\right\rangle.$$

Using a $G[m_0]$-fixing and $G[n-1]$-stable change of basis, we can assume that

$$\sigma_n = \left[\begin{pmatrix}0\\1\end{pmatrix}_{m_i} + \begin{pmatrix}1\\b_n\end{pmatrix}_n\right] \text{ or } \left[\begin{pmatrix}1\\0\end{pmatrix}_{m_{i-1}+1} + \begin{pmatrix}0\\1\end{pmatrix}_n\right],$$

for some $i = l'+1, \cdots, l$ and $b_n \in k$. The change of basis preserves column n of σ_n up to a k-multiple.

Proof. If $l = 0$, then $G[n-1] = G[m_0]$ and σ_n one-extends column m_0, contradicting the definition of m_0. If $l' = l \geq 1$, then every block of $G[n-1]$ have saturated columns, and G one-extends columns $m_{l-1}, \cdots, m_0$ by repeatedly applying lemma 2.3.18, again contradicting the definition of m_0. So we assume that there is at least one block ($l \geq 1$) and that not all of them have saturated columns ($l' \leq l-1$).

Write $\sigma_n = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n\end{pmatrix}\right]$. We can assume that there is at least one non-zero entry in the unsaturated columns $m_{l'}+1, \cdots, n-1$ of blocks, else σ_n one-extends column $l_{l'}$, giving us a contradiction again. If $l' = 0$, then this is precisely lemma 2.3.12. Suppose $l' \geq 1$. Consider how G acts on the subspace $\left\langle x_1, \cdots, x_{m_0},\ x_{m_{l'}+1}, \cdots, n\right\rangle$ corresponding to the columns of $G[m_0]$ and of the unsaturated block columns. It is the same as $G' = \langle G'', \sigma_n\rangle$ where

$$G'' = \left\langle G[m_0], F^{\left\langle m_{l'}, m_{l'+1}\right\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle}\right\rangle.$$

Apply lemma 2.3.12: with a $G[m_0]$-fixing and G''-stable change of basis, assume

$$\begin{aligned}\sigma_n = &\left[\begin{pmatrix} c_{m_0+1} & \cdots & c_{m_{l'}} \\ d_{m_0+1} & \cdots & d_{m_{l'}}\end{pmatrix}_{m_{l'}} + \begin{pmatrix}0\\1\end{pmatrix}_{m_j} + \begin{pmatrix}1\\b_n\end{pmatrix}_n\right] \\ \text{or } &\left[\begin{pmatrix} c_{m_0+1} & \cdots & c_{m_{l'}} \\ d_{m_0+1} & \cdots & d_{m_{l'}}\end{pmatrix}_{m_{l'}} + \begin{pmatrix}1\\0\end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix}0\\1\end{pmatrix}_n\right].\end{aligned}$$

where $l'+1 \leq j \leq l$ and $b_n \in k$. This means σ_n fixes $\langle x_1, \cdots, x_{m_0}\rangle$ and has zeroes in columns of all blocks with unsaturated columns except for $F^{\langle m_{j-1}, m_j\rangle}$.

For each block $F^{\left\langle m_{j'-1}, m_{j'}\right\rangle}$ with saturated columns ($1 \leq j' \leq l'$), consider how G acts on the subspace $\left\langle x_1, x_2,\ x_{m_{j'-1}+1}, \cdots, x_{m_{j'}},\ x_{m_{j-1}+1}, \cdots, x_{m_j},\ x_n\right\rangle$.

It is the same as the subgroup (re-using variables) $G' = \langle G'', \sigma_n \rangle$, where

$$G'' = \left\langle F^{\left\langle m_{j'-1}, m_{j'} \right\rangle}, \tau_{m_{j'}}, F^{\langle m_{j-1}, m_j \rangle} \right\rangle .$$

Apply lemma 2.3.19: with a G''-fixing change of basis, we can assume that σ_n has zeroes in the columns of each block $F^{\left\langle m_{j'-1}, m_{j'} \right\rangle}$. $\square$

We now have the four cases with $[G : G[n-1]] = p^2$ left to consider. If the second block $F^{\langle m_1, n-1 \rangle}$ has saturated columns, then the same argument from before applies. If the first block does not have saturated columns, then we can apply lemma 2.3.17 meant for a single block. If the first block does have saturated columns, then G one-extends column m_0 leading to a contradiction.

In the two remaining cases, the second block $F^{\langle m_1, n-1 \rangle}$ does not have saturated columns. The two cases correspond to whether $F^{\langle 2, m_1 \rangle}$ has saturated columns. We start with the case where it does, which is an easier case.

Lemma 2.3.21. Let $n \geq 6$. Suppose G has no non-trivial reflections, with $[G : G[n-1]] = p^2$, and $G = \langle G', \tau_n \rangle$ where

$$G' = \left\langle F^{\langle 2, m_1 \rangle}, \tau_{m_1}, F^{\langle m_1, n \rangle} \right\rangle ,$$

for some $4 \leq m_1 \leq n-2$, and $\tau_{m_1} \in G[m_1]$ as described in lemma 2.3.17. Without applying any changes of basis, we can assume that

$$\tau_n = \left[\begin{pmatrix} 0 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_{m_1} \end{pmatrix}_{m_1} + \begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_{m_1+1} & d_{m_1+2} & \cdots & d_n \end{pmatrix}_n \right],$$

for some $d_i \in k$ and $d_n \neq 0$.

Proof. Apply lemma 2.3.17: by multiplying with $\sigma_{m_1+2}, \cdots, \sigma_n$, assume that

$$\tau_n = \left[\begin{pmatrix} c_3 & c_4 & \cdots & c_{m_1} \\ d_3 & d_4 & \cdots & d_{m_1} \end{pmatrix}_{m_1} + \begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_{m_1+1} & d_{m_1+2} & \cdots & d_n \end{pmatrix}_n \right],$$

with $d_n \neq 0$. Now apply the steps from lemma 2.3.18. Write $\sigma_i := \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i \right]$ and let $\rho_i := \left[\binom{0}{1}_i\right]$. Lemma 2.3.16 says that $\{\sigma_4, \cdots, \sigma_{m_0}, \tau_{m_1}, \rho_3, \cdots, \rho_{m_0}\}$ forms a basis for $F[m_0]$, Using this basis, we can assume that $c_3 = \cdots = c_{m_1} = 0$. $\square$

The lemmas so far shows that a block with saturated columns is unaffected by elements to the right. It is fixed when a new block starts to the right by lemma 2.3.5. It is fixed when the block to the right increases in width by lemma 2.3.19. It is fixed if and when the columns to the right saturate by lemma 2.3.21. This will be helpful since saturated columns are on the left in proposition 2.3.3.

Going back to $G[n-1]$ having two blocks, it remains to consider the case where neither blocks have saturated columns. A more careful manipulation is required for this, as there are different possible outcomes.

Lemma 2.3.22. Let $n \geq 6$. Suppose G has no non-trivial reflections, with $[G : G[n-1]] = p^2$ and $G = \left\langle F^{\langle 2,m_1\rangle}, F^{\langle m_1,n\rangle}, \tau\right\rangle$. With a change of basis, we can assume that either

(1) G is a single block (so $G = F^{\langle 2,n\rangle}$); or

(2) $G = \left\langle F^{\langle 2,m_1\rangle}, \tau, F^{\langle m_1,n\rangle}\right\rangle$ with a possibly different value of m_1, and a different τ, of the form given in proposition 2.3.3. That is,

$$\tau = \left[\begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_{m_1} \end{pmatrix}_{m_1}\right],$$

for some $d_i \in k$ with $d_{m_1} \neq 0$.

Proof. Induction on n will be used, but the arguments are common to the base and induction steps. Note that the lemma does not require changes of basis to be, say, $G[n-1]$-stable. So no checks for such properties will be done.

Write $\sigma_i = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i\right]$ and $\tau = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{pmatrix}\right]$. Use lemma 2.3.17 on columns $m_1+1, \cdots, n$ and then on columns $3, \cdots, m_1, n$ to assume τ has the form

$$\tau = \left[\begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_{m_1} \end{pmatrix}_{m_1} + \begin{pmatrix} c_{m_1+1} & 0 & \cdots & 0 \\ d_{m_1+1} & d_{m_1+2} & \cdots & d_n \end{pmatrix}_n\right],$$

with $d_{m_1} \neq 0$ and $d_n \neq 0$. Notice that there is a symmetry between the two blocks, in that τ has entries of the form $\left(\begin{smallmatrix} * & 0 & \cdots & 0 \\ * & * & \cdots & * \end{smallmatrix}\right)$ in the columns of both blocks. Using this symmetry, assume that the left block does not have a larger width ($w_1 \leq w_2$) by reordering the basis and blocks if necessary.

The basic idea is to "add every column of the left block to the right block" to have $c_{m_1+1} = 0$, similar to lemma 2.3.9. Apply the change of basis replacing x_{m_1+i} in B by $x_{m_1+i} - c_{m_1+1}x_{2+i}$ for $i = 1, \cdots, w_1$. This forces $c_{m_1+1} = 0$ as desired, but also changes each σ_{2+i} in the left block to the form, for $i = 2, \cdots, w_l$,

$$\sigma_{2+i} = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{2+i} - c_{m_1+1} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{m_1+i}\right],$$

This change can be reverted by replacing σ_{2+i} with $\sigma_{2+i} \cdot \sigma_{m_1+i}^{c_{m_1+1}}$. So now, G contains G' as before, and τ as written above, but with $c_{m_1+1} = 0$.

At this point, it is possible for τ to have all zeroes in the columns of the right block. If this is the case, then $\tau \in G[m_1]$ has the required from for τ_{m_1} for the case $G = \left\langle F^{\langle 2,m_1 \rangle}, \tau, F^{\langle m_1,n \rangle}\right\rangle$, and done.

Assume instead that at least one of $d_{m_1+1}, \cdots, d_n$ is non-zero. Replace τ by $\tau\sigma_{m_1+2}^{-d_{m_1+1}}$ to create a new column of zeroes in τ. That is,

$$\tau = \left[\begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_{m_1} \end{pmatrix}_{m_1} + \begin{pmatrix} 0 & -d_{m_1+1} & \cdots & 0 \\ 0 & d_{m_1+2} & \cdots & d_n \end{pmatrix}_n\right],$$

$$\text{or} \quad \left[\begin{pmatrix} 1 & 0 \\ d_3 & d_{m_1} \end{pmatrix}_{m_1} + \begin{pmatrix} 0 & -d_{m_1+1} \\ 0 & d_{m_1+2} \end{pmatrix}_6\right] \quad \text{if } w_2 = 2 \text{ or equivalently } n = 6.$$

In the ordered basis B, move x_{m_1+1}, which corresponds to the newly-zero column in τ, to after x_n. This moves column $m_1 + 1$ of zeroes in τ to the right end, and reduces the width w_2, if it was not already 2. As a side effect, this change of basis gives $[G : G[n-1]] = p$ because

$$\sigma_{m_1+2} = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{m_1+2}\right] \text{ is changed to } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_1+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_n\right],$$

and all other σ_i along with τ fix column $m_1 + 1$ before the basis reordering.

Let $i \leq n$ be the maximal subscript such that $d_i \neq 0$, with $i \geq m_1 + 2$ by assumption. Consider the case $i = m_1 + 2$ first (which is now in column $m_1 + 1$ after the basis reordering). This includes the base case $n = 6$. Notice that G one-extends columns $m_1, \cdots, n-1$: $\tau \in G[m_1 + 1]$ one-extends column m_1; σ_{i+1} one-extends column $i - 1$ due to the shift; σ_{m_1+2} one-extends column $n-1$. So apply lemma 2.3.8 to get $G = F^{\langle 2,n \rangle}$, and done.

Assume $i \geq m_1 + 3$ instead. Since the base case was shown, we can invoke induction hypothesis: since $d_i \neq 0$, the subgroup $G[i]$ now satisfies the prerequisites of this lemma, with G one-extending columns $i, \cdots, n-1$. Induction hypothesis on $G[i]$ gives two possibilities. If $G[i] = F^{\langle 2,i \rangle}$, then G one-extended columns $i, \cdots, n-1$. Lemma 2.3.8 gives $G = F^{\langle 2,n \rangle}$, and done.

Suppose $G[i] = \left\langle F^{\langle 2,m_1 \rangle}, \tau_{m_1}, F^{\langle m_1,i \rangle} \right\rangle$ for some different $m_1 \leq i - 2$ instead. Since the saturated block is now on the left, lemma 2.3.19 can be used to extend i to n, and done. All cases have now been considered. $\square$

This completes all cases with $[G : G[n-1]] = p^2$ as well, at least for $G[n-1]$ having two blocks. The strategy of either connecting the two blocks or saturating the columns of one of the blocks in the last lemma can be generalised to more than two blocks.

Lemma 2.3.23. Let $n \geq 6$. Suppose G has no non-trivial reflections, with $[G : G[n-1]] = p^2$ and $G = \left\langle F^{\langle m_0,m_1 \rangle}, \cdots, F^{\langle m_{l-1},m_l \rangle}, \tau \right\rangle$, for some $2 = m_0 < m_1 < \cdots < m_l = n$ with $l \geq 1$. With a change of basis, we can assume instead that either

(1) $G = \left\langle F^{\langle m_0,m_1 \rangle}, \cdots, F^{\langle m_{l-2},m_{l-1} \rangle} \right\rangle$, for some different $2 = m_0 < m_1 < \cdots < m_{l-1} = n$ (that is, there is one less block, and τ is "gone"); or

(2) $G = \left\langle F^{\langle m_0,m_1 \rangle}, \cdots, F^{\langle m_{l-1},m_l \rangle}, \tau_{m_1} \right\rangle$, for some different $2 = m_0 < m_1 < \cdots < m_l = n$, and τ_{m_1} as in proposition 2.3.3. That is,

$$\tau_{m_l} = \left[\begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_{m_1} \end{pmatrix}_{m_1} \right],$$

for some $d_i \in k$ with $d_{m_1} \neq 0$.

Proof. We will use induction on the number $l \geq 1$ of blocks. The base case $l = 1$ is exactly lemma 2.3.17, which gives case (2). The case $l = 2$ is lemma 2.3.22.

Suppose $l \geq 2$. Assume that no block has only zeroes in its columns in τ. Otherwise, such a block can be ignored, allowing induction hypothesis to be used with one less block.

Consider the action of G on the subspace $\left\langle x_1, x_2,\ x_{m_{l-2}+2}, \cdots, x_{m_l} \right\rangle$, corresponding to the columns of the right-most two blocks. It is the same as the subgroup $G' = \left\langle F^{\langle m_{l-2}, m_{l-1}\rangle}, F^{\langle m_{l-1}, m_l\rangle}, \tau \right\rangle$. Apply lemma 2.3.22: with a change of basis, we can assume that the action of the subgroup on the subspace satisfies this lemma. But since it is a change of basis that does not stabilise any subgroup, we can only assume that G' becomes either

(1) $G' = \left\langle \sigma_i = \left[\begin{pmatrix} c_{i,3} & \cdots & c_{i,m_{l-2}} \\ d_{i,3} & \cdots & d_{i,m_{l-2}} \end{pmatrix}_{m_{l-2}} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i \right] : i = m_{l-2}+2, \cdots, n \right\rangle$, acting as a single block on the subspace; or

(2) $G' = \left\langle \sigma_i, \tau : i = m_{l-2}+2, \cdots, \widehat{m_{l-1}+1}, \cdots, n \right\rangle$, for some different m_{l-1}, where σ_i is as in case (1) and

$$\tau = \left[\begin{pmatrix} c_3 & c_4 & \cdots & d_{m_{l-2}} & 1 & 0 & \cdots & 0 \\ d_3 & d_4 & \cdots & d_{m_{l-2}} & d_{m_{l-2}+1} & d_{m_{l-2}+2} & \cdots & d_{m_{l-1}} \end{pmatrix}_{m_{l-1}} \right],$$

for some $d_i \in k$ with $d_{m_1} \neq 0$. So the second right-most block now have saturated columns.

We can rebuild these entries from scratch by considering subgroup index. In case (1), since $G[m_{l-2}+1] = G[m_{l-2}]$ and $[G[i] : G[i-1]] = p$ for $i = m_{l-2}+2, \cdots, n$. apply lemma 2.3.13 repeatedly get case (1) of this lemma.

For case (2), consider the action of G on the subspace $\left\langle x_1, \cdots, x_{m_{l-1}} \right\rangle$. It acts as $G[m_{l-1}] = \left\langle F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-2}, m_{l-1}\rangle}, \tau \right\rangle$. Since there is one less block, induction hypothesis can be used: with a change of basis, $G[m_{l-1}]$ satisfies this lemma. This change of basis also changes columns $3, \cdots, m_{l-2}$ of elements in the last block $F^{\langle m_{l-1}, m_l\rangle}$, but those entries were already undetermined. Now we rebuild that block as well. Since $G\left[m_{l-1}+1\right]=G\left[m_{l-1}\right]$ apply lemma 2.3.5 to get $\sigma_{m_{l-1}+2}=\left[\begin{pmatrix}0&1\\1&0\end{pmatrix}_{m_{l-2}+2}\right]$. And since $[G[i]:G[i-1]]=p$ for $i=m_{l-1}+2,\cdots,n$, use lemmas 2.3.20 and possibly 2.3.7 repeatedly to get $\sigma_i=\left[\begin{pmatrix}0&1\\1&0\end{pmatrix}_i\right]$ for each i. This recovers case (2) of this lemma, completing the proof. $\square$

We have now completed the investigation into groups containing exactly two blocks that may or may not have saturated columns. It remains to remove the restriction "G has no non-trivial reflections". The way to approach this is the same as lemma 2.3.11, using a vertical vector space.

Lemma 2.3.24. Let $n\geq 5$. Suppose $G=\left\langle G\left[m_0\right],F^{\langle m_0,n\rangle},\tau\right\rangle$, where

$$\tau=\left[\begin{pmatrix}c_3&\cdots&c_{m_0}&1&0&\cdots&0\\d_3&\cdots&d_{m_0}&d_{m_0+1}&d_{m_0+2}&\cdots&d_n\end{pmatrix}\right],$$

and $3\leq m_0\leq n-2$, with $d_n\neq 0$. With a $G\left[m_0\right]$-fixing and $\left\langle G\left[m_0\right],F^{\langle m_0,n\rangle}\right\rangle$-stable change of basis, we can assume that

$$\tau=\left[\begin{pmatrix}1&0&\cdots&0\\d_{m_0+1}&d_{m_0+2}&\cdots&d_n\end{pmatrix}_n\right],$$

for some d_i with $d_n\neq 0$.

