# On the Hasse norm principle and the Davenport-Hasse lifting theorem

March 2022

**Kazuki Kanai**

Doctoral Program in Fundamental Sciences
Graduate School of Science and Technology
Niigata University

## Acknowledgments

I would like to express my sincere gratitude to my supervisor Professor Akinari Hoshi who gave me various useful suggestions and continued support. His warmhearted guidance leads me to continue my research. I also thank Professors Hideo Kojima and Takeshi Miura who gave me valued advice and assistance. I am grateful to Professor Aiichi Yamasaki of Kyoto University for his kind support and wonderful computational skills.

I am thankful to my senior Dr. Takanori Nagamine, my fellow Dr. Sumito Hasegawa and my junior Yuta Enami who helped me with my PhD research life.

At last special thanks go to my parents and my friends.

# Contents

# Introduction

As in the title of this thesis, we study two subjects "Hasse norm principle" and "Davenport-Hasse lifting theorem". What these two have in common is that they both bear the name of Hasse. Hasse began the study of mathematics at Göttingen University in 1918. His study is very extensive and significant in number theory. Among them, this thesis is particularly relevant to the two papers [**Has31**] and [**DH35**]. Both of them deal with interesting phenomena related to norms, although the base fields are different. This thesis consists of two chapters and we shall discuss the former in Chapter 1 and the later in Chapter 2.

In Chapter 1, we mainly consider the Hasse norm principle. This chapter is based on [**HKY**].

Let $k$ be a global field, $K/k$ be a finite extension and $\mathbb{A}_K^\times$ be the idele group of $K$. We say that the Hasse norm principle (HNP) holds for $K/k$ if

$$\mathrm{Obs}(K/k) := (N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times) = 1$$

where $N_{K/k}$ is the norm map. In 1931, Hasse [**Has31**] proved that if $K/k$ is cyclic, then the HNP holds but HNP does not hold for bicyclic extension $\mathbb{Q}(\sqrt{-39}, \sqrt{-3})/\mathbb{Q}$. This example shows that it is no longer possible to generalize to the Abelian extension.

Following the work of Hasse, Scholze [**Sch36**], [**Sch40**] did pioneering work in seeing the connection with central extension. He defined $\mathrm{Obs}(K/k)$ and called it "number knot".

In the context of the class field theory, for Galois extension $K/k$, Tate [**Tat67**] gave the following theorem:

THEOREM 1.8 (Tate [**Tat67**, page 198]). *Let $k$ be a global field, $K/k$ be a finite Galois extension with Galois group $\mathrm{Gal}(K/k) \simeq G$. Let $V_k$ be the set of all places of $k$ and $G_v$ be the decomposition group of $G$ at $v \in V_k$. Then we have*

$$(N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times) \simeq \mathrm{Coker}\left\{\bigoplus_{v\in V_k} \widehat{H}^{-3}(G_v, \mathbb{Z}) \xrightarrow{\text{cores}} \widehat{H}^{-3}(G, \mathbb{Z})\right\}$$

*where $\widehat{H}$ is the Tate cohomology. In particular, the Hasse norm principle holds for $K/k$ if and only if the restriction map $H^3(G, \mathbb{Z}) \xrightarrow{\text{res}} \bigoplus_{v\in V_k} H^3(G_v, \mathbb{Z})$ is injective.*

The HNP for Galois extensions was investigated by Garbanati, Razer, Gerth, Gurak, ..., Furuta, Morishita, Horie, Takeuchi, Kagawa, ..., etc. However, for non-Galois extensions, very little is known about the HNP.

One of the main theorems of Chapter 1 gives a necessary and sufficient condition for the HNP for $K/k$ with $[K:k] \leq 15$ and $n \neq 12$ by using the theory of norm one tori (Theorem1.18). The HNP is closely rerated to the rationality problem of norm one tori. In the following, we describe the relationship between the HNP and the rationality problem of norm one tori.

Let $k$ be a field and $X$ be an algebraic variety over $k$. It is an important problem to determine whether $X$ is a rational (resp. stably rational, retract rational) variety over $k$. When $X = T$ is an algebraic $k$-torus, its stable (resp. retract) rationality may be determined using a flabby resolution of the character lattice $\widehat{T} = \mathrm{Hom}(T, \mathbb{G}_m)$ of $T$. This efficient technique was introduced by Endo and Miyata [**EM75**] and Voskresenskii [**Vos69**].

Let $k$ be a global field, i.e. a number field (a finite extension of $\mathbb{Q}$) or a function field of an algebraic curve over $\mathbb{F}_q$ (a finite extension of $\mathbb{F}_q(t)$). Let $T$ be an algebraic $k$-torus and $T(k)$ be the group of $k$-rational points of $T$. Then $T(k)$ embeds into $\prod_{v \in V_k} T(k_v)$ by the diagonal map where $V_k$ is the set of all places of $k$ and $k_v$ is the completion of $k$ at $v$. Let $\overline{T(k)}$ be the closure of $T(k)$ in the product $\prod_{v \in V_k} T(k_v)$. The group

$$A(T) = \left( \prod_{v \in V_k} T(k_v) \right) / \overline{T(k)}$$

is called *the kernel of the weak approximation* of $T$. We say that $T$ *has the weak approximation property* if $A(T) = 0$.

Let $E$ be a principal homogeneous space (= torsor) under $T$. *Hasse principle holds for* $E$ means that if $E$ has a $k_v$-rational point for all $k_v$, then $E$ has a $k$-rational point. The set $H^1(k, T)$ classifies all such torsors $E$ up to (non-unique) isomorphism. We define *the Shafarevich-Tate group*

$$Ш(T) = \mathrm{Ker} \left\{ H^1(k, T) \xrightarrow{\mathrm{res}} \bigoplus_{v \in V_k} H^1(k_v, T) \right\}.$$

Then we say that $T$ *satisfies the Hasse principle* if $Ш(T) = 0$.

THEOREM 1.2 (Voskresenskii [**Vos69**, Theorem 5, page 1213], [**Vos70**, Theorem 6, page 9], see also [**Vos98**, Section 11.6, Theorem, page 120]). *Let $k$ be a global field, $T$ be an algebraic*

*k-torus and $X$ be a smooth k-compactification of $T$. Then there exists an exact sequence*

$$0 \to A(T) \to H^1(k, \operatorname{Pic}\overline{X})^\vee \to Ш(T) \to 0$$

*where $M^\vee = \operatorname{Hom}(M, \mathbb{Q}/\mathbb{Z})$ is the Pontryagin dual of $M$. Moreover, if $L$ is the splitting field of $T$ and $L/k$ is an unramified extension, then $A(T) = 0$ and $H^1(k, \operatorname{Pic}\overline{X})^\vee \simeq Ш(T)$.*

It follows that $H^1(k, \operatorname{Pic}\overline{X}) = 0$ if and only if $A(T) = 0$ and $Ш(T) = 0$, i.e. $T$ has the weak approximation property and Hasse principle holds for all torsors $E$ under $T$.

On the other hand, Ono [**Ono63**] established the relationship between the Hasse norm principle for $K/k$ and the Hasse principle for the norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ of $K/k$ :

THEOREM 1.9 (Ono [**Ono63**, page 70], see also Platonov [**Pla82**, page 44], Kunyavskii [**Kun84**, Remark 3], Platonov and Rapinchuk [**PR94**, page 307]). *Let $k$ be a global field and $K/k$ be a finite extension. Then*

$$Ш(R^{(1)}_{K/k}(\mathbb{G}_m)) \simeq (N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times).$$

*In particular, $Ш(R^{(1)}_{K/k}(\mathbb{G}_m)) = 0$ if and only if the Hasse norm principle holds for $K/k$.*

By applying Theorem 1.2 to $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, it follows from Theorem 1.9 that $H^1(k, \operatorname{Pic}\overline{X})$ $= 0$ if and only if $A(T) = 0$ and $Ш(T) = 0$, i.e. $T$ has the weak approximation property and the Hasse norm principle holds for $K/k$. In the algebraic language, the latter condition $Ш(T) = 0$ means that for the corresponding norm hyper surface $f(x_1, \ldots, x_n) = b$, it has a $k$-rational point if and only if it has a $k_v$-rational point for any valuation $v$ of $k$ where $f \in k[x_1, \ldots, x_n]$ is the polynomial of total degree $n$ defined by the norm map $N_{K/k} : K^\times \to k^\times$ and $b \in k^\times$ (see [**Vos98**, Example 4, page 122]).

Motivated by the HNP, we want to get $H^1(k, \operatorname{Pic}\overline{X})$. The following theorems are part of the main theorems of Chapter 1:

THEOREM 1.5 (see Theorem 1.27 for the detailed statement). *Let $k$ be a field, $T$ be an algebraic $k$-torus of dimension 4 and $X$ be a smooth $k$-compactification of $T$. Among the (at most) 216 cases of not retract rational algebraic $k$-tori $T$, there exist 2 (resp. 20, 194) cases of algebraic $k$-tori with $H^1(k, \operatorname{Pic}\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (resp. $H^1(k, \operatorname{Pic}\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$, $H^1(k, \operatorname{Pic}\overline{X}) = 0$).*

THEOREM 1.6 (see Theorem 1.28 for the detailed statement). *Let $k$ be a field, $T$ be an algebraic $k$-torus of dimension 5 and $X$ be a smooth $k$-compactification of $T$. Among the (at most) 3003 cases of not retract rational algebraic $k$-tori $T$, there exist 11 (resp. 263,*

2729) *cases of algebraic k-tori with* $H^1(k, \operatorname{Pic}\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (*resp.* $H^1(k, \operatorname{Pic}\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$, $H^1(k, \operatorname{Pic}\overline{X}) = 0$).

THEOREM 1.15. *Let* $2 \leq n \leq 15$ *be an integer with* $n \neq 12$. *Let* $k$ *be a field,* $K/k$ *be a separable field extension of degree* $n$ *and* $L/k$ *be the Galois closure of* $K/k$. *Assume that* $G = \operatorname{Gal}(L/k) = nTm$ *is a transitive subgroup of* $S_n$ *and* $H = \operatorname{Gal}(L/K)$ *with* $[G : H] = n$. *Let* $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ *be the norm one torus of* $K/k$ *of dimension* $n-1$ *and* $X$ *be a smooth* $k$*-compactification of* $T$. *Then* $H^1(k, \operatorname{Pic}\overline{X}) \neq 0$ *if and only if* $G$ *is given as in Table* 1. *In particular, if* $k$ *is a number field and* $L/k$ *is an unramified extension, then* $A(T) = 0$ *and* $H^1(k, \operatorname{Pic}\overline{X}) \simeq Ш(T)$.

THEOREM 1.17. *Let* $k$ *be a field,* $K/k$ *be a separable field extension of degree* $n$ *and* $L/k$ *be the Galois closure of* $K/k$. *Assume that* $G = \operatorname{Gal}(L/k) = M_n \leq S_n$ $(n = 11, 12, 22, 23, 24)$ *is the Mathieu group of degree* $n$ *and* $H = \operatorname{Gal}(L/K)$ *with* $[G : H] = n$. *Let* $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ *be the norm one torus of* $K/k$ *of dimension* $n-1$ *and* $X$ *be a smooth* $k$*-compactification of* $T$. *Then* $H^1(k, \operatorname{Pic}\overline{X}) = 0$. *In particular, if* $k$ *is a number field, then* $A(T) = 0$ *and* $Ш(T) = 0$.

As applications of the results, we get the group $T(k)/R$ of $R$-equivalence classes over a local field $k$ via Colliot-Thélène and Sansuc's formula and the Tamagawa number $\tau(T)$ over a number field $k$ via Ono's formula $\tau(T) = |H^1(k, \widehat{T})|/|Ш(T)|$.

In Chapter 2, we discus Gauss sums, Jacobi sums, Gaussian periods and multiplication matrices of Gaussian periods and their liftings. This chapter is based on [**HK**].

Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. Write $p^r = ef + 1$. Let $\mathbb{F}_{p^r}$ be the finite field of $p^r$ elements and $\gamma$ be a fixed generator of $\mathbb{F}_{p^r}^\times = \mathbb{F}_{p^r} \setminus \{0\}$. Let $\zeta_n = e^{2\pi i/n}$ be an $n$-th root of unity. For $0 \leq i \leq e-1$, *Gaussian periods* $\eta_r(i)$ *of degree* $e$ *for* $\mathbb{F}_{p^r}$ are defined by

$$\eta_r(i) := \sum_{j=0}^{f-1} \zeta_p^{\operatorname{Tr}(\gamma^{ej+i})}$$

where Tr is the trace map $\operatorname{Tr} : \mathbb{F}_{p^r} \to \mathbb{F}_p$. Note that $\eta_r(i)$ depends on the choice of $\gamma$.

For a nontrivial character $\psi$ on $\mathbb{F}_{p^r}^\times$ and the trivial character $\varepsilon$ on $\mathbb{F}_{p^r}^\times$, we extend them to $\mathbb{F}_{p^r}$ by setting $\psi(0) = 0$ and $\varepsilon(0) = 1$. Let $\psi_1$, $\psi_2$ be characters on $\mathbb{F}_{p^r}$. *Gauss sums* $G_r^*(\psi_1)$ and *Jacobi sums* $J_r^*(\psi_1, \psi_2)$ *for* $\mathbb{F}_{p^r}$ are defined by

$$G_r^*(\psi_1) := \sum_{\alpha \in \mathbb{F}_{p^r}^\times} \psi_1(\alpha)\zeta_p^{\operatorname{Tr}(\alpha)} \quad \text{and} \quad J_r^*(\psi_1, \psi_2) := \sum_{\substack{\alpha \in \mathbb{F}_{p^r} \\ \alpha \neq 0,1}} \psi_1(\alpha)\psi_2(1-\alpha).$$

We have the well-known relation

$$J_r^*(\psi_1, \psi_2) = \frac{G_r^*(\psi_1)G_r^*(\psi_2)}{G_r^*(\psi_1\psi_2)}$$

whenever $\psi_1\psi_2 \neq \varepsilon$.

In 1935, Davenport and Hasse gave the following fundamental theorem:

THEOREM 2.1 (Davenport and Hasse [**DH35**, Relation (0.8)]). *Let $e \geq 2$ be an integer, $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$ and $\psi$ be a nontrivial character on $\mathbb{F}_{p^r}$. Then, for any integer $n \geq 1$, we have*

$$G_{nr}^*(\psi') = (-1)^{n-1}G_r^*(\psi)^n$$

*where $\psi'$ is the lift of $\psi$ from $\mathbb{F}_{p^r}$ to $\mathbb{F}_{p^{nr}}$ defined by $\psi'(\alpha) = \psi(\mathrm{Nr}(\alpha))$ and $\mathrm{Nr}$ is the norm map. In particular, if $\psi_1$, $\psi_2$ and $\psi_1\psi_2$ are nontrivial characters on $\mathbb{F}_{p^r}$, then we have*

$$J_{nr}^*(\psi_1', \psi_2') = (-1)^{n-1}J_r^*(\psi_1, \psi_2)^n.$$

We regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the function $\eta_r : \mathbb{Z}/e\mathbb{Z} \to \mathbb{C}$, $i \mapsto \eta_r(i)$ and the Gauss sums $G_r^*(\chi)$ for $\mathbb{F}_{p^r}$ as the function $G_r^* : \widehat{\mathbb{Z}/e\mathbb{Z}} \to \mathbb{C}$, $\chi \mapsto G_r^*(\chi)$. Then we find that they are each other's finite Fourier transform with some twist and we have:

THEOREM 2.3 (Davenport and Hasse's lifting theorem: the dual form). *Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. We regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the function $\eta_r : \mathbb{Z}/e\mathbb{Z} \to \mathbb{C}$, $i \mapsto \eta_r(i)$. Then, for any integer $n \geq 1$, we have*

$$\eta_{nr}(i) = (-1)^{n-1}\eta_r^{(n)}(i) \quad \textit{for} \quad 0 \leq i \leq e-1$$

*where*

$$\eta_r^{(n)}(i) = \sum_{\substack{k_1+\cdots+k_n \equiv i \,(\mathrm{mod}\, e) \\ 0 \leq k_1, \ldots, k_n \leq e-1}} \eta_r(k_1)\cdots\eta_r(k_n)$$

*is the $n$-fold product of $\eta_r$ with respect to the convolution product.*

For $0 \leq i, j \leq e-1$, *cyclotomic numbers* $\mathrm{Cyc}_r(i,j)$ *of order $e$ for $\mathbb{F}_{p^r}$* are defined by

$$\mathrm{Cyc}_r(i,j) := \#\{(v_1, v_2) \mid 0 \leq v_1, v_2 \leq f-1,\ 1 + \gamma^{ev_1+i} \equiv \gamma^{ev_2+j} \pmod{p^r}\}.$$

We have the following well-known relations between cyclotomic numbers $\mathrm{Cyc}_r(a,b)$ and Jacobi sums $J_r^*(i,j)$ (see [**BEW98**, page 79, Theorem 2.5.1]):

$$\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}(-1)^{fi}\zeta_e^{-(ai+bj)}J_r^*(i,j) = e^2\mathrm{Cyc}_r(a,b)$$

and

$$(-1)^{fi}\sum_{a=0}^{e-1}\sum_{b=0}^{e-1}\mathrm{Cyc}_r(a,b)\zeta_e^{ai+bj}=J_r^*(i,j).$$

Note that both $\mathrm{Cyc}_r(a,b)$ and $J_r^*(i,j)$ depend on the choice of the fixed generator $\gamma$ of $\mathbb{F}_{p^r}^\times$.

We see that the product of the Gaussian periods is represented by a linear combination of the Gaussian periods again and these coefficients are given in terms of the cyclotomic numbers (see [**BEW98**, page 328, Lemma 10.10.2, page 437, Exercise 12.23]):

$$\eta_r(m)\eta_r(m+i)=\sum_{j=0}^{e-1}(\mathrm{Cyc}_r(i,j)-D_if)\eta_r(m+j) \tag{1}$$

where $D_i=\delta_{0,i}$ (resp. $\delta_{e/2,i}$) if $f$ is even (resp. odd). It follows that the Gaussian periods are the eigenvalues of the $e\times e$ matrix $C_r:=[\mathrm{Cyc}_r(i,j)-D_if]_{0\le i,j\le e-1}$ called *the multiplication matrix of* $\eta_r(0),\dots,\eta_r(e-1)$ (see Section 2). Hence the period polynomial $P_{e,r}(X)$ can be obtained as the characteristic polynomial $\mathrm{Char}_X(C_r)$ of the multiplication matrix $C_r$.

According to Thaine [**Tha04**, Section 2], for two $e\times e$ matrices $A=[a_{i,j}]_{0\le i,j\le e-1}$, $B=[b_{i,j}]_{0\le i,j\le e-1}$ and $d\in(\mathbb{Z}/e\mathbb{Z})\setminus\{0\}$, we define *the d-composition* $A\overset{d}{*}B$ *of* $A$ *and* $B$ as

$$A\overset{d}{*}B:=\left[\sum_{s=0}^{e-1}\sum_{t=0}^{e-1}a_{s,t}b_{ds+i,dt+j}\right]_{0\le i,j\le e-1}.$$

For the multiplication matrix $C_1$ (resp. $C_1'$) of Gaussian periods $\eta_1(0),\dots,\eta_1(e-1)$ (resp. $\eta_1'(0),\dots,\eta_1'(e-1)$) of degree $e$ for $\mathbb{F}_{p^1}$, the $d$-composition $C_1\overset{d}{*}C_1'$ gives the multiplication matrix of $\theta_{d,0},\dots,\theta_{d,e-1}$ where $\theta_{d,i}=\sum_{s=0}^{e-1}\eta_1(s)\eta_1'(ds+i)$.

