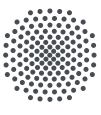
A sieve formula for chains of p-subgroups

Extending Wielandt's proof of Sylow-Frobenius to a congruence modulo $p^{\ell+1}$

Bachelor thesis

Elias Schwesig

July 2024



University of Stuttgart
Germany

Contents

Conventions

Let X, Y be sets. Let G be a group. Let R be a commutative ring.

- We write $[a, b] := \{z \in \mathbb{Z} : a \leqslant z \leqslant b\}$ for $a, b \in \mathbb{Z}$.
- Given $n \in \mathbb{Z}$, we write $\mathbb{Z}_{\geqslant n} := \{z \in \mathbb{Z} : z \geqslant n\}$.
- Given $x \in \mathbb{Z}$ and $T \subseteq [a, b]$ for some $a, b \in \mathbb{Z}$, we write $x - T := \{x - t : t \in T\}$. For example, we have $3 - \{2, 6\} = \{1, -3\}$ and $5 - \emptyset = \emptyset$.
- Given $a, b, x \in R$, we write $a \equiv_x b$ to indicate that $a - b \in xR$.
- Given $n \in \mathbb{Z}$, we write $\mathrm{v}_p(n) := \max\{k \in \mathbb{Z}_{\geqslant 0} : n \equiv_{p^k} 0\}$ if $n \neq 0$, and $\mathrm{v}_p(0) := \infty$.

  Let $z + \infty := \infty$ for $z \in \mathbb{Z}$ and $\infty + \infty := \infty$.

  Furthermore, we stipulate that $\infty \geqslant z$ for $z \in \mathbb{Z}$.
- We write $\mathfrak{P}(X) := \{Y : Y \subseteq X\}$ for the power set of X.
- We write $X \subseteq Y$ if X is a subset of Y.
- We write $X \sqcup Y := X \cup Y$ if the union is disjoint, i.e. $X \cap Y = \emptyset$. Furthermore, given a set U and a tuple $(A_i)_{i \in I}$ of subsets $A_i \subseteq U$ for $i \in I$ which are pairwise disjoint, then we write
$$\bigsqcup_{i \in I} A_i := \bigcup_{i \in I} A_i.$$
- Let $(A_i)_{i \in I}$ be a tuple of sets. Then we write
$$\coprod_{i \in I} A_i := \bigsqcup_{i \in I} \{(i, a) : a \in A_i\} = \{(i, a) : i \in I, a \in A_i\}.$$
- We write $H \leqslant G$ is H is a subgroup of G, and $H < G$ if $H \leqslant G$ and $H \neq G$.
- Let $M \subseteq G$. In this case, we write $M \not\leqslant G$ to indicate that M is a subset, but not a subgroup of G.
- Given $g, x \in G$, we write ${}^x g := xgx^{-1}$ and $g^x := x^{-1}gx$.

  Given $g \in G$ and $H \leqslant G$, we write ${}^g H := \{{}^g h : h \in H\}$ and $H^g := \{h^g : h \in H\}$.
- Let X be a G-set. Let $x \in X$. We write $\mathrm{Stab}(x) := \mathrm{Stab}_G(x) := \{g \in G : g \cdot x = x\}$ for the stabilizer of x in G.
- Let $n \in \mathbb{Z}_{\geqslant 1}$. In the symmetric group S_n, we write $\sigma \cdot \tau \in \mathrm{S}_n$ for the composite of $\sigma \in \mathrm{S}_n$ and $\tau \in \mathrm{S}_n$, where first σ and then τ is applied, e.g. $(1, 2) \cdot (2, 3) = (1, 3, 2)$ in S_3.

  We do this to follow the convention used in Magma [**2**].

1 Introduction

Let G be a finite group. Let p be a prime.

We write $|G| = p^t n$, where $t = \mathrm{v}_p(|G|) \in \mathbb{Z}_{\geqslant 0}$, $n \in \mathbb{Z}_{\geqslant 1}$ and $n \not\equiv_p 0$.

Let $s \in [0, t]$.

1.1 The main result

Let $k \geqslant 0$. Let $I = \{c_1, \ldots, c_k\} \subseteq [0, t]$, where $c_1 > \ldots > c_k$. We write

$$\mathrm{N}(s - I) := |\{(U_1, \ldots, U_k) : U_1 \leqslant U_2 \leqslant \ldots \leqslant U_k \leqslant G,\ |U_i| = p^{s-c_i} \text{ for } i \in [1, k]\}|.$$

That is, $\mathrm{N}(s - I)$ denotes the number of chains of p-subgroups

$$U_1 \leqslant U_2 \leqslant \ldots \leqslant U_k \leqslant G,$$

where U_i has order p^{s-c_i} for $i \in [1, k]$.

Then we obtain the following sieve formula for $\ell \in [0, s]$.

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s - I) \equiv_{p^{\ell+1}} 1.$$

Its name stems from the sieve formula from set theory, also known as inclusion-exclusion principle, because of formal similarities.

1.2 Counting orbit representatives

Let

$$\Omega := \{M \subseteq G : |M| = p^s\}.$$

Note that $|\Omega| = \binom{p^t n}{p^s}$.

Then Ω is a G-set via left multiplication, i.e.

$$g \cdot M := gM = \{gm : m \in M\}$$

for $g \in G$ and $M \in \Omega$.

We write

$$[M] := \{gM : g \in G\}$$

for the orbit of M under G, and

$$\overline{\Omega} := \{[M] : M \in \Omega\}$$

for the set of all orbits.

Let $M \in \Omega$. By the orbit-stabilizer theorem, we have $|[M]| = |G|/|\operatorname{Stab}(M)|$ and so

$$|[M]| \cdot |\operatorname{Stab}(M)| = p^t n.$$

Furthermore, M is a $\operatorname{Stab}(M)$-set via left multiplication, where the orbits are right $\operatorname{Stab}(M)$-cosets. So we have an $\ell \in [0, s]$ such that

$$|\operatorname{Stab}(M)| = p^{s-\ell},$$

i.e.

$$|[M]| = p^{t-s+\ell} n.$$

Given $\ell \in [0, s]$, we write

$$\Omega^\ell := \{M \in \Omega : |[M]| = p^{t-s+\ell} n\} = \{M \in \Omega : |\operatorname{Stab}(M)| = p^{s-\ell}\} \subseteq \Omega$$

and

$$\overline{\Omega}^\ell := \{[M] : M \in \Omega^\ell\}.$$

Then

$$\overline{\Omega} = \bigsqcup_{\ell \in [0,s]} \overline{\Omega}^\ell.$$

Given $\ell \in [0, s]$, we write

$$a_\ell := |\overline{\Omega}^\ell| \in \mathbb{Z}_{\geqslant 0}.$$

Counting orbits while factoring in their sizes yields

$$\binom{p^t n}{p^s} = |\Omega| = \sum_{\ell \in [0,s]} |\overline{\Omega}^\ell| = p^{t-s} n \sum_{\ell \in [0,s]} a_\ell p^\ell.$$

Write $q := \frac{1}{p^{t-s} n} \binom{p^t n}{p^s} \in \mathbb{Z}_{\geqslant 1}$. Then

$$q = \sum_{\ell \in [0,s]} a_\ell p^\ell.$$

In particular, we have

$$q \equiv_{p^{\ell+1}} \sum_{k \in [0,\ell]} a_k p^k$$

for $\ell \in [0, s]$.

1.3 Wielandt's proof of Sylow-Frobenius

Wielandt showed that for $M \in \Omega^0$, the orbit $[M]$ contains exactly one subgroup of G of order p^s, while for $\ell \in [1, s]$ and $M' \in \Omega^\ell$, the orbit $[M']$ does not contain a subgroup.

Consequently,

$$a_0 = |\{U \leqslant G : |U| = p^s\}| = \mathrm{N}(s - \{0\}).$$

This means that

$$q \equiv_p a_0 = \mathrm{N}(s - \{0\}).$$

Here, Graham Higman simplified Wielandt's original proof:[1] Using this congruence in case $G = \mathrm{C}_{p^t n}$ gives $q \equiv_p 1$. Altogether,

$$\mathrm{N}(s - \{0\}) \equiv_p q \equiv_p 1.$$

This is the theorem of Sylow-Frobenius, shown by Sylow **[8,** Th. II] in case $s = t$, and proven by Frobenius **[3,** §4, I.] in case $s \in [0, t]$.

Wielandt's proof of the Theorem of Sylow-Frobenius has entered the standard textbooks on group theory, e.g. **[4,** §7, Thm. 7.2], **[5,** §1, Thm. 1.7], and **[6,** §47, Thm. 27].

1.4 Extending Wielandt's proof

We first shall give a group theoretic meaning not only to a_0, but also to a_ℓ for $\ell \in [0, s]$.

We write

$$\mathrm{b}(\ell) := \binom{p^{t-s+\ell} n - 1}{p^\ell - 1} \in \mathbb{Z}_{\geqslant 0}$$

for $\ell \in [0, s]$.

By a noetherian induction, one may show that

$$a_\ell = \tfrac{1}{p^\ell} \sum_{\substack{I \subseteq [0,\ell] \\ \ell \in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s - I).$$

[1] According to Derek Holt, colleagues of Graham Higman attributed this simplification to him. Cf. also *Mathematics Stack Exchange*, question no. 479839.

Then

$$\begin{aligned} q &\equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} a_k p^k \\ &= \sum_{k\in[0,\ell]} \sum_{\substack{I\subseteq[0,k]\\ k\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\,\mathrm{N}(s-I) \\ &= \sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\,\mathrm{N}(s-I) \\ &= \sum_{k\in[0,\ell]} \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\,\mathrm{N}(s-I) \\ &= \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}\,\mathrm{N}(s-I). \end{aligned}$$

Applying Higman's idea to compare with the case of the cyclic group and to form a difference, we obtain

$$0 \equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}(\mathrm{N}(s-I)-1).$$

Using the congruence

$$\mathrm{b}(k) \equiv_{p^k} \mathrm{b}(k-1)$$

for $k \in [0,\ell]$ and by another noetherian induction, we can remove the factors $\mathrm{b}(k)$ for $k \in [0,\ell]$ to get

$$0 \equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}(\mathrm{N}(s-I)-1)$$

and so the desired sieve formula

$$\sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} (-1)^{|I|+1}\,\mathrm{N}(s-I) \equiv_{p^{\ell+1}} 1.$$

For sake of illustration of the general method, we have also included direct proofs of the sieve formula in the cases $\ell = 1$ and $\ell = 2$, with which we have started.

1.5 Concluding remarks

We give examples that show in the cases $\ell = 1$ and $\ell = 2$ that the exponent cannot be improved in the modulus $p^{\ell+1}$ of the sieve formula.

We have undertaken an attempt to find a shortcut to prove the sieve formula directly from the Theorem of Sylow-Frobenius; cf. Remark 50. Examples show that this seems to be impossible.

Open questions concern a variant of the sieve formula, in which an interval is replaced by an arbitrary subset, and the particular case of G being a p-group.

1.6 Acknowledgements

I would like to thank Matthias Künzer for his support, his competent advice and for his time, both in the preparation of my bachelor's thesis and also throughout my studies.

2 Preliminaries

2.1 Disjoint subsets

Remark 1 *Let X, I be sets. Let $X_i \subseteq X$ be non-empty subsets for $i \in I$.*

Suppose that $X = \bigsqcup_{i\in I} X_i$, i.e. $X = \bigcup_{i\in I} X_i$ and $X_i \cap X_j = \emptyset$ for $i, j \in I$ with $i \neq j$.

Let $J, \hat{J} \subseteq I$ with $\bigsqcup_{j\in J} X_j = \bigsqcup_{j\in \hat{J}} X_j$. Then we have $J = \hat{J}$.

Proof. We show $J \overset{!}{\subseteq} \hat{J}$. The other inclusion follows vice versa.

Suppose given $j \in J$. Choose $x \in X_j$, which is possible since $X_j \neq \emptyset$.

Since $X_j \subseteq \bigsqcup_{j\in J} X_j = \bigsqcup_{j\in \hat{J}} X_j$, we have $x \in \bigsqcup_{j\in \hat{J}} X_j$. So we may choose $k \in \hat{J}$ such that $x \in X_k$.

So $x \in X_j \cap X_k$. This yields $X_j \cap X_k \neq \emptyset$. Hence $j = k \in \hat{J}$. □

2.2 Congruences

Definition 2 Let p be a prime. Let

$$\mathbb{Z}_{(p)} := \{\tfrac{a}{b} : a \in \mathbb{Z},\ b \in \mathbb{Z} \setminus p\mathbb{Z}\} \subseteq \mathbb{Q}.$$

Note that $\mathbb{Z} \subseteq \mathbb{Z}_{(p)}$.

Remark 3 *Suppose given a prime p and $k \in \mathbb{Z}_{\geqslant 0}$.*

(1) *Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus p\mathbb{Z}$. Then we have $\frac{a}{b} \in p^k\mathbb{Z}_{(p)}$ if and only if $a \in p^k\mathbb{Z}$.*

(2) *The following ring morphism is an isomorphism.*

$$\begin{aligned} \mathbb{Z}/p^k\mathbb{Z} &\to \mathbb{Z}_{(p)}/p^k\mathbb{Z}_{(p)}, \\ z + p^k\mathbb{Z} &\mapsto \tfrac{z}{1} + p^k\mathbb{Z}_{(p)} \end{aligned}$$

In particular, if $a, b \in \mathbb{Z}$ are given such that $a \equiv_{p^k} b$ holds in $\mathbb{Z}_{(p)}$, then $a \equiv_{p^k} b$ holds in $\mathbb{Z}$.

Proof. *Ad* (1). Suppose that $a \in p^k\mathbb{Z}$. We may choose $z \in \mathbb{Z}$ with $a = p^k z$. Then

$$\tfrac{a}{b} = \tfrac{p^k z}{b} = p^k \tfrac{z}{b} \in p^k \mathbb{Z}_{(p)}.$$

Conversely, suppose that $\frac{a}{b} \in p^k\mathbb{Z}_{(p)}$. We may choose $c \in \mathbb{Z}$ and $d \in \mathbb{Z} \setminus p\mathbb{Z}$ with $\frac{a}{b} = p^k \frac{c}{d}$. It follows that $ad = p^k cb$ and so

$$\mathrm{v}_p(a) = \mathrm{v}_p(a) + \mathrm{v}_p(d) = \mathrm{v}_p(ad) = \mathrm{v}_p(p^k cb) \geqslant k.$$

Therefore, $a \in p^k\mathbb{Z}$.

Ad (2). *Injective.* Suppose given $z \in \mathbb{Z}$ with $z + p^k\mathbb{Z}_{(p)} = 0$. Then $\frac{z}{1} \in p^k\mathbb{Z}_{(p)}$ and, by (1), $z \in p^k\mathbb{Z}$, i.e. $z + p^k\mathbb{Z} = 0$.

Surjective. Suppose given $\frac{a}{b} \in p^k\mathbb{Z}_{(p)}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{Z} \setminus p\mathbb{Z}$. Then $\gcd(b, p^k) = 1$. Bezout's Lemma gives $s, t \in \mathbb{Z}$ such that $sb + tp^k = 1$. Then $sb - 1 = tp^k$. Hence

$$a(sb - 1) = atp^k \in p^k\mathbb{Z}.$$

By (1), this is equivalent to $\frac{a(sb-1)}{b} = as - \frac{a}{b} \in p^k\mathbb{Z}_{(p)}$. Hence

$$as + p^k\mathbb{Z} \;\mapsto\; as + p^k\mathbb{Z}_{(p)} = \tfrac{a}{b} + p^k\mathbb{Z}_{(p)}. \qquad \square$$

2.3 Noetherian induction

Let $(X, \leqslant)$ be a partially ordered set.

Definition 4

(1) Let $T \subseteq X$. We say that $t \in T$ is *minimal* in T if $\{s \in T : s < t\} = \emptyset$.

(2) We say that $(X, \leqslant)$ is *noetherian* if every non-empty subset $T \subseteq X$ has a minimal element in T.

Lemma 5 *The following assertions are equivalent.*

(1) *The partially ordered set $(X, \leqslant)$ is* not *noetherian.*

(2) *There exist $x_n \in X$ for $n \in \mathbb{Z}_{\geqslant 1}$ such that $x_i > x_{i+1}$ for $i \in \mathbb{Z}_{\geqslant 1}$.*

Proof. *Ad* (1) $\Rightarrow$ (2). Since $(X, \leqslant)$ is not noetherian, we may choose a non-empty subset $T \subseteq X$ with no minimal element.

Choose $x_1 \in T$. Then x_1 is not minimal. Hence, we may choose $x_2 \in T$ such that $x_1 > x_2$.

Then x_2 is not minimal. Hence, we may choose $x_3 \in T$ such that $x_2 > x_3$.

Repeating this, we get a infinite decreasing sequence

$$x_1 > x_2 > x_3 > \dots$$

as desired.

Ad (2) $\Rightarrow$ (1). Choose $x_n \in X$ for $n \in \mathbb{Z}_{\geqslant 1}$ such that $x_i > x_{i+1}$ for $i \in \mathbb{Z}_{\geqslant 1}$. Then the non-empty subset $T := \{x_n : n \in \mathbb{Z}_{\geqslant 1}\} \subseteq X$ has no minimal element in T, hence $(X, \leqslant)$ is not noetherian. □

Corollary 6 *If X is a finite set, then $(X, \leqslant)$ is noetherian.*

Proof. Suppose that $(X, \leqslant)$ is not noetherian. Then we may choose $x_n \in X$ for $n \in \mathbb{Z}_{\geqslant 1}$ such that

$$x_1 > x_2 > x_3 > \dots,$$

cf. Lemma 5.(1 $\Rightarrow$ 2). This implies that $|\{x_n : n \in \mathbb{Z}_{\geqslant 1}\}| = \infty$ and therefore $|X| = \infty$. □

Lemma 7 (Noetherian induction) *Suppose that $(X, \leqslant)$ is noetherian.*

Suppose given a statement $P(x)$ for $x \in X$.