Proof. Align the columns of $\sigma_{m_0+2},\cdots,\sigma_n,\tau$ as follows.

$$\begin{array}{rl}
\text{Column} & \begin{array}{ccccccccc}3&\cdots&m_0&&&\cdots&&n\end{array}\\
\tau_n= & \left[\left(\begin{array}{ccc|cccccc}c_3&\cdots&c_{m_0}&1&0&\cdots&\cdots&0\\d_3&\cdots&d_{m_0}&d_{m_0+1}&d_{m_0+2}&\cdots&\cdots&d_n\end{array}\right)\right]\\
\sigma_{m_0+2}= & \left[\left(\begin{array}{ccc|cccccc}0&\cdots&0&0&1&0&\cdots&0\\0&\cdots&0&1&0&0&\cdots&0\end{array}\right)\right]\\
\vdots & \quad\vdots\qquad\qquad\ddots\\
\sigma_n= & \left[\left(\begin{array}{ccc|cccccc}0&\cdots&0&0&\cdots&0&0&1\\0&\cdots&0&0&\cdots&0&1&0\end{array}\right)\right]
\end{array}$$

Let u_j denote column $j-2$ of the big matrix of dimension $2(n-m_0) \times (n-2)$ on the right. We will construct a basis for the vector space $k^{2(n-m_0)}$. Let i be the largest of $j = m_0, \cdots, 3$ such that u_j contains non-zero entries. Let $\binom{a_i}{b_i} = [\sigma_i, x_i]$, where $\sigma_i \in G[m_0]$ is as constructed in lemma 2.2.3. Let

$$\begin{array}{rcllllll} u'_{m_0+1} & = & (& a_i, b_i, & 0,0, & \cdots, & 0,0 &)^T \\ u'_{m_0+2} & = & (& 0,0, & a_i, b_i, & \cdots, & 0,0 &)^T \\ \vdots & = & & & & \ddots & & \\ u'_n & = & (& 0,0, & 0,0, & \cdots, & a_i, b_i &)^T \end{array}$$

We consider whether the following set is a basis. The set consists of these new elements u'_j and the right-most columns of $F^{\langle m_0, n\rangle}$

$$\left\{u'_{m_0+1}, \cdots, u'_n,\ u_{m_0+1}, \cdots, u_n\right\}.$$

To consider its span, construct a $2(n-m_0) \times 2(n-m_0)$ matrix using its vectors as columns. That is, the matrix

$$\left(\begin{array}{cccc|cccccc} a_i & 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 \\ b_i & 0 & \cdots & 0 & d_{m_0+1} & d_{m_0+2} & \cdots & \cdots & d_n \\ 0 & a_i & & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & b_i & & 0 & 1 & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & & \\ 0 & 0 & \cdots & a_i & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & b_i & 0 & 0 & \cdots & 1 & 0 \end{array}\right).$$

For a contradiction, suppose its columns does not span $k^{2(n-m_0)}$. Then this matrix does not have full column rank nor row rank, and we have $\sum_j \lambda_j \cdot [\text{Row j}] = 0$, for some $\lambda_j \in k$, not all zeroes. Restricting the sum to column 1 gives $\lambda_1 a_i + \lambda_2 b_i = 0$. More generally, $b_i \lambda_j = -a_i \lambda_{j-1}$ for even j. Now split up the zero sum over j into odd and even rows as follows.

$$\begin{aligned}\sum_{\text{Odd j}} b_i\lambda_j \cdot [\text{Row j}] &= -\sum_{\text{Even j}} b_i\lambda_j \cdot [\text{Row j}] \\ &= \sum_{\text{Even j}} a_i\lambda_{j-1} \cdot [\text{Row j}] \\ &= \sum_{\text{Odd j}} a_i\lambda_j \cdot [\text{Row j+1}].\end{aligned}$$

Now we restrict our attention to the $n-m_0$ columns on the right, corresponding to the columns of the elements τ_n and $\sigma_{m_0+2}, \cdots, \sigma_n$. The odd rows correspond to the first rows of these elemnts and the even rows to the second. So adding odd rows together corresponds to finding the first row of say $\sigma = \tau^{\lambda_1}\sigma_{m_0+2}^{\lambda_3}\cdots\sigma_n^{\lambda_{2(n-m_0)-1}}$, with odd j for exponents λ_j. Similarly for second rows. So what the relation says is that

$$b_i \cdot [\text{First row of } \sigma] = a_i \cdot [\text{Second row of } \sigma].$$

But this means every column of σ is a k-multiple of $\binom{a_i}{b_i}$. And so σ one-extends column m_0, whence must be trivial by definition of m_0, and each λ_i are all zeroes. This is a contradiction.

The remaining argument using this vertical basis is the same as lemma 2.3.11. It is roughly as follows: use a change of basis of V^* to force u_i to be a k-linear sum of $u'_{m_0+1}, \cdots, u'_n$, and then multiply both τ and $\sigma_{m_0+2}, \cdots, \sigma_n$ by some powers of σ_i to change u_i to 0. □

We put together the lemmas so far on the case $[G : G[n-1]] = p^2$ to get the following lemma.

Lemma 2.3.25. Suppose $G = \langle G', \tau\rangle$, $[G : G[n-1]] = p^2$ and G' satisfies proposition 2.3.3 and contains at least one block with unsaturated columns. That is,

$$G' = \left\langle G[m_0], F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle}, \tau_{m_j} : 1 \le j \le l' \right\rangle,$$

for some $m_0 < m_1 < \cdots < m_l = n$ with $l \geq 1$, and for some $0 \leq l' \leq l - 1$. Using a $G[m_0]$-fixing change of basis, we can assume that G also satisfies 2.3.3.

Proof. Consider induction on the number $l - l'$ of blocks with unsaturated columns. The base case is $l - l' = 1$. Write $\tau = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ d_3 & \cdots & d_n \end{pmatrix}\right]$. Apply lemma 2.3.17 to assume that

$$\tau = \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} & 1 & 0 & \cdots & 0 \\ d_3 & \cdots & d_{m_0} & d_{m_{l'}+1} & d_{m_{l'}+2} & \cdots & d_n \end{pmatrix}\right].$$

If $l = 1$, then there is only one block. Apply lemma 2.3.24 to force columns $3, \cdots, m_0$ to be zeroes. If $l \geq 2$, then there are blocks with saturated columns. Use lemma 2.3.21 first to assume that

$$\tau = \left[\begin{pmatrix} c_3 & \cdots & c_{m_0} & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ d_3 & \cdots & d_{m_0} & d_{m_0+1} & \cdots & d_{m_{l'}} & d_{m_{l'}+1} & d_{m_{l'}+2} & \cdots & d_{m_l} \end{pmatrix}_{m_l}\right].$$

Lemma 2.3.24 can then be applied afterwards to get the result.

For the induction step, suppose $l - l' \geq 2$. Consider the action of G on the subspace $\langle x_1, x_2, \ x_{m_{l'}+1}, \cdots, x_n \rangle$. It is the same as the subgroup generated by the blocks with unsaturated columns and τ:

$$G' = \left\langle F^{\langle m_{l'}, m_{l'+1} \rangle}, \cdots, F^{\langle m_{l-1}, m_l \rangle}, \tau \right\rangle \leq G.$$

Apply lemma 2.3.23: using a change of basis of the subspace, which is a $G[m_{l'}]$-fixing change of basis of V^*, we can assume that G' acts on the subspace as a $\boxtimes$-product of blocks with at most one (left-most if exist) block having saturated columns.

The elements in G' have the same problem as in the proof of 2.3.23, namely that they can currently have any values in columns $3, \cdots, m_{l'}$. The same solution applies — rebuild blocks. In the case without saturated columns, since $[G[i] : G[i-1]] \leq p$, use lemmas 2.3.5 and 2.3.20 to rebuild blocks. When there is one block with saturated columns, apply first induction hypothesis with on the subgroup $G[m_{l'+1}]$ which satisfies "$l - l' = 1$", and then rebuild the remaining blocks with unsaturated columns. $\square$

With this, all lemmas necessary to prove the general form are shown.

Proof of proposition 2.3.3. Let $G[m_0] \leq G$ be the totally one-extended subgroup from lemma 2.3.4. Start by showing that $G[m_0+2]$ can satisfy the proposition with respect to some basis. By definition of m_0, the group G two-extends column m_0, so $G[m_0+1] = G[m_0]$. By lemma 2.3.5, assume there is $\sigma_{m_0+2} = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{m_0+2}\right] \in G$, using a $G[m_0]$-fixing change of basis. This starts a new block, giving

$$\left\langle G[m_0], F^{\langle m_0, m_0+2\rangle}\right\rangle \leq G[m_0+2],$$

with equality if $[G[m_0+2] : G[m_0+1]] = p$. If not equal, then the subgroup index is p^2 by lemma 2.0.4. And lemma 2.3.17 provides $\tau_{m_0+2} = \left[\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}_{m_0+2}\right]$ of the expected form to saturate the columns of this new block, and gives

$$\left\langle G[m_0], F^{\langle m_0, m_0+2\rangle}, \tau_{m_0+2}\right\rangle = G[m_0+2].$$

This shows that the subgroup $G[m_0+2] \leq G$ satisfies the proposition, regardless of the subgroup index.

Proceed by induction on $i \leq n$ that $G[i]$ satisfies the proposition, so that

$$G[i] = \left\langle G[m_0], F^{\langle m_0, m_1\rangle}, \cdots, F^{\langle m_{l-1}, m_l\rangle}, \tau_{m_j} : 1 \leq j \leq l'\right\rangle,$$

for some $m_0 < m_1 < \cdots < m_l = i$ with $l \geq 1$, and for some $0 \leq l' \leq l$. The base case is $i = m_0 + 2$ as above.

For the induction step, assume $m_0 + 3 \leq i \leq n - 1$. If $G[i+1] = G[i]$, then this is similar to the base case $i = m_0 + 2$: By lemma 2.3.5. using a $G[i]$-fixing change of basis, assume there is $\sigma_{i+2} = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_{i+2}\right] \in G$. This starts a new block. Set $G' = \left\langle G[i], F^{\langle m_l, m_l+2\rangle}\right\rangle \leq G[i+2]$. If $[G[i+2] : G[i+1]] = p$, then there is equality, and $G[i+2] = G'$ has the required from, and done. If the subgroup index is p^2, there is some $\tau_{i+2} \in G[i+2] \setminus G[i+1]$ such that $G[i+2] = \langle G', \tau_{i+2} \rangle$, since the change of basis fixed $G[i]$. Apply lemma 2.3.25 to get the result.

Suppose instead that $G[i+1] > G[i]$. By lemma 2.3.20, using a $G[m_0]$-fixing and $G[i]$-stable change of basis, assume there is

$$\sigma_{i+1} = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_{m_j} + \begin{pmatrix} 1 \\ b_{i+1} \end{pmatrix}_{i+1} \right] \text{ or } \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_{m_{j-1}+1} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}_{i+1} \right] \in G$$

for some $j = l'+1, \cdots, l$ and $b_{i+1} \in k$. Set $G' = \langle G[i], \sigma_{i+1} \rangle \le G[i+1]$ (reusing variable). If $[G[i+1] : G[i]] = p$ also, then $G[i+1] = G'$ can have the required form by applying lemma 2.3.7 to change b_{i+1} to 0, or moving x_{i+1} to before $x_{m_{j-1}+1}$ in B, depending on the form of σ_{i+1}. If the subgroup index is p^2, then σ_{i+1} could be chosen such that it has $\binom{1}{0}$ in column $i+1$ before applying lemma 2.3.20. Since that change of basis was $G[i]$-stable, the subgroup index means that there is $\tau_{i+1} \in G[i+1] \setminus G[i]$ such that $G[i+1] = \langle G', \tau_{i+1} \rangle$. Again, apply lemma 2.3.25 to get the result. $\square$

We have proved that every $G \le F$, up to a change of basis, is of the form

$$G = G[m_0] \boxtimes G' \boxtimes \left(\mathop{\boxtimes}_{l'+1 \le j \le l} F^{\langle 2, 2+w_j \rangle} \right),$$

where G' is generated by blocks with saturated columns. As mentioned at the start of this subsection, we find the invariant ring of the second component G'.

Proposition 2.3.26. Suppose G has no non-trivial reflections and is generated by blocks with saturated columns. Then S^G is a complete intersection. Up to a change of basis of V^*, we have $S^G = k\left[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n, f'_3, \cdots, f'_{2n-m}, f_1, \cdots, f_l\right]$, for some $f_i, f'_i \in Sx_1 + Sx_2$.

Proof. We can assume G is as described in proposition 2.3.3, with $m_0 = 2$, $l > 1$ and $l' = l$. Write $\sigma_i := \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_i\right]$. Define $\rho_{m_j} = \left[\begin{pmatrix} 0 \\ 1 \end{pmatrix}_{m_j}\right]$ for $j = 1, \cdots, l$, and the group $\overline{G} := \langle G, \rho_{m_1}, \cdots, \rho_{m_l} \rangle$. We can see that this group is totally one-extended by considering its elements in the following order.

$$\rho_{m_1}, \cdots, \rho_{m_l} \mid \sigma_{m_1}, \cdots, \sigma_{m_0+2} \mid \cdots \mid \sigma_{m_l}, \cdots, \sigma_{m_{l_1}+2}.$$

This proposition follows from using proposition 2.1.6 on $S^{\overline{G}}$ if we can show that

$$S^G = S^{\overline{G}}[f_1, \cdots, f_l],$$

for some $f_i \in Sx_1 + Sx_2$, and S^G is a complete intersection whenever $S^{\overline{G}}$ is.

We will show this by induction on l. The base case has $l = 1$ block:

$$G = \langle \sigma_i, \tau_{m_1} : i = m_0 + 2, \cdots, m_1 \rangle$$
$$\text{where } \tau_{m_1} := \left[\begin{pmatrix} 1 & 0 & \cdots & 0 \\ d_{m_0+1} & d_{m_0+2} & \cdots & d_{m_1} \end{pmatrix}_{m_1} \right],$$

with entires in k and $d_{m_1} \neq 0$. We use lemma 2.1.1: It is sufficient to, for each of $y = \binom{0}{1}$ and $\binom{1}{*}$, find $\theta \in \rho_{m_1} G$ such that $[\theta, V^*] = \langle y \rangle_{\mathbb{F}_p}$. For $y = \binom{0}{1}$, pick $\theta = \rho_{m_1}$. Suppose $y = \binom{1}{b}$ for some b and write $\phi_i := \left[\binom{1}{b}_i\right]$. By lemma 2.3.16, the following set is a basis of F:

$$\{\tau_{m_1}, \sigma_{m_0+2}, \cdots, \sigma_{m_1}, \phi_{m_0+1}, \cdots, \phi_{m_1}\}.$$

Using this basis, write

$$\begin{aligned} \rho_{m_1} &= \tau_{m_1}^{e_{m_0+1}} \sigma_{m_0+2}^{e_{m_0+2}} \cdots \sigma_{m_1}^{e_{m_1}} \phi_{m_0+1}^{e'_{m_0+1}} \cdots \phi_{m_1}^{e'_{m_1}} \\ \theta := \rho_{m_1} \tau_{m_1}^{-e_{m_0+1}} \sigma_{m_0+2}^{-e_{m_0+2}} \cdots \sigma_{m_1}^{-e_{m_1}} &= \phi_{m_0+1}^{e'_{m_0+1}} \cdots \phi_{m_1}^{e'_{m_1}}, \end{aligned}$$

for some $e_i, e'_i \in \mathbb{F}_p$. The left-hand side shows that $\theta \in \rho_{m_1} G$, and the right-hand side shows that $[\theta, V^*] = \langle y \rangle_{\mathbb{F}_p}$. So lemma 2.1.1 gives $S^G = S^{\langle G, \rho_{m_1} \rangle}[f_1]$, and the proposition holds for $l = 1$.

For the induction step, suppose $l \geq 2$. We will use lemma 2.1.1 again with $\rho = \rho_{m_1}$. The preconditions are satisfied by the same reason as in the base case.

Let $G' = \langle G, \rho_{m_1} \rangle$. By lemma 2.1.1, $S^G = S^{G'}[f_1]$ for some $f_1 \in Sx_1 + Sx_2$. To find the invariant ring of $S^{G'}$, note that $m_0' := m_0(G') = m_1$. Using lemma 2.3.24, we can ensure that $\tau_{m_2}, \cdots, \tau_{m_l} \in G'$ fix $x_3, \cdots, x_{m_0'}$. This means $G' = G'[m_0'] \boxtimes G''$, where G'' is group G with its action restricted to the subspace $\langle x_1, x_2,\ x_{m_0+1}, \cdots, x_n \rangle$ and is generated by $l-1$ blocks with saturated columns. By induction hypothesis, we know the invariant ring of G''. Using lemma 2.0.3, the invariant ring of the $\boxtimes$-product can be expressed as

$$\begin{aligned}
S^{G'} &= S[m_0]^{G'[m_0]} \otimes k[x_1, x_2,\ x_{m_0+1}, \cdots, x_n]^{G''} \\
&= S[m_0]^{G'[m_0]} \otimes k[x_1, x_2,\ x_{m_0+1}, \cdots, x_n]^{\overline{G''}}[f_2, \cdots, f_l] \\
&= S^{G'[m_0] \boxtimes \overline{G''}}[f_2, \cdots, f_l] \\
&= S^{\overline{G}}[f_2, \cdots, f_l].
\end{aligned}$$

Adding f_1 to this gives us the required invariant ring. $\square$

We end this section with an example of a block with saturated columns.

Example 2.3.27. Set $n = 4$. Let $G = \langle \sigma, \tau \rangle$ where

$$\sigma = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right] \text{ and } \tau = \left[\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix} \right].$$

Assume that $b \in k$ are chosen so that G has no non-trivial reflections. So $b \neq 0$ and also $b \neq 1$. Then

$$\begin{aligned}
S^G &= k[\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3, \boldsymbol{N}_4, f_3, f_4], \\
\text{where } f_3 &= [\sigma, x_3]\, \boldsymbol{N}_3^{\langle\sigma\rangle} + b^{-1}[\sigma, x_4]\, \boldsymbol{N}_4^{\langle\sigma\rangle} \\
&= x_2 \prod_{\mu \in k} (x_3 + \mu x_2) + b^{-1} x_1 \prod_{\lambda \in k} (x_4 + \lambda x_1) \\
\text{and } f_4 &= [\tau, x_3]\, \boldsymbol{N}_3^{\langle\tau\rangle} + b^{-1}[\tau, x_4]\, \boldsymbol{N}_4^{\langle\tau\rangle} \\
&= x_1 \prod_{\lambda \in k} (x_3 + \lambda x_1) + x_2 \prod_{\lambda \in k} (x_4 + \lambda \cdot b x_2).
\end{aligned}$$

Proof. Proposition 2.3.26 suggests that we extend the group G using $\rho_i = \left[\binom{0}{1}_i \right]$.