By using Theorem 2.3, we get the main theorem of Chapter 2 which gives lifts of the multiplication matrix $C_r$ of the Gaussian periods $\eta_r(0),\dots,\eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$ via Thaine's $(-1)$-composition $\overset{-1}{*}$:

THEOREM 2.4. *Let $e\ge 2$ be an integer and $p^r$ be a prime power with $p^r\equiv 1 \pmod e$. Let $C_r=[\mathrm{Cyc}_r(i,j)-D_if]_{0\le i,j\le e-1}$ be the multiplication matrix of the Gaussian periods $\eta_r(0),\dots,\eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$. Then, for any integer $n\ge 1$, we have*

$$C_{nr}=(-1)^{n-1}C_r^{(n)}$$

*where $C_r^{(n)}$ is the $n$-fold product of $C_r$ with respect to the $(-1)$-composition $\overset{-1}{*}$. In particular, we have $P_{e,nr}(X)=\mathrm{Char}_X((-1)^{n-1}C_r^{(n)})$.*

CHAPTER 1

# Hasse norm principle


## Abstract

Let $k$ be a field and $T$ be an algebraic $k$-torus. In 1969, over a global field $k$, Voskresenskii proved that there exists an exact sequence $0 \to A(T) \to H^1(k, \operatorname{Pic}\overline{X})^\vee \to Ш(T) \to 0$ where $A(T)$ is the kernel of the weak approximation of $T$, $Ш(T)$ is the Shafarevich-Tate group of $T$, $X$ is a smooth $k$-compactification of $T$, $\overline{X} = X \times_k \overline{k}$, $\operatorname{Pic}\overline{X}$ is the Picard group of $\overline{X}$ and $\vee$ stands for the Pontryagin dual. On the other hand, in 1963, Ono proved that for the norm one torus $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ of $K/k$, $Ш(T) = 0$ if and only if the Hasse norm principle holds for $K/k$. First, we determine $H^1(k, \operatorname{Pic}\overline{X})$ for algebraic $k$-tori $T$ up to dimension 5. Second, we determine $H^1(k, \operatorname{Pic}\overline{X})$ for norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ with $[K : k] = n \leq 15$ and $n \neq 12$. We also show that $H^1(k, \operatorname{Pic}\overline{X}) = 0$ for $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ when the Galois group of the Galois closure of $K/k$ is the Mathieu group $M_n \leq S_n$ with $n = 11, 12, 22, 23, 24$. Third, we give a necessary and sufficient condition for the Hasse norm principle for $K/k$ with $[K : k] = n \leq 15$ and $n \neq 12$. As applications of the results, we get the group $T(k)/R$ of $R$-equivalence classes over a local field $k$ via Colliot-Thélène and Sansuc's formula and the Tamagawa number $\tau(T)$ over a number field $k$ via Ono's formula $\tau(T) = |H^1(k, \widehat{T})|/|Ш(T)|$. This chapter is based on [**HKY**].


## 1. Introduction

Let $k$ be a field, $\overline{k}$ be a fixed separable closure of $k$ and $\mathcal{G} = \operatorname{Gal}(\overline{k}/k)$ be the absolute Galois group of $k$. Let $T$ be an algebraic $k$-torus, i.e. a group $k$-scheme with fiber product (base change) $T \times_k \overline{k} = T \times_{\operatorname{Spec} k} \operatorname{Spec}\overline{k} \simeq (\mathbb{G}_{m,\overline{k}})^n$; $k$-form of the split torus $(\mathbb{G}_m)^n$. Then there exists the minimal (canonical) finite Galois extension $K/k$ with Galois group $G = \operatorname{Gal}(K/k)$ such that $T$ splits over $K$: $T \times_k K \simeq (\mathbb{G}_{m,K})^n$. It is also well-known that there is the duality between the category of $G$-lattices, i.e. finitely generated $\mathbb{Z}[G]$-modules which are $\mathbb{Z}$-free as abelian groups, and the category of algebraic $k$-tori which split over $K$ (see Ono [**Ono61**, Section 1.2], Voskresenskii [**Vos98**, page 27, Example 6] and Knus, Merkurjev, Rost and Tignol [**KMRT98**, page 333, Proposition 20.17]). Indeed, if $T$ is an algebraic $k$-torus,

then the character module $\widehat{T} = \mathrm{Hom}(T, \mathbb{G}_m)$ of $T$ may be regarded as a $G$-lattice. Let $X$ be a smooth $k$-compactification of $T$, i.e. smooth projective $k$-variety $X$ containing $T$ as a dense open subvariety, and $\overline{X} = X \times_k \overline{k}$. There exists such a smooth $k$-compactification of an algebraic $k$-torus $T$ over any field $k$ (due to Hironaka [**Hir64**] for $\mathrm{char}\, k = 0$, see Colliot-Thélène, Harari and Skorobogatov [**CTHS05**, Corollaire 1] for any field $k$). A $\mathcal{G}$-lattice $P$ is said to be *permutation* if $P$ has a $\mathbb{Z}$-basis permuted by $\mathcal{G}$ and a $\mathcal{G}$-lattice $F$ is said to be *flabby* (resp. *coflabby*) if $\widehat{H}^{-1}(\mathcal{H}, F) = 0$ (resp. $H^1(\mathcal{H}, F) = 0$) for any closed subgroup $\mathcal{H} \leq \mathcal{G}$ where $\widehat{H}$ is the Tate cohomology.

Theorem 1.1 (Voskresenskii [**Vos69**, Section 4, page 1213], [**Vos70**, Section 3, page 7], see also [**Vos98**, Section 4.6], [**Kun07**, Theorem 1.9], [**Vos74**] and [**CT07**, Theorem 5.1, page 19] for any field $k$). *Let $k$ be a field and $\mathcal{G} = \mathrm{Gal}(\overline{k}/k)$. Let $T$ be an algebraic $k$-torus, $X$ be a smooth $k$-compactification of $T$ and $\overline{X} = X \times_k \overline{k}$. Then there exists an exact sequence of $\mathcal{G}$-lattices*

$$0 \to \widehat{T} \to \widehat{Q} \to \mathrm{Pic}\, \overline{X} \to 0$$

*where $\widehat{Q}$ is permutation and* Pic $\overline{X}$ *is flabby.*

We have $H^1(k, \mathrm{Pic}\, \overline{X}) \simeq H^1(G, \mathrm{Pic}\, X_K)$ where $K$ is the splitting field of $T$, $G = \mathrm{Gal}(K/k)$ and $X_K = X \times_k K$. Hence Theorem 1.1 says that for $G$-lattices $M = \widehat{T}$ and $P = \widehat{Q}$, the exact sequence $0 \to M \to P \to \mathrm{Pic}\, X_K \to 0$ gives a flabby resolution of $M$ and the flabby class of $M$ is $[M]^{fl} = [\mathrm{Pic}\ X_K]$ as $G$-lattices (see Section 3, cf. Endo and Miyata's theorem [**EM75**, Lemma 1.1] (= Theorem 1.24 in the present paper)).

Let $k$ be a global field, i.e. a number field (a finite extension of $\mathbb{Q}$) or a function field of an algebraic curve over $\mathbb{F}_q$ (a finite extension of $\mathbb{F}_q(t)$). Let $T$ be an algebraic $k$-torus and $T(k)$ be the group of $k$-rational points of $T$. Then $T(k)$ embeds into $\prod_{v \in V_k} T(k_v)$ by the diagonal map where $V_k$ is the set of all places of $k$ and $k_v$ is the completion of $k$ at $v$. Let $\overline{T(k)}$ be the closure of $T(k)$ in the product $\prod_{v \in V_k} T(k_v)$. The group

$$A(T) = \left( \prod_{v \in V_k} T(k_v) \right) / \overline{T(k)}$$

is called *the kernel of the weak approximation* of $T$. We say that $T$ *has the weak approximation property* if $A(T) = 0$.

Let $E$ be a principal homogeneous space (= torsor) under $T$. *Hasse principle holds for* $E$ means that if $E$ has a $k_v$-rational point for all $k_v$, then $E$ has a $k$-rational point. The

set $H^1(k,T)$ classifies all such torsors $E$ up to (non-unique) isomorphism. We define *the Shafarevich-Tate group*

$$Ш(T) = \mathrm{Ker}\left\{ H^1(k,T) \xrightarrow{\mathrm{res}} \bigoplus_{v\in V_k} H^1(k_v,T) \right\}.$$

Then Hasse principle holds for all torsors $E$ under $T$ if and only if $Ш(T) = 0$.

THEOREM 1.2 (Voskresenskii [**Vos69**, Theorem 5, page 1213], [**Vos70**, Theorem 6, page 9], see also [**Vos98**, Section 11.6, Theorem, page 120]). *Let $k$ be a global field, $T$ be an algebraic $k$-torus and $X$ be a smooth $k$-compactification of $T$. Then there exists an exact sequence*

$$0 \to A(T) \to H^1(k, \mathrm{Pic}\,\overline{X})^\vee \to Ш(T) \to 0$$

*where $M^\vee = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z})$ is the Pontryagin dual of $M$. Moreover, if $L$ is the splitting field of $T$ and $L/k$ is an unramified extension, then $A(T) = 0$ and $H^1(k, \mathrm{Pic}\,\overline{X})^\vee \simeq Ш(T)$.*

For the last assertion, see [**Vos98**, Theorem, page 120]. It follows that $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$ if and only if $A(T) = 0$ and $Ш(T) = 0$, i.e. $T$ has the weak approximation property and Hasse principle holds for all torsors $E$ under $T$. Theorem 1.2 was generalized to the case of linear algebraic groups by Sansuc [**San81**].

*The norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ of $K/k$* is the kernel of the norm map $R_{K/k}(\mathbb{G}_m) \to \mathbb{G}_m$ where $R_{K/k}$ is the Weil restriction (see [**Vos98**, page 37, Section 3.12]). Such a torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ is biregularly isomorphic to the norm hypersurface $f(x_1,\ldots,x_n) = 1$ where $f \in k[x_1,\ldots,x_n]$ is the polynomial of total degree $n$ defined by the norm map $N_{K/k} : K^\times \to k^\times$. When $K/k$ is a finite Galois extension, we have that:

THEOREM 1.3 (Voskresenskii [**Vos70**, Theorem 7], Colliot-Thélène and Sansuc [**CTS77**, Proposition 1]). *Let $k$ be a field and $K/k$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$ and $X$ be a smooth $k$-compactification of $T$. Then $H^1(H, \mathrm{Pic}\,X_K) \simeq H^3(H,\mathbb{Z})$ for any subgroup $H$ of $G$. In particular, $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq H^1(G, \mathrm{Pic}\,X_K) \simeq H^3(G,\mathbb{Z})$ which is isomorphic to the Schur multiplier $M(G)$ of $G$.*

In other words, for $G$-lattice $J_G = \widehat{T}$, $H^1(H, [J_G]^{fl}) \simeq H^3(H,\mathbb{Z})$ for any subgroup $H$ of $G$ and $H^1(G, [J_G]^{fl}) \simeq H^3(G,\mathbb{Z}) \simeq H^2(G, \mathbb{Q}/\mathbb{Z})$; the Schur multiplier of $G$. By the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}[G] \to J_G \to 0$, we also have $\delta : H^1(G, J_G) \simeq H^2(G,\mathbb{Z}) \simeq G^{ab} \simeq G/[G,G]$

where $\delta$ is the connecting homomorphism and $G^{ab}$ is the abelianization of $G$ (for details, see Section 2).

Let $K$ be a finitely generated field extension of a field $k$. A field $K$ is called *rational over* $k$ (or $k$-*rational* for short) if $K$ is purely transcendental over $k$, i.e. $K$ is isomorphic to $k(x_1, \ldots, x_n)$, the rational function field over $k$ with $n$ variables $x_1, \ldots, x_n$ for some integer $n$. $K$ is called *stably* $k$-*rational* if $K(y_1, \ldots, y_m)$ is $k$-rational for some algebraically independent elements $y_1, \ldots, y_m$ over $K$. Two fields $K$ and $K'$ are called *stably* $k$-*isomorphic* if $K(y_1, \ldots, y_m) \simeq K'(z_1, \ldots, z_n)$ over $k$ for some algebraically independent elements $y_1, \ldots, y_m$ over $K$ and $z_1, \ldots, z_n$ over $K'$. When $k$ is an infinite field, $K$ is called *retract* $k$-*rational* if there is a $k$-algebra $R$ contained in $K$ such that (i) $K$ is the quotient field of $R$, and (ii) the identity map $1_R : R \to R$ factors through a localized polynomial ring over $k$, i.e. there is an element $f \in k[x_1, \ldots, x_n]$, which is the polynomial ring over $k$, and there are $k$-algebra homomorphisms $\varphi : R \to k[x_1, \ldots, x_n][1/f]$ and $\psi : k[x_1, \ldots, x_n][1/f] \to R$ satisfying $\psi \circ \varphi = 1_R$ (cf. [**Sal84**]). $K$ is called $k$-*unirational* if $k \subset K \subset k(x_1, \ldots, x_n)$ for some integer $n$. It is not difficult to see that "$k$-rational" $\Rightarrow$ "stably $k$-rational" $\Rightarrow$ "retract $k$-rational" $\Rightarrow$ "$k$-unirational".

An algebraic $k$-torus $T$ is said to be $k$-*rational* (resp. *stably* $k$-*rational*, *retract* $k$-*rational*) if the function field $k(T)$ of $T$ is $k$-rational (resp. stably $k$-rational, retract $k$-rational).

Note that an algebraic $k$-torus $T$ is always $k$-unirational (see [**Vos98**, page 40, Example 21]). Tori of dimension $n$ over $k$ correspond bijectively to the elements of the set $H^1(\mathcal{G}, \mathrm{GL}_n(\mathbb{Z}))$ where $\mathcal{G} = \mathrm{Gal}(k_s/k)$ since $\mathrm{Aut}((\mathbb{G}_m)^n) = \mathrm{GL}_n(\mathbb{Z})$. The algebraic $k$-torus $T$ of dimension $n$ is determined uniquely by the integral representation $h : \mathcal{G} \to \mathrm{GL}_n(\mathbb{Z})$ up to conjugacy, and the group $h(\mathcal{G})$ is a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$ (see [**Vos98**, page 57, Section 4.9])).

There are 2 (resp. 13, 73, 710, 6079) $\mathbb{Z}$-classes forming 2 (resp. 10, 32, 227, 955) $\mathbb{Q}$-classes in $\mathrm{GL}_1(\mathbb{Z})$ (resp. $\mathrm{GL}_2(\mathbb{Z})$, $\mathrm{GL}_3(\mathbb{Z})$, $\mathrm{GL}_4(\mathbb{Z})$, $\mathrm{GL}_5(\mathbb{Z})$). It is easy to see that all the 1-dimensional algebraic $k$-tori $T$, i.e. the trivial torus $\mathbb{G}_m$ and the norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ of $K/k$ with $[K : k] = 2$, are $k$-rational. Voskresenskii [**Vos67**] proved that all the 13 cases of 2-dimensional algebraic $k$-tori, which correspond to 13 $\mathbb{Z}$-conjugacy classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$, are $k$-rational. Note that whether all the 13 cases indeed occur or not depends on a base field $k$. The same applies for the numbers 15, 216 and 3003 in Theorems 1.4, 1.5 and 1.6 below. We also note that $T$ is retract $k$-rational $\Rightarrow H^1(k, \mathrm{Pic}\,\overline{X}) = 0$ and over global field $k$, $H^1(k, \mathrm{Pic}\,\overline{X}) = 0 \Rightarrow A(T) \simeq Ш(T) = 0$ (see Section 3 and also Manin [**Man74**, §30]).

Kunyavskii [**Kun90**] solved the rationality problem for 3-dimensional algebraic $k$-tori. In the classification, there exist 73 cases of 3-dimensional algebraic $k$-tori which correspond to 73 $\mathbb{Z}$-conjugacy classes of finite subgroups of $\mathrm{GL}_3(\mathbb{Z})$, and 15 cases of them are not $k$-rational (resp. not stably $k$-rational, not retract $k$-rational). Using the classification, Kunyavskii [**Kun84**] showed that only 2 cases of algebraic $k$-tori of dimension 3 satisfy the non-vanishing $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0$ among the 15 cases of non-rational $k$-tori. These two $k$-tori are norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ with $[K : k] = 4$:

Theorem 1.4 (Kunyavskii [**Kun84**, Proposition 1]). *Let $k$ be a field, $T$ be an algebraic $k$-torus of dimension* 3 *and $X$ be a smooth $k$-compactification of $T$. Then, among the (at most)* 15 *cases of non-rational algebraic $k$-tori $T$,*

$$H^1(k, \mathrm{Pic}\,\overline{X}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } T = R^{(1)}_{K_1/k}(\mathbb{G}_m) \text{ or } R^{(1)}_{K_2/k}(\mathbb{G}_m) \\ 0 & \text{otherwise} \end{cases}$$

*where $K_1/k$ (resp. $K_2/k$) is a field extension of degree* 4 *whose Galois closure $L_1/k$ (resp. $L_2/k$) satisfies $\mathrm{Gal}(L_1/k) \simeq V_4$; the Klein four group (resp. $\mathrm{Gal}(L_2/k) \simeq A_4$; the alternating group of degree* 4*). In particular, if $k$ is a global field, then $A(T) \simeq Ш(T) = 0$ except for $T = R^{(1)}_{K_1/k}(\mathbb{G}_m)$ and $T = R^{(1)}_{K_2/k}(\mathbb{G}_m)$.*

Hoshi and Yamasaki [**HY17**] classified stably/retract $k$-rational algebraic $k$-tori of dimensions 4 and 5. In the classification, there exist 710 (resp. 6079) cases of 4-dimensional (resp. 5-dimensional) algebraic $k$-tori which correspond to 710 (resp. 6079) $\mathbb{Z}$-conjugacy classes of finite subgroups of $\mathrm{GL}_4(\mathbb{Z})$ (resp. $\mathrm{GL}_5(\mathbb{Z})$), and 216 (resp. 3003) cases of them are not retract $k$-rational.

The first main result (Theorem 1.5 and Theorem 1.6) of this chapter is to classify the algebraic $k$-tori $T$ with non-vanishing $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0$ in dimensions 4 and 5:

Theorem 1.5 (see Theorem 1.27 for the detailed statement). *Let $k$ be a field, $T$ be an algebraic $k$-torus of dimension* 4 *and $X$ be a smooth $k$-compactification of $T$. Among the (at most)* 216 *cases of not retract rational algebraic $k$-tori $T$, there exist* 2 *(resp.* 20, 194*) cases of algebraic $k$-tori with $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (resp. $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$, $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$).*

Theorem 1.6 (see Theorem 1.28 for the detailed statement). *Let $k$ be a field, $T$ be an algebraic $k$-torus of dimension* 5 *and $X$ be a smooth $k$-compactification of $T$. Among the (at most)* 3003 *cases of not retract rational algebraic $k$-tori $T$, there exist* 11 *(resp.* 263*,*

2729) *cases of algebraic $k$-tori with* $H^1(k, \operatorname{Pic}\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (*resp.* $H^1(k, \operatorname{Pic}\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$, $H^1(k, \operatorname{Pic}\overline{X}) = 0$).