Suppose that the following property holds.

(N) *If $x \in X$ is given such that $P(x')$ holds for $x' \in X$ with $x' < x$, then $P(x)$ holds.*

Then $P(x)$ holds for $x \in X$.

Proof. Assume that $Z := \{x \in X : \neg P(x)\} \neq \emptyset$. Hence, Z has a minimal element $z \in Z$. Then $z \in X$, and $P(x')$ holds for $x' \in X$ with $x' < z$ since z is minimal in Z. By (N), $P(z)$ holds, which is a *contradiction* to $z \in Z$. □

Throughout the text, we keep the following data:

Let G be a finite group. Let p be a prime. We write $\lvert G\rvert = p^t n$, where $t = \mathrm{v}_p(\lvert G\rvert) \in \mathbb{Z}_{\geqslant 0}$, $n \in \mathbb{Z}_{\geqslant 1}$ and $n \not\equiv_p 0$.

3 A decomposition into orbits

Suppose given $s \in [0, t]$.

3.1 Subsets, p-subgroups and chains of p-subgroups

Definition 8

(1) We write

$$\Omega := \Omega^{[s]} := \{M \subseteq G : |M| = p^s\} \subseteq \mathfrak{P}(G).$$

We remark that $|\Omega^{[s]}| = \binom{p^t n}{p^s}$.

(2) Let $\ell \in [0, t]$. Let

$$\mathrm{Sub}(\ell) := \{U \leqslant G : |U| = p^\ell\}.$$

Let $I = \{c_1, \ldots, c_k\} \subseteq [0, t]$ where $c_1 < \ldots < c_k$. Let

$$\mathrm{Sub}(c_1, \ldots, c_k) := \{(U_1, \ldots, U_k) \in \mathrm{Sub}(c_1) \times \ldots \times \mathrm{Sub}(c_k) : U_1 \leqslant \ldots \leqslant U_k\}.$$

We also write

$$\mathrm{Sub}(I) := \mathrm{Sub}(c_1, \ldots, c_k).$$

Let

$$\mathrm{N}(c_1, \ldots, c_k) := \mathrm{N}_{G,p}(c_1, \ldots, c_k) := |\,\mathrm{Sub}(c_1, \ldots, c_k)|.$$

We also write

$$\mathrm{N}(I) := \mathrm{N}_{G,p}(I) := \mathrm{N}(c_1, \ldots, c_k).$$

Let $s - I := \{s - i : i \in I\}$. Then

$$\mathrm{Sub}(s - I) = \mathrm{Sub}(s - c_k, \ldots, s - c_1),$$

and

$$\mathrm{N}(s - I) = \mathrm{N}(s - c_k, \ldots, s - c_1).$$

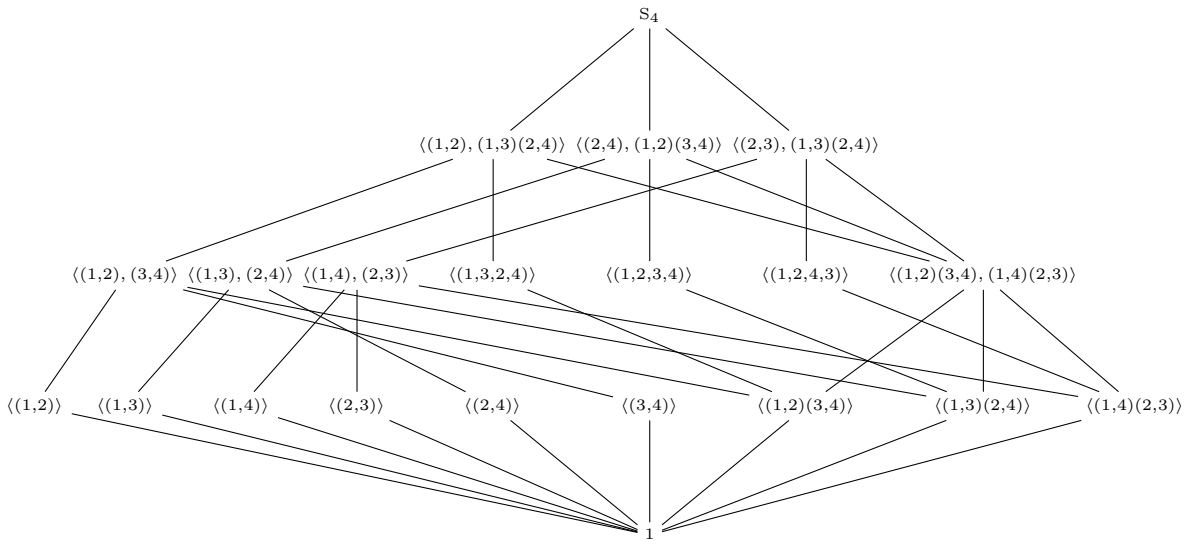
Note that $\mathrm{Sub}(\emptyset) = \{()\}$ and so $\mathrm{N}(\emptyset) = 1$.

(3) Let $I = \{c_1, \ldots, c_k\} \subseteq [0, t]$ where $c_1 < \ldots < c_k$. Let $V \leqslant G$. Let

$$\mathrm{Sub}(I, V) := \{(U_1, \ldots, U_k, V) : (U_1, \ldots, U_k) \in \mathrm{Sub}(c_1, \ldots, c_k),\ U_k \leqslant V\}.$$

Example 9 Let $G = \mathrm{S}_4$ and $p = 2$.

We have the following partially ordered set of 2-subgroups in S_4.



(1) We have

$$\begin{aligned}\mathrm{Sub}(3) &= \{U \leqslant \mathrm{S}_4 : |U| = 2^3\} \\ &= \{\langle (1,2), (1,3)(2,4)\rangle, \langle (2,4), (1,2)(3,4)\rangle, \langle (2,3), (1,3)(2,4)\rangle\}.\end{aligned}$$

(2) We have $\mathrm{N}(3) = \mathrm{N}(\{3\}) = |\,\mathrm{Sub}(3)| = 3$.

(3) We see that

$$1 < \langle (1,2)\rangle < \langle (1,2), (3,4)\rangle$$

is a chain of 2-subgroups of order 2^0, 2^1, 2^2 in S_4. Hence

$$(1, \langle (1,2)\rangle, \langle (1,2), (3,4)\rangle) \in \mathrm{Sub}(0,1,2) = \mathrm{Sub}([0,2]).$$

(4) We have $\mathrm{N}(0,1,2) = |\,\mathrm{Sub}(0,1,2)| = 15$.

Remark 10 *Let $I \subseteq [1,t]$. We have*

$$\mathrm{N}(I) = \mathrm{N}(\{0\} \sqcup I).$$

Proof. Write $I = \{c_1, \ldots, c_k\}$ with $c_1 < \ldots < c_k$.

Note that $\mathrm{Sub}(0) = \{U \leqslant G : |U| = 1\} = \{1\}$. Therefore

$$\begin{aligned}&\mathrm{N}(0, c_1, \ldots, c_k) \\ &= |\,\mathrm{Sub}(0, c_1, \ldots, c_k)| \\ &= |\{(U_0, U_1, \ldots, U_k) \in \mathrm{Sub}(0) \times \mathrm{Sub}(c_1) \times \ldots \times \mathrm{Sub}(c_k) : U_0 \leqslant U_1 \leqslant \ldots \leqslant U_k\}| \\ &= |\{(1, U_1, \ldots, U_k) \in \{1\} \times \mathrm{Sub}(c_1) \times \ldots \times \mathrm{Sub}(c_k) : 1 \leqslant U_1 \leqslant \ldots \leqslant U_k\}| \\ &= |\{(U_1, \ldots, U_k) \in \mathrm{Sub}(c_1) \times \ldots \times \mathrm{Sub}(c_k) : U_1 \leqslant \ldots \leqslant U_k\}| \\ &= \mathrm{N}(c_1, \ldots, c_k).\end{aligned}$$

□

Example 11 We have $\mathrm{N}_{\mathrm{S}_4,2}(1) = \mathrm{N}_{\mathrm{S}_4,2}(0,1) = 9$ and $\mathrm{N}_{\mathrm{S}_4,2}(1,2) = \mathrm{N}_{\mathrm{S}_4,2}(0,1,2) = 15$; cf. Example 9 and Remark 10.

3.2 Orbit lengths

Definition 12 Let G act on Ω via multiplication from the left, that is

$$g \cdot M := gM = \{gm : m \in M\}$$

for $g \in G$ and $M \in \Omega$.

(1) Suppose given $M \in \Omega$. We write

$$[M] := \{gM : g \in G\}$$

for the orbit of M under G. Furthermore, we write

$$\overline{\Omega} := \overline{\Omega}^{[s]} := \{[M] : M \in \Omega\}$$

for the set of G-orbits.

(2) Let

$$\begin{aligned} \rho : \quad & \Omega \to \overline{\Omega} \\ & M \mapsto [M]. \end{aligned}$$

Lemma 13 *Suppose given $M \in \Omega$. Let $U := \mathrm{Stab}(M) = \{g \in G : gM = M\} \leqslant G$.*

(1) *We have $|[M]| \cdot |U| = p^t n$.*

(2) *There exists a unique $\ell \in [0,s]$ such that $|U| = p^{s-\ell}$.*

There exist $m_1, \ldots, m_{p^\ell} \in M$ such that

$$M = \bigsqcup_{i \in [1,p^\ell]} Um_i.$$

We have $|[M]| = p^{t-s+\ell} n$.

Proof. Ad (1). This ensues from the orbit-stabilizer theorem since $|G| = p^t n$.

Ad (2). Let U act on M via multiplication from the left. Given $m \in M$, the orbit Um is a right coset of U, which implies $|Um| = |U|$.

Hence, we get $k \in \mathbb{Z}_{\geqslant 1}$ and $m_1, \ldots, m_k \in M$ such that $M = \bigsqcup_{i \in [1,k]} Um_i$. Thus

$$p^s = |M| = \sum_{i \in [1,k]} |Um_i| = \sum_{i \in [1,k]} |U| = k \cdot |U|.$$

So $|U|$ divides p^s. Therefore, there is a unique $\ell \in [0,s]$ with $|U| = p^{s-\ell}$. This forces $k = p^\ell$.

By (1), we have $|[M]| = \frac{|G|}{|U|} = \frac{p^t n}{p^{s-\ell}} = p^{t-s+\ell} n$. □

Remark 14 *Let $g \in G$. Let $M \in \Omega$. Then we have* $\mathrm{Stab}(gM) = {}^g\mathrm{Stab}(M)$. *In particular, we have* $|\mathrm{Stab}(\hat{M})| = |\mathrm{Stab}(M)|$ *for* $\hat{M} \in [M]$.

Proof. We have

$$\begin{aligned}\mathrm{Stab}(gM) &= \{h \in G : hgM = gM\}\\ &= \{h \in G : g^{-1}hgM = M\}\\ &= \{h \in G : h^gM = M\}\\ &= \{h \in G : h^g \in \mathrm{Stab}(M)\}\\ &= \{h \in G : h \in {}^g\mathrm{Stab}(M)\}\\ &= {}^g\mathrm{Stab}(M).\end{aligned}$$

□

Definition 15 Let $\ell \in [0, s]$.

(1) Let

$$\Omega^\ell := \Omega^{[s],\ell} := \{M \in \Omega^{[s]} : |[M]| = p^{t-s+\ell}n\} \subseteq \Omega.$$

So

$$\Omega = \bigsqcup_{k\in[0,s]} \Omega^k;$$

cf. Lemma 13.(2).

Note that

$$\Omega^\ell = \{M \in \Omega : |\mathrm{Stab}(M)| = p^{s-\ell}\};$$

cf. Lemma 13.(1).

(2) Let

$$\begin{aligned}\overline{\Omega}^\ell &:= \overline{\Omega}^{[s],\ell}\\ &:= \{[M] : M \in \Omega^\ell\}\\ &= \{[M] : M \in \Omega,\ |[M]| = p^{t-s+\ell}n\}\\ &= \{[M] : M \in \Omega,\ |\mathrm{Stab}(M)| = p^{s-\ell}\} \subseteq \overline{\Omega}.\end{aligned}$$

So

$$\overline{\Omega} = \bigsqcup_{k\in[0,s]} \overline{\Omega}^k;$$

cf. Lemma 13.(2).

Note that for $M \in \Omega^\ell$ and $\hat{M} \in [M]$, we have $\hat{M} \in \Omega^\ell$.

Furthermore, we write

$$\overline{\Omega}^{[0,\ell]} := \overline{\Omega}^{[s],[0,\ell]} := \bigsqcup_{k\in[0,\ell]} \overline{\Omega}^k \subseteq \overline{\Omega}.$$

(3) Let

$$a_\ell := |\overline{\Omega}^\ell| \in \mathbb{Z}_{\geqslant 0}.$$

Remark 16 *We have* $|\Omega| = p^{t-s}n \sum_{k\in[0,s]} a_k p^k$.

Proof. Given $k \in [0, s]$, we may choose representatives $M_{k,1}, \ldots, M_{k,a_k} \in \Omega^k$ such that

$$\overline{\Omega}^k = \{[M_{k,j}] : j \in [1, a_k]\}, \qquad \text{i.e.} \qquad \Omega^k = \bigcup_{M\in\Omega^k} [M] = \bigsqcup_{j\in[1,a_k]} [M_{k,j}].$$

Hence

$$\Omega = \bigsqcup_{k\in[0,s]} \Omega^k = \bigsqcup_{k\in[0,s]} \bigsqcup_{j\in[1,a_k]} [M_{k,j}]$$

and therefore

$$|\Omega| = \sum_{k\in[0,s]} \sum_{j\in[1,a_k]} |[M_{k,j}]| = \sum_{k\in[0,s]} \sum_{j\in[1,a_k]} p^{t-s+k}n = \sum_{k\in[0,s]} a_k p^{t-s+k}n = p^{t-s}n \sum_{k\in[0,s]} a_k p^k. \quad \square$$

Definition 17 Let

$$q := \frac{1}{p^{t-s}n}\binom{p^t n}{p^s} \in \mathbb{Z}_{\geqslant 1},$$

cf. Remark 16.

Remark 18 Remark 16 yields

$$q = \sum_{k\in[0,s]} a_k p^k.$$

So for $\ell \in [0, s]$, we get

$$q \equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} a_k p^k.$$

In particular, we get

$$q \equiv_p a_0, \qquad q \equiv_{p^2} a_0 + a_1 p, \qquad q \equiv_{p^3} a_0 + a_1 p + a_2 p^2$$

etc.

3.3 Wielandt's lemma

We shall give an interpretation of the right hand side in terms of members of certain chains of p-subgroups; cf. Proposition 46 below.

Remark 19 *Suppose given* $H \in \mathrm{Sub}(s) \subseteq \Omega^{[s]}$. *Then* $\mathrm{Stab}(H) = H$ *and* $H \in \Omega^0$.

Proof. Suppose given $g \in G$. Then $g \in \mathrm{Stab}(H)$ if and only if $gH = H$, i.e. $g \in H$. Since $|\mathrm{Stab}(H)| = |H| = p^s$, we get $H \in \Omega^0$, cf. Definition 15.(1). $\square$

Lemma 20 (Wielandt, cf. [**9**]) *Let $M \in \Omega$.*

(1) *Given $M \in \Omega^0$, there is a unique $H \in [M]$ with $H \leqslant G$.*

(2) *Given $M \in \Omega^\ell$ for some $\ell \in [1, s]$, we have $M \not\leqslant G$.*

Proof. Ad (1). We have $|\operatorname{Stab}(M)| = p^{s-0} = p^s$; cf. Definition 15.(1). Lemma 13.(2) yields $M = \operatorname{Stab}(M)m$ for some $m \in M$. Hence $m^{-1}M = m^{-1}\operatorname{Stab}(M)m \in [M]$ and $m^{-1}\operatorname{Stab}(M)m = \operatorname{Stab}(M)^m \leqslant G$.

Suppose given $H, \hat{H} \in [M]$ such that $H, \hat{H} \leqslant G$. We may choose $g \in G$ such that $gH = \hat{H}$. Since $H = g^{-1}\hat{H}$, we have $g^{-1} \in H$, thus $g = (g^{-1})^{-1} \in H$. Thus $H = gH = \hat{H}$.

Ad (2). *Assume* that $M \leqslant G$. Then $M \in \Omega^0$, cf. Remark 19, a *contradiction.* □

Example 21 Let $G = \mathrm{S}_4$ and $p = 2$.

Let $M = \{\mathrm{id}, (1,2)\} = \langle (1,2) \rangle \in \Omega^{[1]} = \{M \subseteq \mathrm{S}_4 : |M| = 2^1\}$.

We have

$$\operatorname{Stab}_{\mathrm{S}_4}(M) = \{\sigma \in \mathrm{S}_4 : \sigma M = M\} = \{\mathrm{id}, (1,2)\} = M.$$

So $|\operatorname{Stab}_{\mathrm{S}_4}(M)| = 2^1 = 2^{1-0}$, hence $M \in \Omega^{[1],0}$.