To apply lemma 2.1.1, consider their commutator with the given invariants:

$$\begin{aligned} [\rho_4, f_3] &= b^{-1} x_1 \prod_{\lambda \in k} (x_2 + \lambda x_1) \\ \text{and } \ [\rho_3, f_4] &= x_1 \prod_{\lambda \in k} (x_2 + \lambda x_1) \, . \end{aligned}$$

So applying the lemma gives:

$$S^G = S^{\langle G, \rho_4 \rangle} [f_3] = S^{\langle G, \rho_3, \rho_4 \rangle} [f_3, f_4] = k \left[\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3, \boldsymbol{N}_4, f_3, f_4 \right],$$

noting that $\langle G, \rho_3, \rho_4 \rangle = F$. □

2.4 Two-extended narrow blocks

In this section and the next, we will find the invariant rings of blocks (2.3.1), the last piece of puzzle to find all S^G with $G \leq F$ up to a congruence.

The basic idea is to apply SAGBI/divide-by-x on an invariant fraction ring to use theorem 1.1.3. To make applying the algorithm easier, instead of a block, we will find the invariant ring of $G = \left\langle \sigma_i := \left[\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \right)_i \right] : i = 4, \cdots, n \right\rangle$. We can recover a block from G using the change of basis replacing $x_3, \cdots, x_n$ with $x_n, \cdots, x_3$.

We find first a suitable invariant fraction ring using theorem 1.1.4.

Lemma 2.4.1. $S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_3, x_1^{-1}\right]$, where

$$\begin{aligned}
\mathcal{B}_3 &:= \{x_1, x_2, \boldsymbol{N}_3, f_i, g : 4 \le i \le n-1\},\\
\boldsymbol{N}_3 &= \prod_{\mu\in k}(x_n + \mu x_1) = x_3^p - x_1^{p-1}x_3,\\
f_4 &= x_3\prod_{\lambda\in k}(x_2+\lambda x_1) + x_1\prod_{\mu\in k}(x_4+\mu x_1) = x_2^p x_3 - x_1^{p-1}x_2x_3 - x_1x_4^p + x_1^p x_4,\\
f_i &= x_2\prod_{\lambda\in k}(x_{i-1}+\lambda x_2) + x_1\prod_{\mu\in k}(x_i+\mu x_1) = x_2x_{i-1}^p - x_2^p x_{i-1} + x_1x_i^p - x_1^p x_i,\\
&\qquad\text{for } 5\le i\le n-1, \text{ and}\\
g &:= \sum_{j=3}^{n} x_1^{j-3}(-x_2)^{n-j}x_j = x_1^0(-x_2)^{n-3}x_3 + \cdots + x_1^{n-3}(-x_2)^0 x_n.
\end{aligned}$$

Proof. We show the degree minimality required to use theorem 1.1.4. Note that x_1, x_2 and g each have degree 1 in x_1, x_2 and x_n respectively, For fixed $3 \le i \le n-1$, consider the action of $\langle\sigma_{i+1}\rangle$ on $\langle x_1, \cdots, x_i\rangle_k$. Since $\sigma_{i+1}(x_i) = x_i + x_1$,

$$S[i]^G \le S[i]^{\langle\sigma_{i+1}\rangle} = k\left[x_1, \cdots, x_{i-1}, x_i^p - x_1^{p-1}x_i\right].$$

That is, given any invariant in $S[i]^G$, its degree in x_i must be at least p if positive. And since each f_i has degree p as a polynomial in x_i, we have the required minimality.

By theorem 1.1.4, we have $S^G[f^{-1}] = k[\mathcal{B}_n f^{-1}]$ for some $f \in S^G$. Each f_i also has leading coefficient $-x_1$ or x_1 as a polynomial in x_i over $S[i-1]$ and g has x_1^{n-3} in x_n over $S[n-1]$. So we can pick $f = x_1$ and the lemma follows. $\square$

As mentioned, we want to apply theorem 1.1.3. Using grevlex monomial order with $x_i < x_{i+1}$, as specified by the theorem, the leading terms of the invariants in $\mathcal{B}_3$ are as follows: with $5 \le i \le n-1$,

f	x_1	x_2	$\boldsymbol{N}_3$	f_4	f_i	g
$\mathrm{LT}(f)$	x_1	x_2	x_3^p	$x_2^p x_3$	$x_2x_{i-1}^p$	$(-x_2)^{n-3}x_3$

(2.2)

The set $\mathcal{B}_3$ does not satisfy the preconditions of the theorem. To satisfy them, we can add norms $\boldsymbol{N}_4, \cdots, \boldsymbol{N}_n$ to the set, and apply SAGBI/divide-by-x_1 to find more invariants. Depending on how and what invariants were derived, it may turn out that the norms added were unnecessary, as this case will be. For our extra invariants, it is sufficient to consider SAGBI/divide-by-x_1 on $\mathcal{B}_3$.

In $\mathcal{B}_3$, the tête-a-tête differences to check are those involving $\boldsymbol{N}_3$, f_4 and g. Start with the one using f_4 and g. It depends on the dimension n:

$$\begin{aligned} & f_4 + (-x_2)^{p-(n-3)}\, g && \text{if } n-3 \le p, \\ \text{and } & (-x_2)^{(n-3)-p}\, f_4 + g && \text{if } n-3 > p. \end{aligned}$$

These two possible cases give different results and any following subductions will be directly affected. So they will be studied separately.

Definition 2.4.2. A block $F^{\langle 2,n\rangle}$ is *narrow* if $n \le p+3$. Otherwise, it is *wide.*

We will consider the wide case in the next section. In this section, our result is the following proposition on the invariant ring of a narrow block.

Proposition 2.4.3. Suppose $n \le p+3$. Then $S^G = k\,[\mathcal{B}]$, where

$$\begin{aligned} \mathcal{B} &= [x_1, x_2, \boldsymbol{N}_3, h_i, \boldsymbol{N}_n, g : 4 \le i \le n-1\}\,, \\ \text{and } h_i &:= x_i^p - \sum_{j=3}^{i} x_1^{(p-1)-(i-j)}\,(-x_2)^{i-j}\,x_j - \sum_{j=i}^{n} x_1^{j-i}\,(-x_2)^{(p-1)-(j-i)}\,x_j. \end{aligned}$$

and g as defined in lemma 2.4.1. And S^G is a complete intersection.

If $n=4$, there are no h_i involved and $g = (-x_2)\,x_3 + x_1x_4$, and S^G reduces to the known case of a double transvection. So for the remainder of this section, assume that $n \ge 5$. The rest of this section will be used to prove this proposition.

Compared to $\mathcal{B}$, the set $\mathcal{B}_3$ from lemma 2.4.1 does not have $h_4, \cdots, h_{n-1}$ nor $\boldsymbol{N}_n$, but has instead the invariants $f_4, \cdots, f_{n-1}$. To replace f_4 by h_4, we use the tête-a-tête difference mentioned above.

Lemma 2.4.4. The tête-a-tête difference $f_4 + (-x_2)^{p-(n-3)}\, g$ subducts/divide-by-x_1 to h_4 over $\mathcal{B}_3$. Furthermore, the subduction provides the relation

$$f_4 = -x_1 h_4 - (x_2)^{p-(n-3)}\, g.$$

In particular, $f_n \in k\left[\mathcal{B}_4\right]$, where $\mathcal{B}_4 = (\mathcal{B}_3 \cup \{h_4\}) \setminus \{f_4\}$. It follows that

$$S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_4, x_1^{-1}\right].$$

Proof. In decreasing monomial order, expand the two terms.

$$\begin{aligned} f_4 &= x_2^p x_3 - x_1 x_4^p - x_1^{p-1} x_2 x_3 + x_1^p x_4 \\ (-x_2)^{p-(n-3)}\, g &:= \sum_{j=3}^{n} x_1^{j-3} (-x_2)^{p-(j-3)}\, x_j \\ &= x_1^0 (-x_2)^p\, x_3 + x_1^1 (-x_2)^{p-1}\, x_4 + \cdots + x_1^{n-3} (-x_2)^{p-(n-3)}\, x_n \end{aligned}$$

This shows that the leading term of the tête-a-tête difference is $-x_1 x_4^p$ which has no tête-a-tête in $\mathcal{B}_n$. So subduction completes. Next, divide-by-x_1 to get an invariant with leading term x_4^p.

$$\begin{aligned} \left(-x_1^{-1}\right)\left(f_4 + (-x_2)^{p-(n-3)}\, g\right) &= x_4^p + x_1^{p-2} x_2 x_3 - x_1^{p-1} x_4 \\ &\quad - x_1^0 (-x_2)^{p-1}\, x_4 - \cdots - x_1^{n-4} (-x_2)^{p-(n-3)}\, x_n \\ &= x_4^p - \sum_{j=3}^{4} x_1^{(p-1)-(4-j)} (-x_2)^{4-j}\, x_j \\ &\quad - \sum_{j=4}^{n} x_1^{j-4} (-x_2)^{(p-1)-(j-4)}\, x_j \end{aligned}$$

This is equal to h_4 and relation specified in the lemma follows. □

We will similarly replace each f_i by h_i for $5 \leq i \leq n-1$. Define more generally, for $i = 4, \cdots, n-1$,

$$\begin{aligned}\mathcal{B}_i &:= \mathcal{B}_{i-1} \cup \{h_i\} \setminus \{f_i\} \\ &= \{x_1, x_2, \boldsymbol{N}_3, g\} \cup \{f_j : 4 \leq j \leq i-1\} \cup \{h_j : i \leq j \leq n-1\}.\end{aligned}$$

We show that each of these can also generate the same invariant fraction ring.

Lemma 2.4.5. $S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_i, x_1^{-1}\right]$, for $i = 3, \cdots, n-1$.

Proof. We will use induction on i. Case $i = 3$ and 4 are lemmas 2.4.1 and 2.4.4 respectively. For the induction step, assume $n \geq 6$, fix $i = 5, \cdots, n-1$, and also assume $S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_{i-1}, x_1^{-1}\right]$. There is a tête-a-tête difference in $\mathcal{B}_{i-1}$ given by (f_i defined in 2.4.1 with leading term $x_2 x_{i-1}^p$, and h_{i-1} in 2.4.3 with x_{i-1}^p):

$$\begin{aligned}
&f_i + (-x_2)\, h_{i-1} \\
&= \left[\cancel{x_2 x_{i-1}^p} - x_2^p x_{i-1} + x_1 x_i^p - x_1^p x_i,\right] \\
&\quad + \Bigg[\cancel{(-x_2)\, x_{i-1}^p} - (-x_2) \sum_{j=3}^{i-1} x_1^{(p-1)-((i-1)-j)} (-x_2)^{(i-1)-j} x_j \\
&\qquad + -(-x_2) \sum_{j=i-1}^{n} x_1^{j-(i-1)} (-x_2)^{(p-1)-(j-(i-1))} x_j\Bigg] \\
&= \left[(-x_2)^p x_{i-1} + x_1 x_i^p - x_1^p x_i\right] \\
&\quad + \left[-\sum_{j=3}^{i-1} x_1^{(p-1)-(i-j)+1} (-x_2)^{i-j} x_j - \sum_{j=i-1}^{n} x_1^{j-i+1} (-x_2)^{(p-1)-(j-i)} x_j\right].
\end{aligned}$$

Note that $-x_1^p x_i$ can be merged into the first sum with $j = i$ and $(-x_2)^p x_{i+1}$ can cancel the $j = i-1$ term in the second sum, simplifying to a familiar expression.

$$= x_1 x_i^p - \sum_{j=3}^{i} x_1^{(p-1)-(i-j)+1} (-x_2)^{i-j} x_j - \sum_{j=i}^{n} x_1^{j-i+1} (-x_2)^{(p-1)-(j-i)} x_j = x_1 h_i$$

The leading terms of the two sums, indexed by $j = 3$ and $j = i$ respectively to minimise exponents of x_1, are

$$-x_1^{(p-1)-(i-3)+1} (-x_2)^{i-3} x_n \text{ and } -x_1 (-x_2)^{p-1} x_i.$$

The bounds $p+3 \geq n > i$ guarantees that $x_1 x_i^p$ is greater than both and is the leading term of the tête-a-tête difference:

$$(p-1)-(i-3)+1 = p+3-i \geq 1.$$

The leading term $x_1 x_i^p$ has no tête-a-tête in $\mathcal{B}_{i-1}$ and subduction completes. Divide-by-x_1 then gives the invariant

$$x_1^{-1}\left(f_i + (-x_2)\, h_{i-1}\right) = h_i.$$

The invariant f_{i+1} is redundant as before, giving $S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_i, x_1^{-1}\right]$, and completing the induction step. Snnce only $f_5, \cdots, f_{n-1}$ are defined in the form used, induction stops at $i = n-1$. □

Since $\mathcal{B} = \mathcal{B}_{n-1} \cup \{\boldsymbol{N}_n\}$, we now have $S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_{n-1}, x_1^{-1}\right] = k\left[\mathcal{B}, x_1^{-1}\right]$. and are now in a position to prove proposition 2.4.3.

Proof of proposition 2.4.3. We apply SAGBI/divide-by-x one last time. The elements in $\mathcal{B}$ and their leading terms are as follows: with $i = 4, \cdots, n-1$,

f	x_1	x_2	$\boldsymbol{N}_3$	h_i	$\boldsymbol{N}_n$	g
$\mathrm{LT}(f)$	x_1	x_2	x_3^p	x_i^p	x_n^p	$(-x_2)^{n-3}\, x_3$

There is only one tête-a-tête difference to check, involving $\boldsymbol{N}_3$ and g, both defined in lemma 2.4.1. If it subducts to zero over $\mathcal{B}$, since the set $\mathcal{B}$ satisfies the precondition of theorem 1.1.3, we then have $S^G = k[\mathcal{B}]$ as required.

Let g_4 be the tête-a-tête difference:

$$\begin{aligned} g_4 &:= g^p - \left(-x_2^{p(n-3)}\right) \boldsymbol{N}_3 \\ &= \sum_{j=3}^{n} x_1^{p(j-3)} (-x_2)^{p(n-j)}\, x_j^p - (-x_2)^{p(n-3)} \left(x_3^p - x_1^{p-1} x_3\right) \\ &= \sum_{j=4}^{n} x_1^{p(j-3)} (-x_2)^{p(n-j)}\, x_j^p + x_1^{p-1} (-x_2)^{p(n-3)}\, x_3 \end{aligned}$$

More generally, for $i = 4, \cdots, n$, define

$$g_i := \sum_{j=i}^{n} x_1^{p(j-3)} (-x_2)^{p(n-j)} x_j^p + \sum_{j=3}^{i-1} x_1^{(p-1)(i-3)+(j-3)} (-x_2)^{(p-1)(n-i+1)+(n-j)} x_j.$$

For $i = 4, \cdots, n-1$, we will subduct over $\mathcal{B}$. The leading term of the two sums in g_i are respectively

$$x_1^{p(i-3)} (-x_2)^{p(n-i)} x_i^p \text{ and } x_1^{(p-1)(i-3)} (-x_2)^{(p-1)(n-i+1)+(n-3)} x_3.$$

So the leading term of g_i is the latter. Since g, defined in lemma 2.4.1, has leading term $(-x_2)^{n-3} x_3$, we can subduct g_i over $\mathcal{B}$ using:

$$-x_1^{(p-1)(i-3)} (-x_2)^{(p-1)(n-i+1)} g = -\sum_{j=3}^{n} x_1^{(p-1)(i-3)+(j-3)} (-x_2)^{(p-1)(n-i+1)+(n-j)} x_j$$

The subduction gives

$$\begin{aligned} g_i' &= g_i - x_1^{(p-1)(i-3)} (-x_2)^{(p-1)(n-i+1)} g \\ &= \sum_{j=i}^{n} x_1^{p(j-3)} (-x_2)^{p(n-j)} x_j^p - \sum_{j=i}^{n} x_1^{(p-1)(i-3)+(j-3)} (-x_2)^{(p-1)(n-i+1)+(n-j)} x_j. \end{aligned}$$

This time, the leading term of the two sums are respectively

$$x_1^{p(i-3)} (-x_2)^{p(n-i)} x_i^p \text{ and } x_1^{p(i-3)} (-x_2)^{(p-1)(n-i+1)+(n-i)} x_i.$$

So the leading term of g_i' is the former. Since h_i, defined in proposition 2.4.3, has leading term x_i^p, we can subduct g_i' over $\mathcal{B}$ again.

$$\begin{aligned}
&g_i' - x_1^{p(i-3)}\,(-x_2)^{p(n-i)}\,h_i \\
&= g_i' - x_1^{p(i-3)}\,(-x_2)^{p(n-i)}\,x_i^p + \sum_{j=3}^{i} x_1^{(p-1)-(i-j)+p(i-3)}\,(-x_2)^{(i-j)+p(n-i)}\,x_j \\
&\quad + \sum_{j=i}^{n} x_1^{(j-i)+p(i-3)}\,(-x_2)^{(p-1)-(j-i)+p(n-i)}\,x_j \\
&= \sum_{j=i+1}^{n} x_1^{p(j-3)}\,(-x_2)^{p(n-j)}\,x_j^p + \sum_{j=3}^{i} x_1^{(p-1)-(i-j)+p(i-3)}\,(-x_2)^{(i-j)+p(n-i)}\,x_j.
\end{aligned}$$

This is g_{i+1}. If $i \leq n-2$, then we can subduct g_{i+1} again. Since each iteration reduces i by one, we eventually reach g_n.

The leading term of g_n is $x_1^{p(n-3)}x_n^p$, so we can subduct using $x_1^{p(n-3)}\boldsymbol{N}_n$.

$$\begin{aligned}
&g_n - x_1^{p(n-3)}\boldsymbol{N}_n \\
&= x_1^{p(n-3)}x_n^p + \sum_{j=3}^{n-1} x_1^{(p-1)(n-3)+(j-3)}\,(-x_2)^{(p-1)+(n-j)}\,x_j \\
&\quad - x_1^{p(n-3)}\left(x_n^p - x_2^{p-1}x_n\right) \\
&= g \in \mathcal{B}
\end{aligned}$$

This shows that $g^p - \left(-x_2^{p(n-3)}\boldsymbol{N}_3\right)$ does indeed subduct to zero over $\mathcal{B}$.

This shows that the invariant ring S^G is generated by the $n+1$ elements. Since S^G is graded and has Krull dimension n, it follows that S^G is a complete intersection. Its unique relation can be found by collecting the invariants used in subduction steps in the proof above. It is

$$\begin{aligned}
&g^p - (-x_2)^{p(n-3)}\,\boldsymbol{N}_3 - x_1^{p(n-3)}\boldsymbol{N}_n \\
&\quad - \sum_{i=4}^{n-1} x_1^{(p-1)(i-3)}\,(-x_2)^{(p-1)(n-i+1)}\,g - \sum_{i=4}^{n-1} x_1^{p(i-3)}\,(-x_2)^{p(n-i)}\,h_i = 0.
\end{aligned}$$

$\square$

2.5 Two-extended wide blocks

We move on to the wide case (2.4.2). We will prove the following proposition.