Note that Hoshi and Yamasaki [**HY17**, Chapter 7] showed the vanishing $H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [\widehat{T}]^{fl}) = 0$ for any Bravais group $G$ of dimension $n \leq 6$ (see also [**Vos83**], [**Vos98**, Section 8]). There exists 1 (resp. 5, 14, 64, 189, 841) Bravais group of dimension $n = 1$ (resp. 2, 3, 4, 5, 6) (see [**HY17**, Example 4.16]).

Let $G$ be a finite group and $M$ be a $G$-lattice. We define

$$Ш^i_\omega(G, M) := \operatorname{Ker}\left\{ H^i(G, M) \xrightarrow{\text{res}} \bigoplus_{g \in G} H^i(\langle g \rangle, M) \right\} \quad (i \geq 1).$$

The following is a theorem of Colliot-Thélène and Sansuc [**CTS87**]:

Theorem 1.7 (Colliot-Thélène and Sansuc [**CTS87**, Proposition 9.5 (ii)], see also [**San81**, Proposition 9.8] and [**Vos98**, page 98]). *Let $k$ be a field with* $\operatorname{char} k = 0$ *and $K/k$ be a finite Galois extension with Galois group $G = \operatorname{Gal}(K/k)$. Let $T$ be an algebraic $k$-torus which splits over $K$ and $X$ be a smooth $k$-compactification of $T$. Then we have*

$$Ш^2_\omega(G, \widehat{T}) \simeq H^1(G, \operatorname{Pic} X_K) \simeq \operatorname{Br}(X)/\operatorname{Br}(k)$$

*where* $\operatorname{Br}(X)$ *is the étale cohomological Brauer Group of $X$ (it is the same as the Azumaya-Brauer group of $X$ for such $X$, see* [**CTS87**, page 199]).

In other words, for $G$-lattice $M = \widehat{T}$, we have

$$H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, \operatorname{Pic} X_K) \simeq H^1(G, [M]^{fl}) \simeq Ш^2_\omega(G, M) \simeq \operatorname{Br}(X)/\operatorname{Br}(k)$$

(for the flabby class $[M]^{fl}$ of $M$, see Section 3). Hence Theorem 1.4, Theorem 1.5 and Theorem 1.6 compute $H^1(G, [M]^{fl}) \simeq Ш^2_\omega(G, M) \simeq \operatorname{Br}(X)/\operatorname{Br}(k)$ where $M = \widehat{T}$. We also see $\operatorname{Br}_{\text{nr}}(k(X)/k) = \operatorname{Br}(X) \subset \operatorname{Br}(k(X))$ (see Colliot-Thélène [**CTS07**, Theorem 5.11], Saltman [**Sal99**, Proposition 10.5]).

Let $k$ be a global field, $K/k$ be a finite extension and $\mathbb{A}_K^\times$ be the idele group of $K$. We say that *the Hasse norm principle holds for $K/k$* if $(N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times) = 1$ where $N_{K/k}$ is the norm map.

Hasse [**Has31**, Satz, page 64] proved that the Hasse norm principle holds for any cyclic extension $K/k$ but does not hold for bicyclic extension $\mathbb{Q}(\sqrt{-39}, \sqrt{-3})/\mathbb{Q}$. For Galois extensions $K/k$, Tate [**Tat67**] gave the following theorem:

THEOREM 1.8 (Tate [**Tat67**, page 198]). *Let $k$ be a global field, $K/k$ be a finite Galois extension with Galois group* $\mathrm{Gal}(K/k) \simeq G$. *Let $V_k$ be the set of all places of $k$ and $G_v$ be the decomposition group of $G$ at $v \in V_k$. Then we have*

$$(N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times) \simeq \mathrm{Coker}\left\{\bigoplus_{v\in V_k} \widehat{H}^{-3}(G_v, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(G, \mathbb{Z})\right\}$$

*where $\widehat{H}$ is the Tate cohomology. In particular, the Hasse norm principle holds for $K/k$ if and only if the restriction map $H^3(G, \mathbb{Z}) \xrightarrow{\mathrm{res}} \bigoplus_{v\in V_k} H^3(G_v, \mathbb{Z})$ is injective.*

Let $S_n$ (resp. $A_n$, $D_n$, $C_n$) be the symmetric (resp. the alternating, the dihedral, the cyclic) group of degree $n$ of order $n!$ (resp. $n!/2$, $2n$, $n$). Let $V_4 \simeq C_2 \times C_2$ be the Klein four group.

If $G \simeq C_n$ is cyclic, then $\widehat{H}^{-3}(G, \mathbb{Z}) \simeq H^3(G, \mathbb{Z}) \simeq H^1(G, \mathbb{Z}) = 0$ and hence the Hasse's original theorem follows. If there exists a place $v$ of $k$ such that $G_v = G$, then the Hasse norm principle also holds for $K/k$. For example, the Hasse norm principle holds for $K/k$ with $G \simeq V_4$ if and only if there exists a place $v$ of $k$ such that $G_v = V_4$ because $H^3(V_4, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ and $H^3(C_2, \mathbb{Z}) = 0$. The Hasse norm principle holds for $K/k$ with $G \simeq (C_2)^3$ if and only if (i) there exists a place $v$ of $k$ such that $G_v = G$ or (ii) there exist places $v_1, v_2, v_3$ of $k$ such that $G_{v_i} \simeq V_4$ and $H^3(G, \mathbb{Z}) \xrightarrow{\mathrm{res}} H^3(G_{v_1}, \mathbb{Z}) \oplus H^3(G_{v_2}, \mathbb{Z}) \oplus H^3(G_{v_3}, \mathbb{Z})$ is an isomorphism because $H^3(G, \mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ and $H^3(V_4, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Ono [**Ono63**] established the relationship between the Hasse norm principle for $K/k$ and the Hasse principle for all torsors under the norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ of $K/k$:

THEOREM 1.9 (Ono [**Ono63**, page 70], see also Platonov [**Pla82**, page 44], Kunyavskii [**Kun84**, Remark 3], Platonov and Rapinchuk [**PR94**, page 307]). *Let $k$ be a global field and $K/k$ be a finite extension. Then*

$$Ш(R^{(1)}_{K/k}(\mathbb{G}_m)) \simeq (N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times).$$

*In particular,* $Ш(R^{(1)}_{K/k}(\mathbb{G}_m)) = 0$ *if and only if the Hasse norm principle holds for $K/k$.*

The Hasse norm principle for Galois extensions $K/k$ was investigated by Gerth [**Ger77**], [**Ger78**] and Gurak [**Gur78a**], [**Gur78b**], [**Gur80**] (see also [**PR94**, pages 308–309]), etc. Gurak [**Gur78a**] showed that the Hasse norm principle holds for Galois extension $K/k$ if all the Sylow subgroups of $\mathrm{Gal}(K/k)$ are cyclic. Note that this also follows from Theorem 1.9 and the retract $k$-rationality of $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ due to Endo and Miyata [**EM75**, Theorem 2.3].

However, for non-Galois extension $K/k$, very little is known about the Hasse norm principle. Bartels [**Bar81a**] (resp. [**Bar81b**]) showed that the Hasse norm principle for $K/k$ holds when

$[K : k]$ is prime (resp. $\mathrm{Gal}(L/k) \simeq D_n$). The former case also follows from Theorem 1.9 and the retract $k$-rationality of $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ due to Colliot-Thélène and Sansuc [**CTS87**, Proposition 9.1] (see Theorem 1.19).

THEOREM 1.10 (Voskresenskii and Kunyavskii [**VK84**], see also Voskresenskii [**Vos88**, Theorem 4, Corollary]). *Let $k$ be a number field, $K/k$ be a finite extension of degree $n$ and $L/k$ be the Galois closure of $K/k$ with $\mathrm{Gal}(L/k) \simeq S_n$; the symmetric group of degree $n$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$ and $X$ be a smooth $k$-compactification of $T$. Then $H^1(S_n, \mathrm{Pic}\, X_L) = 0$. In particular, $T$ has the weak approximation property and the Hasse norm principle holds for $K/k$.*

THEOREM 1.11 (Macedo [**Mac20**]). *Let $k$ be a number field, $K/k$ be a finite extension of degree $n \geq 5$ and $L/k$ be the Galois closure of $K/k$ with $\mathrm{Gal}(L/k) \simeq A_n$; the alternating group of degree $n \geq 5$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$. Then $Ш^2_\omega(A_n, \widehat{T}) = 0$. In particular, $T$ has the weak approximation property and the Hasse norm principle holds for $K/k$.*

REMARK 1.12. Applying Theorem 1.2 to $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, it follows from Theorem 1.9 that $H^1(k, \mathrm{Pic}\, \overline{X}) = 0$ if and only if $A(T) = 0$ and $Ш(T) = 0$, i.e. $T$ has the weak approximation property and the Hasse norm principle holds for $K/k$. In the algebraic language, the latter condition $Ш(T) = 0$ means that for the corresponding norm hypersurface $f(x_1, \ldots, x_n) = b$, it has a $k$-rational point if and only if it has a $k_v$-rational point for any valuation $v$ of $k$ where $f \in k[x_1, \ldots, x_n]$ is the polynomial of total degree $n$ defined by the norm map $N_{K/k} : K^\times \to k^\times$ and $b \in k^\times$ (see [**Vos98**, Example 4, page 122]).

Let $nTm$ be the $m$-th transitive subgroup of $S_n$ up to conjugacy (see Butler and McKay [**BM83**], [**GAP**]).

Let $k$ be a number field, $K/k$ be a field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$ with $\mathrm{Gal}(L/k) \simeq G$. Then we may regard $G$ as the transitive subgroup $G = nTm \leq S_n$. Let $v$ be a place of $k$ and $G_v$ be the decomposition group of $G$ at $v$. Using Theorem 1.4, Kunyavskii [**Kun84**] gave a necessary and sufficient condition for the Hasse norm principle for $n = 4$:

THEOREM 1.13 (Kunyavskii [**Kun84**, page 1899]). *Let $k$ be a number field, $K/k$ be a field extension of degree 4 and $L/k$ be the Galois closure of $K/k$. Let $G = \mathrm{Gal}(L/k) = 4Tm$ $(1 \leq m \leq 5)$ be a transitive subgroup of $S_4$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = 4$. Let*

*$T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$. Then $A(T) \simeq Ш(T) = 0$ except for $4T2 \simeq V_4$ and $4T4 \simeq A_4$. For $4T2 \simeq V_4$ and $4T4 \simeq A_4$, either* (i) *$A(T) = 0$ and $Ш(T) \simeq \mathbb{Z}/2\mathbb{Z}$ or* (ii) *$A(T) \simeq \mathbb{Z}/2\mathbb{Z}$ and $Ш(T) = 0$, and the following conditions are equivalent:*
(ii) *$A(T) \simeq \mathbb{Z}/2\mathbb{Z}$ and $Ш(T) = 0$;*
(iii) *there exists a place $v$ of $k$ (which ramifies in $L$) such that $V_4 \leq G_v$.*

Drakokhrust and Platonov [**DP87**] gave a necessary and sufficient condition for the Hasse norm principle for $n = 6$ ($G = 6Tm$ $(1 \leq m \leq 16)$):

THEOREM 1.14 (Drakokhrust and Platonov [**DP87**, Lemma 12, Proposition 6, Lemma 13]). *Let $k$ be a number field, $K/k$ be a field extension of degree 6 and $L/k$ be the Galois closure of $K/k$. Let $G = \mathrm{Gal}(L/k) = 6Tm$ $(1 \leq m \leq 16)$ be a transitive subgroup of $S_6$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = 6$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$. Then $Ш(T) = 0$ except for $6T4 \simeq A_4$ and $6T12 \simeq A_5$. For $6T4 \simeq A_4$ and $6T12 \simeq A_5$,* (i) *$Ш(T) \leq \mathbb{Z}/2\mathbb{Z}$; and* (ii) *$Ш(T) = 0$ if and only if there exists a place $v$ of $k$ (which ramifies in $L$) such that $V_4 \leq G_v$.*

The number of transitive subgroups $nTm$ of $S_n$ $(2 \leq n \leq 15)$ up to conjugacy is given as follows (see Butler and McKay [**BM83**] for $n \leq 11$, Royle [**Roy87**] for $n = 12$, Butler [**But93**] for $n = 14, 15$ and [**GAP**]):

| $n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| # of $nTm$ | 1 | 2 | 5 | 5 | 16 | 7 | 50 | 34 | 45 | 8 | 301 | 9 | 63 | 104 |

The following theorem which is one of the main results of this chapter classifies the norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ with non-vanishing $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0$ for $[K : k] = n \leq 15$ and $n \neq 12$.

THEOREM 1.15. *Let $2 \leq n \leq 15$ be an integer with $n \neq 12$. Let $k$ be a field, $K/k$ be a separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that $G = \mathrm{Gal}(L/k) = nTm$ is a transitive subgroup of $S_n$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$ of dimension $n - 1$ and $X$ be a smooth $k$-compactification of $T$. Then $H^1(k, \mathrm{Pic}\,\overline{X}) \neq 0$ if and only if $G$ is given as in Table 1. In particular, if $k$ is a number field and $L/k$ is an unramified extension, then $A(T) = 0$ and $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq Ш(T)$.*

Table 1: $H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl}) \neq 0$ where $G = nTm$ with $2 \leq n \leq 15$ and $n \neq 12$

| $G$ | $H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl})$ |
|---|---|
| $4T2 \simeq V_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $4T4 \simeq A_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $6T4 \simeq A_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $6T12 \simeq A_5$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T2 \simeq C_4 \times C_2$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T3 \simeq (C_2)^3$ | $(\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$ |
| $8T4 \simeq D_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T9 \simeq D_4 \times C_2$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T11 \simeq (C_4 \times C_2) \rtimes C_2$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T13 \simeq A_4 \times C_2$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T14 \simeq S_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T15 \simeq C_8 \rtimes V_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T19 \simeq (C_2)^3 \rtimes C_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T21 \simeq (C_2)^3 \rtimes C_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T22 \simeq (C_2)^3 \rtimes V_4$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T31 \simeq ((C_2)^4 \rtimes C_2) \rtimes C_2$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T32 \simeq ((C_2)^3 \rtimes V_4) \rtimes C_3$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T37 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $8T38 \simeq (((C_2)^4 \rtimes C_2) \rtimes C_2) \rtimes C_3$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $9T2 \simeq (C_3)^2$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $9T5 \simeq (C_3)^2 \rtimes C_2$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $9T7 \simeq (C_3)^2 \rtimes C_3$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $9T9 \simeq (C_3)^2 \rtimes C_4$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $9T11 \simeq (C_3)^2 \rtimes C_6$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $9T14 \simeq (C_3)^2 \rtimes Q_8$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $9T23 \simeq ((C_3)^2 \rtimes Q_8) \rtimes C_3$ | $\mathbb{Z}/3\mathbb{Z}$ |
| $10T7 \simeq A_5$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9) \simeq A_6$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $10T32 \simeq S_6$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$ | $\mathbb{Z}/2\mathbb{Z}$ |
| $15T9 \simeq (C_5)^2 \rtimes C_3$ | $\mathbb{Z}/5\mathbb{Z}$ |
| $15T14 \simeq (C_5)^2 \rtimes S_3$ | $\mathbb{Z}/5\mathbb{Z}$ |

REMARK 1.16. In Table 1, only the abelian groups of prime exponent appear as $H^1(k, \mathrm{Pic}\,\overline{X})$. However, we find that $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/4\mathbb{Z}$ for $G = 12T31 \simeq (C_4)^2 \rtimes C_3$ and $G = 12T57 \simeq ((C_4 \times C_2) \rtimes C_4) \rtimes C_3$ by using the same technique as in the proof of Theorem 1.15.

In addition, by using the same method of Theorem 1.15, we get the vanishing $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$ for the 5 Mathieu groups $M_n \leq S_n$ where $n = 11, 12, 22, 23, 24$ (see Dixon and Mortimer [**DM96**, Chapter 6], Gorenstein, Lyons and Solomon [**GLS98**, Chapter 5] for the 5 Mathieu groups):

THEOREM 1.17. *Let $k$ be a field, $K/k$ be a separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that $G = \mathrm{Gal}(L/k) = M_n \leq S_n$ $(n = 11, 12, 22, 23, 24)$ is the Mathieu group of degree $n$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$ of dimension $n-1$ and $X$ be a smooth $k$-compactification of $T$. Then $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$. In particular, if $k$ is a number field, then $A(T) = 0$ and $Ш(T) = 0$.*

Let $Z(G)$ be the center of a group $G$, $[G, G]$ be the commutator group of $G$ and $\mathrm{Syl}_p(G)$ be a $p$-Sylow subgroup of $G$ where $p$ is a prime. Let $\mathrm{Orb}_G(i)$ be the orbit of $1 \leq i \leq n$ under the action of $G \leq S_n$.

By Theorem 1.15, we obtain the following theorem which gives a necessary and sufficient condition for the Hasse norm principle for $K/k$ where $[K : k] = n \leq 15$ and $n \neq 12$. Note that a place $v$ of $k$ with non-cyclic decomposition group $G_v$ as in Theorem 1.18 must be ramified in $L$ because if $v$ is unramified, then $G_v$ is cyclic.