This also follows by Remark 19. Note that

$$|[M]| = \tfrac{|\mathrm{S}_4|}{|\operatorname{Stab}_{\mathrm{S}_4}(M)|} = \tfrac{24}{2} = 12.$$

Furthermore, Lemma 20.(1) gives

$$\{H \leqslant G : H \in [M]\} = \{M\}.$$

3.4 Sylow-Frobenius

With these tools, we can already derive Theorem 22, which will also result as the particular case $\ell = 0$ from Theorem 47.

Theorem 22 (cf. [**8,** Th. II], [**3,** §4, I.]) *Let $s \in [0, t]$. We have*

$$\mathrm{N}(s) \equiv_p 1.$$

Proof. Consider $|\Omega| = \binom{p^t n}{p^s} = p^{t-s} \sum_{k \in [0,s]} a_k p^k$, cf. Remark 16. Hence

$$q = \tfrac{1}{p^{t-s}} \binom{p^t n}{p^s} = \sum_{k \in [0,s]} a_k p^k \equiv_p a_0,$$

and Lemma 20.(1, 2) provides $a_0 = \mathrm{N}(s)$. That is $q \equiv_p \mathrm{N}(s)$.

Consider the cyclic group $C := \mathrm{C}_{p^t n}$ of order $p^t n$. It is well-known that $\mathrm{C}_{p^t n}$ has exactly one subgroup of order p^s. Therefore

$$\mathrm{N}_{G,p}(s) \equiv_p q \equiv_p \mathrm{N}_{C,p}(s) = 1.$$ □

4 Counting orbit representatives

Let $s \in [0, t]$.

4.1 Transversals

Let $\ell \in [0, s]$.

Remark 23 *Let $\hat{M} \in \Omega^\ell$. Then there exist $M \in [\hat{M}]$ and $m_2, \dots, m_{p^\ell} \in M$ such that*

$$M = U \sqcup \bigsqcup_{i \in [2, p^\ell]} U m_i,$$

where $U := \mathrm{Stab}(M) \leqslant G$.

Proof. Thanks to Lemma 13.(2), we get $\hat{m}_1, \dots, \hat{m}_{p^\ell} \in \hat{M}$ such that $\hat{M} = \bigsqcup_{i \in [1, p^\ell]} \hat{U} \hat{m}_i$ with $\hat{U} := \mathrm{Stab}(\hat{M})$. Let $m_i := \hat{m}_1^{-1} \hat{m}_i$ for $i \in [1, p^\ell]$ and $U := \hat{U}^{\hat{m}_1}$.

Now $M := \hat{m}_1^{-1} \hat{M} \in [\hat{M}]$, and

$$\begin{aligned} M &= \hat{m}_1^{-1} \left(\textstyle\bigsqcup_{i \in [1, p^\ell]} \hat{U} \hat{m}_i \right) \\ &= \textstyle\bigsqcup_{i \in [1, p^\ell]} \hat{m}_1^{-1} \hat{U} \hat{m}_i \\ &= \textstyle\bigsqcup_{i \in [1, p^\ell]} \hat{m}_1^{-1} \hat{U} \hat{m}_1 \hat{m}_1^{-1} \hat{m}_i \\ &= \textstyle\bigsqcup_{i \in [1, p^\ell]} \hat{U}^{\hat{m}_1} \hat{m}_1^{-1} \hat{m}_i \\ &= \hat{U}^{\hat{m}_1} \sqcup \textstyle\bigsqcup_{i \in [2, p^\ell]} \hat{U}^{m_1} \hat{m}_1^{-1} \hat{m}_i \\ &= U \sqcup \textstyle\bigsqcup_{i \in [2, p^\ell]} U m_i. \end{aligned}$$

Using Remark 14, we get

$$U = \hat{U}^{\hat{m}_1} = {}^{\hat{m}_1^{-1}} \hat{U} = {}^{\hat{m}_1^{-1}} \mathrm{Stab}(\hat{M}) = \mathrm{Stab}(\hat{m}_1^{-1} \hat{M}) = \mathrm{Stab}(M). \qquad \square$$

Reminder 24 Given a subgroup $U \leqslant G$, we call a subset $T \subseteq G$ a *right transversal* for U in G if

$$G = \bigsqcup_{t \in T} U t.$$

Notation 25 Given a subgroup $U \leqslant G$, we choose a right transversal $T \subseteq G$ such that $1 \in T$, and we write

$$\mathrm{tv}(U) := \mathrm{tv}_G(U) := T.$$

The choice of this transversal, that is the choice of representatives, will affect the calculations, but not the outcome of the considerations.

We write

$$\mathrm{Tv}_{p^\ell}(U) := \mathrm{Tv}_{G,p^\ell}(U) := \{T \subseteq (\mathrm{tv}(U) \setminus \{1\}) : |T| = p^\ell - 1\} \subseteq \mathfrak{P}(\mathrm{tv}(U)).$$

Definition 26 We write

$$\mathrm{b}(\ell) := \mathrm{b}_s(\ell) := \binom{p^{t-s+\ell}n - 1}{p^\ell - 1} \in \mathbb{Z}_{\geqslant 0}.$$

Remark 27 Let $U \in \mathrm{Sub}(s-\ell)$ and let $G = \bigsqcup_{t \in \mathrm{tv}(U)} Ut$. Then

$$|\mathrm{tv}(U)| = |G/U| = |G|/|U| = p^t n / p^{s-\ell} = p^{t-s+\ell} n.$$

We have $|\mathrm{tv}(U)| - 1$ elements in $\mathrm{tv}(U) \setminus \{1\}$.

Any $T \in \mathrm{Tv}_{p^\ell}(U)$ contains $p^\ell - 1$ elements.

This leads to

$$|\mathrm{Tv}_{p^\ell}(U)| = \tbinom{|\mathrm{tv}(U)|-1}{p^\ell-1} = \tbinom{p^{t-s+\ell}n-1}{p^\ell-1} = \mathrm{b}(\ell).$$

Recall that we have $t = \mathrm{v}_p(|G|)$ and $n = |G|/p^t$.

Lemma 28 *Let $\ell \in [1, s]$. We have*

$$\mathrm{b}(\ell) \equiv_{p^\ell} \mathrm{b}(\ell - 1).$$

Proof. Write $d := t - s \in \mathbb{Z}_{\geqslant 0}$. We have

$$\begin{aligned}
\mathrm{b}(\ell) &\overset{\text{D. 26}}{=} \binom{p^{t-s+\ell}n - 1}{p^\ell - 1} \\
&= \frac{\prod_{i \in [1, p^\ell - 1]} (p^{d+\ell}n - i)}{\prod_{i \in [1, p^\ell - 1]} (p^\ell - i)} \\
&= \prod_{i \in [1, p^\ell - 1]} \frac{p^{d+\ell}n - i}{p^\ell - i} \\
&= \left(\prod_{\substack{i \in [1, p^\ell - 1] \\ i \equiv_p 0}} \frac{p^{d+\ell}n - i}{p^\ell - i} \right) \cdot \left(\prod_{\substack{i \in [1, p^\ell - 1] \\ i \not\equiv_p 0}} \frac{p^{d+\ell}n - i}{p^\ell - i} \right)
\end{aligned}$$

$$
\begin{aligned}
\overset{i=pj}{=} \quad & \left(\prod_{j\in[1,p^{\ell-1}-1]} \frac{p^{d+\ell}n-pj}{p^\ell-pj}\right)\cdot\left(\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i}\right)\\
= \quad & \left(\prod_{j\in[1,p^{\ell-1}-1]} \frac{p^{d+(\ell-1)}n-j}{p^{\ell-1}-j}\right)\cdot\left(\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i}\right)\\
= \quad & \mathrm{b}(\ell-1)\cdot\left(\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i}\right).
\end{aligned}
$$

Furthermore, we have

$$\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i} \;\in\; \mathbb{Z}_{(p)}$$

because $p^\ell - i \not\equiv_p 0$ for $i \in [1, p^\ell - 1] \setminus p\mathbb{Z}$.

Hence

$$\mathrm{b}(\ell) = \mathrm{b}(\ell-1)\cdot\left(\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i}\right)$$

in $\mathbb{Z}_{(p)}$. And $\frac{p^{d+\ell}n-i}{p^\ell-i} - 1 = \frac{p^{d+\ell}n-p^\ell}{p^\ell-i} = p^\ell\frac{p^dn-1}{p^\ell-i} \in p^\ell\mathbb{Z}_{(p)}$ for $i \in [1, p^\ell - 1] \setminus p\mathbb{Z}$, so

$$\frac{p^{d+\ell}n-i}{p^\ell-i} \equiv_{p^\ell} 1$$

for $i \in [1, p^\ell - 1] \setminus p\mathbb{Z}$, so

$$\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i} \equiv_{p^\ell} 1.$$

Hence

$$\mathrm{b}(\ell) = \mathrm{b}(\ell-1)\cdot\left(\prod_{\substack{i\in[1,p^\ell-1]\\ i\not\equiv_p 0}} \frac{p^{d+\ell}n-i}{p^\ell-i}\right) \equiv_{p^\ell} \mathrm{b}(\ell-1)$$

in $\mathbb{Z}_{(p)}$. Thus we obtain the congruence

$$\mathrm{b}(\ell) \equiv_{p^\ell} \mathrm{b}(\ell-1)$$

in $\mathbb{Z}$ because $\mathrm{b}(\ell), \mathrm{b}(\ell-1) \in \mathbb{Z}$, cf. Remark 3.(2). □

4.2 Constructions

Let $\ell \in [0, s]$.

Definition 29

(1) Let

$$\begin{aligned}\Omega_1^\ell := \Omega_1^{[s],\ell} &:= \{M \in \Omega^{[s],\ell} : 1 \in M\} \\ &= \{M \in \Omega^{[s]} : 1 \in M,\ |\operatorname{Stab}(M)| = p^{s-\ell}\};\end{aligned}$$

cf. Definition 15.(1).

(2) Let

$$\begin{aligned}\Omega_1^{[0,\ell]} &:= \Omega_1^{[s],[0,\ell]} \\ &:= \{U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i : U \in \operatorname{Sub}(s-\ell), \{g_2, \dots, g_{p^\ell}\} \in \operatorname{Tv}_{p^\ell}(U)\} \subseteq \Omega^{[s]}.\end{aligned}$$

Example 30 Let $G = \mathrm{S}_4$ and $p = 2$. Let $s = 3$. Let $\ell = 2$.

Let $U := \langle (1,2) \rangle \leqslant \mathrm{S}_4$. Then $U \in \operatorname{Sub}(1)$ since $|U| = 2^1$.

We choose $\operatorname{tv}_{\mathrm{S}_4}(U)$ such that $T := \{(3,4), (1,2,3), (1,3,4)\} \subseteq \operatorname{tv}_{\mathrm{S}_4}(U)$ by choice of the latter.

Then $T \in \operatorname{Tv}_{2^2}(U)$ since $T \subseteq (\operatorname{tv}_{\mathrm{S}_4}(U) \setminus \{\mathrm{id}\})$ and $|T| = 2^2 - 1$, cf. Notation 25.

Let

$$\begin{aligned}M &:= U \sqcup \bigsqcup_{t\in T} Ut \\ &= U \sqcup U(3,4) \sqcup U(1,2,3) \sqcup U(1,3,4) \\ &= \{\mathrm{id}, (1,2)\} \sqcup \{(3,4), (1,2)(3,4)\} \sqcup \{(1,2,3), (1,3)\} \sqcup \{(1,3,4), (1,2,3,4)\}.\end{aligned}$$

Then $M \in \Omega_1^{[0,2]}$, cf. Definition 29.(2).

Magma gives $\operatorname{Stab}_{\mathrm{S}_4}(M) = \langle (1,2), (3,4) \rangle$. Then $|\operatorname{Stab}_{\mathrm{S}_4}(M)| = 2^2 = 2^{3-1}$, i.e.

$$M \in \Omega_1^1,$$

cf. Definition 29.(1).

Lemma 31 *Suppose given*

$$M = U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i$$

for some $U \in \operatorname{Sub}(s-\ell)$ *and* $\{g_2, \dots, g_{p^\ell}\} \in \operatorname{Tv}_{p^\ell}(U)$.

Then we have

$$U \leqslant \operatorname{Stab}(M).$$

Proof. We show $U \overset{!}{\subseteq} \mathrm{Stab}(M)$. Suppose given $u \in U$. We show $uM \overset{!}{=} M$.

Since $u \in U$, we have $uU = U$ and therefore

$$uM = u\left(U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i\right) = uU \sqcup \bigsqcup_{i\in[2,p^\ell]} uUg_i = U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i = M. \qquad \square$$

Example 32 We continue Example 30.

We have $U = \langle (1,2)\rangle$ and $\mathrm{Stab}_{\mathrm{S}_4}(M) = \langle (1,2),(3,4)\rangle$. Indeed, we have

$$U \leqslant \mathrm{Stab}_{\mathrm{S}_4}(M)$$

as predicted by Lemma 31.

Since $|U| = 2^1$ and $|\mathrm{Stab}_{\mathrm{S}_4}(M)| = 2^2$, we have

$$(U, \mathrm{Stab}_{\mathrm{S}_4}(M)) \in \mathrm{Sub}(1,2).$$

Lemma 33 *We have* $\Omega_1^{[0,\ell]} = \bigsqcup_{k\in[0,\ell]} \Omega_1^k$.

Proof. *Ad* $\subseteq$. Let

$$M := U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i \in \Omega_1^{[0,\ell]},$$

where $U \in \mathrm{Sub}(s-\ell)$ and $\{g_2,\ldots,g_{p^\ell}\} \in \mathrm{Tv}_{p^\ell}(U)$. Then $|M| = p^{s-\ell} + (p^\ell - 1)p^{s-\ell} = p^s$, so $M \in \Omega$.

Let $V := \mathrm{Stab}(M)$. Lemma 13.(2) yields $|V| = p^{s-k}$ for some $k \in [0,s]$. Since $U \leqslant V$ by Lemma 31, $p^{s-\ell}$ divides p^{s-k}, i.e. $s-\ell \leqslant s-k$, i.e. $k \leqslant \ell$. Note that $M \in \Omega^k$. Since $1 \in U \subseteq M$, we have $M \in \Omega_1^k \subseteq \bigsqcup_{i\in[0,\ell]} \Omega_1^i$.

Ad $\supseteq$. Let $M \in \Omega_1^k$ for some $k \in [0,\ell]$. Let $U := \mathrm{Stab}(M)$. Then $|U| = |\mathrm{Stab}(M)| = p^{s-k}$. Lemma 13.(2) gives a decomposition $M = \bigsqcup_{j\in[1,p^k]} Um_j$ for some $m_1,\ldots,m_{p^k} \in M$. Since $1 \in M$, the right coset $U\cdot 1$ is contained in M.

Then we may choose $\{g_2,\ldots,g_{p^k}\} \in \mathrm{Tv}_{p^k}(U)$ such that

$$M = U \sqcup \bigsqcup_{i\in[2,p^k]} Ug_i.$$

Thanks to Theorem 22, we may choose $V \in \mathrm{Sub}(s-\ell)$ with $V \leqslant U$. Then $|U/V| = p^{s-k}/p^{s-\ell} = p^{\ell-k}$. So there exists a unique $\{g_2',\ldots,g_{p^{\ell-k}}'\} \in \mathrm{Tv}_{p^{\ell-k}}(V)$ such that $U = V \sqcup \bigsqcup_{j\in[2,p^{\ell-k}]} Vg_j'$. Write $g_1 := g_1' := 1$. Then

$$M = \bigsqcup_{i\in[1,p^k]} Ug_i = \bigsqcup_{i\in[1,p^k]} (\bigsqcup_{m\in[1,p^{\ell-k}]} Vg_m')g_i = \bigsqcup_{\substack{i\in[1,p^k]\\ m\in[1,p^{\ell-k}]}} Vg_m'g_i = V \sqcup \bigsqcup_{j\in[2,p^\ell]} Vh_j$$

for some $\{h_2,\ldots,h_{p^\ell}\} \in \mathrm{Tv}_{p^\ell}(V)$. Hence, $M \in \Omega_1^{[0,\ell]}$. $\square$

Definition 34

(1) Let

$$\Theta^{(\ell)} := \Theta^{[s],(\ell)} := \coprod_{U\in \mathrm{Sub}(s-\ell)} \mathrm{Tv}_{p^\ell}(U)$$
$$= \{(U, \{g_2, \dots, g_{p^\ell}\}) : U \in \mathrm{Sub}(s-\ell), \{g_2, \dots, g_{p^\ell}\} \in \mathrm{Tv}_{p^\ell}(U)\}.$$

Then

$$|\Theta^{(\ell)}| = |\Theta^{[s],(\ell)}| = \mathrm{b}(\ell)\,\mathrm{N}(s-\ell);$$

cf. Remark 27 and Definition 8.(2).

(2) Let

$$\varphi^{(\ell)} : \qquad \Theta^{(\ell)} \to \Omega_1^{[0,\ell]}$$
$$(U, \{g_2, \dots, g_{p^\ell}\}) \mapsto U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i$$

be the *assembly map*. Let

$$\rho_1^{[0,\ell]} := \rho|^{\overline{\Omega}^{[0,\ell]}}_{\Omega_1^{[0,\ell]}} : \Omega_1^{[0,\ell]} \to \overline{\Omega}^{[0,\ell]}.$$

(3) Let $k \in [0,\ell]$. Let

$$\Theta^{(\ell),k} := \Theta^{[s],(\ell),k} := (\varphi^{(\ell)})^{-1}(\Omega_1^k) \subseteq \Theta^{(\ell)}.$$

So $\Theta^{(\ell)} = \bigsqcup_{i\in[0,\ell]} \Theta^{(\ell),i}$, cf. Lemma 33.