Proposition 2.5.1. Suppose $n \geq p+4$. Then $S^G = k[\mathcal{B}]$, where

$$\mathcal{B} := \left\{x_1, x_2, \boldsymbol{N}_3, \boldsymbol{N}_4, \cdots, \boldsymbol{N}_{n-p}, f_4, \cdots, f_{n-(p-1)}, h_{n-(p-1)}, \cdots, h_{n-1}, \boldsymbol{N}_n\right\},$$

where f_i is as defined in lemma 2.4.1, and h_i will be defined later in lemma 2.5.6 (different from those defined for the narrow case). And S^G is a complete intersection.

This section will assume that the premise of wide block condition $n \geq p+4$ holds and will be dedicated to proving the proposition. We will continue from where the work had split from the narrow case at definition 2.4.2. We will consider SAGBI/divide-by-x_1 on the set $\mathcal{B}_3$ and subduct the tête-a-tête difference $(-x_2)^{(n-3)-p} f_4 + g$. Since the tête-a-tête difference is of the form $\cdots + g$, the subduction result can replace g in $\mathcal{B}_3$ as a k-algebra generating set for $S^G[x^{-1}]$. This subduction will require many iterations of subduction steps, and will be shown in lemmas 2.5.2 to 2.5.6. They will show that our initial tête-a-tête difference subducts/divide-by-x_1 to a new invariant $h_{n-(p-1)}$ whose leading term is $x_{n-(p-1)}^p$.

Since $f_{n-(p-2)} \in \mathcal{B}_3$ has leading term $x_2 x_{n-(p-1)}^p$, the replacement will introduce a new tête-a-tête . Lemma 2.5.7 will show that this in turn subducts/divide-by-x_1 to another invariant $h_{n-(p-2)}$ whose leading term is $x_{n-(p-2)}^p$. Using a similar agument as before, this new invariant will replace $f_{n-(p-2)}$, but will also introduce more tête-a-têtes. This will be repeated until we arrive at h_{n-1}, where we will stop because we do not have f_n defined. And at that point, we will have found the new invariants $h_{n-(p-1)}, \cdots, h_{n-1}$ in $\mathcal{B}$ and shown that $S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}, x_1^{-1}\right]$. We will show (from page 92) that the tête-a-têtes in $\mathcal{B}$ have differences that subduct to zero over $\mathcal{B}$, and the proposition will follow.

We now proceed to proving the proposition as described, starting with the tête-a-tête difference mentioned. We add the following together

$$g = \sum_{j=3}^{n} x_1^{j-3} \left(-x_2\right)^{n-j} x_j = x_1^0 \left(-x_2\right)^{n-3} x_3 + \cdots + x_1^{n-3} \left(-x_2\right)^0 x_n$$

$$\left(-x_2\right)^{(n-3)-p} f_4 = \left(-x_2\right)^{(n-3)-p} \left[x_2^p x_3 - x_1 x_4^p - x_1^{p-1} x_2 x_3 + x_1^p x_4\right].$$

to obtain the tête-a-tête difference

$$\begin{aligned}
& g + \left(-x_2\right)^{(n-3)-p} f_3 \\
&= \left[x_1^1 \left(-x_2\right)^{(n-3)-1} x_4 + \cdots + x_1^{n-3} \left(-x_2\right)^0 x_n\right] \\
&\quad + \left[-x_1 \left(-x_2\right)^{(n-3)-p} x_4^p + x_1^{p-1} \left(-x_2\right)^{(n-3)-(p-1)} x_3 + x_1^p \left(-x_2\right)^{(n-3)-p} x_4\right] \\
&= \sum_{j=4}^{n} x_1^{j-3} \left(-x_2\right)^{n-j} x_j \\
&\quad - x_1 \left(-x_2\right)^{(n-3)-p} x_4^p + \sum_{j=3}^{4} x_1^{(p-1)+(j-3)} \left(-x_2\right)^{(n-j)-(p-1)} x_j.
\end{aligned}$$

This tête-a-tête difference is a special case of the following expression:

$$\begin{aligned}
g_{(i_s)_{s=0}^t, t'} = & \sum_{s=1}^{t} \sum_{j=i_{s-1}}^{i_s} x_1^{(j-3)+(t-s)(p-1)} \left(-x_2\right)^{(n-j)-(t-s)(p-1)} x_j \\
& - x_1^{(i_1-3)+(t-2)(p-1)} \left(-x_2\right)^{(n-i_1)-(t-2)(p-1)-p} \left[\sum_{s=1}^{t'} \left(-x_2\right) x_{i_s}^p + \sum_{t'+1 \le s \le t-1} x_1 x_{i_s}^p\right]
\end{aligned} \tag{2.3}$$

for some sequence $(i_0 = 3 < i_1 < \cdots < i_t = n)$ where $t \ge 2$, and $t' = 1, \cdots, t-1$. We write $g_{(i_s)}$ if $t' = t-1$, dropping the subscript t'. For example, the tête-a-tête difference above is $g_{(3,4,n)}$ with an implicit $t' = 1$.

We will show that applying one subduction step to $g_{(3,4,n)}$ results in another invariant that is also of the form (2.3). Further subductions, if possible, will also result in invariants of the same form. To apply these subduction steps, we will find the leading term of $g_{(i_s),t'}$ in lemma 2.5.2, and show what each subduction step will result in, in lemmas 2.5.3 and 2.5.4. Putting these together, lemmas 2.5.5 and 2.5.6 will give the invariant $h_{n-(p-1)}$ mentioned before.

Not all choices of sequence (i_s) in the subscript is a result of a subduction step. The choices that do will satisfy certain restrictive conditions on the differences between consecutive terms. We will use these conditions to make subduction simpler: (1) It must start with $i_1 - i_0 \leq p$. (2) The subsequenes $(i_1, \cdots, i_{t'})$ and $(i_s : t'+1 \leq s \leq t-1)$ are arithmetic of common difference p. (3) The second of these subsequences can be empty if $t' = t-1$. (4) But if it is non-empty, then the two subsequences are separated by a difference of $i_{t'+1} - i_{t'} = p$.

Note that these conditions mean that $g_{(i_s),t'}$ is uniquely determined by three parameters, such as i_1, t' and t. But a sequence is used in the notation to help visualise the changes between subduction steps. To begin subduction of $g_{(i_s),t'}$, we need to know its leading term.

Lemma 2.5.2. The leading term of $g_{(i_s),t'}$ is

(1) $x_1^{(t-1)(p-1)}\,(-x_2)^{(n-3)-(t-1)(p-1)}\,x_3$ if $i_1 - 3 = p$;

(2) $-x_1^{(i_1-3)+(t-2)(p-1)}\,(-x_2)^{(n-i_1)-(t-2)(p-1)-p+1}\,x_{i_{t'}}^p$ if $i_1 - 3 \leq p-1$.

Proof. We will compare the leading term of the double sum with that of the remaining terms to find the leading term of $g_{(i_s),t'}$. Start with the double sum:

$$\sum_{s=1}^{t}\sum_{j=i_{s-1}}^{i_s} x_1^{(j-3)+(t-s)(p-1)}\,(-x_2)^{(n-j)-(t-s)(p-1)}\,x_j.$$

For a fixed outer sum index $s = 1, \cdots, t$, the leading term of the inner sum is, by minimising j in order to minimise the exponent of x_1,

$$l_s := x_1^{(i_{s-1}-3)+(t-s)(p-1)}\,(-x_2)^{(n-i_{s-1})-(t-s)(p-1)}\,x_{i_{s-1}}$$

Some choice of $s = 1, \cdots, t$ will give the leading term of the double sum.

The sequence (i_s) consists of i_0, i_t and one or two arithmetic subsequences of difference $p-1$. If i_{s-1} and i_{s-2} lie in the same arithmetic sequence, the leading monomials of the corresponding inner sums have equal exponents of x_1 since

$$\begin{aligned}\deg_{x_1}(l_s) &= (i_{s-1}-3)+(t-s)(p-1)\\ &= (i_{s-2}-3)+(t-(s-1))(p-1)=\deg_{x_1}(l_{s-1}).\end{aligned}$$

Applying this to the first subsequence $(i_1,\cdots,i_{t'})$, and the second subsequence $(i_s : t'+1 \le s \le i_{t-1})$ if non-empty, gives

$$\begin{aligned}&\deg_{x_1}(l_2)=\cdots=\deg_{x_1}(l_{t'+1}),\\ &\deg_{x_1}(l_{t'+2})=\cdots=\deg_{x_1}(l_t)\ \text{ if } t'\le t-2,\\ \text{where }\ &\deg_{x_1}(l_t)=(i_{t-1}-3)+(t-t)(p-1)=i_{t-1}-3.\end{aligned}$$

This means we need to use $x_{i_s} < x_{i_{s+1}}$ to determine ordering:

$$\begin{gathered}l_2<\cdots<l_{t'+1},\\ \text{and similarly } l_{t'+2}<\cdots<l_t \text{ if } t'\le t-2.\end{gathered}$$

So, to find the leading monomial of the double sum, it is sufficient to consider only l_s where $s = t'+1$, t and the one not considered so far which is $s = 1$.

We compare $l_{t'+1}$ and l_t. If the second subsequence is non-empty, then the gap between the two subsequences is p and we can write

$$\begin{aligned}i_{t'} &= i_{t'+1}-(p-1)-1\\ (i_{t'}-3)+(t-(t'+1))(p-1) &= (i_{t'+1}-3)+(t-(t'+2))(p-1)-1\\ \deg_{x_1}(l_{t'+1}) &= \deg_{x_1}(l_{t'+2})-1=(i_{t-1}-3)-1.\end{aligned}$$

This shows that $l_{t'+1} > l_t$ holds whenever $t' \le t-2$. And of course, $l_{t'+1} = l_t$ if $t' = t-1$. So this eliminates l_t and we can focus on $s = t'+1$ and 1.

Consider a similar comparison between the remaining two choices of s. In this case, the difference $d := i_1 - i_0 = i_1 - 3$ can be $1, \cdots, p$ instead of a fixed p.

$$\begin{aligned}
\deg_{x_1}(l_1) &= \cancelto{0}{(i_0 - 3)} + (t-1)(p-1) \\
&= (i_1 - 3) - d + (t-2)(p-1) + (p-1) \\
&= \deg_{x_1}(l_2) + (p-1-d) \\
&= \deg_{x_1}(l_{t'}) + (p-1-d).
\end{aligned}$$

With this, we can see that the leading monomial of the double sum is l_s where

(1) $s = t'$ if $d \le p-1$, with $\deg_{x_1}(l_s) = \deg_{x_1}(l_2) = (i_1-3) + (t-2)(p-1)$;

(2) $s = 1$ if $d = p$, with $\deg_{x_1}(l_s) = (i_1-3) + (t-2)(p-1) - 1$.

Going back to $g_{(i_s),t'}$, the remaining two sums of equation 2.3 is

$$-x_1^{(i_1-3)+(t-2)(p-1)}(-x_2)^{(n-i_1)-(t-2)(p-1)-p}\left[\sum_{s=1}^{t'}(-x_2)\,x_{i_s}^p + \sum_{t'+1\le s\le t-1} x_1 x_{i_s}^p\right].$$

Its leading monomial is always $-x_1^{(i_1-3)+(t-2)(p-1)}(-x_2)^{(n-i_1)-(t-2)(p-1)-p+1}\,x_{i_{t'}}^p$ indexed by $s = t'$. Comparing its exponent of x_1 to that of the leading term of the double sum above, since the p-power $x_{i_{t-1}}^p$ guarantees a smaller exponent of x_2 even if the exponents of x_1 are equal, we see that the double sum has a smaller leading term unless $d = p$. This lemma then follows. □

The first step of subudction of a given $g_{(i_s),t'}$ depends on which of the two cases in lemma 2.5.2 holds. Both cases will result in another invariant of the same form. Forward progress is guaranteed by having a smaller leading term after each step. We start with case (2) since it includes the base case $g_{(3,4,n)}$. We subduct the slightly more general form $(-x_2)^e\, g_{(i_s),t'}$. It will be useful later for finding more invariants. (It comes having to subduct $(-x_2)\,h_i - f_i$.)

Lemma 2.5.3. Fix $e = 0, \cdots, p-2$. Suppose $(-x_2)^e\, g_{(i_s),t'} \in S^G$ and that $i_1 - 3 \le p-1$. So by case (2) of lemma 2.5.2, its leading monomial is

$$-x_1^{(i_1-3)+(t-2)(p-1)}(-x_2)^{e+(n-i_1)-(t-2)(p-1)-p+1}\,x_{i_{t'}}^p.$$

(1) If $\deg_{x_2}(l) = 0$ so that $l = x_1^{e+n-p-2} x_{i_{t'}}^p$, or if $i_{t'} = n-1$, then the invariant cannot be subducted any further over $\mathcal{B}_3$. This is the termination condition for the whole subduction process.

If neither termination conditions hold, then one step of subduction produces the new invariant

$$(-x_2)^e \, g_{(i_s),t'} - x_1^{(i_1-3)+(t-2)(p-1)} \, (-x_2)^{e+(n-i_1)-(t-2)(p-1)-p} \, f_{i_{t'}+1}.$$

(2) If $t' > 1$, then the new invariant can be expressed as

$$(-x_2)^e \, g_{\left(i_0,\cdots,i_{t'-1},\ i_{t'}+1,\ i_{t'+1},\cdots,i_t\right),t'-1}.$$

This new invariant satisfies the premise of this lemma. It has a smaller value of " t' ", by one, as shown, and further subductions can be applied.

(3) If $t' = 1$, then the new invariant is

$$(-x_2)^e \, g_{(i_0,i_1+1,i_2,\cdots,i_t),t-1}.$$

It has a greater value of "i_1", and satisfies "$t' = t-1$". There is no guarantee whether or not this new invariant would satisfy the premise of this lemma or the termination condition.

Proof. If either of the termination contidions described in part (1) of this lemma hold, then it is clear that no further subduction over $\mathcal{B}$ is possible, by checking the table of leading terms in table 2.2. So assume instead that $4 \le i_{t'} \le n-2$

and $\deg_{x_2}(l) \geq 1$. We can subduct $(-x_2)^e g_{(i_s),t'}$. Using $f_{i_{t'}+1}$ from lemma 2.4.1

$$\begin{aligned}
f_{i_{t'}+1} &= -(-x_2)\, x_{i_{t'}}^p + (-x_2)^p\, x_{i_{t'}} + x_1 x_{i_{t'}+1}^p - x_1^p x_{i_{t'}+1} \\
f &:= -(-x_2)^e\, x_1^{(i_1-3)+(t-2)(p-1)} (-x_2)^{(n-i_1)-(t-2)(p-1)-p} f_{i_{t'}+1} \\
&= (-x_2)^e \Big(\quad x_1^{(i_1-3)+(t-2)(p-1)} (-x_2)^{(n-i_1)-(t-2)(p-1)-p+1} x_{i_{t'}}^P \\
&\qquad -x_1^{(i_1-3)+(t-2)(p-1)} (-x_2)^{(n-i_1)-(t-2)(p-1)} x_{i_{t'}} \\
&\qquad -x_1^{(i_1-3)+(t-2)(p-1)+1} (-x_2)^{(n-i_1)-(t-2)(p-1)-p} x_{i_{t'}+1}^p \\
&\qquad +x_1^{(i_1-3)+(t-2)(p-1)+p} (-x_2)^{(n-i_1)-(t-2)(p-1)-p} x_{i_{t'}+1} \Big).
\end{aligned}$$

We will add each term to $(-x_2)^e g_{(i_s),t'}$. Recall its double sum (equation 2.3).

$$(-x_2)^e \sum_{s=1}^{t} \sum_{j=i_{s-1}}^{i_s} x_1^{(j-3)+(t-s)(p-1)} (-x_2)^{(n-j)-(t-s)(p-1)} x_j$$

With this expression in mind, consider the second and last term of the above expansion of f. Their exponents of x_1 can be written as follows. Since $(i_1, \cdots, i_{t'})$ is arithmetic of difference $p-1$,

$$\begin{aligned}
(i_1-3) + (t-2)(p-1) &= (i_{t'}-3) + (t-(t'+1))(p-1) \\
(i_1-3) + (t-2)(p-1) + p &= (i_{t'}+1-3) + (t-t')(p-1).
\end{aligned}$$

From this, we can see that the second term cancels the double sum term indexed by $s = t'+1, j = i_{t'}$, and the last creates a term indexed by $s = t', j = i_{t'}+1$.

Explicitly, adding these two terms to the double sum gives

$$\begin{aligned}
&(-x_2)^e \sum_{1\le s\le t'-1} \sum_{j=i_{s-1}}^{i_s} x_1^{(j-3)+(t-s)(p-1)} (-x_2)^{(n-j)-(t-s)(p-1)} x_j \\
+ \quad &(-x_2)^e \left[\sum_{j=i_{s-1}}^{i_s+1} x_1^{(j-3)+(t-s)(p-1)} (-x_2)^{(n-j)-(t-s)(p-1)} x_j \right]_{s=t'} \\
+ \quad &(-x_2)^e \left[\sum_{j=i_{s-1}+1}^{i_s} x_1^{(j-3)+(t-s)(p-1)} (-x_2)^{(n-j)-(t-s)(p-1)} x_j \right]_{s=t'+1} \\
&+ (-x_2)^e \sum_{t'+2\le s\le t} \sum_{j=i_{s-1}}^{i_s} x_1^{(j-3)+(t-s)(p-1)} (-x_2)^{(n-j)-(t-s)(p-1)} x_j .
\end{aligned}$$

This is the double sum in $(-x_2)^e\, g_{\left(i_0,\cdots,i_{t'-1},\ i_{t'}+1,\ i_{t'+1},\cdots,i_t\right),\bar{t}}$ for some $\bar{t}$.

To find $\bar{t}$, consider the remaining terms. From $(-x_2)^e\, g_{(i_s),t'}$ (equation 2.3),

$$-(-x_2)^e\, x_1^{(i_1-3)+(t-2)(p-1)} (-x_2)^{(n-i_1)-(t-2)(p-1)-p} \left[\sum_{s=1}^{t'} (-x_2)\, x_{i_s}^p + \sum_{t'+1\le s\le t-1} x_1 x_{i_s}^p \right].$$

Adding the first and third terms in f to this gives

$$\begin{aligned}
-(-x_2)^e\, x_1^{(i_1-3)+(t-2)(p-1)} (-x_2)^{(n-i_1)-(t-2)(p-1)-p} &\Bigg[\sum_{1\le s\le t'-1} (-x_2)\, x_{i_s}^p \\
&+ x_1 x_{i_{t'}+1}^p + \sum_{t'+1\le s\le t-1} x_1 x_{i_s}^p \Bigg].
\end{aligned}$$

So a similar index shift occurs. If $t' > 1$ holds, as in part (2) of this lemma, then we have $\bar{t} = t' - 1$ since $i_0 < i_{t'-1} = (i_{t'} + 1) - p$, effectively decreasing and increasing the lengths of the first and second arithmetic subsequences respectively. Since $i_1 - 3$ and t remain unchanged, this subduction result still satisfies the precondition of this lemma but not the termination condition. Further subductions over $\mathcal{B}_3$ are possible, each time reducing t' by one.