THEOREM 1.18. *Let $2 \leq n \leq 15$ be an integer with $n \neq 12$. Let $k$ be a number field, $K/k$ be a field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that $G = \mathrm{Gal}(L/k) = nTm$ is a transitive subgroup of $S_n$, $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$ and $G_v$ is the decomposition group of $G$ at a place $v$ of $k$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$ of dimension $n-1$ and $X$ be a smooth $k$-compactification of $T$. Then $A(T) \simeq Ш(T) = 0$ except for the cases in Table 1. For the cases in Table 1 except for $G = 8T3$, either* (a) *$A(T) = 0$ and $Ш(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X})$ or* (b) *$A(T) \simeq H^1(k, \mathrm{Pic}\,\overline{X})$ and $Ш(T) = 0$. For $G = 8Tm$ $(m = 9, 11, 15, 19, 22, 32)$, we assume that $H$ is the stabilizer of one of the letters in $G$. Then a necessary and sufficient condition for $Ш(T) = 0$ is given as in Table 2.*

Table 2: $Ш(T) = 0$ for $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ and $G = \mathrm{Gal}(L/k) = nTm$ as in Table 1

| $G$ | $Ш(T) = 0$ if and only if there exists a place $v$ of $k$ such that |
|---|---|
| $4T2 \simeq V_4$<br>$4T4 \simeq A_4$ | $V_4 \leq G_v$ (Tate [**Tat67**] for $4T2 \simeq V_4$)<br>(Kunyavskii [**Kun84**] for $4T4 \simeq A_4$) |
| $6T4 \simeq A_4$<br>$6T12 \simeq A_5$ | $V_4 \leq G_v$ (Drakokhrust and Platonov [**DP87**]) |
| $8T3 \simeq (C_2)^3$ | (see the second paragraph after Theorem 1.8 (Tate [Tat67])) |
| $8T4 \simeq D_4$<br>$8T13 \simeq A_4 \times C_2$<br>$8T14 \simeq S_4$<br>$8T37 \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ | $V_4 \leq G_v$ (Tate [**Tat67**] for $8T4 \simeq D_4$) |
| $8T2 \simeq C_4 \times C_2$<br>$8T21 \simeq (C_2)^3 \rtimes C_4$ | $G_v = G$ (Tate [**Tat67**] for $8T2 \simeq C_4 \times C_2$) |
| $8T31 \simeq (C_2)^4 \rtimes V_4$<br>$8T38 \simeq 8T31 \rtimes C_3$ | (i) $V_4 \leq G_v$ where $V_4 \cap [\mathrm{Syl}_2(G), \mathrm{Syl}_2(G)] = 1$ with $\mathrm{Syl}_2(G) \lhd G$ (equivalently, $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$), (ii) $C_4 \times C_2 \leq G_v$ where $(C_4 \times C_2) \cap [\mathrm{Syl}_2(G), \mathrm{Syl}_2(G)] \simeq C_2$ (equivalently, $C_4 \times C_2$ is transitive in $S_8$) or (iii) $(C_2)^3 \rtimes C_4 \leq G_v$ |
| $8T9 \simeq D_4 \times C_2$ | (i) $V_4 \leq G_v$ where $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap [G, G] = 1$; or (ii) $C_4 \times C_2 \leq G_v$ |
| $8T11 \simeq Q_8 \rtimes C_2$ | $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is transitive in $S_8$ |
| $8T15 \simeq C_8 \rtimes V_4$ | (i) $V_4 \leq G_v$ where $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 2$ for any $1 \leq i \leq 8$ and $V_4 \cap [G, G] = 1$ (equivalently, $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 2$ for any $1 \leq i \leq 8$ and $V_4$ is not in $A_8$) or (ii) $C_4 \times C_2 \leq G_v$ where $(C_4 \times C_2) \cap [G, G] \simeq C_2$ (equivalently, $C_4 \times C_2$ is transitive in $S_8$) |
| $8T19 \simeq (C_2)^3 \rtimes C_4$ | (i) $V_4 \leq G_v$ where $V_4 \cap Z(G) = 1$ and $V_4 \cap Z^2(G) \simeq C_2$ with the upper central series $1 \leq Z(G) \leq Z^2(G) \leq G$ (equivalently, $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$); or (ii) $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is not transitive in $S_8$ or $[G, G] \leq C_4 \times C_2$ |
| $8T22 \simeq (C_2)^3 \rtimes V_4$<br>$8T32 \simeq 8T22 \rtimes C_3$ | (i) $V_4 \leq G_v$ where $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$ or (ii) $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is transitive in $S_8$ |
| $9T2 \simeq (C_3)^2$<br>$9T5 \simeq (C_3)^2 \rtimes C_2$<br>$9T7 \simeq (C_3)^2 \rtimes C_3$<br>$9T9 \simeq (C_3)^2 \rtimes C_4$<br>$9T11 \simeq (C_3)^2 \rtimes C_6$<br>$9T14 \simeq (C_3)^2 \rtimes Q_8$<br>$9T23 \simeq 9T14 \rtimes C_3$ | $(C_3)^2 \leq G_v$ (Tate [**Tat67**] for $9T2 \simeq (C_3)^2$) |
| $10T7 \simeq A_5$ | $V_4 \leq G_v$ |
| $10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9)$ | $D_4 \leq G_v$ |
| $10T32 \simeq S_6$ | (i) $V_4 \leq G_v$ where $N_{\widetilde{G}}(V_4) \simeq C_8 \rtimes (C_2 \times C_2)$ for the normalizer $N_{\widetilde{G}}(V_4)$ of $V_4$ in $\widetilde{G}$ with the normalizer $\widetilde{G} = N_{S_{10}}(G) \simeq \mathrm{Aut}(G)$ of $G$ in $S_{10}$ (equivalently, $\lvert\mathrm{Orb}_{V_4}(i)\rvert = 2$ for any $1 \leq i \leq 10$) or (ii) $D_4 \leq G_v$ where $D_4 \leq [G, G] \simeq A_6$ |
| $14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$ | $V_4 \leq G_v$ |
| $15T9 \simeq (C_5)^2 \rtimes C_3$<br>$15T14 \simeq (C_5)^2 \rtimes S_3$ | $(C_5)^2 \leq G_v$ |

We organize this chapter as follows. In Section 2, we prepare some basic definitions and known results about the rationality problem for norm one tori. In Section 3, we recall our basic tool "flabby resolution of $G$-lattices" to investigate algebraic $k$-tori. In Section 4, we give the proof of Theorem 1.5 and Theorem 1.6. In Section 5, the proofs of Theorem 1.15 and Theorem 1.17 are given. In Section 6, we prove Theorem 1.18 by using Drakokhrust and Platonov's method for the Hasse norm principle for $K/k$. In Section 7, we will give an application of Theorem 1.5, Theorem 1.6 and Theorem 1.15 to obtain the group $T(k)/R$ of $R$-equivalence classes over a local field $k$ via the formula of Colliot-Thélène and Sansuc. In Section 8, we also give an application of Theorem 1.5, Theorem 1.6 and Theorem 1.18 to evaluate the Tamagawa number $\tau(T)$ over a number field $k$ via Ono's formula. In Section 9, we will give GAP computations of $H^1(G, J_{G/H})$ as the appendix of this chapter. GAP algorithms will be given in Section 10 which are also available from `https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/Norm1ToriHNP`.

## 2. Rationality problem for norm one tori

Let $k$ be a field, $K/k$ be a separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. The Galois group $G$ may be regarded as a transitive subgroup of the symmetric group $S_n$ of degree $n$ via an injection $G \to S_n$ which is derived from the action of $G$ on the left cosets $\{g_1H, \dots, g_nH\}$ by $g(g_iH) = (gg_i)H$ for any $g \in G$ and we may assume that $H$ is the stabilizer of one of the letters in $G$, i.e. $L = k(\theta_1, \dots, \theta_n)$ and $K = k(\theta_i)$ for some $1 \leq i \leq n$. The norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ has the Chevalley module $J_{G/H}$ as its character module where $J_{G/H} = (I_{G/H})^\circ = \mathrm{Hom}_{\mathbb{Z}}(I_{G/H}, \mathbb{Z})$ is the dual lattice of $I_{G/H} = \mathrm{Ker}\,\varepsilon$ and $\varepsilon : \mathbb{Z}[G/H] \to \mathbb{Z}$ is the augmentation map (see [**Vos98**, Section 4.8]). We have the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G/H] \to J_{G/H} \to 0$$

and rank $J_{G/H} = n - 1$. Write $J_{G/H} = \oplus_{1 \leq i \leq n-1} \mathbb{Z}u_i$. We define the action of $G$ on $L(x_1, \dots, x_{n-1})$ by $\sigma(x_i) = \prod_{j=1}^n x_j^{a_{i,j}} (1 \leq i \leq n)$ for any $\sigma \in G$, when $\sigma(u_i) = \sum_{j=1}^n a_{i,j}u_j$ ($a_{i,j} \in \mathbb{Z}$). Then the invariant field $L(x_1, \dots, x_{n-1})^G$ may be identified with the function field of the norm one torus $R^{(1)}_{K/k}(\mathbb{G}_m)$ (see [**EM75**, Section 1]).

Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$. The rationality problem for norm one tori is investigated by [**EM75**], [**CTS77**], [**Hür84**], [**CTS87**], [**LeB95**], [**CK00**], [**LL00**], [**Flo**], [**End11**], [**HY17**], [**HY21**], [**HHY20**].

THEOREM 1.19 (Colliot-Thélène and Sansuc [**CTS87**, Proposition 9.1], [**LeB95**, Theorem 3.1], [**CK00**, Proposition 0.2], [**LL00**], Endo [**End11**, Theorem 4.1], see also [**End11**, Remark 4.2 and Theorem 4.3]). *Let $K/k$ be a non-Galois separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that* $\mathrm{Gal}(L/k) = S_n$*, $n \geq 3$, and* $\mathrm{Gal}(L/K) = S_{n-1}$ *is the stabilizer of one of the letters in $S_n$. Then we have:*
(i) $R^{(1)}_{K/k}(\mathbb{G}_m)$ *is retract $k$-rational if and only if $n$ is a prime;*
(ii) $R^{(1)}_{K/k}(\mathbb{G}_m)$ *is (stably) $k$-rational if and only if $n = 3$.*

THEOREM 1.20 (Endo [**End11**, Theorem 4.4], Hoshi and Yamasaki [**HY17**, Corollary 1.11]). *Let $K/k$ be a non-Galois separable field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that* $\mathrm{Gal}(L/k) = A_n$*, $n \geq 4$, and* $\mathrm{Gal}(L/K) = A_{n-1}$ *is the stabilizer of one of the letters in $A_n$. Then we have:*
(i) $R^{(1)}_{K/k}(\mathbb{G}_m)$ *is retract $k$-rational if and only if $n$ is a prime.*
(ii) $R^{(1)}_{K/k}(\mathbb{G}_m)$ *is stably $k$-rational if and only if $n = 5$.*

A necessary and sufficient condition for the classification of stably/retract rational norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ with $[K : k] = n \leq 15$, but with one exception $G = 9T27 \simeq \mathrm{PSL}_2(\mathbb{F}_8)$ for the stable rationality, was given in Hoshi and Yamasaki [**HY21**] (for the case $n$ is a prime number or the case $n \leq 10$) and Hasegawa, Hoshi and Yamasaki [**HHY20**] (for $n = 12, 14, 15$).

## 3. Strategy: flabby resolution of $G$-lattices

We recall some basic facts of the theory of flabby (flasque) $G$-lattices (see [**CTS77**], [**Swa83**], [**Vos98**, Chapter 2], [**Lor05**, Chapter 2], [**Swa10**]). Recall also that we may take the $G$-lattice $\widehat{T}$ for an algebraic $k$-torus $T$ (see Section 1).

DEFINITION 1.21. Let $G$ be a finite group and $M$ be a $G$-lattice (i.e. finitely generated $\mathbb{Z}[G]$-module which is $\mathbb{Z}$-free as an abelian group).
(i) $M$ is called a *permutation* $G$-lattice if $M$ has a $\mathbb{Z}$-basis permuted by $G$, i.e. $M \simeq \oplus_{1 \leq i \leq m} \mathbb{Z}[G/H_i]$ for some subgroups $H_1, \ldots, H_m$ of $G$.
(ii) $M$ is called a *stably permutation* $G$-lattice if $M \oplus P \simeq P'$ for some permutation $G$-lattices $P$ and $P'$.
(iii) $M$ is called *invertible* (or *permutation projective*) if it is a direct summand of a permutation $G$-lattice, i.e. $P \simeq M \oplus M'$ for some permutation $G$-lattice $P$ and a $G$-lattice $M'$.
(iv) $M$ is called *flabby* (or *flasque*) if $\widehat{H}^{-1}(H, M) = 0$ for any subgroup $H$ of $G$ where $\widehat{H}$ is the

Tate cohomology.
(v) $M$ is called *coflabby* (or *coflasque*) if $H^1(H, M) = 0$ for any subgroup $H$ of $G$.

DEFINITION 1.22 (see [**EM75**, Section 1], [**Vos98**, Section 4.7]). Let $\mathcal{C}(G)$ be the category of all $G$-lattices. Let $\mathcal{S}(G)$ be the full subcategory of $\mathcal{C}(G)$ of all permutation $G$-lattices and $\mathcal{D}(G)$ be the full subcategory of $\mathcal{C}(G)$ of all invertible $G$-lattices. Let

$$\mathcal{H}^i(G) = \{M \in \mathcal{C}(G) \mid \widehat{H}^i(H, M) = 0 \text{ for any } H \leq G\} \ (i = \pm 1)$$

be the class of "$\widehat{H}^i$-vanish" $G$-lattices where $\widehat{H}^i$ is the Tate cohomology. Then we have the inclusions $\mathcal{S}(G) \subset \mathcal{D}(G) \subset \mathcal{H}^i(G) \subset \mathcal{C}(G)$ $(i = \pm 1)$.

DEFINITION 1.23. We say that two $G$-lattices $M_1$ and $M_2$ are *similar* if there exist permutation $G$-lattices $P_1$ and $P_2$ such that $M_1 \oplus P_1 \simeq M_2 \oplus P_2$. We denote the similarity class of $M$ by $[M]$. The set of similarity classes $\mathcal{C}(G)/\mathcal{S}(G)$ becomes a commutative monoid (with respect to the sum $[M_1] + [M_2] := [M_1 \oplus M_2]$ and the zero $0 = [P]$ where $P \in \mathcal{S}(G)$).

THEOREM 1.24 (Endo and Miyata [**EM75**, Lemma 1.1], Colliot-Thélène and Sansuc [**CTS77**, Lemma 3], see also [**Swa83**, Lemma 8.5], [**Lor05**, Lemma 2.6.1]). *For any $G$-lattice $M$, there exists a short exact sequence of $G$-lattices $0 \to M \to P \to F \to 0$ where $P$ is permutation and $F$ is flabby.*

DEFINITION 1.25. The exact sequence $0 \to M \to P \to F \to 0$ as in Theorem 1.24 is called a *flabby resolution* of the $G$-lattice $M$. $\rho_G(M) = [F] \in \mathcal{C}(G)/\mathcal{S}(G)$ is called *the flabby class* of $M$, denoted by $[M]^{fl} = [F]$. Note that $[M]^{fl}$ is well-defined: if $[M] = [M']$, $[M]^{fl} = [F]$ and $[M']^{fl} = [F']$ then $F \oplus P_1 \simeq F' \oplus P_2$ for some permutation $G$-lattices $P_1$ and $P_2$, and therefore $[F] = [F']$ (cf. [**Swa83**, Lemma 8.7]). We say that $[M]^{fl}$ is *invertible* if $[M]^{fl} = [E]$ for some invertible $G$-lattice $E$.

For $G$-lattice $M$, it is not difficult to see

$$\begin{array}{ccccccc} \text{permutation} & \Rightarrow & \text{stably permutation} & \Rightarrow & \text{invertible} & \Rightarrow & \text{flabby and coflabby} \\ & & \Downarrow & & \Downarrow & & \\ & & [M]^{fl} = 0 & \Rightarrow & [M]^{fl} \text{ is invertible.} & & \end{array}$$

The above implications in each step cannot be reversed (see, for example, [**HY17**, Section 1]).

Let $T$ be an algebraic $k$-torus and $\widehat{T} = \mathrm{Hom}(T, \mathbb{G}_m)$ be the character module of $T$. Then $\widehat{T}$ becomes a $G$-lattice where $G = \mathrm{Gal}(L/k)$ is the Galois group of $L/k$ and $L$ is the minimal splitting field of $T$. The flabby class $\rho_G(\widehat{T}) = [\widehat{T}]^{fl}$ plays crucial role in the rationality problem for $T$ as follows (see Voskresenskii's fundamental book [**Vos98**, Section 4.6] and Kunyavskii [**Kun07**], see also e.g. Swan [**Swa83**], Kunyavskii [**Kun90**, Section 2], Lemire, Popov and Reichstein [**LPR06**, Section 2], Kang [**Kan12**], Yamasaki [**Yam12**], Hoshi and Yamasaki [**HY17**]):

THEOREM 1.26 (Endo and Miyata [**EM73**], Voskresenskii [**Vos74**], Saltman [**Sal84**]). *Let $T$ and $T'$ be algebraic $k$-tori with the same minimal splitting field $L$. Then we have:*
(i) (Endo and Miyata [**EM73**, Theorem 1.6]) $[\widehat{T}]^{fl} = 0$ *if and only if $T$ is stably $k$-rational;*
(ii) (Voskresenskii [**Vos74**, Theorem 2]) $[\widehat{T}]^{fl} = [\widehat{T'}]^{fl}$ *if and only if $T$ and $T'$ are stably $k$-isomorphic;*
(iii) (Saltman [**Sal84**, Theorem 3.14]) $[\widehat{T}]^{fl}$ *is invertible if and only if $T$ is retract $k$-rational.*

For norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$, recall that $\widehat{T} = J_{G/H}$. Hence we have

$$\begin{aligned} [J_{G/H}]^{fl} = 0 \quad \Rightarrow \quad [J_{G/H}]^{fl} \text{ is invertible} \quad &\Rightarrow \quad H^1(G, [J_{G/H}]^{fl}) = 0 \\ &\Rightarrow \quad A(T) = 0 \text{ and } Ш(T) = 0 \end{aligned}$$

where the last implication holds over a global field $k$ (see also Colliot-Thélène and Sansuc [**CTS77**, page 29]). The last conditions mean that $T$ has the weak approximation property and the Hasse norm principle holds for $K/k$ (see Section 1). In particular, it follows from Theorem 1.19 that $H^1(G, [J_{G/H}]^{fl}) = 0$ and hence $A(T) = 0$ and $Ш(T) = 0$ when $G = pTm \leq S_p$ is a transitive subgroup of $S_p$ of prime degree $p$ and $H \leq G$ with $[G : H] = p$ (see [**HY17**, Lemma 2.17] and also the first paragraph of Section 5).

## 4. Proof of Theorem 1.5 and Theorem 1.6

We will give the proof of Theorem 1.27 and Theorem 1.28 which are detailed statements of Theorem 1.5 and Theorem 1.6 respectively:

THEOREM 1.27. *Let $k$ be a field, $T$ be an algebraic $k$-torus of dimension 4 and $X$ be a smooth $k$-compactification of $T$. Among the (at most) 216 cases of not retract rational algebraic $k$-tori $T$, there exist 2 (resp. 20, 194) cases of algebraic $k$-tori with $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (resp. $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$, $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$). Moreover, for the character module $\widehat{T} \simeq M_G$ of $T$ with $H^1(k, \mathrm{Pic}\,\overline{X}) \simeq H^1(G, [M_G]^{fl})$, we have*

(i) $H^1(G,[M_G]^{fl}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ *if and only if the* GAP ID *of* $G$ *is one of* $(4,32,1,2)$ *and* $(4,33,3,1)$ *where* $M_G$ *is an indecomposable* $G$*-lattice of rank* 4 *and* $G$ *is isomorphic to* $Q_8$ *and* $\mathrm{SL}_2(\mathbb{F}_3)$ *respectively;*
(ii) $H^1(G,[M_G]^{fl}) \simeq \mathbb{Z}/2\mathbb{Z}$ *if and only if*
(ii-1) *the* GAP ID *of* $G$ *is one of* $(4,5,1,12)$, $(4,5,2,8)$, $(4,6,2,10)$, $(4,12,2,6)$, $(4,12,4,12)$, $(4,12,5,10)$, $(4,18,1,3)$, $(4,18,4,4)$, $(4,32,2,2)$, $(4,32,3,2)$, $(4,32,4,2)$, $(4,32,6,2)$, $(4,33,5,1)$, $(4,33,6,1)$, $(4,33,9,1)$ *where* $M_G$ *is an indecomposable* $G$*-lattice of rank* 4 *and* $G$ *is isomorphic to* $V_4$, $(C_2)^3$, $(C_2)^3$, $C_4 \times C_2$, $D_4$, $C_2 \times D_4$, $C_4 \times C_2$, $C_2 \times D_4$, $Q_{16}$, $QD_8$, $(C_4 \times C_2) \rtimes C_2$, $C_8 \rtimes V_4$, $((C_4 \times C_2) \rtimes C_2) \rtimes C_3$, $\mathrm{GL}_2(\mathbb{F}_3)$, $\mathrm{GL}_2(\mathbb{F}_3) \rtimes C_2$ *respectively; or*
(ii-2) *the* GAP ID *of* $G$ *is one of* $(4,4,3,6)$, $(4,5,1,9)$, $(4,6,2,9)$, $(4,24,1,5)$, $(4,25,2,4)$ *where* $M_G$ *is a decomposable* $G$*-lattice of rank* $4 = 3+1$ *and* $G$ *is isomorphic to* $V_4$, $V_4$, $(C_2)^3$, $A_4$, $C_2 \times A_4$ *respectively.*

Proof. It follows from [**HY17**, Theorem 1.9] that among the 710 cases of 4-dimensional algebraic $k$-tori, there exist 216 cases of algebraic $k$-tori which are not retract $k$-rational. Because if $T$ is retract $k$-rational, then $H^1(k,\mathrm{Pic}\,\overline{X}) \simeq H^1(G,[M_G]^{fl}) = 0$, we should check only the 216 cases. The GAP IDs of such 216 groups $G \leq \mathrm{GL}_4(\mathbb{Z})$ with $[M_G]^{fl}$ is not invertible, are given in [**HY17**, Tables 3, 4] (see [**HY17**, Chapter 3] for the explanation of GAP ID). They are also given in [**HY17**, Example 10.1] as the lists `N4` (resp. `N31`) when $M_G$ is indecomposable (resp. decomposable with rank $4 = 3+1$) and available from
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/MultInvField/NonInv.dat`.