Let

$$\varphi^{(\ell),k} := \varphi^{(\ell)}|^{\Omega_1^k}_{\Theta^{(\ell),k}} : \Theta^{(\ell),k} \to \Omega_1^k.$$

and

$$\rho_1^k := \rho_1^{[0,\ell]}|^{\overline{\Omega}^k}_{\Omega_1^k} : \Omega_1^k \to \overline{\Omega}^k.$$

The situation can be illustrated as follows.

$$\begin{array}{ccccccccccccc}
 & & \Theta^{(\ell)} & = & \Theta^{(\ell),0} & \sqcup & \Theta^{(\ell),1} & \sqcup & \dots & \sqcup & \Theta^{(\ell),\ell} \\
 & & \downarrow{\scriptstyle \varphi^{(\ell)}} & & \downarrow{\scriptstyle \varphi^{(\ell),0}} & & \downarrow{\scriptstyle \varphi^{(\ell),1}} & & & & \downarrow{\scriptstyle \varphi^{(\ell),\ell}} \\
\Omega & \supseteq & \Omega_1^{[0,\ell]} & = & \Omega_1^0 & \sqcup & \Omega_1^1 & \sqcup & \dots & \sqcup & \Omega_1^\ell \\
\downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho_1^{[0,\ell]}} & & \downarrow{\scriptstyle \rho_1^0} & & \downarrow{\scriptstyle \rho_1^1} & & & & \downarrow{\scriptstyle \rho_1^\ell} \\
\overline{\Omega} & \supseteq & \overline{\Omega}^{[0,\ell]} & = & \overline{\Omega}^0 & \sqcup & \overline{\Omega}^1 & \sqcup & \dots & \sqcup & \overline{\Omega}^\ell
\end{array}$$

Example 35 We continue Example 30. Recall that $s = 3$.

Since $U \in \mathrm{Sub}(3-2)$ and $T \in \mathrm{Tv}_{2^2}(U)$, we have

$$\theta := (U, T) \in \Theta^{(2)},$$

cf. Definition 34.(1).

Consider $\varphi^{(2)} : \Theta^{(2)} \to \Omega_1^{[0,2]}$. We have

$$\begin{aligned}
\varphi^{(2)}(\theta) &= \varphi^{(2)}\Big((U, T)\Big) \\
&= \varphi^{(2)}\Big((U, \{(3,4), (1,2,3), (1,3,4)\})\Big) \\
&= U \sqcup \bigsqcup_{g \in \{(3,4),(1,2,3),(1,3,4)\}} Ug \\
&= U \sqcup U(3,4) \sqcup U(1,2,3) \sqcup U(1,3,4) \\
&= M,
\end{aligned}$$

cf. Definition 34.(2).

Since

$$M = \varphi^{(2)}(\theta) \overset{\text{Ex. } 30}{\in} \Omega_1^1 \subseteq \Omega_1^0 \sqcup \Omega_1^1 \sqcup \Omega_1^2 \overset{\text{L. } 33}{=} \Omega_1^{[0,2]},$$

we have

$$(U, T) \in (\varphi^{(2)})^{-1}(\{M\}) = \Theta^{(2),1},$$

and

$$(U, T) \overset{\varphi^{(2),1}}{\longmapsto} M,$$

cf. Definition 34.(3).

4.3 Some properties of the assembly map

Let $\ell \in [0, s]$.

4.3.1 A characterization

Lemma 36

(1) *The map* $\varphi^{(\ell)} : \Theta^{(\ell)} \to \Omega_1^{[0,\ell]}$ *is surjective.*

(2) *The map* $\varphi^{(\ell),k} : \Theta^{(\ell),k} \to \Omega_1^k$ *is surjective for* $k \in [0, \ell]$.

Proof. Ad (1). Cf. Definition 29.(2) and Definition 34.(1).

Ad (2). Cf. (1) and Definition 34.(2, 3). □

Lemma 37 *Let* $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell)}$. *Let*

$$M := U \sqcup \bigsqcup_{i \in [2, p^\ell]} U g_i = \varphi^{(\ell)}(U, \{g_2, \dots, g_{p^\ell}\}) \in \Omega_1^{[0,\ell]}.$$

The following assertions are equivalent.

(1) *We have* $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell),\ell}$.

(2) *We have* $M \in \Omega_1^\ell$.

(3) *We have* $U = \mathrm{Stab}(M)$.

Proof. Ad (1) $\Leftrightarrow$ (2). By Definition 34.(2), we have $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell),\ell}$ if and only if $\varphi^{(\ell)}(U, \{g_2, \dots, g_{p^\ell}\}) \in \Omega_1^\ell$.

Ad (2) $\Rightarrow$ (3). We have $M = U \sqcup \bigsqcup_{i \in [2,p]} U g_i \in \Omega_1^\ell$. Lemma 31 yields $U \leqslant \mathrm{Stab}(M)$. We have $|U| = p^{s-\ell}$ by Definition 34.(1). We have $|\mathrm{Stab}(M)| = p^{s-\ell}$ by Definition 15.(1). This yields $U = \mathrm{Stab}(M)$.

Ad (3) $\Rightarrow$ (2). If $U = \mathrm{Stab}(M)$, then $|\mathrm{Stab}(M)| = |U| = p^{s-\ell}$; cf. Definition 34.(1). So $M \in \Omega^\ell$; cf. Definition 15.(1). Since $1 \in U \subseteq M$, we get $M \in \Omega_1^\ell$. □

Example 38 We continue Example 30. Recall that $s = 3$.

We have

$$U = \langle (1,2) \rangle < \langle (1,2), (3,4) \rangle = \mathrm{Stab}_{\mathrm{S}_4}(M),$$

and therefore $M \notin \Omega_1^2$, cf. Lemma 37.($\neg 3 \Rightarrow \neg 2$).

Actually, we have already seen that $M \in \Omega_1^1$; cf. Example 30.

Now let $\ell = 1$ and consider $V := \mathrm{Stab}_{\mathrm{S}_4}(M)$. Suppose that $(1,2,3) \in \mathrm{tv}_{\mathrm{S}_4}(V)$ by choice of the latter. Then $V \in \mathrm{Sub}(3-1)$ and $\{(1,2,3)\} \in \mathrm{Tv}_2(V)$, and we get

$$M = V \sqcup V(1,2,3) = \varphi^{(1)}\Big((V, \{(1,2,3)\})\Big).$$

The equivalent assertions of Lemma 37 all hold: We have $(V, \{(1,2,3)\}) \in \Theta^{(1),1}$, $M \in \Omega_1^1$ and $V = \mathrm{Stab}_{\mathrm{S}_4}(M)$. In particular, $M = \varphi^{(1),1}\Big((V, \{(1,2,3)\})\Big)$.

4.3.2 Three bijections

Lemma 39 *We have the bijective map*

$$\begin{aligned} \Theta^{(\ell),0} &\to \mathrm{Sub}(s-\ell, s) \\ (U, \{g_2, \dots, g_{p^\ell}\}) &\mapsto (U, U \sqcup \textstyle\bigsqcup_{i \in [2,p^\ell]} U g_i). \end{aligned}$$

In particular, we have

$$|\Theta^{(\ell),0}| = \mathrm{N}(s-\ell, s),$$

cf. Definition 8.(2).

Proof. Well-defined. Given $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell),0}$, we have

$$\varphi^{(\ell),0}\Big((U, \{g_2, \dots, g_{p^\ell}\})\Big) = U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i =: M \in \Omega_1^0.$$

Let $V := \mathrm{Stab}(M)$. We have $|V| = p^s$; cf. Definition 15.(1). We have $U \leqslant V$; cf. Lemma 31. Since $|[M]| = p^{t-s}n$, we get $M = Vm$ for some $m \in M$; cf. Lemma 13.(2). But $1 \in M = Vm$, so $V1 = Vm$ and therefore $M = V \leqslant G$. Hence $(U, V) \in \mathrm{Sub}(s-\ell, s)$.

Surjective. Suppose given $(U, V) \in \mathrm{Sub}(s-\ell, s)$. We have $|V|/|U| = p^s/p^{s-\ell} = p^\ell$, so we may choose $\{g_2, \dots, g_{p^\ell}\} \in \mathrm{Tv}_{p^\ell}(U)$ with $U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i = V$. Then $V \in \Omega_1^0$, cf. Remark 19. Since

$$V = \varphi^{(\ell)}\Big((U, \{g_2, \dots, g_{p^\ell}\})\Big) \in \Omega_1^0,$$

we have $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell),0}$.

Injective. Given $(U, \{g_2, \dots, g_{p^\ell}\}), (\hat{U}, \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\}) \in \Theta^{(\ell),0}$ with

$$(U, U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i) = (\hat{U}, \hat{U} \sqcup \bigsqcup_{i\in[2,p^\ell]} \hat{U}\hat{g}_i),$$

it follows first that $U = \hat{U}$.

Since $\{g_2, \dots, g_{p^\ell}\}, \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\} \in \mathrm{Tv}_{p^\ell}(U)$ and $U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i = U \sqcup \bigsqcup_{i\in[2,p^\ell]} U\hat{g}_i$, we conclude that

$$\{g_2, \dots, g_{p^\ell}\} = \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\},$$

cf. Remark 1. □

Lemma 40 *The map*

$$\varphi^{(\ell),\ell} : \Theta^{(\ell),\ell} \to \Omega_1^\ell,\ (U, \{g_2, \dots, g_{p^\ell}\}) \mapsto U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i$$

is bijective. Moreover,

$$U = \mathrm{Stab}(U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i)$$

for $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell),\ell}$*, cf. Lemma* 37.$(2 \Rightarrow 3)$.

Proof. Surjective. Cf. Lemma 36.(2).

Injective. Let $(U, \{g_2, \dots, g_{p^\ell}\}), (\hat{U}, \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\}) \in \Theta^{(\ell),\ell}$ with

$$M := \varphi^{(\ell),\ell}(U, \{g_2, \dots, g_{p^\ell}\}) = \varphi^{(\ell),\ell}(\hat{U}, \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\}),$$

i.e.

$$U \sqcup \bigsqcup_{i\in[2,p^\ell]} Ug_i = \hat{U} \sqcup \bigsqcup_{i\in[2,p^\ell]} \hat{U}\hat{g}_i.$$

Then $U = \mathrm{Stab}(M) = \hat{U}$, cf. Lemma 37.$(2 \Rightarrow 3)$. Since $\mathrm{Tv}_{p^\ell}(U) = \mathrm{Tv}_{p^\ell}(\hat{U})$ and since $\{Ug_2, \dots, Ug_{p^\ell}\} = \{U\hat{g}_2, \dots, U\hat{g}_{p^\ell}\}$, it follows that

$$\{g_2, \dots, g_{p^\ell}\} = \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\},$$

cf. Remark 1. So

$$(U, \{g_2, \dots, g_{p^\ell}\}) = (\hat{U}, \{\hat{g}_2, \dots, \hat{g}_{p^\ell}\}).$$ □

Lemma 41 *Let $k \in [0,\ell]$. Let $M \in \Omega_1^k$. We have the bijective map*

$$\begin{aligned} \kappa : \qquad & (\varphi^{(\ell),k})^{-1}(\{M\}) \to \mathrm{Sub}(s-\ell, \mathrm{Stab}(M)) \\ & (V, \{h_2, \dots, h_{p^\ell}\}) \mapsto V \end{aligned}$$

In particular, we have

$$|(\varphi^{(\ell),k})^{-1}(\{M\})| = |\,\mathrm{Sub}(s-\ell, \mathrm{Stab}(M))|.$$

Proof. There exists a unique $(U, \{g_2, \dots, g_{p^k}\}) \in \Theta^{(k),k}$ such that

$$M = U \sqcup \bigsqcup_{i \in [2,p^k]} Ug_i,$$

where $U = \mathrm{Stab}(M)$, cf. Lemma 40.

Well-defined. Suppose given $(V, \{h_2, \dots, h_{p^\ell}\}) \in (\varphi^{(\ell),k})^{-1}(\{M\}) \subseteq \Theta^{(\ell),k}$. Then

$$V \sqcup \textstyle\bigsqcup_{j\in[2,p^\ell]} Vh_j = M = U \sqcup \bigsqcup_{i\in[2,p^k]} Ug_i,$$

and, by Lemma 31, $V \leqslant \mathrm{Stab}(M) = U$, so $V \in \mathrm{Sub}(s-\ell, U)$.

Surjective. Suppose given $V \in \mathrm{Sub}(s-\ell)$ with $V \leqslant U$.

There exists a unique $\{g_2', \dots, g_{p^{\ell-k}}'\} \in \mathrm{Tv}_{p^{\ell-k}}(V)$ such that $U = V \sqcup \bigsqcup_{m\in[2,p^{\ell-k}]} Vg_m'$.

Write $g_1 := g_1' := 1$. We get

$$M = \bigsqcup_{i\in[1,p^k]} Ug_i = \bigsqcup_{i\in[1,p^k]} (\textstyle\bigsqcup_{m\in[1,p^{\ell-k}]} Vg_m')g_i = \bigsqcup_{\substack{i\in[1,p^k] \\ m\in[1,p^{\ell-k}]}} Vg_m'g_i = V \sqcup \bigsqcup_{j\in[2,p^\ell]} Vh_j$$

for some $\{h_2, \dots, h_{p^\ell}\} \in \mathrm{Tv}_{p^\ell}(V)$.

Since $M \in \Omega_1^k$, we have $(V, \{h_2, \dots, h_{p^\ell}\}) \in \Theta^{(\ell),k}$.

Moreover, since $M = V \sqcup \bigsqcup_{j\in[2,p^\ell]} Vh_j = \varphi^{(\ell),k}\Big((V, \{h_2, \dots, h_{p^\ell}\})\Big)$, we have

$$(V, \{h_2, \dots, h_{p^\ell}\}) \in (\varphi^{(\ell),k})^{-1}(\{M\}).$$

Hence

$$V = \kappa\Big((V, \{h_2, \dots, h_{p^\ell}\})\Big) \in \kappa\Big((\varphi^{(\ell),k})^{-1}(\{M\})\Big).$$

Note that we had a similar calculation in Lemma 33, where $\bigsqcup_{k\in[0,\ell]} \Omega_1^k \overset{!}{\subseteq} \Omega_1^{[0,\ell]}$ was shown.

Injective. Given $(V, \{h_2, \dots, h_{p^\ell}\}), (\hat{V}, \{\hat{h}_2, \dots, \hat{h}_{p^\ell}\}) \in (\varphi^{(\ell),k})^{-1}(\{M\})$ which map to the same element $V = \hat{V}$ under κ, we have

$$V \sqcup \textstyle\bigsqcup_{j\in[2,p^\ell]} Vh_j = M = V \sqcup \bigsqcup_{j\in[2,p^\ell]} V\hat{h}_j.$$

Therefore, $\{h_2, \dots, h_{p^\ell}\} = \{\hat{h}_2, \dots, \hat{h}_{p^\ell}\}$, cf. Remark 1. □

Example 42 Let $G = \mathrm{S}_4$ and $p = 2$. Let $s = 3$.

(1) Let $\ell = 1$. We want to find an element

$$M \in \Omega_1^1 = \Omega_1^{[3],1} = \{M \subseteq \mathrm{S}_4 : |M| = 2^3,\ |\operatorname{Stab}_{\mathrm{S}_4}(M)| = 2^{3-1}\}$$

by making use of Lemma 40.

Recall that

$$\Theta^{(1)} = \Theta^{[3],(1)} = \{(U, \{g_2\}) : U \in \mathrm{Sub}(3-1),\ \{g_2\} \in \mathrm{Tv}_{2^1}(U)\},$$

cf. Definition 34.(1).

Recall that we have $\Theta^{(1)} = \Theta^{(1),0} \sqcup \Theta^{(1),1}$, cf. Definition 34.(3).

Suppose given $(U, \{g_2\}) \in \Theta^{(1)}$, recall that we have $(U, \{g_2\}) \in \Theta^{(1),1}$ if and only if $\varphi^{(1)}\Big((U, \{g_2\})\Big) = U \sqcup Ug_2 \nleqslant \mathrm{S}_4$, cf. Lemma 39 and Lemma 20.(2).

Let $U := \{\mathrm{id}, (1,2), (3,4), (1,2)(3,4)\} = \langle (1,2), (3,4)\rangle \in \mathrm{Sub}(3-1)$.

We suppose that $(2,3) \in \mathrm{tv}_{\mathrm{S}_4}(U)$ by choice of the latter.

So $(U, \{(2,3)\}) \in \Theta^{(1)}$.

Let

$$\begin{aligned} M &:= \varphi^{(1)}\Big((U, \{g_2\})\Big) = U \sqcup U(2,3) \\ &= \{\mathrm{id}, (1,2), (3,4), (1,2)(3,4), (2,3), (1,3,2), (2,3,4), (1,3,4,2)\}. \end{aligned}$$

Then $M \nleqslant G$ since $(1,2,3) \in M$ and $|\langle (1,2,3)\rangle| = 3$ does not divide $|M| = 8$.

Thus, $(U, \{(2,3)\}) \in \Theta^{(1),1}$, i.e. $M \in \Omega_1^1$.

Furthermore, Lemma 40 gives $\operatorname{Stab}_{\mathrm{S}_4}(M) = U$.

(2) Now let $\ell = 2$. Let $M \in \Omega_1^1$ be as in (1).

We want to consider the bijection

$$\begin{aligned} \kappa : \qquad & (\varphi^{(2),1})^{-1}(\{M\}) \to \mathrm{Sub}(3-2, U) \\ & (V, \{h_2, h_3, h_4\}) \mapsto V \end{aligned}$$

as in Lemma 41, where $k = 1$.