It can be repeated until $t' = 1$, where we are in part (3) of this lemma. Suppose $t' = 1$, so that the first subsequence has length 1. Some care is needed since we cannot reduce the length to zero, due to the restrictions on (i_s). Now, since the range $1 \leq s \leq t' - 1$ is empty, we can rewrite the expression above as

$$\begin{aligned} &- (-x_2)^e \, x_1^{(i_1-3)+(t-2)(p-1)} \, (-x_2)^{(n-i_1)-(t-2)(p-1)-p} \left[x_1 x_{i_{t'}+1}^p + \sum_{t'+1 \leq s \leq t-1} x_1 x_{i_s}^p \right] \\ &= - (-x_2)^e \, x_1^{(i_1+1-3)+(t-2)(p-1)} \, (-x_2)^{(n-i_1-1)-(t-2)(p-1)-p} \Bigg[(-x_2) \, x_{i_{t'}+1}^p \\ &\qquad\qquad + \sum_{t'+1 \leq s \leq t-1} (-x_2) \, x_{i_s}^p \Bigg]. \end{aligned}$$

This shows that we now have $\bar{t} = t - 1$, essentially relabelling the second arithmetic subsequence as the first if it was not empty. This time, the result does have a greater value of "i_1", by one. This means that both cases (1) and (2) of lemma 2.5.2 are possible for this subduction result $(-x_2)^e \, g_{(i_0, i_1+1, i_2, \cdots, i_t), t-1}$, depending on whether $(i_1 + 1) - 3 = p$ or not respectively. $\square$

We now consider subducting $(-x_2)^e \, g_{(i_s), t'}$ where case (1) of lemma 2.5.2 applies to $g_{(i_s), t'}$. We will assume that $(-x_2)^e \, g_{(i_s), t'}$ is the result of applying part (3) of lemma 2.5.3. It will be shown that, applying one subduction step to $(-x_2)^e \, g_{(i_s), t'}$ gives an invariant that satisfies the premise of lemma 2.5.3 again. And since the base case $(-x_2)^e \, g_{(3,4,n)}$ also satisfy the premise of lemma 2.5.3, this assumption is well-founded.

This assumption allows us to assume $t' = t - 1$. Furthermore, consider the invariant to which lemma 2.5.3 can be applied to get $(-x_2)^e \, g_{(i_s)}$. It cannot satisfy the termination condition from part (1) of the lemma, for otherwise a subduction step could not be applied to get $(-x_2)^e \, g_{(i_s)}$. In particular, it had satisfied "$i_1 \leq e + n - (t-1)(p-1) - 1$" before the subduction step. Part (3) of lemma 2.5.3 increases "i_1" by one. So our assumption also provides the bound $i_1 \leq e + n - (t-1)(p-1)$.

Lemma 2.5.4. Fix $e = 0, \cdots, p-2$. Suppose $(-x_2)^e \, g_{(i_s)} \in S^G$ and $i_1 - 3 = p$. Using case (1) of lemma 2.5.2, its leading term is

$$x_1^{(t-1)(p-1)} \, (-x_2)^{e+(n-3)-(t-1)(p-1)} \, x_3.$$

One step of subduction produces the new invariant

$$\begin{aligned}
&\left(-x_2\right)^e g_{(i_s)} + \left(-x_2\right)^e x_1^{(t-1)(p-1)} \left(-x_2\right)^{(n-3)-(t-1)(p-1)-p} f_4 \\
&= \left(-x_2\right)^e g_{(i_0,4,i_1,\cdots,i_t)}.
\end{aligned}$$

This new invariant satisfies the premise of lemma 2.5.3 since "$i_1 - 3$" is now 1. It is possible for the termination condition "$i_{t'} = n - 1$" from lemma 2.5.3 to hold for this new invariant.

Proof. We can subduct $\left(-x_2\right)^e g_{(i_s)}$ over $\mathcal{B}_3$. Using f_4 from lemma 2.4.1

$$\begin{aligned}
f_4 &= -\left(-x_2\right)^p x_3 - x_1 x_4^p + x_1^{p-1}\left(-x_2\right) x_3 + x_1^p x_4 \\
f &:= \left(-x_2\right)^e x_1^{(t-1)(p-1)} \left(-x_2\right)^{(n-3)-(t-1)(p-1)-p} f_4 \\
&= \left(-x_2\right)^e \Big(-x_1^{(t-1)(p-1)} \left(-x_2\right)^{(n-3)-(t-1)(p-1)} x_3 \\
&\qquad -x_1^{(t-1)(p-1)+1} \left(-x_2\right)^{(n-3)-(t-1)(p-1)-p} x_4^p \\
&\qquad +x_1^{t(p-1)} \left(-x_2\right)^{(n-3)-(t-1)(p-1)-p+1} x_3 \\
&\qquad +x_1^{t(p-1)+1} \left(-x_2\right)^{(n-3)-(t-1)(p-1)-p} x_4 \Big) \\
&= \left(-x_2\right)^e \Bigg(- \left[x_1^{(j-3)+(t-s)(p-1)} \left(-x_2\right)^{(n-j)-(t-s)(p-1)} x_j \right]_{\substack{s=1 \\ j=i_{s-1}=3}} \\
&\qquad -x_1^{(i_1-3)+(t-2)(p-1)} \left(-x_2\right)^{(n-i_1)-(t-2)(p-1)-p} \left[\left(-x_2\right) x_4^p\right] \\
&\qquad + \left[\sum_{j=3}^{4} x_1^{(j-3)+(t-s)(p-1)} \left(-x_2\right)^{(n-j)-(t-s)(p-1)} x_j \right]_{s=0} \Bigg).
\end{aligned}$$

The argument is similar to the proof for lemma 2.5.3. We add this to $\left(-x_2\right)^e g_{(i_s)}$ using the expression of $g_{(i_s),t'}$ in equation 2.3. The first of the three terms cancels the term in the double sum similarly indexed. The last two lines then changes the subscript from $(i_0, i_1, \cdots, i_t)$ to $(i_0, 4, i_1 \cdots, i_t)$, increasing its length. □

We put the two lemmas together to subduct $\left(-x_2\right)^e g_{(i_s)}$ over $\mathcal{B}_3$. We can assume that $\left(-x_2\right)^e g_{(i_s)}$ satisfies $i_1 - 3 \leq p - 1$, since lemma 2.5.4 ensures we always go back to case (1) of lemma 2.5.2.

Lemma 2.5.5. Fix $e = 0, \cdots, p-2$. Suppose $(-x_2)^e\, g_{(i_s)} \in S^G$ and $i_1 - 3 \leq p-1$. Then a subduction of $(-x_2)^e\, g_{(i_s)}$ over $\mathcal{B}_3$ is $(-x_2)^e\, g_{\left(\bar{i}_s\right)} \in S^G$, where

$$\bar{i}_s = e + n - (t-s)(p-1)$$

for $s = 1, \cdots, \bar{t} - 1$.

Proof. Let $(-x_2)^e\, g_{\left(\bar{i}_s\right)_{s=0}^{\bar{t}}, \bar{t}'}$ be the result of subducting $(-x_2)^e\, g_{(i_s)}$ according to lemmas 2.5.3 and 2.5.4. The subduction can only terminate after the subduction step in part (3) of lemma 2.5.3 or after the step in lemma 2.5.4. In both cases, we have $\bar{t}' = \bar{t} - 1$. So we can assume that $\left(\bar{i}_1, \cdots, \bar{i}_{\bar{t}-1}\right)$ is arithmetic.

One of the two termination conditions given in part (1) of lemma 2.5.3 is

$$\begin{aligned} 0 &= \deg_{x_2}\left(\mathrm{LT}\left((-x_2)^e\, g_{\left(\bar{i}_s\right)}\right)\right) \\ &= e + \left(n - \bar{i}_1\right) - \left(\bar{t} - 2\right)(p-1) - p + 1 \\ \bar{i}_1 &= e + n - \left(\bar{t} - 1\right)(p-1). \end{aligned}$$

The values for each $\bar{i}_s$ follows from noting that $\left(\bar{i}_1, \cdots, \bar{i}_{\bar{t}-1}\right)$ is arithmetic. The other termination condition is the sequence $\left(\bar{i}_s\right)$ ending in $(\cdots, n-1, n)$. This sequence also necessarily has the required form with $e = p-2$. $\square$

Apply this lemma to the case $(i_s) = (3, 4, n)$, and divide-by-x_1 to get $h_{n-(p-1)}$.

Lemma 2.5.6. Let $e = 0, \cdots, p-2$. Let $(-x_2)^e\, g_{(i_s)_{s=0}^t}$ be the subduction of $(-x_2)^e\, g_{(3,4,n)}$ as described by lemma 2.5.5, so that $i_s = e + n - (t-s)(p-1)$. Set $i = i_{t-1}$. A subduction/divide-by-x_1 of $(-x_2)^e\, g_{(3,4,n)}$ over $\mathcal{B}_3$ is

$$\begin{aligned} h_i &:= x_1^{-e-n+(p+2)}(-x_2)^e\, g_{(i_s)} \\ &= \sum_{s=1}^{t} \sum_{j=i_{s-1}}^{i_s} x_1^{j-i_{s-1}}(-x_2)^{i_s-j} x_j - \sum_{s=1}^{t-1} x_{i_s}^p. \end{aligned}$$

This defines h_i for $i = n-(p-1), \cdots, n-1$ with leading term x_i^p. $\square$

Note that the only choice of e we know for which $(-x_2)^e\, g_{3,4,n}$ is a tête-a-tête difference in $\mathcal{B}_n$ is $e = 0$. This means we can only conclude that the subduction/divide-by-x_1 of $g_{(3,4,n)}$, which is $h_{n-(p-1)}$, is a new invariant. We now show how to make use of the general form to find the remaining invariants h_j mentioned in proposition 2.5.1 at the start of the section.

Lemma 2.5.7. The polynomials $h_{n-(p-1)}, \cdots, h_{n-1}$ defined in lemma 2.5.6 are G-invariant. Furthermore, over $\mathcal{B}_3$,

1. $h_{n-(p-1)}$ is a subduction/divide-by-x_1 of $g + (-x_2)^{(n-3)-p} f_3$; and
2. h_{i+1} is of $f_{i+1} + (-x_2) h_i$, for $i = n - (p-1), \cdots, n-2$.

Proof. We will show that $h_i \in G$ by induction on $i = n - (p-1), \cdots, n-1$. Take the base case $i = n-(p-1)$. As mentioned, by lemma 2.5.6 with $e = 0$, the polynomial h_i is the subduction/divide-by-x of $g_{(3,4,n)}$, which is the tête-a-tête difference $g + (-x_2)^{(n-3)-p} f_3$ in $\mathcal{B}_3$. By theorem 1.1.3, h_i is G-invariant.

For the induction step, fix $i = n - (p-1), \cdots, n-2$. Assume that the lemma holds for h_i. Since h_i is G-invariant, by lemma 2.4.1,

$$S^G\left[x_1^{-1}\right] = k\left[\mathcal{B}_3, x_1^{-1}\right] \leq k\left[\mathcal{B}_3, h_i, x_1^{-1}\right] \leq S^G\left[x_1^{-1}\right].$$

Since h_i has leading monomial x_i^p, theorem 1.1.3 can be applied to the set $\mathcal{B}_3 \cup \{h_i\} \cup \{\boldsymbol{N}_4, \cdots, \boldsymbol{N}_n\}$ of invariants to obtain more invariants. By showing that the subduction/divide-by-x_1 of the tête-a-tête difference $f_{i+1} + (-x_2) h_i$ over the set $\mathcal{B}_3 \cup \{h_i\} \cup \{\boldsymbol{N}_4, \cdots, \boldsymbol{N}_n\}$ is h_{i+1}, it will follow that $h_{i+1} \in S^G$. The steps to this subduction are the same as those in lemmas 2.5.3 and 2.5.4. We will "reverse" subduction in order to take advantage of them.

A subduction of $f_{i+1} + (-x_2) h_i$ over $\mathcal{B}_3 \cup \{h_i\} \cup \{\boldsymbol{N}_4, \cdots, \boldsymbol{N}_n\}$ can be found by subducting it over $\mathcal{B}_3$ instead, provided that the result has a leading term not divisible by x_i^p nor by $x_4^{p^2}, \cdots, x_{n-1}^{p^2}, x_n^p$ in S. And subducting it over $\mathcal{B}_3$ is the same as subducting $(-x_2) h_i$ over $\mathcal{B}_3$, since the only tête-a-tête in $\mathcal{B}_3$ that pairs with $(-x_2) h_i$, which has leading term $-(-x_2) x_i^p$, is f_{i+1} (see 2.2 for a table of leading terms). Now, using the definition of h_i in lemma 2.5.6, we have

$$x_1^{e+n-(p+1)} (-x_2) h_i = (-x_2)^{e+1} g_{(i_s)},$$

where $e = i - n + (p-1)$ and $i_s = e + n - (t-s)(p-1)$. Since multiplying by x_1 does not change the result of subduction/divide-by-x_1, we can also subduct/divide-by-x_1 the right-hand side instead. By lemma 2.5.5, it subducts to $(-x_2)^{e+1} g_{(3,\cdots,i+1,n)}$, and h_{i+1} is defined in lemma 2.5.6 as the divide-by-x_1 of this, as required. □

Now that the extra invariants specified in proposition 2.5.1 are found, we are in a position to prove the proposition.

Proof of 2.5.1. Lemma 2.5.7 showed that $h_{n-(p-1)}, \cdots, h_{n-1}$ are invariants. Due to the tête-a-tête differences used in finding them, if we adjoin them to $\mathcal{B}_3$, then the lemma also showed that $g, f_{n-(p-2)}, \cdots, f_{n-1}$ are redundant as k-algebra generators of $S^G\left[x_1^{-1}\right]$. So we now have

$$S^G\left[x_1^{-1}\right] = k\left[x_1, x_2, \boldsymbol{N}_3, f_4, \cdots, f_{n-(p-1)}, h_{n-(p-1)}, \cdots, h_{n-1}, x_1^{-1}\right]$$

This new set of invariants does not satisfy precondition (2) of theorem 1.1.3. We adjoin the orbit products $\boldsymbol{N}_4, \cdots, \boldsymbol{N}_{n-p}$ and $\boldsymbol{N}_n$ in order to apply the theorem. This gives us the set $\mathcal{B}$ of invariants defined in proposition 2.5.1. So it is sufficient to check that its tête-a-tête differences subduct to zero.

The leading terms of elements of $\mathcal{B}$ are, for $i = n-(p-1), \cdots, n-1$:

f	$\boldsymbol{x}_1$	$\boldsymbol{x}_2$	$\boldsymbol{N}_3$	f_4	$\boldsymbol{N}_4$	$\cdots$	$\boldsymbol{N}_{n-p}$	f_5	$\cdots$	$f_{n-(p-1)}$	h_i	$\boldsymbol{N}_n$
$\mathrm{LT}(f)$	x_1	x_2	x_3^p	$x_2^p x_3$	$x_4^{p^2}$	$\cdots$	$x_{n-p}^{p^2}$	$x_2 x_4^p$	$\cdots$	$x_2 x_{n-p}^p$	x_i^p	x_n^p

From this table, we can see that the tête-a-tête differences to check are

(1) $f_i^p + (-x_2)^p \boldsymbol{N}_{i-1}$ for $5 \le i \le n-(p-1)$; and

(2) $f_4^p + (-x_2)^{p^2} \boldsymbol{N}_3$.

And for this, we will show the following:

$$\begin{aligned} f_i^p - x_2^p \boldsymbol{N}_{i-1} &= \left(x_1 x_2^p - x_1^p x_2\right)^{p-1} f_i + x_1^p \boldsymbol{N}_i, \\ \text{and } f_4^p - \left(x_2^p - x_1^{p-1} x_2\right)^p \boldsymbol{N}_3 &= \left(x_1 x_2^p - x_1 x_2\right)^{p-1} f_4 - x_1^p \boldsymbol{N}_4. \end{aligned}$$

for $5 \leq i \leq n-(p-1)$. Expand the norms as

$$\begin{aligned}
\boldsymbol{N}_i &= \left(x_i^p - x_1^{p-1}x_i\right)^p - \left(x_2^p - x_1^{p-1}x_2\right)^{p-1}\left(x_i^p - x_1^{p-1}x_i\right) \\
\boldsymbol{N}_{i-1} &= \left(x_{i-1}^p - x_2^{p-1}x_{i-1}\right)^p - \left(x_1^p - x_2^{p-1}x_1\right)^{p-1}\left(x_{i-1}^p - x_2^{p-1}x_{i-1}\right).
\end{aligned}$$

For $5 \leq i \leq n-(p-1)$, it is sufficient to note that the following sums to zero:

$$\begin{aligned}
f_i^p &= \left(x_2x_{i-1}^p - x_2^px_{i-1}\right)^p + \left(x_1x_i^p - x_1^px_i\right)^p \\
-x_2^p\boldsymbol{N}_{i-1} &= -\left(x_2x_{i-1}^p - x_2^px_{i-1}\right)^p \\
&\quad + \left(x_2x_1^p - x_2^px_1\right)^{p-1}\left(x_2x_{i-1}^p - x_2^px_{i-1}\right) \\
-\left(x_1x_2^p - x_1^px_2\right)^{p-1} f_i &= -\left(x_1x_2^p - x_1^px_2\right)^{p-1}\left(x_2x_{i-1}^p - x_2^px_{i-1}\right) \\
&\quad - \left(x_1x_2^p - x_1^px_2\right)^{p-1}\left(x_1x_i^p - x_1^px_i\right) \\
\text{and } -x_1^p\boldsymbol{N}_i &= -\left(x_1x_i^p - x_1^px_i\right)^p + \left(x_1x_2^p - x_1^2x_2\right)^{p-1}\left(x_1x_i^p - x_1^px_i\right).
\end{aligned}$$

The special case for $i=4$ can be shown in the same way:

$$\begin{aligned}
f_4^p &= \left(x_2^p - x_1^{p-1}x_2\right)^p x_3^p - \left(x_1x_4^p - x_1^px_4\right)^p \\
-\left(x_2^p - x_1^{p-1}x_2\right)^p \boldsymbol{N}_3 &= -\left(x_2^p - x_1^{p-1}x_2\right)^p x_3^p + x_1^{p-1}\left(x_2^p - x_1^{p-1}x_2\right)^p x_3 \\
-\left(x_1x_2^p - x_1^px_2\right)^{p-1} f_4 &= -\left(x_1x_2^p - x_1^px_2\right)^{p-1}\left(x_2^p - x_1^{p-1}x_2\right)x_3 \\
&\quad + \left(x_1x_2^p - x_1^px_2\right)^{p-1}\left(x_1x_4^p - x_1^px_4\right) \\
\text{and } x_1^p\boldsymbol{N}_4 &= \left(x_1x_4^p - x_1^px_4\right)^p \\
&\quad - \left(x_1x_2^p - x_1^px_2\right)^{p-1}\left(x_1x_4^p - x_1^px_4\right).
\end{aligned}$$

It might be helpful to note that:

$$\begin{aligned}
&\left(x_1x_2^p - x_1^px_2\right)^{p-1}\left(x_2^p - x_1^{p-1}x_2\right) \\
&= x_1^{-1}\cdot\left(x_1x_2^p - x_1^px_2\right)^p \\
&= x_1^{p-1}x_2^{p^2} - x_1^{p^2-1}x_2^p.
\end{aligned}$$

With this, we have shown that there are no non-trivial tête-a-tête differences that subduct to zero over $\mathcal{B}$. By theorem 1.1.3, we have $S^G = k[\mathcal{B}]$.