Then we apply the function `FlabbyResolutionLowRank(`$G$`).actionF` (see also [**HHY20**, Algorithm 4.1]) which returns a suitable flabby class $F$ of $M_G$ ($[F] = [M_G]^{fl}$) with low rank by using the backtracking techniques. The function `H1` may compute the group $H^1(G,F)$ (see Example 1.30). The related functions are available from
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbNorm1Tori/`. □

Theorem 1.28. *Let* $k$ *be a field,* $T$ *be an algebraic* $k$*-torus of dimension* 5 *and* $X$ *be a smooth* $k$*-compactification of* $T$*. Among the* (*at most*) 3003 *cases of not retract rational algebraic* $k$*-tori* $T$*, there exist* 11 (*resp.* 263, 2729) *cases of algebraic* $k$*-tori with* $H^1(k,\mathrm{Pic}\,\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ (*resp.* $H^1(k,\mathrm{Pic}\,\overline{X}) \simeq \mathbb{Z}/2\mathbb{Z}$, $H^1(k,\mathrm{Pic}\,\overline{X}) = 0$)*. Moreover, for the character module* $\widehat{T} \simeq M_G$ *of* $T$ *with* $H^1(k,\mathrm{Pic}\,\overline{X}) \simeq H^1(G,[M_G]^{fl})$*, we have*
(i) $H^1(G,[M_G]^{fl}) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ *if and only if*
(i-1) *the* CARAT ID *of* $G$ *is one of the* 6 *triples* $(5,31,26)$, $(5,31,27)$, $(5,664,2)$, $(5,669,2)$, $(5,670,2)$, $(5,773,4)$ *where* $M_G$ *is an indecomposable* $G$*-lattice of rank* 5 *and* $G$ *is isomorphic*

*to* $(C_2)^3$, $(C_2)^3$, $C_2 \times Q_8$, $(C_4 \times C_2) \rtimes C_2$, $(C_4 \times C_2) \rtimes C_2$, $Q_8$ *respectively; or*
(i-2) *the* CARAT ID *of* $G$ *is one of the* 5 *triples* $(5, 664, 1)$, $(5, 773, 3)$, $(5, 774, 3)$, $(5, 691, 1)$, $(5, 730, 1)$ *where* $M_G$ *is a decomposable* $G$*-lattice of rank* $5 = 4 + 1$ *and* $G$ *is isomorphic to* $C_2 \times Q_8$, $Q_8$, $Q_8$, $\mathrm{SL}_2(\mathbb{F}_3)$, $C_2 \times \mathrm{SL}_2(\mathbb{F}_3)$ *respectively.*
(ii) $H^1(G, [M_G]^{fl}) \simeq \mathbb{Z}/2\mathbb{Z}$ *if and only if*
(ii-1) *the* CARAT ID *of* $G$ *is one of the* 141 *triples as in Example 1.31 where* $M_G$ *is an indecomposable* $G$*-lattice of rank* 5*;*
(ii-2) *the* CARAT ID *of* $G$ *is one of the* 73 *triples as in Example 1.31 where* $M_G$ *is a decomposable* $G$*-lattice of rank* $5 = 4 + 1$*;*
(ii-3) *the* CARAT ID *of* $G$ *is one of the* 36 *triples as in Example 1.31 where* $M_G$ *is a decomposable* $G$*-lattice of rank* $5 = 3 + 2$*; or*
(ii-4) *the* CARAT ID *of* $G$ *is one of the* 13 *triples as in Example 1.31 where* $M_G$ *is a decomposable* $G$*-lattice of rank* $5 = 3 + 1 + 1$.

Proof. The method is the same as in the proof of Theorem 1.27. By [**HY17**, Theorem 1.12], among the 6079 cases of 5-dimensional algebraic $k$-tori, there exist 3003 cases of algebraic $k$-tori which are not retract $k$-rational. The CARAT IDs of such 3003 groups $G \leq \mathrm{GL}_5(\mathbb{Z})$ with $[M_G]^{fl}$ is not invertible, are given in [**HY17**, Tables 12, 13, 14, 15]. They are also given in [**HY17**, Example 4.12 and Example 11.1] as the lists `N5`, `N41`, `N32`, `N311` when $M_G$ is indecomposable (resp. decomposable with rank $5 = 4 + 1$, $5 = 3 + 1$, $5 = 3 + 1 + 1$) and available from
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/MultInvField/NonInv5.dat`.

Then we apply the functions `FlabbyResolutionLowRank(`$G$`).actionF` in [**HHY20**, Algorithm 4.1] and `H1` to get $H^1(G, [M_G]^{fl})$ (see Example 1.31 and also the proof of Theorem 1.27). □

Example 1.29 (Classification of $H^1(G, [M_G]^{fl}) \neq 0$ for $G \leq \mathrm{GL}_3(\mathbb{Z})$).

```
gap> Read("FlabbyResolutionFromBase.gap");
gap> Read("NonInv.dat");
# N3 is the list of GAP IDs (Crystcat IDs) of indecomposable lattice of rank 3
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
gap> N3;
[ [ 3, 3, 1, 3 ], [ 3, 3, 3, 3 ], [ 3, 3, 3, 4 ], [ 3, 4, 3, 2 ], [ 3, 4, 4, 2 ],
  [ 3, 4, 6, 3 ], [ 3, 4, 7, 2 ], [ 3, 7, 1, 2 ], [ 3, 7, 2, 2 ], [ 3, 7, 2, 3 ],
  [ 3, 7, 3, 2 ], [ 3, 7, 3, 3 ], [ 3, 7, 4, 2 ], [ 3, 7, 5, 2 ], [ 3, 7, 5, 3 ] ]
```

```
gap> Length(N3); # there exist 15 not retract rational tori in dim=3 [HY17, Table 1]
15
gap> N3g:=List(N3,x->MatGroupZClass(x[1],x[2],x[3],x[4]));;
gap> List(N3g,StructureDescription);
[ "C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C4 x C2", "D8", "D8", "C2 x D8",
"A4", "C2 x A4", "C2 x A4", "S4", "S4", "S4", "C2 x S4", "C2 x S4" ]
gap> N3gF:=List(N3g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N3H1F:=List(N3gF,x->Filtered(H1(x),y->y>1)); # H1(F)
[ [ 2 ], [  ], [  ], [  ], [  ], [  ], [  ], [ 2 ], [  ], [  ], [  ], [  ], [  ], [  ], [  ] ]
gap> N3H1FC2:=Filtered([1..Length(N3gF)],x->N3H1F[x]=[2]);
[ 1, 8 ]
gap> List(N3H1FC2,x->N3[x]); # GAP ID's of F with H1(F)=C2
[ [ 3, 3, 1, 3 ], [ 3, 7, 1, 2 ] ]
gap> List(N3H1FC2,x->StructureDescription(N3g[x]));
[ "C2 x C2", "A4" ]
```

EXAMPLE 1.30 (Classification of $H^1(G,[M_G]^{fl}) \neq 0$ for $G \leq \mathrm{GL}_4(\mathbb{Z})$).

```
gap> Read("FlabbyResolutionFromBase.gap");
gap> Read("NonInv.dat");
# N4 is the list of GAP IDs (Crystcat IDs) of indecomposable lattice of rank 4
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
gap> N4;
[ [ 4, 5, 1, 12 ], [ 4, 5, 2, 5 ], [ 4, 5, 2, 8 ], [ 4, 5, 2, 9 ], [ 4, 6, 1, 6 ],
  [ 4, 6, 1, 11 ], [ 4, 6, 2, 6 ], [ 4, 6, 2, 10 ], [ 4, 6, 2, 12 ], [ 4, 6, 3, 4 ],
  [ 4, 6, 3, 7 ], [ 4, 6, 3, 8 ], [ 4, 12, 2, 5 ], [ 4, 12, 2, 6 ], [ 4, 12, 3, 11 ],
  [ 4, 12, 4, 10 ], [ 4, 12, 4, 11 ], [ 4, 12, 4, 12 ], [ 4, 12, 5, 8 ], [ 4, 12, 5, 9 ],
  [ 4, 12, 5, 10 ], [ 4, 12, 5, 11 ], [ 4, 13, 1, 5 ], [ 4, 13, 2, 5 ], [ 4, 13, 3, 5 ],
  [ 4, 13, 4, 5 ], [ 4, 13, 5, 4 ], [ 4, 13, 5, 5 ], [ 4, 13, 6, 5 ], [ 4, 13, 7, 9 ],
  [ 4, 13, 7, 10 ], [ 4, 13, 7, 11 ], [ 4, 13, 8, 5 ], [ 4, 13, 8, 6 ], [ 4, 13, 9, 4 ],
  [ 4, 13, 9, 5 ], [ 4, 13, 10, 4 ], [ 4, 13, 10, 5 ], [ 4, 18, 1, 3 ], [ 4, 18, 2, 4 ],
  [ 4, 18, 2, 5 ], [ 4, 18, 3, 5 ], [ 4, 18, 3, 6 ], [ 4, 18, 3, 7 ], [ 4, 18, 4, 4 ],
  [ 4, 18, 4, 5 ], [ 4, 18, 5, 5 ], [ 4, 18, 5, 6 ], [ 4, 18, 5, 7 ], [ 4, 19, 1, 2 ],
  [ 4, 19, 2, 2 ], [ 4, 19, 3, 2 ], [ 4, 19, 4, 3 ], [ 4, 19, 4, 4 ], [ 4, 19, 5, 2 ],
  [ 4, 19, 6, 2 ], [ 4, 22, 1, 1 ], [ 4, 22, 2, 1 ], [ 4, 22, 3, 1 ], [ 4, 22, 4, 1 ],
  [ 4, 22, 5, 1 ], [ 4, 22, 5, 2 ], [ 4, 22, 6, 1 ], [ 4, 22, 7, 1 ], [ 4, 22, 8, 1 ],
  [ 4, 22, 9, 1 ], [ 4, 22, 10, 1 ], [ 4, 22, 11, 1 ], [ 4, 24, 2, 4 ], [ 4, 24, 2, 6 ],
  [ 4, 24, 4, 4 ], [ 4, 24, 5, 4 ], [ 4, 24, 5, 6 ], [ 4, 25, 1, 3 ], [ 4, 25, 2, 3 ],
  [ 4, 25, 2, 5 ], [ 4, 25, 3, 3 ], [ 4, 25, 4, 3 ], [ 4, 25, 5, 3 ], [ 4, 25, 5, 5 ],
```

```
  [ 4, 25, 6, 3 ], [ 4, 25, 6, 5 ], [ 4, 25, 7, 3 ], [ 4, 25, 8, 3 ], [ 4, 25, 9, 3 ],
  [ 4, 25, 9, 5 ], [ 4, 25, 10, 3 ], [ 4, 25, 10, 5 ], [ 4, 25, 11, 3 ], [ 4, 25, 11, 5 ],
  [ 4, 29, 1, 1 ], [ 4, 29, 1, 2 ], [ 4, 29, 2, 1 ], [ 4, 29, 3, 1 ], [ 4, 29, 3, 2 ],
  [ 4, 29, 3, 3 ], [ 4, 29, 4, 1 ], [ 4, 29, 4, 2 ], [ 4, 29, 5, 1 ], [ 4, 29, 6, 1 ],
  [ 4, 29, 7, 1 ], [ 4, 29, 7, 2 ], [ 4, 29, 8, 1 ], [ 4, 29, 8, 2 ], [ 4, 29, 9, 1 ],
  [ 4, 32, 1, 2 ], [ 4, 32, 2, 2 ], [ 4, 32, 3, 2 ], [ 4, 32, 4, 2 ], [ 4, 32, 5, 2 ],
  [ 4, 32, 5, 3 ], [ 4, 32, 6, 2 ], [ 4, 32, 7, 2 ], [ 4, 32, 8, 2 ], [ 4, 32, 9, 4 ],
  [ 4, 32, 9, 5 ], [ 4, 32, 10, 2 ], [ 4, 32, 11, 2 ], [ 4, 32, 11, 3 ], [ 4, 32, 12, 2 ],
  [ 4, 32, 13, 3 ], [ 4, 32, 13, 4 ], [ 4, 32, 14, 3 ], [ 4, 32, 14, 4 ], [ 4, 32, 15, 2 ],
  [ 4, 32, 16, 2 ], [ 4, 32, 16, 3 ], [ 4, 32, 17, 2 ], [ 4, 32, 18, 2 ], [ 4, 32, 18, 3 ],
  [ 4, 32, 19, 2 ], [ 4, 32, 19, 3 ], [ 4, 32, 20, 2 ], [ 4, 32, 20, 3 ], [ 4, 32, 21, 2 ],
  [ 4, 32, 21, 3 ], [ 4, 33, 1, 1 ], [ 4, 33, 3, 1 ], [ 4, 33, 4, 1 ], [ 4, 33, 5, 1 ],
  [ 4, 33, 6, 1 ], [ 4, 33, 7, 1 ], [ 4, 33, 8, 1 ], [ 4, 33, 9, 1 ], [ 4, 33, 10, 1 ],
  [ 4, 33, 11, 1 ], [ 4, 33, 12, 1 ], [ 4, 33, 13, 1 ], [ 4, 33, 14, 1 ], [ 4, 33, 14, 2 ],
  [ 4, 33, 15, 1 ], [ 4, 33, 16, 1 ] ]
gap> Length(N4); # there exist 152 not retract rational tori in dim=4 [HY17, Table 4]
152
gap> N4g:=List(N4,x->MatGroupZClass(x[1],x[2],x[3],x[4]));;
gap> N4gF:=List(N4g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N4H1F:=List(N4gF,x->Filtered(H1(x),y->y>1));;
gap> Collected(N4H1F);
[ [ [  ], 135 ], [ [ 2 ], 15 ], [ [ 2, 2 ], 2 ] ]

gap> N4H1FC2xC2:=Filtered([1..Length(N4H1F)],x->N4H1F[x]=[2,2]);
[ 106, 138 ]
gap> List(N4H1FC2xC2,x->N4[x]); # GAP ID's of F with H1(F)=C2xC2
[ [ 4, 32, 1, 2 ], [ 4, 33, 3, 1 ] ]
gap> List(N4H1FC2xC2,x->StructureDescription(N4g[x]));
[ "Q8", "SL(2,3)" ]

gap> N4H1FC2:=Filtered([1..Length(N4H1F)],x->N4H1F[x]=[2]);
[ 1, 3, 8, 14, 18, 21, 39, 45, 107, 108, 109, 112, 140, 141, 144 ]
gap> List(N4H1FC2,x->N4[x]); # GAP ID's of F with H1(F)=C2
[ [ 4, 5, 1, 12 ], [ 4, 5, 2, 8 ], [ 4, 6, 2, 10 ], [ 4, 12, 2, 6 ], [ 4, 12, 4, 12 ],
  [ 4, 12, 5, 10 ], [ 4, 18, 1, 3 ], [ 4, 18, 4, 4 ], [ 4, 32, 2, 2 ], [ 4, 32, 3, 2 ],
  [ 4, 32, 4, 2 ], [ 4, 32, 6, 2 ], [ 4, 33, 5, 1 ], [ 4, 33, 6, 1 ], [ 4, 33, 9, 1 ] ]
gap> List(N4H1FC2,x->StructureDescription(N4g[x]));
[ "C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C4 x C2", "D8", "C2 x D8", "C4 x C2",
  "C2 x D8", "C8 : C2", "QD16", "(C4 x C2) : C2", "C8 : (C2 x C2)",
```

```
  "((C4 x C2) : C2) : C3", "GL(2,3)", "GL(2,3) : C2" ]

# N31 is the list of GAP IDs (Crystcat IDs) of decomposable lattice of rank 4=3+1
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
gap> N31;
[ [ 4, 4, 3, 6 ], [ 4, 4, 4, 4 ], [ 4, 4, 4, 6 ], [ 4, 5, 1, 9 ], [ 4, 5, 2, 4 ],
  [ 4, 5, 2, 7 ], [ 4, 6, 1, 4 ], [ 4, 6, 1, 8 ], [ 4, 6, 2, 4 ], [ 4, 6, 2, 8 ],
  [ 4, 6, 2, 9 ], [ 4, 6, 3, 3 ], [ 4, 6, 3, 6 ], [ 4, 7, 3, 2 ], [ 4, 7, 4, 3 ],
  [ 4, 7, 5, 2 ], [ 4, 7, 7, 2 ], [ 4, 12, 2, 4 ], [ 4, 12, 3, 7 ], [ 4, 12, 4, 6 ],
  [ 4, 12, 4, 8 ], [ 4, 12, 4, 9 ], [ 4, 12, 5, 6 ], [ 4, 12, 5, 7 ], [ 4, 13, 1, 3 ],
  [ 4, 13, 2, 4 ], [ 4, 13, 3, 4 ], [ 4, 13, 4, 3 ], [ 4, 13, 5, 3 ], [ 4, 13, 6, 3 ],
  [ 4, 13, 7, 6 ], [ 4, 13, 7, 7 ], [ 4, 13, 7, 8 ], [ 4, 13, 8, 3 ], [ 4, 13, 8, 4 ],
  [ 4, 13, 9, 3 ], [ 4, 13, 10, 3 ], [ 4, 24, 1, 5 ], [ 4, 24, 2, 3 ], [ 4, 24, 2, 5 ],
  [ 4, 24, 3, 5 ], [ 4, 24, 4, 3 ], [ 4, 24, 4, 5 ], [ 4, 24, 5, 3 ], [ 4, 24, 5, 5 ],
  [ 4, 25, 1, 2 ], [ 4, 25, 1, 4 ], [ 4, 25, 2, 4 ], [ 4, 25, 3, 2 ], [ 4, 25, 3, 4 ],
  [ 4, 25, 4, 4 ], [ 4, 25, 5, 2 ], [ 4, 25, 5, 4 ], [ 4, 25, 6, 2 ], [ 4, 25, 6, 4 ],
  [ 4, 25, 7, 2 ], [ 4, 25, 7, 4 ], [ 4, 25, 8, 2 ], [ 4, 25, 8, 4 ], [ 4, 25, 9, 4 ],
  [ 4, 25, 10, 2 ], [ 4, 25, 10, 4 ], [ 4, 25, 11, 2 ], [ 4, 25, 11, 4 ] ]
gap> Length(N31); # there exist 64 not retract rational tori in dim=4=3+1 [HY17, Table 3]
64
gap> N31g:=List(N31,x->MatGroupZClass(x[1],x[2],x[3],x[4]));;
gap> N31gF:=List(N31g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N31H1F:=List(N31gF,x->Filtered(H1(x),y->y>1));;
gap> Collected(N31H1F);
[ [ [  ], 59 ], [ [ 2 ], 5 ] ]
gap> N31H1FC2:=Filtered([1..Length(N31H1F)],x->N31H1F[x]=[2]);
[ 1, 4, 11, 38, 48 ]

gap> List(N31H1FC2,x->N31[x]); # GAP ID's of F with H1(F)=C2
[ [ 4, 4, 3, 6 ], [ 4, 5, 1, 9 ], [ 4, 6, 2, 9 ], [ 4, 24, 1, 5 ], [ 4, 25, 2, 4 ] ]
gap> List(N31H1FC2,x->StructureDescription(N31g[x]));
[ "C2 x C2", "C2 x C2", "C2 x C2 x C2", "A4", "C2 x A4" ]
```