Let $V_1 := \langle (1,2)\rangle$, $V_2 := \langle (3,4)\rangle$ and $V_3 := \langle (1,2)(3,4)\rangle$.

Then $V_1, V_2, V_3 \in \mathrm{Sub}(3-2)$, and we have $\mathrm{Sub}(3-2, U) = \{V_1, V_2, V_3\}$.

We have $M = V_1 \sqcup V_1(3,4) \sqcup V_1(2,3) \sqcup V_1(2,3,4)$.

Supposing $\{(3,4), (2,3), (2,3,4)\} \subseteq \mathrm{tv}_{\mathrm{S}_4}(V_1)$ by choice of the latter, we have

$$(V_1, \{(3,4), (2,3), (2,3,4)\}) \overset{\kappa}{\mapsto} V_1.$$

We have $M = V_2 \sqcup V_2(1,2) \sqcup V_2(2,3) \sqcup V_2(1,3,2)$.

Supposing $\{(1,2),(2,3),(1,3,2)\} \subseteq \mathrm{tv}_{\mathrm{S}_4}(V_2)$ by choice of the latter, we have

$$(V_2, \{(1,2),(2,3),(1,3,2)\}) \overset{\kappa}{\mapsto} V_2.$$

We have $M = V_3 \sqcup V_3(1,2) \sqcup V_3(2,3) \sqcup V_3(1,3,2)$.

Supposing $\{(1,2),(2,3),(1,3,2)\} \subseteq \mathrm{tv}_{\mathrm{S}_4}(V_3)$ by choice of the latter, we have

$$(V_3, \{(1,2),(2,3),(1,3,2)\}) \overset{\kappa}{\mapsto} V_3.$$

4.4 A formula for a_ℓ

Lemma 43 *Let $\ell \in [0,s]$. Let $k \in [0,\ell]$. Let $\hat{I} \subseteq [\ell,s]$. We have*

$$\sum_{(U,\{g_2,\ldots,g_{p^\ell}\}) \in \Theta^{(\ell),k}} |\operatorname{Sub}(s-\hat{I},U)| = \sum_{\substack{I \subseteq [0,k] \\ k \in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s-(I \cup \{\ell\} \cup \hat{I})).$$

Cf. Definitions 8.(2, 3, 4) *and* 26.

Proof. Let $X := \{(k,\ell) \in \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0} : k \leqslant \ell \leqslant s\}$. For $(k,\ell),(k',\ell') \in X$, we define:

$$(k,\ell) \preccurlyeq (k',\ell') \ :\Leftrightarrow\ k \leqslant k' \text{ and } \ell \leqslant \ell'.$$

Then $(X, \preccurlyeq)$ is a partially ordered set. By Corollary 6, $(X, \preccurlyeq)$ is noetherian.

Therefore, we can use noetherian induction over $(X, \preccurlyeq)$ to prove the lemma, cf. Lemma 7.

Let $(k,\ell) \in X$. Suppose that the claim is true for every $(i,j) \in X$ with $(i,j) \prec (k,\ell)$. We obtain

$$\begin{aligned}
&\sum_{(U,\{g_2,\ldots,g_{p^\ell}\}) \in \Theta^{(\ell),k}} |\operatorname{Sub}(s-\hat{I},U)| \\
\overset{\text{D. 34.(3)}}{=} &\sum_{M \in \Omega_1^k} \sum_{(U,\{g_2,\ldots,g_{p^\ell}\}) \in (\varphi^{(\ell),k})^{-1}(\{M\})} |\operatorname{Sub}(s-\hat{I},U)| \\
\overset{\text{L. 41}}{=} &\sum_{M \in \Omega_1^k} \sum_{U \in \operatorname{Sub}(s-\ell,\operatorname{Stab}(M))} |\operatorname{Sub}(s-\hat{I},U)| \\
\overset{\text{L. 40}}{=} &\sum_{(V,\{h_2,\ldots,h_{p^k}\}) \in \Theta^{(k),k}} \sum_{U \in \operatorname{Sub}(s-\ell,V)} |\operatorname{Sub}(s-\hat{I},U)|
\end{aligned}$$

$$
\begin{aligned}
&= && \sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k),k}} && |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)| \\
&\overset{\text{D. 34.(3)}}{=} && \sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k)}} && |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)| \\
&\quad - && \sum_{j\in[0,k-1]} \sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k),j}} && |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)| \\
&\overset{\text{D. 34.(1), R. 27}}{=} && && \mathrm{b}(k)\,\mathrm{N}(s-(\{k,\ell\}\cup\hat{I})) \\
&\quad - && \sum_{j\in[0,k-1]} \sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k),j}} && |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)|.
\end{aligned}
$$

For $j\in[0,k-1]$, we have $(j,k)\prec(k,\ell)$ and $\{\ell\}\cup\hat{I}\subseteq[k,s]$, and so

$$
\sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k),j}} |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)| = \sum_{\substack{I\subseteq[0,j]\\ j\in I}} (-1)^{|I|+1}\mathrm{b}(\min I)\,\mathrm{N}(s-(I\sqcup(\{k,\ell\}\cup\hat{I})))
$$

by induction hypothesis. Hence

$$
\begin{aligned}
& \sum_{j\in[0,k-1]} \sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k),j}} && |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)| \\
\overset{\text{IH}}{=}\ & \sum_{j\in[0,k-1]} \sum_{\substack{I\subseteq[0,j]\\ j\in I}} && (-1)^{|I|+1}\mathrm{b}(\min I)\,\mathrm{N}(s-(I\sqcup(\{k,\ell\}\cup\hat{I}))) \\
= & \sum_{\substack{I\subseteq[0,k-1]\\ I\neq\emptyset}} && (-1)^{|I|+1}\mathrm{b}(\min I)\,\mathrm{N}(s-(I\sqcup(\{k,\ell\}\cup\hat{I}))) \\
\overset{I'=I\cup\{k\}}{=}\ & \sum_{\substack{I'\subseteq[0,k]\\ I'\neq\{k\},\ k\in I'}} && (-1)^{|I'|}\mathrm{b}(\min I')\,\mathrm{N}(s-(I'\cup\{\ell\}\cup\hat{I})).
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
& && && \mathrm{b}(k)\,\mathrm{N}(s-(\{k,\ell\}\cup\hat{I})) \\
& - && \sum_{j\in[0,k-1]} \sum_{(V,\{h_2,\dots,h_{p^k}\})\in\Theta^{(k),j}} && |\operatorname{Sub}(s-(\{\ell\}\cup\hat{I}),V)| \\
= & && && \mathrm{b}(k)\,\mathrm{N}(s-(\{k\}\cup\{\ell\}\cup\hat{I})) \\
& - && \sum_{\substack{I'\subseteq[0,k]\\ I'\neq\{k\},\ k\in I'}} && (-1)^{|I'|}\mathrm{b}(\min I')\,\mathrm{N}(s-(I'\cup\{\ell\}\cup\hat{I})) \\
= & && \sum_{\substack{I\subseteq[0,k]\\ k\in I}} && (-1)^{|I|+1}\mathrm{b}(\min I)\,\mathrm{N}(s-(I\cup\{\ell\}\cup\hat{I})),
\end{aligned}
$$

which completes the induction. □

Corollary 44 *Let $\ell \in [0,s]$. Let $k \in [0,\ell]$. We have*

$$|\Theta^{(\ell),k}| = \sum_{\substack{I \subseteq [0,k] \\ k \in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s - (I \cup \{\ell\}))$$

Proof. We have

$$\begin{aligned}
& & |\Theta^{(\ell),k}| & \\
&= \sum_{(U,\{g_2,\dots,g_{p^\ell}\}) \in \Theta^{(\ell),k}} & 1 & \\
&\overset{|U| = p^{s-\ell}}{=} \sum_{(U,\{g_2,\dots,g_{p^\ell}\}) \in \Theta^{(\ell),k}} & |\operatorname{Sub}(s - \{\ell\}, U)| & \\
&\overset{\text{L. 43}}{=} \sum_{\substack{I \subseteq [0,k] \\ k \in I}} & (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s - (I \cup \{\ell\} \cup \{\ell\})) & \\
&= \sum_{\substack{I \subseteq [0,k] \\ k \in I}} & (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s - (I \cup \{\ell\})). & \qquad \square
\end{aligned}$$

Lemma 45 *Let $\ell \in [0,s]$. Let $M \in \Omega_1^\ell$.*

Let

$$\overline{\varphi}^{(\ell),\ell} := \rho_1^\ell \circ \varphi^{(\ell),\ell} : \Theta^{(\ell),\ell} \to \overline{\Omega}^\ell.$$

Note that

$$\begin{aligned}
(U, \{g_2, \dots, g_{p^\ell}\}) &\overset{\varphi^{(\ell),\ell}}{\longmapsto} U \sqcup \bigsqcup_{i \in [2,p^\ell]} U g_i \\
&\overset{\rho_1^\ell}{\longmapsto} [U \sqcup \bigsqcup_{i \in [2,p^\ell]} U g_i] = \overline{\varphi}^{(\ell),\ell}\Big((U, \{g_2, \dots, g_{p^\ell}\})\Big)
\end{aligned}$$

for $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell)}$.

The map $\overline{\varphi}^{(\ell),\ell}$ is surjective; cf. Lemma 36.(2).

(1) *We have $|(\overline{\varphi}^{(\ell),\ell})^{-1}(\{[M]\})| = p^\ell$.*

(2) *We have $a_\ell = |\overline{\Omega}^\ell| = \frac{1}{p^\ell} |\Theta^{(\ell),\ell}|$, cf. Definition* 15.(3).

Proof. Ad (1). By Lemma 40, there exists a unique $(U, \{g_2, \dots, g_{p^\ell}\}) \in \Theta^{(\ell),\ell}$ such that

$$M = U \sqcup \bigsqcup_{i \in [2,p^\ell]} U g_i,$$

where $U = \operatorname{Stab}(M)$.

In the following, let us write $g_1 := 1 \in G$ and $r := p^\ell \in \mathbb{Z}_{\geqslant 1}$.

We define the mapping

$$\begin{aligned}\lambda : [1,r] &\to (\overline{\varphi}^{(\ell),\ell})^{-1}(\{[M]\})\\ k &\mapsto ({}^{g_k^{-1}}U, \{g_{k,2},\dots,g_{k,r}\})\end{aligned}$$

where $\{g_{k,2},\dots,g_{k,r}\} \in \mathrm{Tv}_r({}^{g_k^{-1}}U)$ is such that

$$\{{}^{g_k^{-1}}Ug_{k,2},\dots,{}^{g_k^{-1}}Ug_{k,r}\} = \{{}^{g_k^{-1}}Ug_k^{-1}g_j : j \in [1,r]\setminus\{k\}\}$$

holds.

We *claim* that λ is a well-defined, bijective map.

Well-defined. Let $k \in [1,r]$.

(i) We recall that $(\overline{\varphi}^{(\ell),\ell})^{-1}(\{[M]\}) \subseteq \Theta^{(\ell)} = \coprod_{U\in\mathrm{Sub}(s-\ell)} \mathrm{Tv}_{p^\ell}(U)$, cf. Definition 34.(1).

(a) We have ${}^{g_k^{-1}}U \in \mathrm{Sub}(s-\ell)$ since $|{}^{g_k^{-1}}U| = |U| = p^{s-\ell}$.

(b) Let $j, j' \in [1,r]\setminus\{k\}$ with $j \neq j'$. We have to show ${}^{g_k^{-1}}Ug_k^{-1}g_j \cap {}^{g_k^{-1}}Ug_k^{-1}g_{j'} \overset{!}{=} \emptyset$.

We obtain $g_k^{-1}Ug_j = {}^{g_k^{-1}}Ug_k^{-1}g_j$ and $g_k^{-1}Ug_{j'} = {}^{g_k^{-1}}Ug_k^{-1}g_{j'}$. Since $Ug_j \cap Ug_{j'} = \emptyset$, we have $g_k^{-1}Ug_j \cap g_k^{-1}Ug_{j'} = \emptyset$.

(c) Let $j \in [1,r]\setminus\{k\}$. We have to show ${}^{g_k^{-1}}Ug_k^{-1}g_j \cap {}^{g_k^{-1}}U \overset{!}{=} \emptyset$.

We obtain $g_k^{-1}Ug_j = {}^{g_k^{-1}}Ug_k^{-1}g_j$ and $g_k^{-1}Ug_k = {}^{g_k^{-1}}U$. Since $j \neq k$, we have $Ug_j \cap Ug_k = \emptyset$ and therefore $g_k^{-1}Ug_j \cap g_k^{-1}Ug_k = \emptyset$.

By (a, b, c), we see that the elements of $\{{}^{g_k^{-1}}U\} \sqcup \{{}^{g_k^{-1}}Ug_k^{-1}g_j : j \in [1,r]\setminus\{k\}\}$ are pairwise distinct right-cosets of ${}^{g_k^{-1}}U$.

Therefore, there is a unique $\{g_{k,2},\dots,g_{k,r}\} \in \mathrm{Tv}_r({}^{g_k^{-1}}U)$ satisfying

$$\{{}^{g_k^{-1}}Ug_{k,2},\dots,{}^{g_k^{-1}}Ug_{k,r}\} = \{{}^{g_k^{-1}}Ug_k^{-1}g_j : j \in [1,r]\setminus\{k\}\}.$$

All in all, we have shown that $({}^{g_k^{-1}}U, \{g_{k,2},\dots,g_{k,r}\}) \in \Theta^{(\ell)}$.

(ii) We have to show that $({}^{g_k^{-1}}U, \{g_{k,2},\dots,g_{k,r}\}) \in (\overline{\varphi}^{(\ell),\ell})^{-1}(\{[M]\})$, i.e.

$$\overline{\varphi}^{(\ell),\ell}\Big(({}^{g_k^{-1}}U, \{g_{k,2},\dots,g_{k,r}\})\Big) = [M],$$

i.e.

$$[{}^{g_k^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}Ug_{k,i}] = [M].$$

We obtain

$$\begin{aligned}{}^{g_k^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}Ug_{k,i} &= {}^{g_k^{-1}}U \sqcup \bigsqcup_{j\in[1,r]\setminus\{k\}} {}^{g_k^{-1}}Ug_k^{-1}g_j\\ &= g_k^{-1}(Ug_k \sqcup \bigsqcup_{j\in[1,r]\setminus\{k\}} Ug_j)\\ &= g_k^{-1}(U \sqcup \bigsqcup_{i\in[2,r]} Ug_i)\\ &= g_k^{-1}M.\end{aligned}$$

Hence

$$[{}^{g_k^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}Ug_{k,i}] = [g_k^{-1}M] = [M].$$

Surjective. Let $(\hat{U}, \{\hat{g}_2, \dots, \hat{g}_r\}) \in (\overline{\varphi}^{(\ell),\ell})^{-1}(\{[M]\}) \subseteq \Theta^{(\ell)}$. Then we have

$$\overline{\varphi}^{(\ell),\ell}\Big((\hat{U}, \{\hat{g}_2, \dots, \hat{g}_r\})\Big) = [M] = \overline{\varphi}^{(\ell),\ell}\Big((U, \{g_2, \dots, g_r\})\Big),$$

i.e.

$$[\hat{U} \sqcup \bigsqcup_{i\in[2,r]} \hat{U}\hat{g}_i] = [M] = [U \sqcup \bigsqcup_{i\in[2,r]} Ug_i].$$

Write $\hat{M} := \varphi^{(\ell)}\Big((\hat{U}, \{\hat{g}_2, \dots, \hat{g}_r\})\Big) = \hat{U} \sqcup \bigsqcup_{i\in[2,r]} \hat{U}\hat{g}_i$.

Then $1 \in \hat{M}$ and $|[\hat{M}]| = |[M]| = p^{t-s+\ell}n$, so $\hat{M} \in \Omega_1^\ell$, so $\hat{U} = \mathrm{Stab}(\hat{M})$, cf. Definition 15.(1) and Lemma 37.($2 \Rightarrow 3$).

We have $[\hat{M}] = [M]$, and so $\hat{M} \in [M]$. Thus, we may choose $g \in G$ such that $gM = \hat{M}$.

We have

$$\hat{U} = \mathrm{Stab}(\hat{M}) = \mathrm{Stab}(gM) \overset{\text{R. 14}}{=} {}^g\,\mathrm{Stab}(M) = {}^gU.$$

So $\hat{M} = {}^gU \sqcup \bigsqcup_{i\in[2,r]} {}^gU\hat{g}_i$. Since $gM = \hat{M}$, we have $M = g^{-1}\hat{M}$, i.e.

$$U \sqcup \bigsqcup_{i\in[2,r]} Ug_i = M = g^{-1}\hat{M} = g^{-1}({}^gU \sqcup \bigsqcup_{i\in[2,r]} {}^gU\hat{g}_i) = Ug^{-1} \sqcup \bigsqcup_{i\in[2,r]} Ug^{-1}\hat{g}_i.$$

Again, let us write $g_1 = 1$ and $\hat{g}_1 := 1$ in G. Then

$$\bigsqcup_{j\in[1,r]} Ug_j = \bigsqcup_{j\in[1,r]} Ug^{-1}\hat{g}_j.$$

Then there is a unique $k \in [1, r]$ with $Ug^{-1}\hat{g}_1 = Ug_k$, i.e. $Ug^{-1} = Ug_k$, i.e. $g^{-1} \in Ug_k$, i.e. $g \in g_k^{-1}U$, i.e. we may choose $u \in U$ such that $g = g_k^{-1}u$. So $\hat{M} = gM = g_k^{-1}uM = g_k^{-1}M$ since $u \in U = \mathrm{Stab}(M)$.