Note that $|\mathcal{B}| = 2n - p - 2$, whereas the number of non-trivial tête-a-têtes in $\mathcal{B}$ is $n - p - 2$. It follows that S^G is a complete intersection, with a relation ideal generated by the non-trivial tête-a-tête differences. $\square$

2.6 Subgroups with one-dimensional invariant subspace

So far in chapter 2, we have considered the subgroups of F, the maximal two-row subgroup that fixes $\langle x_1, x_2\rangle_k$. However, in the maximal two-row group E, there are other abelian subgroups, namely ones that do not fix x_2. In this section, we will show that the remaining abelian subgroups of E consist of one-row groups and groups are congruent to one of two forms to be given in lemma 2.6.2. We determine their invariant rings up to a congruence in proposition 2.6.3, and show that they are complete intersections. Lastly, in theorem 2.6.5, we summarise our results in chapter 2 on invariant rings.

We start by finding the possible abelian subgroups of E not in F. By considering matrix block action, we can see that the centre of E, denoted by $C(E)$, is the largest one-row subgroup of F with commutator $[C(E), V^*] = \langle x_1\rangle_k$. So,

$$C(E) := \left\{ \left(\begin{array}{c|ccc} \multirow{2}{*}{$I_{2\times 2}$} & a_3 & \cdots & a_n \\ & 0 & \cdots & 0 \\ \hline 0 & & I_{(n-2)\times(n-2)} & \end{array} \right) \in \mathrm{GL}(V) : a_3, \cdots, a_n \in k \right\}.$$

Given $\sigma \in E \setminus C(E)$, its centraliser is $C_E(\sigma) = F$ if $\sigma \in F \setminus C(E)$, and it is $\langle \sigma, C(E)\rangle$ if $\sigma \notin F$. Using this we find the remaining abelian subgroups of F.

Lemma 2.6.1. Let $G \leq E$. Write $G' = G \cap F$ for its subgroup fixing x_2. Then G' is abelian, of index $[G : G'] = 1$ or p. And G is abelian if and only if one of the following holds:

(0) $G = G'$, and so $G \leq F$; or

(1) $G = \langle \tau_3, G' \rangle$ for some $\tau_3 \in G \setminus G'$, and $G' \leq C(E)$.

Proof. The subgroup $G' \leq F$ is certainly abelian. For its index, let $\sigma, \tau \in G$. Then $\sigma\tau^{-1} \in G'$ if and only if $[\sigma, x_2] = [\tau, x_2]$. There are at most p possible choices for $[\sigma, x_2] \in \langle x_1 \rangle_k$, and so $[G : G'] = 1$ or p.

Suppose G is abelian. Assume $G' < G$ is strict. Pick $\tau_3 \in G \setminus G'$ so that $G = \langle G', \tau_3 \rangle$. Then G must be a subgroup of the centraliser of τ_3 in E. The centraliser is $\langle \tau_3, C(E) \rangle$, and form (2) follows. □

So the abelian subgroups of E that are not in F are of form (2) in lemma 2.6.1 with the subgroup $G \cap F \leq C(E)$ being one-row. If there is a one-row element say $\tau_3 \in G \setminus G'$, then G is itself one-row, a reflection group, with polynomial invariant ring. So consider instead the case when there are no one-row $\tau_3 \in G \setminus G'$. We will show that all such groups G can be generated by G' and the symmetric square from theorem 1.0.9.

Lemma 2.6.2. Let $n \geq 3$ and $G \leq E$. Suppose G is abelian, not one-row and not in F. Up to a change of basis, we have $G = \langle \tau_3, \sigma_j : i \leq j \leq n \rangle$ with $i = 3$ or 4 depending on whether $|G| = n-1$ or $n-2$ respectively , where

$$\tau_3 = \begin{pmatrix} 1 & 2 & 1 & 0 & \cdots \\ 0 & 1 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \quad \text{and } \sigma_i := \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_i \right].$$

Proof. Since G does not fix x_2, and p is odd, we can assume there is a two-row $\tau_3 \in G$ of the form, with entries in k,

$$\tau_3 = \begin{pmatrix} 1 & 2 & a_3 & a_4 & \cdots \\ 0 & 1 & b_3 & b_4 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Then $G = \langle \tau_3, G \cap C(E) \rangle$ by lemma 2.6.1. Replace x_j in B by $x_j - 2^{-1}a_3x_2$ to assume that $a_j = 0$ for $j = 3, \cdots, n$. That is,

$$\tau_3 = \begin{pmatrix} 1 & 2 & 0 & 0 & \cdots \\ 0 & 1 & b_3 & b_4 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

There is some $b_i \neq 0$, otherwise $G = \langle \tau_3, G \cap C(E) \rangle$ would be one-row. Reorder $x_3, \cdots, x_n$ in B so that $b_3 \neq 0$. And for $j \geq 4$, replace x_j in B by $b_3 x_j - b_j x_3$ to assume $b_j = 0$. This gives

$$\tau_3 = \begin{pmatrix} 1 & 2 & 0 & 0 & \cdots \\ 0 & 1 & b_3 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Lastly for τ_3, replace x_3 in B by $2^{-1}x_2 + b_3^{-1}x_3$ to get the required form.

$$\tau_3 = \begin{pmatrix} 1 & 2 & 1 & 0 & \cdots \\ 0 & 1 & 1 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

We now pick σ_i, from the one-row subgroup in $G' := G \cap C(E) \leq F$ that fixes x_2. Let $G'' \leq G'$ be the subgroup that fixes x_3. Since τ_3 fixes x_i for $i \geq 4$, it is clear that we are free to pick $\sigma_i = \left[\binom{1}{0}_i\right]$ for each $i \geq 4$ in this one-row subgroup, by using lemma 2.1.4 or otherwise. If $G' = G''$, then done.

Suppose instead $G'' < G'$ is strict. There is $\sigma_3 \in G'$ that does not fix x_3, say

$$\sigma_3 = \left[\begin{pmatrix} c_3 & \cdots & c_n \\ 0 & \cdots & 0 \end{pmatrix}\right],$$

with entries in k and $c_3 \neq 0$. If $n \geq 4$, replace σ_3 by $\sigma_3 \sigma_4^{-c_4} \cdots, \sigma_n^{-c_n}$, to assume that $c_4 = \cdots = c_n = 0$. We replace σ_3 by $\sigma_3^{c_3^{-1}}$ to have the required form. $\square$

Lemma 2.6.2 gave us two forms to consider, depending on whether $G \cap C(E)$ fixes x_3. We find the invariant ring of both.

Proposition 2.6.3. Let $n \geq 3$ and $G = \langle \tau_3, \sigma_j : i \leq j \leq n \rangle$ with $i = 3$ or 4 with τ_3, τ_j as defined in lemma 2.6.2. Then $S^G = k\left[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n, f\right]$ is a complete intersection, where, depending on whether $i = 3$ or 4, respectively

$$f = x_2^2 - x_1x_3 \quad \text{or} \quad 2x_1x_3^p - 2x_1^px_3 + x_1^px_2 - x_2^{p+1}.$$

Proof. Write $G = \langle G\left[3\right], G'' \rangle$ where

$$G\left[3\right] = \langle \tau_3 \rangle \quad \text{or} \quad \langle \tau_3, \sigma_3 \rangle$$
$$\text{and } G'' = \left\langle \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix}_j\right] : 4 \leq j \leq n \right\rangle$$

Similar lemma 2.0.3 on ⊠-products, since G'' fixes x_1 x_2 and x_3, we can write

$$\begin{aligned} S^G &= k\left[x_1, x_2, x_3\right]^{G[3]} \otimes_{k[x_1]} k\left[x_i : i \neq 2 \text{ and } i \neq 3\right]^{G''} \\ &= k\left[x_1, x_2, x_3\right]^{G[3]}\left[\boldsymbol{N}_i : i \geq 4\right]. \end{aligned}$$

So it remains to find $S\left[3\right]^{G[3]}$. The case $G\left[3\right] = \langle \tau_3 \rangle$ is theorem 1.0.9. We leave the other case in the following lemma. □

Lemma 2.6.4. Let $n = 3$. Let $G = \langle \tau, \sigma \rangle \leq E$ where

$$\tau = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \sigma = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The invariant ring S^G is a complete intersection, given by

$$S^G := k\left[\boldsymbol{N}_1^G, \boldsymbol{N}_2^G, \boldsymbol{N}_3^G, f\right],$$
$$\text{where } f = 2x_1x_3^p - 2x_1^px_3 + x_1^px_2 - x_2^{p+1}.$$

Proof. We will mimic lemma 2.1.1. Let $\rho = \left[\binom{0}{1}_3\right]$. Then G is a maximal subgroup of $\langle G, \rho \rangle = E$, and we can use proposition 1.1.1: If $[\rho, f] \in S^E$ and

$\left[\rho, S^G\right] \subseteq S \cdot [\rho, f]$, then $S^G = S^E[f]$. The first precondition is clear since

$$[\rho, f] = 2x_1x_2^p - 2x_1^p x_2 = 2x_1 \prod_{\lambda \in \mathbb{F}_p} (x_2 + \lambda x_1) \in S^E.$$

For the second, note that $[\rho\tau^{-1}, V^*] = \langle x_1 \rangle_k$ and $\left[\rho\sigma^\lambda, V^*\right] = \langle x_2 + \lambda x_1 \rangle_k$ for $\lambda \in k$. This means $x_1 \prod_{\lambda \in k} (x_2 + \lambda x_1)$ divides $[\rho, g]$ for all $g \in S$. So $\left[\rho, S^G\right] \subseteq S \cdot [\rho, f]$. This gives $S^G = S^E[f]$. The lemma follows, since E is Nakajima. □

We summarise our result of this chapter as follows.

Theorem 2.6.5. Let V^* be a representation of dimension n of an abelian two-row unipotent group G over an odd prime field $k = \mathbb{F}_p$. Then G is congruent to one of the following

(1) A one-row group if $\dim_k [G, V^*] = 1$;

(2) A group generated by a symmetric square representation (1.0.9) and a one-row group as described in lemma 2.6.2 with S^G found in proposition 2.6.3, if $\dim_k [G, V^*] = 2$ and $[G, V^*] \not\subset (V^*)^G$;

or one of the following if $\dim_k [G, V^*] = 2$ and $[G, V^*] = (V^*)^G$

(3) A totally one-extended group (2.2.2) with S^G found in proposition 2.2.5;

(4) A block (2.3.1) with S^G found in propositions 2.4.3 and 2.5.1;

(5) A group generated by blocks with saturated columns (2.3.15), with S^G found in proposition 2.3.26;

(6) A $\boxtimes$-product of the above three (2.0.2) with S^G in proposition 2.0.3.

In all cases, S^G is a complete intersection.

Chapter 3

Computing Macaulay inverses

There is a Catalecticant matrix algorithm for finding the result of applying the bijection $\mathcal{M} \to \mathcal{I}$ in theorem 1.2.2. The first section introduces an algorithm for the inverse map $\mathcal{I} \to \mathcal{M}$. In later sections, we determine the Macaulay inverses for the Hilbert ideals of certain invariant rings.

3.1 A constructing algorithm

The Macaulay inverse algorithm to be introduced assumes that its input I lies in $\mathcal{I}$. That is, the ideal $I \triangleleft S$ is homogeneous, S_+-primary and irreducible. Assuming that the first two of the properties already hold or that the computation system used such as MAGMA [1] can check them,[1] we will first show how to check for irreducibility of I.

Algorithm 3.1.1. (In) Let $I \trianglelefteq S$ be a homogeneous S_+-primary ideal.

(Out) Whether the ideal I is irreducible.

(1) Let $J \trianglelefteq S$ be a homogeneous S_+-primary irreducible ideal included in I.[2]

(2) Let X be a minimal set of homogeneous ideal generators of the ideal quotient $(J : I)$.[3]

(3) Remove all polynomials in X that lies in J.

[1]In MAGMA we can check that IsHomogeneous(I) and IsZeroDimensional(I) are true.

[2]In MAGMA, we can use J := Ideal(RegularSequence(I)) since S is Cohen-Macaulay. Since I is S_+-primary, we can also use $J = Sx_1^{e_1} + \cdots + Sx_n^{e_n}$ for sufficiently large $e_1, \cdots, e_n$.

[3]In MAGMA, we can use X := Generators(ColonIdeal(J)).

(4) The ideal I is irreducible if and only if X is a singleton set.

Proof. This follows from the correspondence between over-ideals I of J that are in $\mathcal{I}$ and principal ideal quotients $(I : J)$ over I from theorem 1.2.3. $\square$

We now have the necessary tools for validating the input ideal. The Macaulay inverse algorithm for $\mathcal{I} \to \mathcal{M}$ is as follows.

Algorithm 3.1.2. (In) An ideal $I \in \mathcal{I}$.

(Out) A Macaulay inverse θ for I.

(1) Let t be the top degree of the Poincaré duality algebra $P := S/I$.[4]

(2) Fix a graded monomial order in S. (For example, grevlex.) For each monomial $x^{\boldsymbol{e}} \in S_t$ of degree t, determine its normal form modulo the ideal I, and set $\lambda_{\boldsymbol{e}} \in k$ to be the leading coefficient of the normal form.

(3) Construct a homogeneous inverse polynomial $\theta \in S_t^{-1}$ of degree t, by setting the coefficient of each $x^{-\boldsymbol{e}}$ term to $\lambda_{\boldsymbol{e}}$. That is, set the required Macaulay inverse output to

$$\theta := \sum_{\substack{\boldsymbol{e} \in \mathbb{Z}^n_{\geq 0} \\ |\boldsymbol{e}| = t}} \lambda_{\boldsymbol{e}} x^{-\boldsymbol{e}}.$$

Proof. (2): Reduction of monomials with respect to a graded ordering preserves their homogeneous degrees. So the normal forms found in this step are zeroes and homogeneous polynomials also of degree t. Since the top degree component of P has dimension 1 over k, the non-zero normal forms are unique up to a k-scalar multiple. Their leading coefficients $\lambda_{\boldsymbol{e}}$ record the ratios betweeen the normal forms.

(3): Write $\theta = \sum_{\boldsymbol{e}} \theta_{\boldsymbol{e}} x^{-\boldsymbol{e}}$, summing over tuples with $|\boldsymbol{e}| = e_1 + \cdots + e_n = t$. The aim is to determine all $\theta_{\boldsymbol{e}}$, or possible combinations of choices thereof. Take

[4] In MAGMA, we can use t := Degree(HilbertSeries(P)).

any homogeneous $g = \sum_{\boldsymbol{f}} \mu_{\boldsymbol{f}} x^{\boldsymbol{f}} \in I$ of degree t with coefficients $\mu_{\boldsymbol{f}} \in k$. Then

$$0 = \theta \cdot g = \sum_{\boldsymbol{e}} \sum_{\boldsymbol{f}} (\theta_{\boldsymbol{e}} \mu_{\boldsymbol{f}})\, x^{-\boldsymbol{e}} \cdot x^{\boldsymbol{f}} = \sum_{\boldsymbol{e}} \theta_{\boldsymbol{e}} \mu_{\boldsymbol{e}}.$$

This holds for any choice of g in the homogeneous component I_t of degree t.

Let $m = \dim_k (S_t)$. The k-vector space I_t has dimension $m-1$ since S/I satisfies Poincaré duality of top degree t. Applying the above annihilating condition to each $g \in I_t$ then sets up system of $m-1$ linear equations with m unknowns in the m entries of $\theta_{\boldsymbol{e}}$. Poincaré duality guarantees this system is consistent with a solution unique up to k-multiple. On the other hand, using the normal forms of each $x^{\boldsymbol{e}}$, say $\lambda_{\boldsymbol{e}} \cdot h$ for some fixed non-zero homogeneous $h \in S$, the normal form of g is

$$0 = \sum_{\boldsymbol{e}} \mu_{\boldsymbol{e}} \lambda_{\boldsymbol{e}} \cdot h.$$

This gives us the choice of $\theta_{\boldsymbol{e}}$ up to a unique k-multiple. □

3.2 Nakajima groups

In this section, we apply the above algorithm to find the Macaulay inverse for the Hilbert ideal $S_+^G S$ where G is a Nakajima group.

Corollary 3.2.1. Let $I = Sx_1^{e_1} + \cdots + Sx_n^{e_n} \in \mathcal{I}$ for some $\boldsymbol{e} = (e_1, \cdots, e_n) \in \mathbb{Z}_{\geq 0}^n$.

(1) $\mathrm{Ann}_{S^{-1}}(I) = S^{-1} \cdot \left(x_1^{1-e_1} \cdots x_n^{1-e_n}\right)$;

(2) There is a correspondence between monomials in $\mathcal{M}$ and ideals in $\mathcal{I}$ of the above form given by

$$S^{-1} \cdot \left(x_1^{1-e_1} \cdots x_n^{1-e_n}\right) \mapsto Sx_1^{e_1} + \cdots + Sx_n^{e_n}$$

Proof. (1): Let $t = e_1 + \cdots + e_n - n \in \mathbb{Z}_{\geq 0}$. Take any monomial $x^{\boldsymbol{f}} = x_1^{f_1} \cdots x_n^{f_n} \in S$. If $\deg\left(x^{\boldsymbol{f}}\right) = t+1$, then $f_i \geq e_i$ for some i, by the pigeon hole principle on the exponents, and so $x^{\boldsymbol{f}} \in Sx_i^{e_i}$. From this, $S_{t+1} \subseteq I$ and $\mathrm{topdeg}\,(S/I) \leq t$.