EXAMPLE 1.31 (Classification of $H^1(G,[M_G]^{fl}) \neq 0$ for $G \leq \mathrm{GL}_5(\mathbb{Z})$).

```
gap> Read("FlabbyResolutionFromBase.gap");
gap> Read("caratnumber.gap");
gap> Read("NonInv5.dat");
# N5 is the list of CARAT IDs of indecomposable lattice of rank 5
```

```
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
gap> N5g:=List(N5,x->CaratMatGroupZClass(x[1],x[2],x[3]));;
gap> Length(N5g); # there exist 1141 not retract rational tori in dim=5 [HY17, Table 15]
1141
gap> N5gF:=List(N5g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N5H1F:=List(N5gF,x->Filtered(H1(x),y->y>1));;
gap> Collected(N5H1F);
[ [ [  ], 994 ], [ [ 2 ], 141 ], [ [ 2, 2 ], 6 ] ]

gap> N5H1FC2xC2:=Filtered([1..Length(N5H1F)],x->N5H1F[x]=[2,2]);
[ 69, 70, 906, 913, 915, 1064 ]
gap> List(N5H1FC2xC2,x->N5[x]); # CARAT ID's of F with H1(F)=C2xC2
[ [ 5, 31, 26 ], [ 5, 31, 27 ], [ 5, 664, 2 ], [ 5, 669, 2 ], [ 5, 670, 2 ], [ 5, 773, 4 ] ]
gap> List(N5H1FC2xC2,x->StructureDescription(N5g[x]));
[ "C2 x C2 x C2", "C2 x C2 x C2", "C2 x Q8", "(C4 x C2) : C2", "(C4 x C2) : C2", "Q8" ]

gap> N5H1FC2:=Filtered([1..Length(N5H1F)],x->N5H1F[x]=[2]);
[ 3, 4, 5, 6, 8, 11, 19, 20, 27, 36, 37, 42, 43, 61, 63, 67, 71, 72, 74, 78, 79, 86, 88, 89,
  96, 99, 100, 103, 115, 116, 128, 129, 130, 131, 142, 143, 158, 159, 160, 173, 174, 178,
  179, 185, 186, 187, 188, 191, 193, 199, 200, 221, 222, 238, 242, 243, 253, 254, 288, 292,
  293, 316, 317, 318, 324, 327, 331, 333, 334, 337, 339, 348, 358, 362, 375, 376, 378, 389,
  401, 403, 404, 406, 407, 410, 414, 419, 423, 425, 440, 470, 480, 495, 511, 523, 540, 573,
  588, 590, 591, 592, 593, 595, 596, 597, 606, 680, 715, 723, 762, 852, 853, 854, 855, 908,
  909, 912, 916, 918, 921, 922, 948, 957, 961, 964, 970, 971, 973, 974, 976, 980, 982, 984,
  1037, 1060, 1065, 1114, 1115, 1116, 1117, 1129, 1130 ]
gap> List(N5H1FC2,x->N5[x]); # CARAT ID's of F with H1(F)=C2
[ [ 5, 18, 23 ], [ 5, 19, 17 ], [ 5, 20, 14 ], [ 5, 20, 17 ], [ 5, 21, 17 ], [ 5, 24, 23 ],
  [ 5, 25, 27 ], [ 5, 25, 28 ], [ 5, 26, 21 ], [ 5, 26, 40 ], [ 5, 26, 41 ], [ 5, 27, 14 ],
  [ 5, 27, 15 ], [ 5, 30, 24 ], [ 5, 30, 28 ], [ 5, 31, 18 ], [ 5, 31, 31 ], [ 5, 31, 32 ],
  [ 5, 31, 36 ], [ 5, 31, 44 ], [ 5, 31, 45 ], [ 5, 32, 36 ], [ 5, 32, 44 ], [ 5, 32, 51 ],
  [ 5, 39, 5 ], [ 5, 71, 19 ], [ 5, 71, 22 ], [ 5, 71, 25 ], [ 5, 72, 34 ], [ 5, 72, 36 ],
  [ 5, 73, 32 ], [ 5, 73, 34 ], [ 5, 73, 36 ], [ 5, 73, 37 ], [ 5, 75, 34 ], [ 5, 75, 36 ],
  [ 5, 76, 49 ], [ 5, 76, 50 ], [ 5, 76, 51 ], [ 5, 78, 12 ], [ 5, 78, 15 ], [ 5, 78, 28 ],
  [ 5, 78, 31 ], [ 5, 79, 12 ], [ 5, 79, 15 ], [ 5, 79, 17 ], [ 5, 79, 18 ], [ 5, 79, 31 ],
  [ 5, 79, 36 ], [ 5, 80, 12 ], [ 5, 80, 15 ], [ 5, 83, 15 ], [ 5, 83, 17 ], [ 5, 86, 9 ],
  [ 5, 87, 9 ], [ 5, 87, 11 ], [ 5, 88, 34 ], [ 5, 88, 36 ], [ 5, 93, 9 ], [ 5, 94, 9 ],
  [ 5, 94, 11 ], [ 5, 99, 23 ], [ 5, 99, 24 ], [ 5, 99, 25 ], [ 5, 100, 12 ], [ 5, 100, 23 ],
  [ 5, 100, 28 ], [ 5, 101, 17 ], [ 5, 101, 18 ], [ 5, 102, 9 ], [ 5, 102, 17 ],
  [ 5, 105, 5 ], [ 5, 109, 5 ], [ 5, 109, 14 ], [ 5, 112, 5 ], [ 5, 112, 7 ], [ 5, 113, 4 ],
```

```
  [ 5, 116, 20 ], [ 5, 118, 18 ], [ 5, 119, 4 ], [ 5, 119, 5 ], [ 5, 119, 10 ],
  [ 5, 119, 12 ], [ 5, 120, 5 ], [ 5, 120, 14 ], [ 5, 121, 13 ], [ 5, 122, 9 ],
  [ 5, 122, 15 ], [ 5, 127, 11 ], [ 5, 134, 9 ], [ 5, 136, 18 ], [ 5, 140, 23 ],
  [ 5, 142, 14 ], [ 5, 143, 23 ], [ 5, 148, 5 ], [ 5, 154, 15 ], [ 5, 160, 4 ],
  [ 5, 160, 7 ], [ 5, 161, 5 ], [ 5, 161, 7 ], [ 5, 162, 5 ], [ 5, 224, 9 ], [ 5, 227, 11 ],
  [ 5, 232, 14 ], [ 5, 242, 9 ], [ 5, 526, 11 ], [ 5, 534, 11 ], [ 5, 536, 13 ],
  [ 5, 546, 11 ], [ 5, 580, 2 ], [ 5, 604, 2 ], [ 5, 604, 4 ], [ 5, 605, 2 ], [ 5, 665, 4 ],
  [ 5, 666, 4 ], [ 5, 668, 2 ], [ 5, 670, 3 ], [ 5, 671, 2 ], [ 5, 672, 2 ], [ 5, 673, 2 ],
  [ 5, 704, 3 ], [ 5, 706, 8 ], [ 5, 708, 2 ], [ 5, 709, 3 ], [ 5, 713, 2 ], [ 5, 714, 2 ],
  [ 5, 715, 2 ], [ 5, 716, 2 ], [ 5, 717, 2 ], [ 5, 719, 2 ], [ 5, 720, 2 ], [ 5, 721, 2 ],
  [ 5, 763, 3 ], [ 5, 770, 2 ], [ 5, 774, 4 ], [ 5, 948, 1 ], [ 5, 948, 2 ], [ 5, 948, 3 ],
  [ 5, 948, 4 ], [ 5, 952, 1 ], [ 5, 952, 3 ] ]
gap> List(N5H1FC2,x->StructureDescription(N5g[x]));
[ "C2 x C2", "C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2 x C2",
  "C2 x C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "D8",
  "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8",
  "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8",
  "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8",
  "C2 x D8", "C2 x D8", "C4 x C2 x C2", "C4 x C2 x C2", "C4 x C2 x C2", "C4 x C2 x C2",
  "C4 x C2 x C2", "C2 x C2 x D8", "C2 x C2 x D8", "C2 x C2 x D8", "C2 x C2 x D8",
  "C2 x C2 x D8", "D8", "D8", "D8", "D8", "D8", "D8", "C4 x C2", "C4 x C2", "C4 x C2",
  "C4 x C2", "C4 : C4", "(C4 x C2) : C2", "(C4 x C2) : C2", "C4 x C2 x C2", "C4 x C2 x C2",
  "C4 x C4", "(C4 x C2) : C2", "(C4 x C2) : C2", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8",
  "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C4 x D8", "(C4 x C4) : C2",
  "(C2 x C2 x C2 x C2) : C2", "(C4 x C2 x C2) : C2", "(C2 x C2 x C2 x C2) : C2",
  "(C4 x C2 x C2) : C2", "C2 x C2 x D8", "D8 x D8", "C4 x C2", "C4 x C2", "C4 x C2",
  "C4 x C2", "C4 x C2", "C6 x C2", "D12", "D12", "C2 x C2 x S3", "C2 x C2 x A4", "C2 x S4",
  "C2 x S4", "C2 x C2 x S4", "A4", "C2 x A4", "C2 x A4", "C2 x A4", "C8 : C2", "C8 : C2",
  "(C4 x C2) : C2", "(C4 x C2) : C2", "(C4 x C2) : C2", "QD16", "QD16", "(C2 x C2 x C2) : C4",
  "(C2 x C2 x C2) : C4", "(C2 x C2 x C2) : (C2 x C2)", "(C2 x C2 x C2) : (C2 x C2)",
  "C8 : (C2 x C2)", "C8 : (C2 x C2)", "C8 : (C2 x C2)", "C8 : (C2 x C2)", "C8 : (C2 x C2)",
  "C2 x ((C4 x C2) : C2)", "C2 x (C8 : C2)", "C2 x QD16", "((C2 x C2 x C2) : (C2 x C2)) : C2",
  "C2 x (C8 : (C2 x C2))", "Q8", "C2 x A5", "C2 x A5", "C2 x A5", "C2 x A5", "A5", "A5" ]

# N41 is the list of CARAT IDs of decomposable lattice of rank 5=4+1
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
```

```
gap> N41g:=List(N41,x->CaratMatGroupZClass(x[1],x[2],x[3]));;
gap> Length(N41g); # there exist 768 not retract rational tori in dim=5=4+1 [HY17, Table 14]
768
gap> N41gF:=List(N41g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N41H1F:=List(N41gF,x->Filtered(H1(x),y->y>1));;
gap> Collected(N41H1F);
[ [ [  ], 690 ], [ [ 2 ], 73 ], [ [ 2, 2 ], 5 ] ]

gap> N41H1FC2xC2:=Filtered([1..Length(N41H1F)],x->N41H1F[x]=[2,2]);
[ 589, 590, 591, 720, 721 ]
gap> List(N41H1FC2xC2,x->N41[x]);
[ [ 5, 664, 1 ], [ 5, 773, 3 ], [ 5, 774, 3 ], [ 5, 691, 1 ], [ 5, 730, 1 ] ]
gap> List(N41H1FC2xC2,x->StructureDescription(N41g[x]));
[ "C2 x Q8", "Q8", "Q8", "SL(2,3)", "C2 x SL(2,3)" ]

gap> N41H1FC2:=Filtered([1..Length(N41H1F)],x->N41H1F[x]=[2]);
[ 1, 2, 3, 4, 9, 10, 11, 12, 13, 14, 36, 37, 38, 39, 40, 41, 42, 74, 75, 76, 77, 93, 94, 95,
  96, 97, 112, 113, 114, 115, 116, 117, 118, 254, 255, 256, 257, 281, 282, 283, 284, 285,
  592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 610, 611, 612, 613,
  614, 615, 616, 727, 728, 729, 730, 731, 732, 738, 739, 740, 741 ]
gap> List(N41H1FC2,x->N41[x]); # CARAT ID's of F with H1(F)=C2
[ [ 5, 18, 18 ], [ 5, 18, 21 ], [ 5, 19, 10 ], [ 5, 32, 23 ], [ 5, 20, 10 ], [ 5, 20, 13 ],
  [ 5, 25, 14 ], [ 5, 30, 14 ], [ 5, 31, 16 ], [ 5, 31, 29 ], [ 5, 21, 10 ], [ 5, 24, 18 ],
  [ 5, 24, 21 ], [ 5, 26, 19 ], [ 5, 31, 22 ], [ 5, 31, 25 ], [ 5, 32, 30 ], [ 5, 66, 5 ],
  [ 5, 83, 7 ], [ 5, 101, 4 ], [ 5, 102, 4 ], [ 5, 63, 12 ], [ 5, 65, 12 ], [ 5, 76, 31 ],
  [ 5, 99, 5 ], [ 5, 100, 5 ], [ 5, 48, 12 ], [ 5, 71, 8 ], [ 5, 72, 26 ], [ 5, 75, 26 ],
  [ 5, 78, 26 ], [ 5, 79, 26 ], [ 5, 88, 26 ], [ 5, 112, 3 ], [ 5, 160, 3 ], [ 5, 161, 3 ],
  [ 5, 162, 3 ], [ 5, 119, 3 ], [ 5, 120, 11 ], [ 5, 121, 11 ], [ 5, 122, 14 ],
  [ 5, 148, 3 ], [ 5, 665, 3 ], [ 5, 666, 3 ], [ 5, 667, 3 ], [ 5, 720, 1 ], [ 5, 672, 1 ],
  [ 5, 673, 1 ], [ 5, 674, 1 ], [ 5, 675, 1 ], [ 5, 721, 1 ], [ 5, 668, 1 ], [ 5, 669, 1 ],
  [ 5, 670, 1 ], [ 5, 671, 1 ], [ 5, 719, 1 ], [ 5, 713, 1 ], [ 5, 714, 1 ], [ 5, 715, 1 ],
  [ 5, 716, 1 ], [ 5, 717, 1 ], [ 5, 718, 1 ], [ 5, 770, 1 ], [ 5, 731, 1 ], [ 5, 732, 1 ],
  [ 5, 775, 1 ], [ 5, 733, 1 ], [ 5, 734, 1 ], [ 5, 776, 1 ], [ 5, 682, 1 ], [ 5, 780, 1 ],
  [ 5, 781, 1 ], [ 5, 783, 1 ] ]
gap> List(N41H1FC2,x->StructureDescription(N41g[x]));
[ "C2 x C2", "C2 x C2", "C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2", "C4 x C2", "C4 x C2 x C2", "C4 x C2", "C4 x C2", "D8", "D8", "C2 x D8",
```

```
  "D8", "D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8", "C2 x D8",
  "C2 x C2 x D8", "C4 x C2 x C2", "C4 x C2", "C4 x C2", "C4 x C2", "C2 x D8", "C2 x D8",
  "C2 x D8", "C2 x D8", "C2 x C2 x D8", "C8 : C2", "C8 : C2", "C8 : C2", "C2 x (C8 : C2)",
  "QD16", "QD16", "QD16", "QD16", "C2 x QD16", "(C4 x C2) : C2", "(C4 x C2) : C2",
  "(C4 x C2) : C2", "(C4 x C2) : C2", "C2 x ((C4 x C2) : C2)", "C8 : (C2 x C2)",
  "C8 : (C2 x C2)", "C8 : (C2 x C2)", "C8 : (C2 x C2)", "C8 : (C2 x C2)", "C8 : (C2 x C2)",
  "C2 x (C8 : (C2 x C2))", "((C4 x C2) : C2) : C3", "((C4 x C2) : C2) : C3",
  "C2 x (((C4 x C2) : C2) : C3)", "GL(2,3)", "GL(2,3)", "C2 x GL(2,3)", "C2 x (GL(2,3) : C2)",
  "(((C4 x C2) : C2) : C3) : C2", "(((C4 x C2) : C2) : C3) : C2",
  "(((C4 x C2) : C2) : C3) : C2" ]

# N32 is the list of CARAT IDs of decomposable lattice of rank 5=3+2
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
gap> N32g:=List(N32,x->CaratMatGroupZClass(x[1],x[2],x[3]));;
gap> Length(N32g); # there exist 849 not retract rational tori in dim=5=3+2 [HY17, Table 13]
849
gap> N32gF:=List(N32g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N32H1F:=List(N32gF,x->Filtered(H1(x),y->y>1));;
gap> Collected(N32H1F);
[ [ [  ], 813 ], [ [ 2 ], 36 ] ]]

gap> N32H1FC2:=Filtered([1..Length(N32H1F)],x->N32H1F[x]=[2]);
[ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,
  22, 23, 24, 25, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588 ]
gap> List(N32H1FC2,x->N32[x]); # CARAT ID's of F with H1(F)=C2
[ [ 5, 14, 8 ], [ 5, 18, 19 ], [ 5, 24, 19 ], [ 5, 26, 20 ], [ 5, 31, 17 ],
  [ 5, 32, 17 ], [ 5, 78, 8 ], [ 5, 78, 27 ], [ 5, 80, 8 ], [ 5, 86, 5 ],
  [ 5, 93, 5 ], [ 5, 100, 11 ], [ 5, 102, 8 ], [ 5, 224, 4 ], [ 5, 227, 5 ],
  [ 5, 228, 3 ], [ 5, 232, 4 ], [ 5, 232, 9 ], [ 5, 237, 3 ], [ 5, 242, 4 ],
  [ 5, 242, 14 ], [ 5, 247, 3 ], [ 5, 247, 7 ], [ 5, 253, 4 ],
  [ 5, 259, 3 ], [ 5, 520, 17 ], [ 5, 525, 2 ], [ 5, 560, 3 ],
  [ 5, 566, 3 ], [ 5, 580, 1 ], [ 5, 590, 1 ], [ 5, 605, 1 ], [ 5, 620, 1 ],
  [ 5, 629, 1 ], [ 5, 634, 1 ], [ 5, 634, 3 ] ]
gap> List(N32H1FC2,x->StructureDescription(N32g[x]));
[ "C2 x C2", "C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2", "C2 x D8", "C2 x D8", "C2 x D8", "C4 x C2 x C2",
  "C2 x C2 x D8", "D8", "C4 x C2", "C6 x C2", "D12", "C6 x C2", "D12",
  "D12", "C6 x C2 x C2", "C2 x C2 x S3", "C2 x C2 x S3", "C2 x C2 x S3",
  "C2 x C2 x S3", "C2 x C2 x S3", "C2 x C2 x C2 x S3", "C2 x A4",
```

```
  "C2 x C2 x A4", "C4 x A4", "A4 x D8", "A4", "C2 x A4 x S3", "C2 x A4",
  "C3 x A4", "C6 x A4", "A4 x S3", "A4 x S3" ]

# N311 is the list of CARAT IDs of decomposable lattice of rank 5=3+1+1
# whose flabby class [M_G]^fl is not invertible [HY17, Example 4.12]
gap> N311g:=List(N311,x->CaratMatGroupZClass(x[1],x[2],x[3]));;
gap> Length(N311g); # there exist 245 not retract rational tori in dim=5=3+1+1 [HY17, Table 12]
245
gap> N311gF:=List(N311g,x->FlabbyResolutionLowRank(x).actionF);;
gap> N311H1F:=List(N311gF,x->Filtered(H1(x),y->y>1));;
gap> Collected(N311H1F);
[ [ [  ], 232 ], [ [ 2 ], 13 ] ]

gap> N311H1FC2:=Filtered([1..Length(N311H1F)],x->N311H1F[x]=[2]);
[ 1, 2, 3, 4, 5, 6, 7, 8, 9, 164, 165, 166, 167 ]
gap> List(N311H1FC2,x->N311[x]); # CARAT ID's of F with H1(F)=C2
[ [ 5, 11, 4 ], [ 5, 14, 4 ], [ 5, 18, 7 ], [ 5, 19, 5 ], [ 5, 21, 5 ],
  [ 5, 24, 7 ], [ 5, 26, 3 ], [ 5, 31, 4 ], [ 5, 32, 10 ], [ 5, 502, 6 ],
  [ 5, 505, 1 ], [ 5, 520, 16 ], [ 5, 525, 1 ] ]
gap> List(N311H1FC2,x->StructureDescription(N311g[x]));
[ "C2 x C2", "C2 x C2", "C2 x C2", "C2 x C2", "C2 x C2 x C2",
  "C2 x C2 x C2", "C2 x C2 x C2 x C2", "C2 x C2 x C2", "C2 x C2 x C2",
  "A4", "C2 x A4", "C2 x A4", "C2 x C2 x A4" ]
```