We get $\hat{U} = {}^gU = {}^{g_k^{-1}u}U = {}^{g_k^{-1}}U$, and so $\{\hat{g}_2, \dots, \hat{g}_p\} \in \mathrm{Tv}_r(\hat{U}) = \mathrm{Tv}_r({}^{g_k^{-1}}U)$.

We obtain

$$\hat{M} = {}^gU \sqcup \bigsqcup_{i\in[2,r]} {}^gU\hat{g}_i = {}^{g_k^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}U\hat{g}_i$$

and

$$\hat{M} = g_k^{-1}M = g_k^{-1}(\bigsqcup_{j\in[1,r]} Ug_j) = \bigsqcup_{j\in[1,r]} {}^{g_k^{-1}}Ug_k^{-1}g_j = {}^{g_k^{-1}}U \sqcup \bigsqcup_{j\in[1,r]\setminus\{k\}} {}^{g_k^{-1}}Ug_k^{-1}g_j.$$

So

$${}^{g_k^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}U\hat{g}_i = {}^{g_k^{-1}}U \sqcup \bigsqcup_{j\in[1,r]\setminus\{k\}} {}^{g_k^{-1}}Ug_k^{-1}g_j.$$

So

$$\{{}^{g_k^{-1}}U\hat{g}_2, \dots, {}^{g_k^{-1}}U\hat{g}_r\} = \{{}^{g_k^{-1}}Ug_k^{-1}g_j : j \in [1, r] \setminus \{k\}\}.$$

So

$$(\hat{U}, \{\hat{g}_2, \ldots, \hat{g}_r\}) = ({}^{g_k^{-1}}U, \{\hat{g}_2, \ldots, \hat{g}_r\}) = \lambda(k) \in \lambda([1, r]).$$

Injective. Suppose given $k, k' \in [1, r]$ such that $\lambda(k) = \lambda(k')$. That means

$$({}^{g_k^{-1}}U, \{g_{k,2}, \ldots, g_{k,r}\}) = ({}^{g_{k'}^{-1}}U, \{g_{k',2}, \ldots, g_{k',r}\})$$

with $\{g_{k,2}, \ldots, g_{k,r}\} \in \mathrm{Tv}_r({}^{g_k^{-1}}U)$ and $\{g_{k',2}, \ldots, g_{k',r}\} \in \mathrm{Tv}_r({}^{g_{k'}^{-1}}U)$ satisfying

$$\{{}^{g_k^{-1}}Ug_{k,2}, \ldots, {}^{g_k^{-1}}Ug_{k,r}\} = \{{}^{g_k^{-1}}Ug_k^{-1}g_j : j \in [1, r] \setminus \{k\}\}$$

and

$$\{{}^{g_{k'}^{-1}}Ug_{k',2}, \ldots, {}^{g_{k'}^{-1}}Ug_{k',r}\} = \{{}^{g_{k'}^{-1}}Ug_{k'}^{-1}g_j : j \in [1, r] \setminus \{k'\}\}.$$

Then ${}^{g_k^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}Ug_{k,i} = {}^{g_{k'}^{-1}}U \sqcup \bigsqcup_{i\in[2,r]} {}^{g_{k'}^{-1}}Ug_{k',i}$.

We have

$$\begin{aligned}
g_k^{-1}M &= g_k^{-1}(\textstyle\bigsqcup_{j\in[1,r]} Ug_j) \\
&= {}^{g_k^{-1}}U \sqcup \textstyle\bigsqcup_{j\in[1,r]\setminus\{k\}} {}^{g_k^{-1}}Ug_k^{-1}g_j \\
&= {}^{g_k^{-1}}U \sqcup \textstyle\bigsqcup_{i\in[2,r]} {}^{g_k^{-1}}Ug_{k,i} \\
&= {}^{g_{k'}^{-1}}U \sqcup \textstyle\bigsqcup_{i\in[2,r]} {}^{g_{k'}^{-1}}Ug_{k',i} \\
&= {}^{g_{k'}^{-1}}U \sqcup \textstyle\bigsqcup_{j\in[1,r]\setminus\{k'\}} {}^{g_{k'}^{-1}}Ug_{k'}^{-1}g_j \\
&= g_{k'}^{-1}(\textstyle\bigsqcup_{j\in[1,r]} Ug_j) \\
&= g_{k'}^{-1}M.
\end{aligned}$$

We conclude that $g_kg_{k'}^{-1}M = M$, i.e. $g_kg_{k'}^{-1} \in \mathrm{Stab}(M) = U$, i.e. $g_k \in Ug_{k'}$, which means $Ug_k = Ug_{k'}$ and therefore $g_k = g_{k'}$, which yields $k = k'$.

Hence, λ is bijective. This shows the *claim.* The assertion follows.

Ad (2). Each fibre of the map $\overline{\varphi}^{(\ell),\ell} : \Theta^{(\ell),\ell} \to \overline{\Omega}^\ell$ has cardinality p^k by (1). So

$$|\Theta^{(\ell),\ell}| = p^\ell \cdot |\overline{\Omega}^\ell|. \qquad \square$$

Proposition 46 *Let $\ell \in [0, s]$. We have*

$$a_\ell = \tfrac{1}{p^\ell} \sum_{\substack{I\subseteq[0,\ell]\\ \ell\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\,\mathrm{N}(s - I).$$

Proof. We obtain

$$\begin{aligned}
a_\ell &\overset{\text{L. 45.(2)}}{=} \tfrac{1}{p^\ell}|\Theta^{(\ell),\ell}| \\
&\overset{\text{C. 44}}{=} \tfrac{1}{p^\ell} \sum_{\substack{I\subseteq[0,\ell]\\ \ell\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\,\mathrm{N}(s - (I \cup \{\ell\})) \\
&= \tfrac{1}{p^\ell} \sum_{\substack{I\subseteq[0,\ell]\\ \ell\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\,\mathrm{N}(s - I). \qquad \square
\end{aligned}$$

5 Counting p-subgroups

5.1 The sieve formula

Theorem 47 *Recall that G is a finite group of order $|G| = p^t n$.*

Let $s \in [0,t]$. Let $\ell \in [0,s]$.

Recall that, given $I = \{c_1, \ldots, c_k\} \subseteq [0,\ell]$ where $c_1 < \ldots < c_k$, we denote by $\mathrm{N}(s-I)$ the number of chains of p-subgroups $U_1 \leqslant \ldots \leqslant U_k \leqslant G$, where $U_1 \in \mathrm{Sub}(s-c_1), \ldots, U_k \in \mathrm{Sub}(s-c_k)$, cf. Definition 8.(2).

We have

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s-I) \equiv_{p^{\ell+1}} 1.$$

Proof. Claim. We have

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} (\mathrm{N}(s-I) - 1) \equiv_{p^{\ell+1}} 0.$$

Write $f(J) := (-1)^{|I|+1}(\mathrm{N}(J)-1) \in \mathbb{Z}$ for $J \subseteq [s-\ell, s]$.

The claim amounts to showing

$$(\diamond_{\ell,s}) \qquad \sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} f(s-I) \stackrel{!}{\equiv}_{p^{\ell+1}} 0.$$

Let $X := \{(\ell, s) \in \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0} : \ell \leqslant s \leqslant t\}$. For $(\ell, s), (\ell', s') \in X$, we define:

$$(\ell, s) \preccurlyeq (\ell', s') \ :\Leftrightarrow \ \ell \leqslant \ell' \text{ and } s \leqslant s'.$$

Then $(X, \preccurlyeq)$ is a partially ordered set. By Corollary 6, $(X, \preccurlyeq)$ is noetherian.

Therefore, we can use Noetherian induction over $(X, \preccurlyeq)$ to prove $(\diamond_{\ell,s})$ for $(\ell, s) \in X$, cf. Lemma 7.

Suppose given $(\ell, s) \in X$. We may suppose that

$$(\diamond_{\ell',s'}) \qquad \sum_{\substack{I \subseteq [0,\ell'] \\ I \neq \emptyset}} f(s'-I) \equiv_{p^{\ell'+1}} 0$$

holds for $(\ell', s') \in X$ with $(\ell', s') \prec (\ell, s)$. We have to show $(\diamond_{\ell,s})$.

Induction step. By Remark 18, we have

$$q \equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} a_k p^k$$

where

$$a_k = \tfrac{1}{p^k} \sum_{\substack{I\subseteq[0,k]\\ k\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s-I)$$

for $k \in [0, \ell]$, thanks to Proposition 46. Then

$$\begin{aligned}
q &\equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} a_k p^k \\
&= \sum_{k\in[0,\ell]} \sum_{\substack{I\subseteq[0,k]\\ k\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s-I) \\
&= \sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s-I) \\
&= \sum_{k\in[0,\ell]} \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1} \cdot \mathrm{b}(\min I)\, \mathrm{N}(s-I) \\
&= \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}\, \mathrm{N}(s-I).
\end{aligned}$$

Considering the cyclic group $C := \mathrm{C}_{p^t n}$ with $p^t n$ elements, we have $\mathrm{N}_{C,p}(s-I) = 1$ for $I \subseteq [0, \ell]$ and therefore

$$q \equiv_{p^{\ell+1}} \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}.$$

So

$$\begin{aligned}
0 &\equiv_{p^{\ell+1}} \left(\sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}\, \mathrm{N}(s-I)\right) - q \\
&\equiv_{p^{\ell+1}} \left(\sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}\, \mathrm{N}(s-I)\right) - \left(\sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1}\right) \\
&= \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} (-1)^{|I|+1} (\mathrm{N}(s-I) - 1) \\
&= \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I).
\end{aligned}$$

Subclaim. We have

$$\sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I) \equiv_{p^{\ell+1}} \left(\sum_{k\in[0,\ell-j-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell-j)\left(\sum_{\substack{I\subseteq[\ell-j,\ell]\\ I\neq\emptyset}} f(s-I)\right).$$

for $j \in [0, \ell]$.

To prove the subclaim, we proceed by induction on j. For the base case $j = 0$, we obtain

$$\sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I) = \left(\sum_{k\in[0,\ell-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell)\left(\sum_{\substack{I\subseteq[\ell,\ell]\\ I\neq\emptyset}} f(s-I)\right).$$

Let $j \in [0, \ell - 1]$. Suppose that the statement holds for j. We show the statement for $j + 1$.

We see that

$$\begin{aligned}
&\sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\\
\overset{\mathsf{IH}}{\equiv}_{p^{\ell+1}} \quad &\left(\sum_{k\in[0,\ell-j-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell-j)\left(\sum_{\substack{I\subseteq[\ell-j,\ell]\\ I\neq\emptyset}} f(s-I)\right)\\
= \quad &\left(\sum_{k\in[0,\ell-j-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell-j)\left(\sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I)\right).
\end{aligned}$$

We have $(j, s-(\ell-j)) \prec (\ell, s)$. Since

$$(\diamond_{j,s-(\ell-j)}) \qquad \sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I) \equiv_{p^{j+1}} 0$$

holds thanks to our outer induction hypothesis of the proof of the claim, and since

$$\mathrm{b}(\ell-j) \equiv_{p^{\ell-j}} \mathrm{b}(\ell-j-1)$$

thanks to Lemma 28, we conclude that

$$\mathrm{b}(\ell-j)\left(\sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I)\right) \equiv_{p^{\ell+1}} \mathrm{b}(\ell-j-1)\left(\sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I)\right).$$

So we may continue to get

$$\begin{aligned}
& \left(\sum_{k\in[0,\ell-j-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell-j)\left(\sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I)\right) \\
\equiv_{p^{\ell+1}} \quad & \left(\sum_{k\in[0,\ell-j-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell-j-1)\left(\sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I)\right) \\
= \quad & \left(\sum_{k\in[0,\ell-j-2]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) \\
& + \quad \mathrm{b}(\ell-j-1)\left(\sum_{\substack{I\subseteq[\ell-j-1,\ell]\\ \ell-j-1\in I}} f(s-I) + \sum_{\substack{I\subseteq[0,j]\\ I\neq\emptyset}} f((s-(\ell-j))-I)\right) \\
= \quad & \left(\sum_{k\in[0,\ell-j-2]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) \\
& + \quad \mathrm{b}(\ell-j-1)\left(\sum_{\substack{I\subseteq[\ell-j-1,\ell]\\ \ell-j-1\in I}} f(s-I) + \sum_{\substack{I\subseteq[\ell-j,\ell]\\ I\neq\emptyset}} f(s-I)\right) \\
= \quad & \left(\sum_{k\in[0,\ell-j-2]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(\ell-j-1)\left(\sum_{\substack{I\subseteq[\ell-j-1,\ell]\\ I\neq\emptyset}} f(s-I)\right).
\end{aligned}$$

This shows the subclaim. Using the subclaim for $j=\ell$ yields

$$\begin{aligned}
0 \quad \equiv_{p^{\ell+1}} \quad & \sum_{k\in[0,\ell]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I) \\
\equiv_{p^{\ell+1}} \quad & \left(\sum_{k\in[0,-1]} \mathrm{b}(k) \sum_{\substack{I\subseteq[k,\ell]\\ k\in I}} f(s-I)\right) + \mathrm{b}(0)\left(\sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} f(s-I)\right) \\
= \quad & \sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} f(s-I) \\
= \quad & \sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} (-1)^{|I|+1}(\mathrm{N}(s-I)-1).
\end{aligned}$$

This shows the *claim*.

To simplify the term further, note that

$$\sum_{\substack{I\subseteq[0,\ell]\\ I\neq\emptyset}} (-1)^{|I|+1} = 1 - \sum_{I\subseteq[0,\ell]} (-1)^{|I|} = 1 - \sum_{m\in[0,\ell]} (-1)^m \binom{\ell}{m} = 1.$$

So

$$0 \equiv_{p^{\ell+1}} \sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} (\mathrm{N}(s-I) - 1) = \left(\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s-I) \right) - 1,$$

i.e.

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s-I) \equiv_{p^{\ell+1}} 1. \qquad \square$$

Remark 48 Theorem 47 has formal similarities with the sieve formula from set theory: Let X be a finite set and $Y_0, \ldots, Y_\ell \subseteq X$ be subsets such that $X = \bigcup_{k \in [0,\ell]} Y_k$. Let

$$Y_I := \bigcap_{i \in I} Y_i$$

for $I \subseteq [0,\ell]$. Then

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} |Y_I| = |X|.$$

Remark 49 Let $s \in [0,t]$. Consider the case $\ell = s$ in Theorem 47. We have

$$\begin{aligned}
& \sum_{I \subseteq [0,s]} (-1)^{|I|+1} \mathrm{N}(s-I) \\
= \quad & \sum_{\substack{I \subseteq [0,s] \\ s \in I}} (-1)^{|I|+1} \mathrm{N}(s-I) + \sum_{\substack{I \subseteq [0,s] \\ s \notin I}} (-1)^{|I|+1} \mathrm{N}(s-I) \\
= \quad & \sum_{I \subseteq [0,s-1]} (-1)^{|I|+1} \mathrm{N}(s-(I \sqcup \{s\})) + \sum_{I \subseteq [0,s-1]} (-1)^{|I|} \mathrm{N}(s-I) \\
\overset{\text{R. 10}}{=} \quad & \sum_{I \subseteq [0,s-1]} (-1)^{|I|+1} \mathrm{N}(s-I) + \sum_{I \subseteq [0,s-1]} (-1)^{|I|} \mathrm{N}(s-I) \\
= \quad & 0,
\end{aligned}$$

i.e.

$$\sum_{\substack{I \subseteq [0,s] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s-I) = 1.$$

5.2 A shortcut using Sylow?

Remark 50 One could ask whether the formula from Theorem 47 follows directly by the Theorem of Sylow-Frobenius.

We have

$$\mathrm{N}(s-\ell) - 1 \equiv_p 0$$

for $\ell \in [0,s]$, cf. Theorem 22, and therefore

$$\prod_{k\in[0,\ell]} (\mathrm{N}(s-k)-1) = \sum_{I\subseteq[0,\ell]} (-1)^{|I|} \prod_{i\in I} \mathrm{N}(s-i) \equiv_{p^{\ell+1}} 0$$

for $\ell \in [0,s]$.

We consider some cases.