Using the same argument, if $\deg\left(x^{\boldsymbol{f}}\right) = t$, then $f_i \geq e_i$ for some i, unless $f_i = e_i - 1$ for all i. This shows that $\operatorname{topdeg}(S/I) = t$ and that, except $x_1^{e_1-1} \cdots x_n^{e_n-1}$, all monomials of degree t has zero normal form modulo I (with respect to any graded monomial ordering, say glex). Apply algorithm 3.1.2 to get the desired result.

(2): Follows from the Macaulay inverses correspondence. □

This correspondence can be used to find $S_+^G S$ when G is Nakajima.

Corollary 3.2.2. Let k be finite. Suppose G is Nakajima with respect to B.

(1) $S_+^G S = Sx_1^{|G_1|} + \cdots + Sx_n^{|G_n|}$;
(2) $\operatorname{Ann}_{S^{-1}}\left(S_+^G S\right) = S^{-1} \cdot \left(x_1^{1-|G_1|} \cdots x_n^{1-|G_n|}\right)$.

Proof. (1): Consider induction on n. The base case $n = 1$ is clear since $G = G_1 = 1$. Suppose instead $n \geq 2$. By induction hypothesis

$$\begin{aligned} S_+^G S &= S\boldsymbol{N}_1 + \cdots + S\boldsymbol{N}_{n-1} + S\boldsymbol{N}_n \\ &= Sx_1^{|G_1|} + \cdots + Sx_{n-1}^{|G_{n-1}|} + S\boldsymbol{N}_n. \end{aligned}$$

Write $\boldsymbol{N}_n = \sum_i f_i x_i$ as a monic polynomial in x_n over $S[n-1]$. Note that $G_{n-1} \cdots G_1$ fixes $\boldsymbol{N}_n \in S^G$. Since it fixes x_n, it must also fix the coefficients f_i. Since $\boldsymbol{N}_n$ is monic in x_n, the required equality follows.

(2): Apply lemma 3.2.1 to result of part (1). □

3.3 Two-row groups

In this section, we show that, if G is an abelian unipotent two-row group, that is the groups investigated in chatper 2, then there is a basis of V^* with respect to which the Macaulay inverse for $S_+^G S$ is an inverse monomial. Most of them are easy to find, except for two-row blocks, which we will investigate first.

Lemma 3.3.1. Let G be a two-row block with unsaturated columns. There is a basis B with respect to which $S_+^G S = S_+^N S$, where $N = \operatorname{Nak}_+^B(G)$.

Proof. Use a change of basis to assume that

$$G = \left\langle \sigma_i := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_i : i = 4, \cdots, n \right\rangle,$$

since our propositions on invariant rings are on blocks in such a form. Note that, with respect to the current basis, $\boldsymbol{N}_i^G$ has degree p^2 for $4 \leq i \leq n-1$.

We consider the narrow case $n \leq p+3$ first. With respect to the current basis, by proposition 2.4.3, we have

$$S_+^G S = Sx_1 + Sx_2 + Sx_3^p + \cdots + Sx_n^p.$$

We will find a change of basis of $\langle x_3, \cdots, x_n \rangle_{\mathbb{F}_p}$ that fixes x_3 and x_n such that, with respect to the new basis, G satisfies $[G, x_i] = \left\langle \binom{a_i}{b_i} \right\rangle_{\mathbb{F}_p}$ where $\binom{a_i}{b_i} = \binom{1}{i-3}$ for $i = 3, \cdots, n-1$ and $\binom{a_i}{b_i} = \binom{0}{1}$. The ideal $S_+^G S$ is stable under this change in the sense that the equality above remains true. And in this new basis, we will have $\boldsymbol{N}_i^G$ of degree p for $i = 3, \cdots, n$. Since $[G, V^*] = \langle x_1, x_2 \rangle_k$ is fixed by G, so that G is nice, by lemmas 1.2.5, 1.2.6 and corollary 3.2.2, we will have

$$S_+^N S = Sx_1 + Sx_2 + Sx_3^p + \cdots + Sx_n^p = S_+^G S.$$

The arguments for finding the change of basis will be the same as those in the proof of lemma 2.3.11. Let $4 \leq i \leq n-1$ be the left-most column such that $[G, x_i] \neq \left\langle \binom{a_i}{b_i} \right\rangle_{\mathbb{F}_p}$. If there are none, then we have the necessary basis. Form a $2(n-3) \times (n-2)$ matrix by aligning the columns of $\sigma_4, \cdots, \sigma_n$ as in the right of expression 2.1 with $m_0 = 2$. Let u_j denote column $j-2$ of this big matrix for $j = 3, \cdots, n$, and define for $j = 4, \cdots, n$

$$u_j' = \left(\underbrace{0, 0, \ \cdots, \ 0, 0}_{2 \times (j-4) \text{ zeroes}}, \ a_j, b_j, \ \underbrace{0, 0, \ \cdots, \ 0, 0}_{2 \times (n-j) \text{ zeroes}} \right)^T.$$

The set $\{u_3, \cdots, \widehat{u_i}, \cdots, u_n, \ u_4', \cdots, u_n'\}$ forms a basis of a vector space $\mathbb{F}_p^{2(n-3)}$. Using this basis, we can find basis change replacing x_i by some $\mathbb{F}_p$-linear combination of $x_3, \cdots, x_n$ such that u_i becomes an $\mathbb{F}_p$-linear combination of $u'_4, \cdots, u'_n$. This means the left-most column j with $\dim_{\mathbb{F}_p}[G, x_j] \neq \left\langle \binom{a_j}{b_j} \right\rangle_{\mathbb{F}_p}$ is now either $j \geq i+1$ or there is no such column. This argument can be repeated until $\dim_{\mathbb{F}_p}[G, x_j] = \left\langle \binom{a_j}{b_j} \right\rangle_{\mathbb{F}_p}$ for $j = 3, \cdots, n$, as required.

It remains to consider the wide case where $|G| \geq p^{p+1}$. By proposition 2.5.1,

$$S_+^G S = Sx_1 + Sx_2 + Sx_3^p + \sum_{i=4}^{n-p} Sx_i^{p^2} + \sum_{i=n-(p-1)}^{n-1} Sy_i^p + Sx_n^p,$$

where $y_i = x_i + \sum_{j \in L_i} x_j$ with $L_i = \{4 \leq j \leq n-(p-2) : p-1 \text{ divides } i-j\}$. Restrict our attention to the subspace $\langle x_1, x_2,\ x_{n-p}, \cdots, x_n \rangle_{\mathbb{F}_p}$. The action of G on this subspace is the same as the subgroup $\langle \sigma_{n-p}, \cdots, \sigma_n \rangle_{\mathbb{F}_p}$, in which σ_{n-p} acts as a reflection $\left[\binom{0}{1}_{n-p}\right]$ and the subgroup $G' := \left\langle \sigma_{n-(p-1)}, \cdots, \sigma_n \right\rangle_{\mathbb{F}_p}$ is a narrow block. We can apply a change of basis as above, so that $[G', x_j] = \left\langle \binom{a_j}{b_j} \right\rangle_{\mathbb{F}_p}$ for $j = n-p, \cdots, n$. Since the change of basis replaced $x_{n-(p-1)}, \cdots, x_{n-1}$, it has other side effects. Firstly, σ_{n-p} now takes the form $\left[\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & * & \cdots & * \end{pmatrix}_{n-1}\right]$, in which $\binom{1}{0}$ is in column $n-(p+1)$. And secondly, for each $i = n-(p-1), \cdots, n-1$, the x_i term in the sum y_i is affected. Explicitly, the sum y_i becomes $x'_i + \sum_{j \in L_i} x_j$, where $x'_i := \sum_{j=n-(p-1)}^{n-1} \lambda_{i,j} x_j$ for some $\lambda_{i,j} \in \mathbb{F}_p$, such that $\left\{x'_{n-(p-1)}, \cdots, x'_{n-1}\right\}$ remains an $\mathbb{F}_p$-linearly independent set.

We proceed from here, by downwards induction on $i = n-(p-1), \cdots, 4$ that σ_i is of the form $\left[\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & * & \cdots & * \end{pmatrix}_{n-1}\right]$, in which $\binom{1}{0}$ is in column $i-1$, and

$$[\langle \sigma_{i+1}, \cdots, \sigma_n \rangle, x_j] = \left\langle \begin{pmatrix} a_i \\ b_i \end{pmatrix} \right\rangle_{\mathbb{F}_p}, \text{ for } j = n-(p-1), \cdots, n.$$

Base case is $j = n-(p-1)$ as constructed above. For the induction step, suppose the hypothesis is true for some j. Note that $a_j = 1$ and $b_j \neq 0$. So we can apply a change of basis replacing each x_j by $x_j + e_j x_{i-1}$ for some e_j such that $[\sigma_i, x_j] \in \left\langle \binom{a_j}{b_j} \right\rangle$, for $j = n-(p-1), \cdots, n-1$. If $i \geq 5$, the basis change also changes σ_{i-1} to $\left[\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & * & \cdots & * \end{pmatrix}_{n-1}\right]$, in which $\binom{1}{0}$ is in column $i-2$. This would complete the induction step. We repeat until $i = 4$, at which point we simply have $[G, x_j] \in \left\langle \binom{a_j}{b_j} \right\rangle$, for the same range of j. Because the changes of basis used in the induction replaced x_i for $i = n-(p-1), \cdots, n-1$, we now have y_i taking the form $\sum_{j=3}^{n-1} \lambda_{i,j} x_j$ for some more $\lambda_{i,j} \in \mathbb{F}_p$.

We want $\lambda_{i,j} = 0$ for $4 \leq j \leq n-p$. By viewing $\lambda_{i,j}$ as a $(p-1) \times (n-3)$ matrix, of rank $p-1$ because $\left\{x_j'\right\}_{j=n-(p-1)}^{n-1}$ is linearly independent, we can find a change of basis replacing $x_4, \cdots, x_{n-p}$ to get our zero entires. Using the same linear independence, with respect to the current basis,

$$Sx_3^p + \sum_{i=n-(p-1)}^{n-1} Sy_i^p = Sx_3^p + \sum_{i=n-(p-1)}^{n-1} Sx_i^p.$$

With this, we can write, for some $\mu_{i,j} \in \mathbb{F}_p$ from the change of basis,

$$\begin{aligned} S_+^G S &= Sx_1 + Sx_2 + Sx_3^p \\ &\quad + \sum_{i=4}^{n-p} S\left(x_i + \mu_{i,n-(p-1)} x_{n-(p-1)} + \cdots + \mu_{i,n-1} x_{n-1}\right)^{p^2} + \sum_{i=n-(p-1)}^{n} Sx_i^p \\ &= Sx_1 + Sx_2 + Sx_3^p + \sum_{i=4}^{n-p} Sx_i^{p^2} + \sum_{i=n-(p-1)}^{n} Sx_i^p. \end{aligned}$$

And since this last change of basis did not change x_j for $j = n-(p-1), \cdots, n$, we still have the property that $[G, x_j] \in \left\langle \binom{a_j}{b_j} \right\rangle$ for the same range of j. As in the narrow case, we can deduce from this that $S_+^G S = S_+^N S$. $\square$

And now, we prove something similar for the remaining two-row groups.

Theorem 3.3.2. Let V^* be a representation of dimension n of an abelian two-row unipotent group G over an odd prime field $k = \mathbb{F}_p$. Write $N = \mathrm{Nak}_+^B(G)$. Then $S_+^G S \geq S_+^N S$ with respect to all choices of basis B.

The inclusion $S_+^G S = S_+^N S$ with respect to some choice of basis of V^* if and only if either $\dim_{\mathbb{F}_p}[G, V^*] = 1$ or $|G| = p^{n-2}$ are false.

Regardless of possible equality, there is a basis with repsect to which $S_+^G S$ is generated by powers of $x_1, \cdots, x_n$, whence the Macaulay dual for $S_+^G S$ is an inverse monomial in that basis,

Proof. We check the invariant rings of groups listed in theorem 2.6.5. If G is one-row, then it is congruent to a Nakajima group. This case is clear.

Suppose G contains the symmetric square representation, as given in lemma 2.6.2. Its invariant ring is, $S^G = k\left[\boldsymbol{N}_1, \cdots, \boldsymbol{N}_n, f\right]$ by proposition 2.6.3, where

$$f = x_2^2 - x_1x_3 \quad \text{or} \quad 2x_1x_3^p - 2x_1^px_3 + x_1^px_2 - x_2^{p+1}$$

depending on whether $|G| = p^{n-2}$ or p^{n-1} respectively. Since G acts as a one-row group on $\langle x_1, \cdots, \widehat{x_3}, \cdots, x_n\rangle_k$, it is clear that $\boldsymbol{N}_i^N = \boldsymbol{N}_i^G$ for $i \neq 3$. When $i = 3$, since N contains the transvection defined by $x_2 \mapsto x_2 + 2x_1$ and one by $x_3 \mapsto x_3 + x_2 + x_1$, we know that the degree of $\boldsymbol{N}_3^N$ is p^2 with

$$\boldsymbol{N}_3^N = \prod_{\lambda,\mu\in k} \left(x_3 + \lambda x_1 + \mu x_2\right)$$
$$\text{and } S_+^N S = Sx_1 + Sx_2^p + Sx_3^{p^2} + \sum_{4\leq i\leq n} Sx_i^p.$$

If $|G| = p^{n-1}$, then G contains $\left[\binom{1}{0}_3\right]$ as well giving $\boldsymbol{N}_i^G = \boldsymbol{N}_i^N$. In this case, it is clear that $f \in S_+^N S$, and so $S_+^G S = S_+^N S$.

Suppose $|G| = p^{n-2}$ instead. In this case, we have, using 1.0.9 for the norm,

$$\boldsymbol{N}_3^G = \prod_{c\in\mathbb{F}_p} \left(x_3 + 2cx_2 + c^2x_1\right)$$
$$f = x_2^2 - x_1x_3.$$

This gives the following coset equivalences

$$f + Sx_1 = -x_2^2 + Sx_1$$
$$\boldsymbol{N}_3^G + Sx_1 = \prod_{c\in\mathbb{F}_p} \left(x_3 + 2cx_2\right) + Sx_1$$
$$\boldsymbol{N}_3^G + Sx_1 + Sx_2^2 = x_3^p + Sx_1 + Sx_2^2.$$

With this, we have

$$\begin{aligned} S_+^G S &= S_+^N S + Sx_2^2 + Sx_3^{p^2} \\ &= Sx_1 + Sx_2^2 + Sx_3^p + \sum_{4 \le i \le n} Sx_i^p, \end{aligned}$$

generated by powers of $x_1, \cdots, x_n$. The homogeneous component $\left(S_+^G S\right)_2$ of degree 2 has dimension $n+1$ over $\mathbb{F}_p$. On the other hand, since $S_+^N S$ is an ideal generated by norms of degrees 1, p and p^2, with p odd and $(V^*)^G = \langle x_1 \rangle_k$, the degree 2 component of the ideal $S_+^N S$ can only have dimension n over k, with respect to all basis. However, the dimension of homogeneous components of $S_+^G S$ is stable under all changes of basis, so $S_+^G S$ cannot be equal to $S_+^N S$ with respect to any basis of V^*.

The remaining cases have $\dim_{\mathbb{F}_p} [G, V^*] = 2$ and $[G, V^*] = (V^*)^G$. By lemmas 1.2.5 and 1.2.6, we have $\boldsymbol{N}_i^G = \boldsymbol{N}_i^N$ for all i. If G is totally one-extended or is generated by blocks with saturated columns, by propositions 2.2.5 and 2.3.26, we have $S^G = S^N [f_3, \cdots, f_m]$ for some $f_i \in S\boldsymbol{N}_1 + S\boldsymbol{N}_2$. Equality of Hilbert ideals is clear here.

If G is a block with unsaturated columns, then the Hilbert ideals are also equal by lemma 3.3.1. And it is also clear that, if G is a $\boxtimes$-product of groups G' each satisfying $S_+^{G'} S = S_+^{\mathrm{Nak}_+^B(G')} S$, then $S_+^G S = S_+^N S$ as well. All cases have been checked, completing the proof. □

3.4 A type-two exceptional group

When G is abelian two-row over $\mathbb{F}_p$, in the proof of theorem 3.3.2, we used niceness defined in definition 1.2.4 which happened to be a sufficient, though not necessary, condition to have the equality $S_+^G S = S_+^{\mathrm{Nak}_B^+(G)} S$ with respect to some basis B. The exceptional groups of type two defined in 1.2.8 are also nice, and it is clear that, when $k = \mathbb{F}_p$, such groups satisfy $S_+^G S = S_+^{\mathrm{Nak}_B^+(G)} S$ in some basis B by checking the invariants in theorem 1.2.9.

The group G considered in this section is the only group in this thesis that is not over a prime field. We will show again that it satisfies $S^G_+S = S^{\mathrm{Nak}^+_B(G)}_+S$, by computing S^G_+S without finding S^G.

Example 3.4.1. Let $k = \mathbb{F}_q$ for some prime power $q = p^r$, with $r > 1$. Let $K \le \mathbb{F}_q$ be a non-trivial $\mathbb{F}_p$-vector subspace of some dimension $d \le r$. Let $n = 6$. Let G be an exceptional group of type two given by

$$G := \langle g_2 := w_{1,0,0},\ g_3 := w_{0,1,0},\ g_{1,\alpha} := w_{0,0,\alpha} : \alpha \in K \rangle\,.$$

Write, with respect to some basis of V^*,

$$g_2 := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix};\ g_3 := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix};$$
$$\text{and } g_{1,\alpha} := \begin{pmatrix} 1 & 0 & 0 & 0 & -\alpha & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & \alpha \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $S^G_+S = S^{\mathrm{Nak}^+_B(G)}_+S$. In particular, the Macaulay inverse for S^G_+S is an inverse monomial.

Proof. Let $N := \mathrm{Nak}^+_B(G) \ge G$ be its Nakajima overgroup. Since $[G, V^*] \subseteq \langle x_1, x_2, x_3 \rangle_k \le (V^*)^G$, the type-two group G is nice with respect to the current basis B by lemma 1.2.5, and $\boldsymbol{N}^G_i = \boldsymbol{N}^N_i$ by lemma 1.2.6. So we can write

$$S^N = k\,[\boldsymbol{N}_1, \boldsymbol{N}_2, \boldsymbol{N}_3, \boldsymbol{N}_4, \boldsymbol{N}_5, \boldsymbol{N}_6] \le S^G,$$

where $\boldsymbol{N}_1 = x_1$, $\boldsymbol{N}_2 = x_2$, $\boldsymbol{N}_3 = x_3$ and

$$\begin{aligned} \boldsymbol{N}_4 &:= \prod_{i,j=0}^{p-1} (x_4 + ix_1 + jx_3) \\ \boldsymbol{N}_5 &:= \prod_{j=0}^{p-1} \prod_{\alpha \in K} (x_5 + \alpha x_1 + jx_2) \\ \boldsymbol{N}_6 &:= \prod_{j=0}^{p-1} \prod_{\alpha \in K} (x_6 + ix_2 + \alpha x_3) \, . \end{aligned}$$

By corrollary 3.2.2, we have $S^N_+ S = Sx_1 + Sx_2 + Sx_3 + Sx_4^{p^2} + Sx_5^{p^{d+1}} + Sx_6^{p^{d+1}}$.