## 5. Proof of Theorem 1.15 and Theorem 1.17

Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be a norm one torus of $K/k$. We have the character module $\widehat{T} = J_{G/H}$ of $T$ and then $H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl})$ (see Section 2). We may assume that $H$ is the stabilizer of one of the letters in $G$, i.e. $L = k(\theta_1, \ldots, \theta_n)$ and $K = k(\theta_i)$ for some $1 \leq i \leq n$. In order to compute $H^1(G, [J_{G/H}]^{fl})$, we apply the functions `Norm1TorusJ`$(n, m)$ and `FlabbyResolutionLowRankFromGroup`$(G$,$nTm)$`.actionF` in [**HHY20**, Algorithm 4.1]. `Norm1TorusJ`$(n, m)$ returns $J_{G/H}$ for $G = nTm \leq S_n$ and $H$ is the stabilizer of one of the letters in $G$ and `FlabbyResolutionLowRankFromGroup`$(G$,$nTm)$`.actionF` returns a suitable flabby class $F = [J_{G/H}]^{fl}$ with low rank by using the backtracking techniques for $G = nTm \leq S_n$.

*Proof of Theorem 1.15.*

For $G = nTm$ $(2 \leq n \leq 11)$, the computation is described in Example 1.32.

For $G = nTm$ $(12 \leq n \leq 15)$, it needs much time and computer resources (memory) in computations. At present, we do not know the complete solutions for $n = 12$.

For $13 \leq n \leq 15$, we wish to compute $H^1(G, [J_{G/H}]^{fl})$ for each of the cases $G = 13Tm$ $(1 \leq m \leq 9)$, $G = 14Tm$ $(1 \leq m \leq 63)$, $G = 15Tm$ $(1 \leq m \leq 104)$. This is achievable except for the each last two groups $G = 13T8 \simeq A_{13}$, $13T9 \simeq S_{13}$, $14T62 \simeq A_{14}$, $14T63 \simeq S_{14}$, $15T103 \simeq A_{15}$, $15T104 \simeq S_{15}$ because of the computer resources reason (see Example 1.33). However, for the exceptional cases, we already know that $H^1(G, [J_{G/H}]^{fl}) = 0$ by Theorem 1.10 and Theorem 1.11.

The last assertion follows from Theorem 1.2. □

*Proof of Theorem 1.17.*

For $G = 11T6 \simeq M_{11} \leq S_{11}$ and $G = 23T5 \simeq M_{23} \leq S_{23}$, it follows from Theorem 1.19 that $H^1(G, [J_{G/H}]^{fl}) = 0$ (see also the paragraph after Theorem 1.26). For $G = 24T24680 \simeq M_{24} \leq S_{24}$, we know that the Schur multiplier of $G$ vanishes: $M(G) \simeq H^3(G, \mathbb{Z}) = 0$ (see Mazet [**Maz82**]). We know that the Mathieu groups are simple groups and a subgroup $H \leq M_{24}$ with $[M_{24} : H] = 24$ is isomorphic to $M_{23}$ which is the stabilizer of one of the letters in $M_{24}$ (see e.g. [**DM96**, Exercises 6.8.8]). Hence it follows from $0 = H^{ab} \simeq H^2(H, \mathbb{Z}) \simeq H^2(G, \mathbb{Z}[G/H]) \to H^2(G, J_{G/H}) \xrightarrow{\delta} H^3(G, \mathbb{Z}) = 0$ that $H^2(G, J_{G/H}) = 0$. Thus we have $H^1(G, [J_{G/H}]^{fl}) \simeq Ш^2_\omega(G, J_{G/H}) = 0$.

For $G = 12T295 \simeq M_{12} \leq S_{12}$ and $G = 22T38 \simeq M_{22} \leq S_{22}$, the computation is described in Example 1.34. □

Some related functions for Example 1.32, Example 1.33 and Example 1.34 are available from

`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbNorm1Tori/`.

Example 1.32 (Computation of $H^1(G, [J_{G/H}]^{fl})$ where $G = nTm$ $(n \leq 11)$).

```
gap> Read("FlabbyResolutionFromBase.gap");
gap> for n in [2..11] do for m in [1..NrTransitiveGroups(n)] do
> F:=FlabbyResolutionLowRankFromGroup(Norm1TorusJ(n,m),TransitiveGroup(n,m)).actionF;
> Print([[n,m],Length(F.1),Filtered(H1(F),x->x>1)],"\n");od;Print("\n");od;
[ [ 2, 1 ], 1, [  ] ]

[ [ 3, 1 ], 1, [  ] ]
[ [ 3, 2 ], 4, [  ] ]
```

```
[ [ 4, 1 ], 1, [  ] ]
[ [ 4, 2 ], 5, [ 2 ] ]
[ [ 4, 3 ], 7, [  ] ]
[ [ 4, 4 ], 9, [ 2 ] ]
[ [ 4, 5 ], 15, [  ] ]

[ [ 5, 1 ], 1, [  ] ]
[ [ 5, 2 ], 6, [  ] ]
[ [ 5, 3 ], 16, [  ] ]
[ [ 5, 4 ], 16, [  ] ]
[ [ 5, 5 ], 16, [  ] ]

[ [ 6, 1 ], 1, [  ] ]
[ [ 6, 2 ], 7, [  ] ]
[ [ 6, 3 ], 9, [  ] ]
[ [ 6, 4 ], 10, [ 2 ] ]
[ [ 6, 5 ], 21, [  ] ]
[ [ 6, 6 ], 10, [  ] ]
[ [ 6, 7 ], 19, [  ] ]
[ [ 6, 8 ], 19, [  ] ]
[ [ 6, 9 ], 27, [  ] ]
[ [ 6, 10 ], 27, [  ] ]
[ [ 6, 11 ], 19, [  ] ]
[ [ 6, 12 ], 10, [ 2 ] ]
[ [ 6, 13 ], 27, [  ] ]
[ [ 6, 14 ], 31, [  ] ]
[ [ 6, 15 ], 60, [  ] ]
[ [ 6, 16 ], 60, [  ] ]

[ [ 7, 1 ], 1, [  ] ]
[ [ 7, 2 ], 8, [  ] ]
[ [ 7, 3 ], 15, [  ] ]
[ [ 7, 4 ], 36, [  ] ]
[ [ 7, 5 ], 15, [  ] ]
[ [ 7, 6 ], 36, [  ] ]
[ [ 7, 7 ], 36, [  ] ]

[ [ 8, 1 ], 1, [  ] ]
```

```
[ [ 8, 2 ], 9, [ 2 ] ]
[ [ 8, 3 ], 17, [ 2, 2, 2 ] ]
[ [ 8, 4 ], 9, [ 2 ] ]
[ [ 8, 5 ], 9, [  ] ]
[ [ 8, 6 ], 11, [  ] ]
[ [ 8, 7 ], 21, [  ] ]
[ [ 8, 8 ], 11, [  ] ]
[ [ 8, 9 ], 21, [ 2 ] ]
[ [ 8, 10 ], 21, [  ] ]
[ [ 8, 11 ], 21, [ 2 ] ]
[ [ 8, 12 ], 25, [  ] ]
[ [ 8, 13 ], 19, [ 2 ] ]
[ [ 8, 14 ], 13, [ 2 ] ]
[ [ 8, 15 ], 43, [ 2 ] ]
[ [ 8, 16 ], 29, [  ] ]
[ [ 8, 17 ], 43, [  ] ]
[ [ 8, 18 ], 91, [  ] ]
[ [ 8, 19 ], 51, [ 2 ] ]
[ [ 8, 20 ], 29, [  ] ]
[ [ 8, 21 ], 49, [ 2 ] ]
[ [ 8, 22 ], 49, [ 2 ] ]
[ [ 8, 23 ], 31, [  ] ]
[ [ 8, 24 ], 31, [  ] ]
[ [ 8, 25 ], 49, [  ] ]
[ [ 8, 26 ], 67, [  ] ]
[ [ 8, 27 ], 29, [  ] ]
[ [ 8, 28 ], 83, [  ] ]
[ [ 8, 29 ], 99, [  ] ]
[ [ 8, 30 ], 67, [  ] ]
[ [ 8, 31 ], 49, [ 2 ] ]
[ [ 8, 32 ], 61, [ 2 ] ]
[ [ 8, 33 ], 99, [  ] ]
[ [ 8, 34 ], 123,[  ] ]
[ [ 8, 35 ], 99, [  ] ]
[ [ 8, 36 ], 49, [  ] ]
[ [ 8, 37 ], 49, [ 2 ] ]
[ [ 8, 38 ], 61, [ 2 ] ]
[ [ 8, 39 ], 211, [  ] ]
[ [ 8, 40 ], 115, [  ] ]
```

```
[ [ 8, 41 ], 123, [  ] ]
[ [ 8, 42 ], 123, [  ] ]
[ [ 8, 43 ], 91, [  ] ]
[ [ 8, 44 ], 211, [  ] ]
[ [ 8, 45 ], 123, [  ] ]
[ [ 8, 46 ], 123, [  ] ]
[ [ 8, 47 ], 123, [  ] ]
[ [ 8, 48 ], 483, [  ] ]
[ [ 8, 49 ], 539, [  ] ]
[ [ 8, 50 ], 539, [  ] ]

[ [ 9, 1 ], 1, [  ] ]
[ [ 9, 2 ], 10, [ 3 ] ]
[ [ 9, 3 ], 10, [  ] ]
[ [ 9, 4 ], 13, [  ] ]
[ [ 9, 5 ], 28, [ 3 ] ]
[ [ 9, 6 ], 31, [  ] ]
[ [ 9, 7 ], 31, [ 3 ] ]
[ [ 9, 8 ], 28, [  ] ]
[ [ 9, 9 ], 28, [ 3 ] ]
[ [ 9, 10 ], 70, [  ] ]
[ [ 9, 11 ], 70, [ 3 ] ]
[ [ 9, 12 ], 61, [  ] ]
[ [ 9, 13 ], 40, [  ] ]
[ [ 9, 14 ], 64, [ 3 ] ]
[ [ 9, 15 ], 64, [  ] ]
[ [ 9, 16 ], 34, [  ] ]
[ [ 9, 17 ], 31, [  ] ]
[ [ 9, 18 ], 70, [  ] ]
[ [ 9, 19 ], 64, [  ] ]
[ [ 9, 20 ], 61, [  ] ]
[ [ 9, 21 ], 70, [  ] ]
[ [ 9, 22 ], 40, [  ] ]
[ [ 9, 23 ], 88, [ 3 ] ]
[ [ 9, 24 ], 70, [  ] ]
[ [ 9, 25 ], 40, [  ] ]
[ [ 9, 26 ], 88, [  ] ]
[ [ 9, 27 ], 64, [  ] ]
[ [ 9, 28 ], 40, [  ] ]
```

```
[ [ 9, 29 ], 70, [  ] ]
[ [ 9, 30 ], 70, [  ] ]
[ [ 9, 31 ], 70, [  ] ]
[ [ 9, 32 ], 232, [  ] ]
[ [ 9, 33 ], 1744, [  ] ]
[ [ 9, 34 ], 1744, [  ] ]

[ [ 10, 1 ], 1, [  ] ]
[ [ 10, 2 ], 11, [  ] ]
[ [ 10, 3 ], 13, [  ] ]
[ [ 10, 4 ], 13, [  ] ]
[ [ 10, 5 ], 31, [  ] ]
[ [ 10, 6 ], 53, [  ] ]
[ [ 10, 7 ], 26, [ 2 ] ]
[ [ 10, 8 ], 36, [  ] ]
[ [ 10, 9 ], 63, [  ] ]
[ [ 10, 10 ], 63, [  ] ]
[ [ 10, 11 ], 31, [  ] ]
[ [ 10, 12 ], 31, [  ] ]
[ [ 10, 13 ], 36, [  ] ]
[ [ 10, 14 ], 36, [  ] ]
[ [ 10, 15 ], 51, [  ] ]
[ [ 10, 16 ], 51, [  ] ]
[ [ 10, 17 ], 83, [  ] ]
[ [ 10, 18 ], 83, [  ] ]
[ [ 10, 19 ], 83, [  ] ]
[ [ 10, 20 ], 83, [  ] ]
[ [ 10, 21 ], 63, [  ] ]
[ [ 10, 22 ], 31, [  ] ]
[ [ 10, 23 ], 51, [  ] ]
[ [ 10, 24 ], 61, [  ] ]
[ [ 10, 25 ], 61, [  ] ]
[ [ 10, 26 ], 46, [ 2 ] ]
[ [ 10, 27 ], 83, [  ] ]
[ [ 10, 28 ], 83, [  ] ]
[ [ 10, 29 ], 61, [  ] ]
[ [ 10, 30 ], 91, [  ] ]
[ [ 10, 31 ], 67, [  ] ]
[ [ 10, 32 ], 46, [ 2 ] ]
```

```
[ [ 10, 33 ], 83, [  ] ]
[ [ 10, 34 ], 61, [  ] ]
[ [ 10, 35 ], 91, [  ] ]
[ [ 10, 36 ], 61, [  ] ]
[ [ 10, 37 ], 61, [  ] ]
[ [ 10, 38 ], 61, [  ] ]
[ [ 10, 39 ], 61, [  ] ]
[ [ 10, 40 ], 83, [  ] ]
[ [ 10, 41 ], 83, [  ] ]
[ [ 10, 42 ], 83, [  ] ]
[ [ 10, 43 ], 83, [  ] ]
[ [ 10, 44 ], 378, [  ] ]
[ [ 10, 45 ], 378, [  ] ]

[ [ 11, 1 ], 1, [  ] ]
[ [ 11, 2 ], 12, [  ] ]
[ [ 11, 3 ], 45, [  ] ]
[ [ 11, 4 ], 100, [  ] ]
[ [ 11, 5 ], 56, [  ] ]
[ [ 11, 6 ], 100, [  ] ]
[ [ 11, 7 ], 100, [  ] ]
[ [ 11, 8 ], 100, [  ] ]
```