(1) Let $\ell = 1$. Then

$$\begin{array}{lll} & \sum_{I\subseteq[0,1]}(-1)^{|I|}\prod_{i\in I}\mathrm{N}(s-i) \\ = & (-1)^0\cdot 1 + (-1)^1(\mathrm{N}(s)+\mathrm{N}(s{-}1)) + (-1)^2\,\mathrm{N}(s{-}1)\,\mathrm{N}(s) \\ \equiv_{p^2} & 0, \end{array}$$

i.e.

$$\mathrm{N}(s) + \mathrm{N}(s{-}1) - \mathrm{N}(s{-}1)\,\mathrm{N}(s) \equiv_{p^2} 1.$$

By Theorem 47, we have

$$\mathrm{N}(s) + \mathrm{N}(s{-}1) - \mathrm{N}(s{-}1,s) \equiv_{p^2} 1.$$

Hence

$$\mathrm{N}(s{-}1)\,\mathrm{N}(s) \equiv_{p^2} \mathrm{N}(s{-}1,s).$$

(2) Let $\ell = 2$. Then

$$\begin{array}{lll} & \sum_{I\subseteq[0,2]}(-1)^{|I|}\prod_{i\in I}\mathrm{N}(s-i) \\ = & (-1)^0\cdot 1 + (-1)^1(\mathrm{N}(s)+\mathrm{N}(s{-}1)+\mathrm{N}(s{-}2)) \\ & \quad + (-1)^2(\mathrm{N}(s{-}1)\,\mathrm{N}(s) + \mathrm{N}(s{-}2)\,\mathrm{N}(s) + \mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1)) \\ & \quad + (-1)^3\mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1)\,\mathrm{N}(s) \\ \equiv_{p^3} & 0, \end{array}$$

i.e.

$$\begin{array}{l} \mathrm{N}(s) + \mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) - \mathrm{N}(s{-}1)\,\mathrm{N}(s) \\ \quad - \mathrm{N}(s{-}2)\,\mathrm{N}(s) - \mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1) + \mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1)\,\mathrm{N}(s) \equiv_{p^3} 1. \end{array}$$

By Theorem 47, we have

$$\begin{array}{l} \mathrm{N}(s) + \mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) - \mathrm{N}(s{-}1,s) \\ \quad - \mathrm{N}(s{-}2,s) - \mathrm{N}(s{-}2,s{-}1) + \mathrm{N}(s{-}2,s{-}1,s) \equiv_{p^3} 1. \end{array}$$

Hence

$$\begin{array}{ll} & \mathrm{N}(s{-}1)\,\mathrm{N}(s) + \mathrm{N}(s{-}2)\,\mathrm{N}(s) + \mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1) - \mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1)\,\mathrm{N}(s) \\ \equiv_{p^3} & \mathrm{N}(s{-}1,s) + \mathrm{N}(s{-}2,s) + \mathrm{N}(s{-}2,s{-}1) - \mathrm{N}(s{-}2,s{-}1,s). \end{array}$$

This congruence does not necessarily imply that

$$\mathrm{N}(s{-}2)\,\mathrm{N}(s{-}1)\,\mathrm{N}(s) \equiv_{p^3} \mathrm{N}(s{-}2, s{-}1, s).$$

For instance, if we take $G = \mathrm{S}_5$, $p = 2$ and $s = 3$, then Magma gives

$$\mathrm{N}_{\mathrm{S}_5,2}(1) = 25, \quad \mathrm{N}_{\mathrm{S}_5,2}(2) = 35, \quad \mathrm{N}_{\mathrm{S}_5,2}(3) = 15,$$

and

$$\mathrm{N}_{\mathrm{S}_5,2}(1, 2, 3) = 105,$$

but $25 \cdot 35 \cdot 15 = 13125 \equiv_8 5 \not\equiv_8 1 \equiv_8 105$.

(3) The example in (2) shows that we do not have the congruence

$$\prod_{i \in I} \mathrm{N}(i) \equiv_{p^{|I|}} \mathrm{N}(I)$$

for $\emptyset \neq I \subseteq [0, t]$ in general.

So it seems to be impossible to conclude Theorem 47 from Theorem 22 solely.

6 Examples

In the following, we will discuss Theorem 47 for certain values of ℓ. We will give direct proofs for $\ell \in \{1, 2\}$, which is possible without induction and which might be useful for one who is interested in these particular cases.

6.1 Case $\ell = 0$

Let $s \in [0, t]$.

Recall that $\Omega^0 = \{M \in \Omega : |[M]| = p^{t-s}n\}$, cf. Definition 15.(1).

Remark 51 Recall that $a_0 = |\overline{\Omega}^0|$, cf. Definition 15.(3).

We have

$$a_0 = \mathrm{N}(s),$$

either by Lemma 20 or by Proposition 46. The congruence

$$\mathrm{N}(s) \equiv_p 1$$

follows from Theorem 22 or from Theorem 47.

So the number $\mathrm{N}(s)$ of subgroups U of G with $|U| = p^s$ is congruent to 1 modulo p.

This congruence is the statement of the Theorem of Sylow-Frobenius [**8,** Th. II].

6.2 Case $\ell = 1$

Let $s \in [1, t]$.

Recall that $\Omega_1^k = \{M \in \Omega : 1 \in M,\ |[M]| = p^{t-s+k}n\}$ for $k \in [0, 1]$, cf. Definitions 29.(1) and 15.(1).

We have the following situation, cf. Definition 34.

$$\begin{array}{ccccccc}
 & & \Theta^{(1)} & = & \Theta^{(1),0} & \sqcup & \Theta^{(1),1} \\
 & & \downarrow{\scriptstyle \varphi^{(1)}} & & \downarrow{\scriptstyle \varphi^{(1),0}} & & \downarrow{\scriptstyle \varphi^{(1),1}} \\
\Omega & \supseteq & \Omega_1^{[0,1]} & = & \Omega_1^0 & \sqcup & \Omega_1^1 \\
\downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho_1^{[0,1]}} & & \downarrow{\scriptstyle \rho_1^0} & & \downarrow{\scriptstyle \rho_1^1} \\
\overline{\Omega} & \supseteq & \overline{\Omega}^{[0,1]} & = & \overline{\Omega}^0 & \sqcup & \overline{\Omega}^1
\end{array}$$

Remark 52 Recall that $a_1 = |\overline{\Omega}^1|$, cf. Definition 15.(3). We have

$$a_1 = \tfrac{1}{p}(\mathrm{b}(1)\,\mathrm{N}(s-1) - \mathrm{N}(s-1,s)),$$

cf. Proposition 46.

We can also see this by a direct calculation, obtaining

$$\begin{array}{lll}
a_1 & \overset{\text{D. 15.(3)}}{=} & |\overline{\Omega}^1| \\
 & \overset{\text{L. 45.(2)}}{=} & \tfrac{1}{p}|\Theta^{(1),1}| \\
 & \overset{\text{D. 34.(3)}}{=} & \tfrac{1}{p}(|\Theta^{(1)}| - |\Theta^{(1),0}|) \\
 & \overset{\text{D. 34.(1)}}{=} & \tfrac{1}{p}(\mathrm{b}(1)\,\mathrm{N}(s-1) - |\Theta^{(1),0}|) \\
 & \overset{\text{L. 39}}{=} & \tfrac{1}{p}(\mathrm{b}(1)\,\mathrm{N}(s-1) - \mathrm{N}(s-1,s)).
\end{array}$$

Remark 53 *We have*

$$\mathrm{N}(s) + \mathrm{N}(s-1) - \mathrm{N}(s-1,s) \equiv_{p^2} 1.$$

Proof. By Remark 18, we have

$$q \equiv_{p^2} a_0 + a_1 p,$$

where

$$a_0 = \mathrm{N}(s),$$

and

$$a_1 = \tfrac{1}{p}(\mathrm{b}(1)\,\mathrm{N}(s-1) - \mathrm{N}(s-1,s)),$$

thanks to Remarks 51 and 52.

Then

$$\begin{array}{lll}
q & \equiv_{p^2} & a_0 + a_1 p \\
 & = & \mathrm{N}(s) + \mathrm{b}(1)\,\mathrm{N}(s-1) - \mathrm{N}(s-1,s).
\end{array}$$

Considering $C := \mathrm{C}_{p^t n}$, we get

$$q \equiv_{p^2} \mathrm{N}_{C,p}(s) + \mathrm{b}(1)\,\mathrm{N}_{C,p}(s-1) - \mathrm{N}_{C,p}(s-1,s) = 1 + \mathrm{b}(1) - 1.$$

Since $\mathrm{b}(1) \equiv_p \mathrm{b}(0) = 1$ by Lemma 28 and $\mathrm{N}(s-1) \equiv_p 1$ by Theorem 22, we conclude that

$$\begin{aligned} 0 &\equiv_{p^2} (\mathrm{N}(s)-1) + \mathrm{b}(1)(\mathrm{N}(s-1)-1) - (\mathrm{N}(s-1,s)-1) \\ &\equiv_{p^2} (\mathrm{N}(s)-1) + 1 \cdot (\mathrm{N}(s-1)-1) - (\mathrm{N}(s-1,s)-1) \\ &\equiv_{p^2} \mathrm{N}(s) - 1 + \mathrm{N}(s-1) - \mathrm{N}(s-1,s). \end{aligned}$$

□

Note that e.g. for $p = 2$ and $s \in [1, t-1]$, we get

$$\mathrm{b}(1) = \binom{2^{t-s+1}n - 1}{2-1} = 2^{t-s+1}n - 1 \equiv_{2^2} 3.$$

Example 54 The following examples have been obtained using the computer algebra system Magma [**2**].

(1) Let $G = \mathrm{S}_3$ and $p = 2$. Magma gives the following.

$$\mathrm{N}(1) = 3, \qquad \mathrm{N}(0) = 1, \qquad \mathrm{N}(0,1) = 3.$$

Then we get the following result for $s = 1$.

$$\mathrm{N}(1) + \mathrm{N}(0) - \mathrm{N}(0,1) = 3 + 1 - 3 = 1 \equiv_4 1,$$

Cf. also Remark 10.

(2) Let $G = \mathrm{S}_4$ and $p = 2$. Magma gives the following.

$$\begin{aligned} \mathrm{N}(3) = 3, \qquad & \mathrm{N}(2) = 7\ , \qquad & \mathrm{N}(1) = 9, \qquad & \mathrm{N}(0) = 1, \\ \mathrm{N}(2,3) = 9, \qquad & \mathrm{N}(1,2) = 15, \qquad & \mathrm{N}(0,1) = 9. & \end{aligned}$$

Cf. also Example 9.

Then we get the following results for $s = 3$, $s = 2$ and $s = 1$, respectively.

$$\begin{aligned} \mathrm{N}(3) + \mathrm{N}(2) - \mathrm{N}(2,3) &= 3 + 7 - 9 &&= 1 &&\equiv_4 1, \\ \mathrm{N}(2) + \mathrm{N}(1) - \mathrm{N}(1,2) &= 7 + 9 - 15 &&= 1 &&\equiv_4 1, \\ \mathrm{N}(1) + \mathrm{N}(0) - \mathrm{N}(0,1) &= 9 + 1 - 9 &&= 1 &&\equiv_4 1. \end{aligned}$$

(3) Let $G = \mathrm{S}_6$ and $p = 3$. Then $|G| = 720 = 3^2 \cdot 80$. Therefore, we have $t = 2$ and $n = 80$.

We choose $s = 2 \in [1, 2]$. Magma gives the following.

$$\mathrm{N}_{\mathrm{S}_6,3}(2) = 10, \qquad \mathrm{N}_{\mathrm{S}_6,3}(1) = 40, \qquad \mathrm{N}_{\mathrm{S}_6,3}(1,2) = 40.$$

Then

$$\mathrm{N}_{\mathrm{S}_6,3}(2) + \mathrm{N}_{\mathrm{S}_6,3}(1) - \mathrm{N}_{\mathrm{S}_6,3}(1,2) = 10 + 40 - 40 = 10 \equiv_9 1.$$

Note that $10 \not\equiv_{27} 1$.

(4) We have

$$\mathrm{N}_{\mathrm{A}_5,2}(2) + \mathrm{N}_{\mathrm{A}_5,2}(1) - \mathrm{N}_{\mathrm{A}_5,2}(1,2) = 5 + 15 - 15 = 5 \equiv_4 1.$$

Note that $5 \not\equiv_8 1$.

(5) We have

$$\mathrm{N}_{\mathrm{A}_6,2}(3) + \mathrm{N}_{\mathrm{A}_5,6}(2) - \mathrm{N}_{\mathrm{A}_6,2}(2,3) = 45 + 75 - 135 = -15 \equiv_4 1.$$

(6) We have

$$\mathrm{N}_{\mathrm{GL}_3(\mathbb{F}_2),2}(2) + \mathrm{N}_{\mathrm{GL}_3(\mathbb{F}_2),2}(1) - \mathrm{N}_{\mathrm{GL}_3(\mathbb{F}_2),2}(1,2) = 35 + 21 - 63 = -7 \equiv_4 1.$$

(7) We have

$$\mathrm{N}_{\mathrm{GL}_3(\mathbb{F}_5),2}(5) + \mathrm{N}_{\mathrm{GL}_3(\mathbb{F}_5),2}(4) - \mathrm{N}_{\mathrm{GL}_3(\mathbb{F}_5),2}(4,5) = 15 + 35 - 45 = 5 \equiv_4 1.$$

(8) We have

$$\mathrm{N}_{\mathrm{SL}_3(\mathbb{F}_3),2}(2) + \mathrm{N}_{\mathrm{SL}_3(\mathbb{F}_3),2}(1) - \mathrm{N}_{\mathrm{SL}_3(\mathbb{F}_3),2}(1,2) = 585 + 117 - 1053 = -351 \equiv_4 1.$$

(9) We consider the Mathieu group

$$\mathrm{M}_{11} := \langle (1,2,3,4,5,6,7,8,9,10,11), (3,7,11,8)(4,10,5,6) \rangle \leqslant \mathrm{S}_{11}\,.$$

Note that $|\,\mathrm{M}_{11}\,| = 7920 = 2^4 \cdot 495$. We have

$$\mathrm{N}_{\mathrm{M}_{11},2}(4) + \mathrm{N}_{\mathrm{M}_{11},2}(3) - \mathrm{N}_{\mathrm{M}_{11},2}(3,4) = 495 + 1155 - 1485 = 165 \equiv_4 1.$$

6.3 Case $\ell = 2$

Let $s \in [2,t]$.

Recall that $\Omega_1^k = \{M \in \Omega : 1 \in M,\ |[M]| = p^{t-s+k}n\}$ for $k \in [0,2]$, cf. Definitions 29.(1) and 15.(1).

We have the following situation, cf. Definition 34.

$$\begin{array}{ccccccccccc}
 & & \Theta^{(2)} & = & \Theta^{(2),0} & \sqcup & \Theta^{(2),1} & \sqcup & \Theta^{(2),2} \\
 & & \downarrow{\scriptstyle \varphi^{(2)}} & & \downarrow{\scriptstyle \varphi^{(2),0}} & & \downarrow{\scriptstyle \varphi^{(2),1}} & & \downarrow{\scriptstyle \varphi^{(2),2}} \\
\Omega & \supseteq & \Omega_1^{[0,2]} & = & \Omega_1^0 & \sqcup & \Omega_1^1 & \sqcup & \Omega_1^2 \\
\downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \rho_1^{[0,2]}} & & \downarrow{\scriptstyle \rho_1^0} & & \downarrow{\scriptstyle \rho_1^1} & & \downarrow{\scriptstyle \rho_1^2} \\
\overline{\Omega} & \supseteq & \overline{\Omega}^{[0,2]} & = & \overline{\Omega}^0 & \sqcup & \overline{\Omega}^1 & \sqcup & \overline{\Omega}^2
\end{array}$$

Remark 55 Recall that $a_2 = |\overline{\Omega}^2|$, cf. Definition 15.(3). We have

$$a_2 = \tfrac{1}{p^2}(\mathrm{b}(2)\,\mathrm{N}(s-2) - \mathrm{N}(s-2,s) - \mathrm{b}(1)\,\mathrm{N}(s-2,s-1) + \mathrm{N}(s-2,s-1,s)),$$

cf. Proposition 46.

We can also see this by a direct calculation.

First, note that

$$\begin{aligned}
|\Theta^{(2),1}| &\overset{\text{D. 34.(3)}}{=} \sum_{M\in\Omega_1^1} |(\varphi^{(2),1})^{-1}(\{M\})| \\
&\overset{\text{L. 41}}{=} \sum_{M\in\Omega_1^1} |\operatorname{Sub}(s-2,\operatorname{Stab}(M))| \\
&\overset{\text{L. 40}}{=} \sum_{(U,\{g_2,\ldots,g_p\})\in\Theta^{(1),1}} |\operatorname{Sub}(s-2,U)| \\
&\overset{\text{D. 34.(3)}}{=} \sum_{(U,\{g_2,\ldots,g_p\})\in\Theta^{(1)}} |\operatorname{Sub}(s-2,U)| \\
&\quad - \sum_{(U,\{g_2,\ldots,g_p\})\in\Theta^{(1),0}} |\operatorname{Sub}(s-2,U)| \\
&\overset{\text{D. 34.(1), R. 27}}{=} \sum_{U\in\mathrm{Sub}(s-1)} \mathrm{b}(1)|\operatorname{Sub}(s-2,U)| \\
&\quad - \sum_{(U,\{g_2,\ldots,g_p\})\in\Theta^{(1),0}} |\operatorname{Sub}(s-2,U)| \\
&\overset{\text{L. 39}}{=} \sum_{U\in\mathrm{Sub}(s-1)} \mathrm{b}(1)|\operatorname{Sub}(s-2,U)| \\
&\quad - \sum_{(U,V)\in\mathrm{Sub}(s-1,s)} |\operatorname{Sub}(s-2,U)| \\
&\overset{\text{D. 8.(2)}}{=} \mathrm{b}(1)\,\mathrm{N}(s-2,s-1) - \mathrm{N}(s-2,s-1,s),
\end{aligned}$$

cf. also Corollary 44. Then

$$\begin{aligned}
a_2 &\overset{\text{D. 15.(3)}}{=} |\overline{\Omega}^2| \\
&\overset{\text{L. 45.(2)}}{=} \tfrac{1}{p^2}|\Theta^{(2),2}| \\
&\overset{\text{D. 34.(3)}}{=} \tfrac{1}{p^2}(|\Theta^{(2)}| - |\Theta^{(2),0}| - |\Theta^{(2),1}|) \\
&\overset{\text{D. 34.(1)}}{=} \tfrac{1}{p^2}(\mathrm{b}(2)\,\mathrm{N}(s-2) - |\Theta^{(2),0}| - |\Theta^{(2),1}|) \\
&\overset{\text{L. 39}}{=} \tfrac{1}{p^2}(\mathrm{b}(2)\,\mathrm{N}(s-2) - \mathrm{N}(s-2,s) - |\Theta^{(2),1}|) \\
&= \tfrac{1}{p^2}(\mathrm{b}(2)\,\mathrm{N}(s-2) - \mathrm{N}(s-2,s) \\
&\qquad - (\mathrm{b}(1)\,\mathrm{N}(s-2,s-1) - \mathrm{N}(s-2,s-1,s))).
\end{aligned}$$

Remark 56 *We have*

$$\begin{aligned} 1 \equiv_{p^3} \quad & \mathrm{N}(s) + \mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) \\ & - \mathrm{N}(s{-}1, s) - \mathrm{N}(s{-}2, s) - \mathrm{N}(s{-}2, s{-}1) \\ & + \mathrm{N}(s{-}2, s{-}1, s). \end{aligned}$$

Proof. By Remark 18, we have

$$q \equiv_{p^3} a_0 + a_1 p + a_2 p^2,$$

where

$$a_0 = \mathrm{N}(s),$$
$$a_1 = \tfrac{1}{p}(\mathrm{b}(1)\,\mathrm{N}(s{-}1) - \mathrm{N}(s{-}1, s)),$$

and

$$a_2 = \tfrac{1}{p^2}(\mathrm{b}(2)\,\mathrm{N}(s{-}2) - \mathrm{N}(s{-}2, s) - \mathrm{b}(1)\,\mathrm{N}(s{-}2, s{-}1) + \mathrm{N}(s{-}2, s{-}1, s)),$$

thanks to Remarks 51, 52 and 55.