The inclusion $S^G_+ S \trianglerighteq S^N_+ S$ always holds for overgroups $N \geq G$. For the converse inclusion, consider a contradiction. Suppose there is a homogeneous polynomial $f \in S^G$ not in $S^N_+ S$. Since $S_i \subseteq S^N_+ S$ for all $i \geq p^2 + p^{d+1} + p^{d+1} - 3$, the polynomial f must have a monomial term of the form

$$m := x_4^{e_4} x_5^{e_5} x_6^{e_6},$$

for some $e_4 < p^2$, $e_5 < p^{d+1}$ and $e_6 < p^{d+1}$ not all zero. It will be shown that this is not possible.

Consider S^G as the intersection of $S^{\langle g_2 \rangle}$, $S^{\langle g_3 \rangle}$ and S^H where

$$H := \langle g_{1,\alpha} : \alpha \in K \rangle \leq G.$$

These invariant subrings, all of which must contain f, are each generated as k-algebrae by 7 polynomials

	$S^{\langle g_2 \rangle}$	$S^{\langle g_3 \rangle}$	S^H
Generators	x_1, x_2, x_3, x_5	x_1, x_2, x_3, x_6	x_1, x_2, x_3, x_4
	$f_{2,4} := x_4^p - x_1^{p-1} x_4$	$f_{3,4} := x_4^p - x_3^{p-1} x_4$	$f_{1,5} := \prod_{\alpha \in K} (x_5 + \alpha x_1)$
	$f_{2,6} := x_6^p - x_2^{p-1} x_6$	$f_{3,6} := x_5^p - x_2^{p-1} x_5$	$f_{1,6} := \prod_{\alpha \in K} (x_6 + \alpha x_3)$
	$f_{2,7} := x_1 x_6 - x_2 x_4$	$f_{3,7} := x_2 x_4 - x_3 x_5$	$f_{1,7} := x_1 x_6 + x_3 x_5$

Since f lies in $S^{\langle g_2 \rangle}$, it must be expressible as a polynomial in

$$x_1, x_2, x_3, x_5, f_{2,4}, f_{2,6}, f_{2,7}.$$

In particular, the monomial m must be a product of the monomial terms of these k-algebra generators, say

$$m = \left(x_4^p\right)^{a_4} x_5^{a_5} \left(x_6^p\right)^{a_6},$$

for some $a_4, a_5, a_6 \in \mathbb{Z}_{\geq 0}$ not all zero. This shows that $p \mid e_4$ and so $e_4 = pd_4$, for some $d_4 < p$. Similarly, applying this to S^H shows that $e_5 = p^d d_5$ and $e_6 = p^d d_6$, for some $d_5 < p$ and $d_6 < p$. In this proof, "a decomposition of a monomial m in an invariant ring R" will refer to an expression of the monomial as a product of the monomial terms of k-algebra generators of R as above. This decomposition will be used repeatedly. It provides information about the possible choices of polynomials in R that may have m as a monomial term.

Suppose $d_4 > 0$. The above decomposition of m in $S^{\langle g_2 \rangle}$ shows that m only appears from the expansion of $f_{2,4}^{d_4} x_5^{d_5 p^d} f_{2,6}^{d_6 p^{d-1}}$. That is, f must be of the form (or some k-scalar multiple of)

$$\begin{aligned}
f &= f_{2,4}^{d_4} x_5^{d_5 p^d} f_{2,6}^{d_6 p^{d-1}} + \cdots \\
&= \left(x_4^p - x_1^{p-1} x_4\right)^{d_4} x_5^{d_5 p^d} \left(x_6^p - x_1^{p-1} x_6\right)^{d_6} + \cdots \\
&= x_4^{d_4 p} x_5^{d_5 p^d} x_6^{d_6 p^d} - x_1^{p-1} x_4^{(d_4-1)p+1} x_5^{d_5 p^d} x_6^{d_6 p^d} + \cdots
\end{aligned}$$

The first monomial written out in the expansion is m. Let m_1 be the second (unsigned). It will be shown that m_1 also only appears from the expansion of $f_{2,4}^{d_4} x_5^{d_5 p^d} f_{2,6}^{d_6 p^{d-1}}$. Decompose m_1 in $S^{\langle g_2 \rangle}$ as

$$m_1 := x_1^{a_1} x_5^{a_5} \left(x_4^p\right)^{a_4} \left(x_1^{p-1} x_4\right)^{a_2} \left(x_6^p\right)^{a_6} \left(x_1 x_6\right)^{a_3},$$

for some other $a_1, \cdots, a_6 \in \mathbb{Z}_{\geq 0}$. These exponents must satisfy

$$\begin{aligned} a_1 + a_2\,(p-1) + a_3 &= p-1 \\ a_4 p + a_2 &= (d_4 - 1)\,p + 1 \\ a_5 &= d_5 p^d \\ a_6 p + a_3 &= d_6 p^d. \end{aligned}$$

Using the first equality, a_2 must be either 1 or 0, since a_1 and a_3 are non-negative. But $a_2 \equiv 1 \pmod{p}$ by the second equality, so $a_2 = 1$. It follows that $a_1 = a_3 = 0$, $a_4 = (d_4 - 1)$, $a_5 = d_5 p^d$ and $a_6 = d_6 p^d$. But this is just the second term in above expansion of f. In particular, if m appears as a monomial term in f, then so must m_1, since there are no other ways to negate m_1.

Now consider any possible choice of polynomials in $S^{\langle g_3 \rangle}$ that contain m_1. If such a choice exists, then the monomial m_1 can be decomposed in $S^{\langle g_3 \rangle}$ as

$$m_1 = x_1^{a_1} x_6^{a_6} \left(x_4^p\right)^{a_4} \left(x_5^p\right)^{a_5},$$

for some other $a_1, a_4, a_5, a_6 \in \mathbb{Z}_{\geq 0}$. The exponents must satisfy $a_4 p = (d_4 - 1)\,p-$ 1 which is not possible. This shows that m_1, and whence m, cannot be a monomial term of f if $d_4 > 0$.

Set $d_4 = 0$ so that $m = x_5^{d_5 p} x_6^{d_6 p}$. Suppose $d_5 > 0$. As before, the only way to obtain m as a monomial term in S^H is from the expansion

$$
\begin{aligned}
f &= \left[\prod_{\alpha\in K}(x_5+\alpha x_1)\right]^{d_5}\left[\prod_{\alpha\in K}(x_6+\alpha x_3)\right]^{d_6}+\cdots\\
&= \left[x_5^{p^d}+\cdots+\left(\prod_{\alpha\in K\setminus 0}\alpha\right)x_1^{p^d-1}x_5\right]^{d_5}\left[x_6^{p^d}+\cdots\right]^{d_6}+\cdots\\
&= \left[x_5^{d_5p^d}+\cdots+\left(\prod_{\alpha\in K\setminus 0}\alpha\right)^{d_5}x_1^{d_5\left(p^d-1\right)}x_5^{d_5}\right]\left[x_6^{d_6p^d}+\cdots\right]+\cdots\\
&= x_5^{d_5p^d}x_6^{d_6p^d}+\cdots+\left(\prod_{\alpha\in K\setminus 0}\alpha\right)^{d_5}x_1^{d_5\left(p^d-1\right)}x_5^{d_5}x_6^{d_6p^d}+\cdots
\end{aligned}
$$

Let $m_2 := x_1^{d_5\left(p^d-1\right)}x_5^{d_5}x_6^{d_6p^d}$ be the other monomial term written out in the expansion. Write, using theorem [3, 2.3] if necessary,

$$
f_{1,5}=\prod_{\alpha\in K}(x_5+\alpha x_1)=\sum_{i=0}^{d}\lambda_i x_5^{p^i}x_1^{p^d-p^i},
$$

for some $\lambda_i\in k$. Noting that $d_5<p$, all possible decomposition of m_2 in S^H are of the form

$$
m_2=x_1^{a_1}\left(x_5x_1^{p^d-1}\right)^{a_5}\left(x_6^{p^d}\right)^{a_6}(x_1x_6)^{a_2},
$$

for some other $a_i\in\mathbb{Z}_{\geq 0}$. These exponents satisfy

$$
\begin{aligned}
a_1+a_5\left(p^d-1\right)+a_2 &= d_5\left(p^d-1\right)\\
a_5 &= d_5\\
a_6p^d+a_2 &= d_6p^d.
\end{aligned}
$$

There is only one set of solutions. Namely, $a_5=d_5$, $a_1=a_2=0$ and $a_6=d_6$, which corresponds to the above expansion of f. As before, if m is a monomial term in f, then so is m_2.

Now consider any possible choice of polynomials in $S^{\langle g_3\rangle}$ that contains m_2 as a monomial term. If such a choice exists, then m_2 can be decomposed in $S^{\langle g_3\rangle}$ as

$$m_2 = x_1^{a_1} x_6^{a_6} \left(x_5^p\right)^{a_5},$$

for some other $a_i \in \mathbb{Z}_{\geq 0}$. The exponents satisfy $a_5 p = d_5 < p$, forcing $a_5 = 0$ and $d_5 = 0$, contradicting the assumption on d_5.

Lastly, set $d_5 = 0$ so that $m = x_6^{d_6 p}$. Suppose $d_6 > 0$. As before, the only way to obtain m as a monomial term in S^H is from the expansion

$$\begin{aligned} f &= \left[\prod_{\alpha \in K} (x_6 + \alpha x_3)\right]^{d_6} + \cdots \\ &= \left[x_6^{p^d} + \cdots + \left(\prod_{\alpha \in K\setminus 0} \alpha\right) x_3^{p^d - 1} x_6\right]^{d_6} + \cdots \\ &= x_6^{d_6 p^d} + \cdots + \left(\prod_{\alpha \in K\setminus 0} \alpha\right)^{d_6} x_3^{d_6\left(p^d-1\right)} x_6^{d_6} + \cdots \end{aligned}$$

Let $m_3 := x_3^{d_6\left(p^d-1\right)} x_6^{d_6}$ be the other monomial term written out in the expansion. Noting that $d_6 < p$, all possible decomposition of m_3 in S^H are of the from

$$m_3 = (x_3)^{a_3} \left(x_6 x_3^{p^d-1}\right)^{a_6},$$

for some other exponents $a_3, a_6 \in \mathbb{Z}_{\geq 0}$ satisfying

$$\begin{aligned} a_3 + a_6\left(p^d - 1\right) &= d_6\left(p^d - 1\right) \\ a_6 &= d_6. \end{aligned}$$

As before, there is a unique solution. It is $a_6 = d_6$ and $a_3 = 0$, corresponding to the above expansion of f. And so, if m is a monomial term in f, then so is m_3.

Now consider any possible choice of polynomials in $S^{\langle g_2\rangle}$ that contains m_3 as a monomial term. If such a choice exists, then m_3 can be decomposed in $S^{\langle g_2\rangle}$

as

$$m_3 = x_3^{a_3}\,(x_6^p)^{a_6}\,,$$

for some other $a_3, a_6 \in \mathbb{Z}_{\geq 0}$. The exponents satisfy $a_6 p = d_6 < p$, forcing $a_6 = 0$ and $d_6 = 0$, contradicting the assumption on d_6. This shows that $e_4 = e_5 = e_6 = 0$ if $f \in S^G$, as required, completing the proof. □

We collect the groups used in this chapter.

Corollary 3.4.2. Let G be a Nakajima group, a two-row abelian group over $\mathbb{F}_p$ or the exception group of type two over a finite field given in example 3.4.1. Then the Macaulay inverse for $S_+^G S$ is an inverse monomial with respect to some basis of V^*. □

Closing remarks

We finish this thesis by looking at some problems left open. As we have just seen, many unipotent pure bireflection groups G have Hilbert ideals $S_+^G S$ whose Macaulay inverses are inverse monomials with respect to some basis of V^*. Using the invariant ring of type one exceptional groups for $k = \mathbb{F}_p$ with odd p found in [8, 6.1.6], we can see that it holds for those groups as well. However, $S_+^G S = S_+^{\mathrm{Nak}_B^+(G)} S$ does not hold under any basis for that group. It would be interesting to see which of these properties hold for other pure bireflection groups listed in theorem 1.0.6.

Staying with the pure bireflection groups, the work in chapter 2 tells us that every abelian unipotent two-row group can be written as a ⊠-product of three components. Using this ⊠-product representation, propositions 2.4.3 and 2.5.1 on invariant rings of blocks, together with repeated applications of proposition 1.1.1 and theorem 1.1.2 is enough to find invariant rings of all abelian two-row groups, as long as appropriate reflections are chosen to form over-groups. The invariant rings found allow us to remove one entry from theorem 1.0.8 to get

Theorem 3.4.3. Suppose $k = \mathbb{F}_p$ with p odd. Let G be a (finite unipotent) pure bireflection p-group. If S^G is not a complete intersection, then G is one of the following: (1) a non-abelian two-row group; (2) a two-column group; or (3) an abelian hook group with $[G, [G, V^*]] \neq 0$.

Amongst this list, little is known about two-column groups.

And finally, using algorithm 3.1.2 on finding Macaulay duals for irreducible ideals, the classification of Macauly duals for complete intersection ideals can be changed into a problem of classifying homogeneous complete intersection ideals instead, up to a change of basis.

Symbols

$B = \{x_1, \cdots, x_n\}$ Dual basis in V^*. 1

$C_G(X) = \{\sigma \in G : [\sigma, X] = 0\}$ Centraliser of X in a group G. 19

E The maximal two-row group. 4

$F^{\langle i_1, i_2 \rangle}$ Two-row block of width $i_2 - i_1$. 36

$G \leq \mathrm{GL}(V)$ A finite subgroup. 1

$\gamma \in S^{-1}$ An inverse polynomial. 11

$G_i \leq G$ One-column subgroup at column i. 3

$\mathcal{I}$ The set of homogeneous S_+-primary irreducible ideals of S. 11

k A field, usually $\mathbb{F}_p$ for some prime p. 1

$\mathrm{LM}(f)$ Leading monomial of a polynomial $f \in S$. 6

$\mathcal{M}$ The set of non-trivial homogeneous cyclic S-submodules of S^{-1}. 11

n Dimension of V over k. 1

$\mathrm{Nak}_B^+(G)$ Nakajima overgroup of G with respect to B. 3

$\boldsymbol{N}_i^G = \prod_{g \in Gx_i} g$ The G-orbit product of x_i. 3

p Characteristic of k. 1

S^G The G-invariant ring. 1

$S_+^G S$ The Hilbert ideal of the ring extension $S \geq S^G$. 10

$S = \mathbf{Sym}(V^*) = k[V]$ Polynomial ring. 1

$S^{-1} = k\left[x_1^{-1}, \cdots, x_n^{-1}\right]$ The inverse polynomial ring. 11

$S[m] = k[x_1, \cdots, x_m]$ Polynomial subring. 7

$S_+ = Sx_1 + \cdots + Sx_n \lhd S$ The polynomial ideal. 11

$[\sigma, f] = (\sigma - 1)(f)$ Commutator. 3

$S_G = S/S_+^G S$ Coinvariant ring. 10

$T(\sigma)$ Tail matrix of a two-row element $\sigma \in F$. 15

V A finite-dimensional representation of G over k. 1

V^* Dual space of V over k. 1

$x^{\boldsymbol{e}}$ Monomial $x_1^{e_1} \cdots x_n^{e_n}$ where $\boldsymbol{e} = (e_1, \cdots, e_n)$. 11

x_i The dual of v_i in V^*. 1

References

[1] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997), pp. 235–265. ISSN: 0747-7171. URL: `http://dx.doi.org/10.1006/jsco.1996.0125`.

[2] H. E. A. Campbell and I. Hughes. "Rings of Invariants of Certain p-Groups over the Field $\mathbb{F}_p$". In: *Journal of Algebra* 211.2 (1999), pp. 549–561.

[3] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau. "Rings of Invariants for Modular Representations of Elementary Abelian p-groups". In: *Transformation Groups* 18.1 (2013), pp. 1–22.

[4] H. E. A. Campbell and D. L. Wehlau. *Modular Invariant Theory*. Encyclopaedia Of Mathematical Sciences. New York: Springer, 2011.

[5] H. Campbell and J. Chuai. "Invariant Fields and Localized Invariant Rings of p-groups". In: *The Quarterly Journal of Mathematics* 58.2 (2007), pp. 151–157.

[6] W. Dwyer and C. Wilkerson. "Poincaré duality and Steinberg's theoremon rings of coinvariants". In: *Proceedings of the American Mathematical Society* 138.10 (2010), pp. 3769–3775.

[7] T. Harima, A. Wachi, and J. Watanabe. "A characterization of the Macaulay dual generators for quadratic complete intersection". In: *arXiv preprint arXiv:1703.07199* (2017).

[8] K. Horan. "On the invariant theory of finite unipotent groups generated by bireflections". PhD thesis. University of Kent, 2017. URL: `https://kar.kent.ac.uk/65736/`.

[9] K. Horan and P. Fleischmann. "The finite unipotent groups consisting of bireflections". In: *Journal of Group Theory* 22.2 (2019), pp. 191–230.

[10] I. Hughes and N. Kechagias. "Rings of invariants of modular p-groups which are hypersurfaces". In: *Journal of Algebra* 291.1 (2005), pp. 72–89.

[11] R. Kane. "Poincaré duality and the ring of coinvariants". In: *Canad. Math. Bull* 37.1 (1994), pp. 82–88.

[12] D. M. Meyer and L. Smith. *Poincaré duality algebras, Macaulay's dual systems, and Steenrod operations*. Vol. 167. Cambridge University Press, 2005.

[13] H. Nakajima. "Regular rings of invariants of unipotent groups". In: *Journal of Algebra* 85.2 (1983), pp. 253–286.

[14] M. Sezer and W. Zhang. “Poincaré duality in modular coinvariant rings”. In: *Proceedings of the American Mathematical Society* 144.12 (2016), pp. 5113–5120.

[15] L. Smith. *Polynomial invariants of finite groups*. AK Peters/CRC Press, 1995.

[16] Y. Wu. “Invariants of Modular Two-Row Groups”. PhD thesis. Queen’s University, 2009. URL: `https://qspace.library.queensu.ca/handle/1974/5258`.