Then

$$\begin{aligned} q \quad & \equiv_{p^3} \quad a_0 + a_1 p + a_2 p^2 \\ & \equiv_{p^3} \quad \mathrm{N}(s) + \mathrm{b}(1)\,\mathrm{N}(s{-}1) - \mathrm{N}(s{-}1, s) \\ & \qquad\qquad + \mathrm{b}(2)\,\mathrm{N}(s{-}2) - \mathrm{N}(s{-}2, s) \\ & \qquad\qquad - \mathrm{b}(1)\,\mathrm{N}(s{-}2, s{-}1) + \mathrm{N}(s{-}2, s{-}1, s). \end{aligned}$$

Considering $C := \mathrm{C}_{p^t n}$, we get

$$\begin{aligned} q \quad & \equiv_{p^3} \quad \mathrm{N}_{C,p}(s) + \mathrm{b}(1)\,\mathrm{N}_{C,p}(s{-}1) - \mathrm{N}_{C,p}(s{-}1, s) \\ & \qquad\qquad + \mathrm{b}(2)\,\mathrm{N}_{C,p}(s{-}2) - \mathrm{N}_{C,p}(s{-}2, s) \\ & \qquad\qquad - \mathrm{b}(1)\,\mathrm{N}_{C,p}(s{-}2, s{-}1) + \mathrm{N}_{C,p}(s{-}2, s{-}1, s) \\ & = \quad 1 + \mathrm{b}(1) - 1 + \mathrm{b}(2) - 1 - \mathrm{b}(1) + 1. \end{aligned}$$

So

$$\begin{aligned} 0 \quad \equiv_{p^3} \quad & (\mathrm{N}(s) - 1) + \mathrm{b}(1)(\mathrm{N}(s{-}1) - 1) - (\mathrm{N}(s{-}1, s) - 1) \\ & + \mathrm{b}(2)(\mathrm{N}(s{-}2) - 1) - (\mathrm{N}(s{-}2, s) - 1) \\ & - \mathrm{b}(1)(\mathrm{N}(s{-}2, s{-}1) - 1) + (\mathrm{N}(s{-}2, s{-}1, s) - 1). \end{aligned}$$

Since $\mathrm{b}(2) \equiv_{p^2} \mathrm{b}(1)$ by Lemma 28 and $\mathrm{N}(s-2) \equiv_p 1$ by Theorem 22, we conclude that

$$\begin{aligned} & (\mathrm{N}(s) - 1) + \mathrm{b}(1)(\mathrm{N}(s{-}1) - 1) - (\mathrm{N}(s{-}1, s) - 1) \\ & \qquad + \mathrm{b}(2)(\mathrm{N}(s{-}2) - 1) - (\mathrm{N}(s{-}2, s) - 1) \\ & \qquad - \mathrm{b}(1)(\mathrm{N}(s{-}2, s{-}1) - 1) + (\mathrm{N}(s{-}2, s{-}1, s) - 1) \\ \equiv_{p^3} \quad & (\mathrm{N}(s) - 1) + \mathrm{b}(1)(\mathrm{N}(s{-}1) - 1) - (\mathrm{N}(s{-}1, s) - 1) \\ & \qquad + \mathrm{b}(1)(\mathrm{N}(s{-}2) - 1) - (\mathrm{N}(s{-}2, s) - 1) \\ & \qquad - \mathrm{b}(1)(\mathrm{N}(s{-}2, s{-}1) - 1) + (\mathrm{N}(s{-}2, s{-}1, s) - 1) \\ = \quad & \mathrm{N}(s) - \mathrm{N}(s{-}1, s) - \mathrm{N}(s{-}2, s) + \mathrm{N}(s{-}2, s{-}1, s) \\ & \qquad + \mathrm{b}(1)(\mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) - \mathrm{N}(s{-}2, s{-}1) - 1). \end{aligned}$$

Since $\mathrm{b}(1) \equiv_p \mathrm{b}(0) = 1$ by Lemma 28 and

$$\mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) - \mathrm{N}(s{-}2, s{-}1) \equiv_{p^2} 1$$

by Remark 53, we conclude that

$$\begin{aligned} & \mathrm{N}(s) - \mathrm{N}(s{-}1, s) - \mathrm{N}(s{-}2, s) + \mathrm{N}(s{-}2, s{-}1, s) \\ & \quad + \mathrm{b}(1)(\mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) - \mathrm{N}(s{-}2, s{-}1) - 1) \\ \equiv_{p^3} \ & \mathrm{N}(s) - \mathrm{N}(s{-}1, s) - \mathrm{N}(s{-}2, s) + \mathrm{N}(s{-}2, s{-}1, s) \\ & \quad + \mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) - \mathrm{N}(s{-}2, s{-}1) - 1. \end{aligned}$$

Hence

$$\begin{aligned} 1 \ \equiv_{p^3} \quad & \mathrm{N}(s) + \mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) \\ & - \mathrm{N}(s{-}1, s) - \mathrm{N}(s{-}2, s) - \mathrm{N}(s{-}2, s{-}1) \\ & + \mathrm{N}(s{-}2, s{-}1, s). \end{aligned}$$

□

Example 57 Let

$$G = \mathrm{F}_9 = \langle a, b, c \mid a^3,\, b^3,\, c^3,\, [a, b],\, a^c = b, b^c = ab^2 \rangle \backsimeq (\mathrm{C}_3 \times \mathrm{C}_3) \rtimes \mathrm{C}_8$$

be the Frobenius group of order 72.

Let $p = 2$. Then Magma produces the following result for $s = 3$.

$$\begin{aligned} & \mathrm{N}(3) + \mathrm{N}(2) + \mathrm{N}(1) - \mathrm{N}(2, 3) - \mathrm{N}(1, 3) - \mathrm{N}(1, 2) + \mathrm{N}(1, 2, 3) \\ = \ & 9 + 9 + 9 - 9 - 9 - 9 + 9 \\ = \ & 9 \\ \equiv_8 \ & 1. \end{aligned}$$

Note that $9 \not\equiv_{16} 1$.

6.4 Further questions

Question 58 Let $s \in [0, t]$. Let $J \subseteq [0, s]$ such that $J \neq \emptyset$.

Does the congruence

$$\sum_{\substack{I \subseteq J \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s - I) \equiv_{p^{|J|}} 1$$

hold?

Question 59 Let $s \in [0,t]$. Suppose G to be a p-group, i.e. $|G| = p^t$. Let $\ell \in [0,s]$.

Does the congruence

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} \, \mathrm{N}(s-I) \equiv_{p^{\frac{(\ell+1)(\ell+2)}{2}}} 1$$

hold?

Remark 60 Investigating Question 59 via Magma [**2**], where we used the Small Groups Library [**1**], gives the following results.

(1) Let $s \in [1,t]$. Let $\ell = 1$. Then

$$\mathrm{N}(s) + \mathrm{N}(s-1) - \mathrm{N}(s-1,s) \equiv_{p^3} 1$$

holds for p-groups of order

$$|G| \in \{2^1, \ldots, 2^7, 3^1, \ldots, 3^5, 5^1, \ldots, 5^5, 7^1, \ldots, 7^3\}.$$

(2) Let $s \in [2,t]$. Let $\ell = 2$. Then

$$\begin{aligned} 1 \equiv_{p^6} \quad & \mathrm{N}(s) + \mathrm{N}(s-1) + \mathrm{N}(s-2) \\ & - \mathrm{N}(s-1,s) - \mathrm{N}(s-2,s) - \mathrm{N}(s-2,s-1) \\ & + \mathrm{N}(s-2,s-1,s) \end{aligned}$$

holds for p-groups of order

$$|G| \in \{2^2, \ldots, 2^7, 3^2, \ldots, 3^5, 5^2, \ldots, 5^4, 7^2, 7^3\}.$$

(3) Let $s \in [3,t]$. Let $\ell = 3$. Then

$$\begin{aligned} 1 \equiv_{p^{10}} \quad & \mathrm{N}(s) + \mathrm{N}(s-1) + \mathrm{N}(s-2) + \mathrm{N}(s-3) \\ & - \mathrm{N}(s-1,s) - \mathrm{N}(s-2,s) - \mathrm{N}(s-2,s-1) \\ & - \mathrm{N}(s-3,s) - \mathrm{N}(s-3,s-1) - \mathrm{N}(s-3,s-2) \\ & + \mathrm{N}(s-2,s-1,s) + \mathrm{N}(s-3,s-1,s) + \mathrm{N}(s-3,s-2,s) + \mathrm{N}(s-3,s-2,s-1) \\ & - \mathrm{N}(s-3,s-2,s-1,s) \end{aligned}$$

holds for p-groups of order

$$|G| \in \{2^3, \ldots, 2^6, 3^3, \ldots, 3^5, 5^3, 7^3\}.$$

(4) Let $s \in [4,t]$. Let $\ell = 4$. Then

$$\begin{aligned} 1 \equiv_{p^{15}} \quad & \mathrm{N}(s) + \mathrm{N}(s{-}1) + \mathrm{N}(s{-}2) + \mathrm{N}(s{-}3) + \mathrm{N}(s{-}4) \\ & - \mathrm{N}(s{-}1,s) - \mathrm{N}(s{-}2,s) - \mathrm{N}(s{-}2,s{-}1) \\ & - \mathrm{N}(s{-}3,s) - \mathrm{N}(s{-}3,s{-}1) - \mathrm{N}(s{-}3,s{-}2) \\ & - \mathrm{N}(s{-}4,s) - \mathrm{N}(s{-}4,s{-}1) - \mathrm{N}(s{-}4,s{-}2) - \mathrm{N}(s{-}4,s{-}3) \\ & + \mathrm{N}(s{-}2,s{-}1,s) + \mathrm{N}(s{-}3,s{-}1,s) + \mathrm{N}(s{-}3,s{-}2,s) \\ & + \mathrm{N}(s{-}3,s{-}2,s{-}1) + \mathrm{N}(s{-}4,s{-}1,s) + \mathrm{N}(s{-}4,s{-}2,s) \\ & + \mathrm{N}(s{-}4,s{-}2,s{-}1) + \mathrm{N}(s{-}4,s{-}3,s) + \mathrm{N}(s{-}4,s{-}3,s{-}1) \\ & + \mathrm{N}(s{-}4,s{-}3,s{-}2) \\ & - \mathrm{N}(s{-}3,s{-}2,s{-}1,s) - \mathrm{N}(s{-}4,s{-}2,s{-}1,s) - \mathrm{N}(s{-}4,s{-}3,s{-}1,s) \\ & - \mathrm{N}(s{-}4,s{-}3,s{-}2,s) - \mathrm{N}(s{-}4,s{-}3,s{-}2,s{-}1) \\ & + \mathrm{N}(s{-}4,s{-}3,s{-}2,s{-}1,s) \end{aligned}$$

holds for p-groups of order

$$|G| \in \{2^4, \ldots, 2^6, 3^4, 3^5\}.$$

Remark 61 Examples 54.(3, 4) show that the assumption that G is a p-group in Question 59 cannot be omitted.

Bibliography

[1] Besche, H. U.; Eick, B.; O'Brien, E. A. A Millennium Project: Constructing Small Groups. *Internat. J. Algebra Comput.* **12** (2002), 623–644.

[2] Bosma, W.; Cannon, J.; Playoust, C. The Magma Algebra System I: The User Language. *J. Symbolic Comput.* **24** (1997), 235–265.

[3] Frobenius, F. G. Verallgemeinerung des Sylow'schen Satzes. *Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften zu Berlin* (1895), 981–993.

[4] Huppert, B. Endliche Gruppen I. Springer-Verlag Berlin, 1967.

[5] Isaacs, I. M. Finite Group Theory. *Graduate Studies in Mathematics* **92**, American Mathematical Society, 2008.

[6] Ledermann, W. Introduction to Group Theory. Longman, 1976.

[7] van Lint, J. H.; Wilson, R. M. A Course in Combinatorics. Cambridge University Press, 2001.

[8] Sylow, L. Théorèmes sur les groupes de substitutions. *Math. Ann.* **5** (1872), 584–594.

[9] Wielandt, H. Ein Beweis für die Existenz der Sylowgruppen. *Arch. Math* **10** (1959), 401–402.

Zusammenfassung

Sei G eine endliche Gruppe. Sei p eine Primzahl.

Wir schreiben $|G| = p^t n$, wobei $t = \mathrm{v}_p(|G|) \in \mathbb{Z}_{\geqslant 0}$, $n \in \mathbb{Z}_{\geqslant 1}$ und $n \not\equiv_p 0$.

Sei $s \in [0, t]$.

Für $k \geqslant 0$ und $I = \{c_1, \ldots, c_k\} \subseteq [0, t]$, wobei $c_1 > \ldots > c_k$, schreiben wir

$$\mathrm{N}(s - I) := |\{(U_1, \ldots, U_k) : U_1 \leqslant U_2 \leqslant \ldots \leqslant U_k \leqslant G,\ |U_i| = p^{s-c_i} \text{ für } i \in [1, k]\}|.$$

Es bezeichnet also $\mathrm{N}(s - I)$ die Anzahl der Ketten von p-Untergruppen

$$U_1 \leqslant U_2 \leqslant \ldots \leqslant U_k \leqslant G,$$

wobei U_i Ordnung p^{s-c_i} hat für $i \in [1, k]$.

Wir erhalten folgende Siebformel für $\ell \in [0, s]$.

$$\sum_{\substack{I \subseteq [0,\ell] \\ I \neq \emptyset}} (-1)^{|I|+1} \mathrm{N}(s - I) \equiv_{p^{\ell+1}} 1.$$

Der Name „Siebformel“ entlehnt sich der Tatsache, dass die Kongruenz formale Ähnlichkeiten mit der Siebformel aus der Mengenlehre hat, die auch als Prinzip von Inklusion und Exklusion bekannt ist.

Für $\ell = 0$ wurde die Siebformel im Fall $s = t$ bereits von Sylow **[8,** Th. II] gezeigt und als ein Teil der Sylowsätze bekannt. Frobenius **[3,** §4, I.] hat sie für den allgemeinen Fall $s \in [0, t]$ bewiesen.

Im Jahr 1959 hat Wielandt **[9]** einen alternativen Beweis im Fall $\ell = 0$ angeführt, in dem er eine Gruppenoperation von G auf der Menge aller Teilmengen von G, die p^s Elemente haben, definiert, und dann durch geschicktes Abzählen von Bahnen gewisser Länge die Kongruenz

$$\binom{p^t n}{p^s} \equiv_p \mathrm{N}(s - \{0\})$$

erhält, die nur von $|G|$ und nicht von G selbst abhängt.

Graham Higman verkürzte Wielandts Beweis, indem er diese Kongruenz auf die zyklische Gruppe $\mathrm{C}_{p^t n}$ angewandt hat und so ohne weitere zahlentheoretische Überlegungen die Kongruenz

$$\binom{p^t n}{p^s} \equiv_p 1$$

erhielt. Es folgt in diesem Fall die behauptete Aussage

$$\mathrm{N}(s - \{0\}) \equiv_p 1.$$

Beim Beweis der Siebformel sind wir Wielandts Idee gefolgt, wir haben uns jedoch nicht nur auf das Abzählen von Bahnen gewisser Länge beschränkt, sondern haben Bahnen beliebiger Länge abgezählt. Hat man diese Anzahlen in der Hand, ermöglicht das einem, eine Kongruenz modulo $p^{\ell+1}$ aufzustellen, und in einem weiteren Schritt zur behaupteten Siebformel umzuformen, wobei sich wie bei Higman ein Vergleich mit dem Fall der zyklischen Gruppe als hilfreich erwies.

Wir haben zudem Beispiele angeführt, die im Fall $\ell = 1$ und $\ell = 2$ zeigen, dass die Kongruenz nicht verbessert werden kann.

Versicherung

Hiermit versichere ich, Elias Schwesig,

(1) dass ich meine Arbeit selbstständig verfasst habe,

(2) dass ich keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommenen Aussagen als solche gekennzeichnet habe,

(3) dass die eingereichte Arbeit weder vollständig noch in wesentlichen Teilen Gegenstand eines anderen Prüfungsverfahrens gewesen ist,

(4) dass das elektronische Exemplar mit den anderen Exemplaren übereinstimmt.

Stuttgart, im Juli 2024

Elias Schwesig