EXAMPLE 1.33 (Computation of $H^1(G, [J_{G/H}]^{fl})$ where $G = 13Tm$ $(1 \leq m \leq 9, m \neq 8, 9)$, $G = 14Tm$ $(1 \leq m \leq 63, m \neq 62, 63)$, $G = 15Tm$ $(1 \leq m \leq 104, m \neq 103, 104)$).

```
gap> Read("FlabbyResolutionFromBase.gap");
gap> for m in [1..NrTransitiveGroups(13)-2] do
> F:=FlabbyResolutionLowRankFromGroup(Norm1TorusJ(13,m),TransitiveGroup(13,m)).actionF;
> Print([[n,i],Length(F.1),Filtered(H1(F),x->x>1)],"\n");od;Print("\n");od;
[ [ 13, 1 ], 1, [  ] ]
[ [ 13, 2 ], 14, [  ] ]
[ [ 13, 3 ], 27, [  ] ]
[ [ 13, 4 ], 40, [  ] ]
[ [ 13, 5 ], 66, [  ] ]
[ [ 13, 6 ], 144, [  ] ]
[ [ 13, 7 ], 40, [  ] ]

gap> for m in [1..NrTransitiveGroups(14)-2] do
```

```
> F:=FlabbyResolutionLowRankFromGroup(Norm1TorusJ(14,m),TransitiveGroup(14,m)).actionF;
> Print([[14,m],Length(F.1),Filtered(H1(F),x->x>1)],"\n");od;
[ [ 14, 1 ], 1, [  ] ]
[ [ 14, 2 ], 15, [  ] ]
[ [ 14, 3 ], 17, [  ] ]
[ [ 14, 4 ], 31, [  ] ]
[ [ 14, 5 ], 31, [  ] ]
[ [ 14, 6 ], 50, [  ] ]
[ [ 14, 7 ], 57, [  ] ]
[ [ 14, 8 ], 101, [  ] ]
[ [ 14, 9 ], 78, [  ] ]
[ [ 14, 10 ], 64, [  ] ]
[ [ 14, 11 ], 86, [  ] ]
[ [ 14, 12 ], 115, [  ] ]
[ [ 14, 13 ], 115, [  ] ]
[ [ 14, 14 ], 129, [  ] ]
[ [ 14, 15 ], 129, [  ] ]
[ [ 14, 16 ], 31, [  ] ]
[ [ 14, 17 ], 92, [  ] ]
[ [ 14, 18 ], 92, [  ] ]
[ [ 14, 19 ], 31, [  ] ]
[ [ 14, 20 ], 115, [  ] ]
[ [ 14, 21 ], 78, [  ] ]
[ [ 14, 22 ], 171, [  ] ]
[ [ 14, 23 ], 171, [  ] ]
[ [ 14, 24 ], 171, [  ] ]
[ [ 14, 25 ], 171, [  ] ]
[ [ 14, 26 ], 129, [  ] ]
[ [ 14, 27 ], 99, [  ] ]
[ [ 14, 28 ], 99, [  ] ]
[ [ 14, 29 ], 78, [  ] ]
[ [ 14, 30 ], 92, [ 2 ] ]
[ [ 14, 31 ], 171, [  ] ]
[ [ 14, 32 ], 171, [  ] ]
[ [ 14, 33 ], 92, [  ] ]
[ [ 14, 34 ], 92, [  ] ]
[ [ 14, 35 ], 92, [  ] ]
[ [ 14, 36 ], 171, [  ] ]
[ [ 14, 37 ], 171, [  ] ]
```

```
[ [ 14, 38 ], 99, [  ] ]
[ [ 14, 39 ], 183, [  ] ]
[ [ 14, 40 ], 127, [  ] ]
[ [ 14, 41 ], 127,[  ] ]
[ [ 14, 42 ], 92, [  ] ]
[ [ 14, 43 ], 92, [  ] ]
[ [ 14, 44 ], 99, [  ] ]
[ [ 14, 45 ], 171, [  ] ]
[ [ 14, 46 ], 57, [  ] ]
[ [ 14, 47 ], 57, [  ] ]
[ [ 14, 48 ], 127, [  ] ]
[ [ 14, 49 ], 57, [  ] ]
[ [ 14, 50 ], 92, [  ] ]
[ [ 14, 51 ], 92, [  ] ]
[ [ 14, 52 ], 129, [  ] ]
[ [ 14, 53 ], 127, [  ] ]
[ [ 14, 54 ], 127, [  ] ]
[ [ 14, 55 ], 127, [  ] ]
[ [ 14, 56 ], 127, [  ] ]
[ [ 14, 57 ], 127, [  ] ]
[ [ 14, 58 ], 171, [  ] ]
[ [ 14, 59 ], 171, [  ] ]
[ [ 14, 60 ], 171, [  ] ]
[ [ 14, 61 ], 171, [  ] ]

gap> for m in [1..NrTransitiveGroups(15)-2] do
> F:=FlabbyResolutionLowRankFromGroup(Norm1TorusJ(15,m),TransitiveGroup(15,m)).actionF;
> Print([[15,m],Length(F.1),Filtered(H1(F),x->x>1)],"\n");od;
[ [ 15, 1 ], 1, [  ] ]
[ [ 15, 2 ], 16, [  ] ]
[ [ 15, 3 ], 14, [  ] ]
[ [ 15, 4 ], 21, [  ] ]
[ [ 15, 5 ], 21, [  ] ]
[ [ 15, 6 ], 39, [  ] ]
[ [ 15, 7 ], 17, [  ] ]
[ [ 15, 8 ], 36, [  ] ]
[ [ 15, 9 ], 79, [ 5 ] ]
[ [ 15, 10 ], 36, [  ] ]
[ [ 15, 11 ], 27, [  ] ]
```

```
[ [ 15, 12 ], 94, [  ] ]
[ [ 15, 13 ], 82, [  ] ]
[ [ 15, 14 ], 97, [ 5 ] ]
[ [ 15, 15 ], 51, [  ] ]
[ [ 15, 16 ], 36, [  ] ]
[ [ 15, 17 ], 127, [  ] ]
[ [ 15, 18 ], 97, [  ] ]
[ [ 15, 19 ], 124, [  ] ]
[ [ 15, 20 ], 81, [  ] ]
[ [ 15, 21 ], 66, [  ] ]
[ [ 15, 22 ], 39, [  ] ]
[ [ 15, 23 ], 27, [  ] ]
[ [ 15, 24 ], 36, [  ] ]
[ [ 15, 25 ], 79, [  ] ]
[ [ 15, 26 ], 96, [  ] ]
[ [ 15, 27 ], 127, [  ] ]
[ [ 15, 28 ], 81, [  ] ]
[ [ 15, 29 ], 27, [  ] ]
[ [ 15, 30 ], 94, [  ] ]
[ [ 15, 31 ], 169, [  ] ]
[ [ 15, 32 ], 154, [  ] ]
[ [ 15, 33 ], 111, [  ] ]
[ [ 15, 34 ], 186, [  ] ]
[ [ 15, 35 ], 201, [  ] ]
[ [ 15, 36 ], 96, [  ] ]
[ [ 15, 37 ], 199, [  ] ]
[ [ 15, 38 ], 124, [  ] ]
[ [ 15, 39 ], 94, [  ] ]
[ [ 15, 40 ], 169, [  ] ]
[ [ 15, 41 ], 186, [  ] ]
[ [ 15, 42 ], 201, [  ] ]
[ [ 15, 43 ], 201, [  ] ]
[ [ 15, 44 ], 111, [  ] ]
[ [ 15, 45 ], 201, [  ] ]
[ [ 15, 46 ], 186, [  ] ]
[ [ 15, 47 ], 156, [  ] ]
[ [ 15, 48 ], 169, [  ] ]
[ [ 15, 49 ], 199, [  ] ]
[ [ 15, 50 ], 94, [  ] ]
```

```
[ [ 15, 51 ], 169, [  ] ]
[ [ 15, 52 ], 201, [  ] ]
[ [ 15, 53 ], 456, [  ] ]
[ [ 15, 54 ], 201, [  ] ]
[ [ 15, 55 ], 201, [  ] ]
[ [ 15, 56 ], 186, [  ] ]
[ [ 15, 57 ], 124, [  ] ]
[ [ 15, 58 ], 199, [  ] ]
[ [ 15, 59 ], 124, [  ] ]
[ [ 15, 60 ], 169, [  ] ]
[ [ 15, 61 ], 471, [  ] ]
[ [ 15, 62 ], 471, [  ] ]
[ [ 15, 63 ], 456, [  ] ]
[ [ 15, 64 ], 201, [  ] ]
[ [ 15, 65 ], 199, [  ] ]
[ [ 15, 66 ], 199, [  ] ]
[ [ 15, 67 ], 124, [  ] ]
[ [ 15, 68 ], 199, [  ] ]
[ [ 15, 69 ], 456, [  ] ]
[ [ 15, 70 ], 471, [  ] ]
[ [ 15, 71 ], 111, [  ] ]
[ [ 15, 72 ], 156, [  ] ]
[ [ 15, 73 ], 199, [  ] ]
[ [ 15, 74 ], 199, [  ] ]
[ [ 15, 75 ], 124, [  ] ]
[ [ 15, 76 ], 471, [  ] ]
[ [ 15, 77 ], 471, [  ] ]
[ [ 15, 78 ], 456, [  ] ]
[ [ 15, 79 ], 201, [  ] ]
[ [ 15, 80 ], 201, [  ] ]
[ [ 15, 81 ], 111, [  ] ]
[ [ 15, 82 ], 199, [  ] ]
[ [ 15, 83 ], 471, [  ] ]
[ [ 15, 84 ], 201, [  ] ]
[ [ 15, 85 ], 201, [  ] ]
[ [ 15, 86 ], 201, [  ] ]
[ [ 15, 87 ], 201, [  ] ]
[ [ 15, 88 ], 471, [  ] ]
[ [ 15, 89 ], 471, [  ] ]
```

```
[ [ 15, 90 ], 471, [  ] ]
[ [ 15, 91 ], 471, [  ] ]
[ [ 15, 92 ], 124, [  ] ]
[ [ 15, 93 ], 471, [  ] ]
[ [ 15, 94 ], 199, [  ] ]
[ [ 15, 95 ], 124, [  ] ]
[ [ 15, 96 ], 199, [  ] ]
[ [ 15, 97 ], 199, [  ] ]
[ [ 15, 98 ], 124, [  ] ]
[ [ 15, 99 ], 199, [  ] ]
[ [ 15, 100 ], 199, [  ] ]
[ [ 15, 101 ], 124, [  ] ]
[ [ 15, 102 ], 199, [  ] ]
```

EXAMPLE 1.34 (Computation of $H^1(G, [J_{G/H}]^{fl}) = 0$ where $G = 12T295 \simeq M_{12}$ and $G = 22T38 \simeq M_{22}$).

```
gap> Read("FlabbyResolutionFromBase.gap");


gap> G:=TransitiveGroup(12,295);
M(12)
gap> F:=FlabbyResolutionLowRankFromGroup(Norm1TorusJ(12,295),G).actionF;
<matrix group with 2 generators>
gap> [[12,295],Length(F.1),Filtered(H1(F),x->x>1)];
[ [ 12, 295 ], 814, [  ] ]


gap> G:=TransitiveGroup(22,38);
t22n38
gap> StructureDescription(G);
"M22"
gap> F:=FlabbyResolutionLowRankFromGroup(Norm1TorusJ(22,38),G).actionF;
<matrix group with 2 generators>
gap> [[22,38],Length(F.1),Filtered(H1(F),x->x>1)];
[ [ 22, 38 ], 672, [  ] ]
```

## 6. Proof of Theorem 1.18

Let $k$ be a number field, $K/k$ be a finite extension, $\mathbb{A}_K^\times$ be the idele group of $K$ and $L/k$ be the Galois closure of $K/k$. Let $G = \mathrm{Gal}(L/k) = nTm$ be a transitive subgroup of $S_n$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$.

For $x, y \in G$, we denote $[x, y] = x^{-1}y^{-1}xy$ the commutator of $x$ and $y$, and $[G, G]$ the commutator group of $G$. Let $V_k$ be the set of all places of $k$ and $G_v$ be the decomposition group of $G$ at $v \in V_k$.

Definition 1.35 (Drakokhrust and Platonov [**PD85a**, page 350], [**DP87**, page 300]). Let $k$ be a number field, $L \supset K \supset k$ be a tower of finite extensions where $L$ is normal over $k$.

We call the group

$$\mathrm{Obs}(K/k) = (N_{K/k}(\mathbb{A}_K^\times) \cap k^\times)/N_{K/k}(K^\times)$$

*the total obstruction to the Hasse norm principle for* $K/k$ and

$$\mathrm{Obs}_1(L/K/k) = \left(N_{K/k}(\mathbb{A}_K^\times) \cap k^\times\right) / \left((N_{L/k}(\mathbb{A}_L^\times) \cap k^\times)N_{K/k}(K^\times)\right)$$

*the first obstruction to the Hasse norm principle for* $K/k$ *corresponding to the tower* $L \supset K \supset k$.

Note that (i) $\mathrm{Obs}(K/k) = 1$ if and only if the Hasse norm principle holds for $K/k$; and (ii) $\mathrm{Obs}_1(L/K/k) = \mathrm{Obs}(K/k)/(N_{L/k}(\mathbb{A}_L^\times) \cap k^\times)$.

Drakokhrust and Platonov gave a formula for computing the first obstruction $\mathrm{Obs}_1(L/K/k)$:

Theorem 1.36 (Drakokhrust and Platonov [**PD85a**, page 350], [**PD85b**, pages 789–790], [**DP87**, Theorem 1]). *Let* $k$ *be a number field,* $L \supset K \supset k$ *be a tower of finite extensions where* $L$ *is normal over* $k$. *Let* $G = \mathrm{Gal}(L/k)$ *and* $H = \mathrm{Gal}(L/K)$. *Then*

$$\mathrm{Obs}_1(L/K/k) \simeq \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2)$$

*where in the the commutative diagram*

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\psi_1} & G/[G,G] \\ \uparrow{\scriptstyle \varphi_1} & & \uparrow{\scriptstyle \varphi_2} \\ \displaystyle\bigoplus_{v\in V_k}\left(\bigoplus_{w|v} H_w/[H_w,H_w]\right) & \xrightarrow{\psi_2} & \displaystyle\bigoplus_{v\in V_k} G_v/[G_v,G_v], \end{array}$$

*$\psi_1$, $\varphi_1$ and $\varphi_2$ are defined by the inclusions $H \subset G$, $H_w \subset H$ and $G_v \subset G$ respectively, and*

$$\psi_2(h[H_w, H_w]) = x^{-1}hx[G_v, G_v]$$

*for $h \in H_w = H \cap x^{-1}hx[G_v, G_v]$ $(x \in G)$.*

Let $\psi_2^v$ be the restriction of $\psi_2$ to the subgroup $\bigoplus_{w|v} H_w/[H_w, H_w]$ with respect to $v \in V_k$ and $\psi_2^{\mathrm{nr}}$ (resp. $\psi_2^{\mathrm{r}}$) be the restriction of $\psi_2$ to the unramified (resp. the ramified) places $v$ of $k$.

PROPOSITION 1.37 (Drakokhrust and Platonov [**DP87**]). *Let $k$, $L \supset K \supset k$, $G$ and $H$ be as in Theorem 1.36.*
(i) ([**DP87**, Lemma 1]) *Places $w_i \mid v$ of $K$ are in one-to-one correspondence with the set of double cosets in the decomposition $G = \cup_{i=1}^{r_v} H x_i G_v$ where $H_{w_i} = H \cap x_i G_v x_i^{-1}$;*
(ii) ([**DP87**, Lemma 2]) *If $G_{v_1} \leq G_{v_2}$, then $\varphi_1(\operatorname{Ker} \psi_2^{v_1}) \subset \varphi_1(\operatorname{Ker} \psi_2^{v_2})$;*
(iii) ([**DP87**, Theorem 2]) $\varphi_1(\operatorname{Ker} \psi_2^{\mathrm{nr}}) = \Phi^G(H)/[H,H]$ *where* $\Phi^G(H) = \langle [h,x] \mid h \in H \cap xHx^{-1}, x \in G \rangle$*;*
(iv) ([**DP87**, Lemma 8]) *If $[K:k] = p^r$ $(r \geq 1)$ and $\operatorname{Obs}(K_p/k_p) = 1$ where $k_p = L^{G_p}$, $K_p = L^{H_p}$, $G_p$ and $H_p \leq H \cap G_p$ are $p$-Sylow subgroups of $G$ and $H$ respectively, then $\operatorname{Obs}(K/k) = 1$.*

REMARK 1.38. The inverse direction of Proposition 1.37 (iv) does not hold in general. For example, if $n = 8$, $G = 8T13 \simeq A_4 \times C_2$ and there exists a place $v$ of $k$ such that $G_v \simeq V_4$, then $\operatorname{Obs}(K/k) = 1$ but $G_2 = 8T3 \simeq (C_2)^3$ and $\operatorname{Obs}(K_2/k_2) \neq 1$ may occur (see Theorem 1.18 and Table 2).

THEOREM 1.39 (Drakokhrust and Platonov [**DP87**, Theorem 3, Corollary 1]). *Let $k$, $L \supset K \supset k$, $G$ and $H$ be as in Theorem 1.36. Let $H_i \leq G_i \leq G$ $(1 \leq i \leq m)$, $H_i \leq H \cap G_i$, $k_i = L^{G_i}$ and $K_i = L^{H_i}$. If $\operatorname{Obs}(K_i/k_i) = 1$ for all $1 \leq i \leq m$ and*

$$\bigoplus_{i=1}^{m} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\text{cores}} \widehat{H}^{-3}(G, \mathbb{Z})$$

*is surjective, then $\operatorname{Obs}(K/k) = \operatorname{Obs}_1(L/K/k)$. In particular, if $[K:k] = n$ is square-free, then $\operatorname{Obs}(K/k) = \operatorname{Obs}_1(L/K/k)$.*

We note that if $L/k$ is an unramified extension, then $A(T) = 0$ and $H^1(G, [J_{G/H}]^{fl}) \simeq Ш(T) \simeq \operatorname{Obs}(K/k)$ where $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ (see Theorem 1.2 and Theorem 1.9). If, in addition, $\operatorname{Obs}(K/k) = \operatorname{Obs}_1(L/K/k)$ (e.g. $[K:k] = 6, 10, 14, 15$; square-free, see Theorem 1.39), then $\operatorname{Obs}(K/k) = \operatorname{Obs}_1(L/K/k) = \operatorname{Ker} \psi_1/\varphi_1(\operatorname{Ker} \psi_2^{\mathrm{nr}}) \simeq \operatorname{Ker} \psi_1/(\Phi^G(H)/[H,H])$ (see Proposition 1.37 (iii)).

THEOREM 1.40 (Drakokhrust [**Dra89**, Theorem 1], see also Opolka [**Opo80**, Satz 3] for the existence of $\widetilde{L}$). *Let $k$, $L \supset K \supset k$, $G$ and $H$ be as in Theorem 1.36. Assume that $\widetilde{L} \supset L \supset k$ is a tower of Galois extensions with $\widetilde{G} = \operatorname{Gal}(\widetilde{L}/k)$ and $\widetilde{H} = \operatorname{Gal}(\widetilde{L}/K)$ which correspond to a central extension $1 \to A \to \widetilde{G} \to G \to 1$ with $A \cap [\widetilde{G}, \widetilde{G}] \simeq M(G) = H^2(G, \mathbb{C}^\times)$; the Schur multiplier of $G$ (this is equivalent to the inflation $M(G) \to M(\widetilde{G})$ being the zero map, see* Beyl and Tappe [**BT82**, Proposition 2.13, page 85]). *Then $\operatorname{Obs}(K/k) = \operatorname{Obs}_1(\widetilde{L}/K/k)$. In particular, if $\widetilde{G}$ is a Schur cover of $G$, i.e. $A \simeq M(G)$, then $\operatorname{Obs}(K/k) = \operatorname{Obs}_1(\widetilde{L}/K/k)$.*

Indeed, Drakokhrust [**Dra89**, Theorem 1] shows that $\mathrm{Obs}(K/k) \simeq \mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2)$ where the maps $\widetilde{\psi}_1, \widetilde{\psi}_2$ and $\widetilde{\varphi}_1$ are defined as in [**Dra89**, page 31, the paragraph before Proposition 1]. The proof of [**Dra89**, Proposition 1] shows that this group is the same as $\mathrm{Obs}_1(\widetilde{L}/K/k)$ (see also [**Dra89**, Lemma 2, Lemma 3 and Lemma 4]).

We made the following functions of GAP ([**GAP**]) which will be used in the proof of Theorem 1.18.

`FirstObstructionN(`$G, H$`).ker` returns the list $[l_1, [l_2, l_3]]$ where $l_1$ is the abelian invariant of the numerator of the first obstruction $\mathrm{Ker}\,\psi_1 = \langle y_1, \ldots, y_t \rangle$ with respect to $G$, $H$ as in Theorem 1.36, $l_2 = [e_1, \ldots, e_m]$ is the abelian invariant of $H^{ab} = H/[H,H] = \langle x_1, \ldots, x_m \rangle$ with $e_i = \mathrm{order}(x_i)$ and $l_3 = [l_{3,1}, \ldots, l_{3,t}]$, $l_{3,i} = [r_{i,1}, \ldots, r_{i,m}]$ is the list with $y_i = x_1^{r_{i,1}} \cdots x_m^{r_{i,m}}$ for $H \leq G \leq S_n$.

`FirstObstructionN(`$G$`).ker` returns the same as `FirstObstructionN(`$G, H$`).ker` where $H = \mathrm{Stab}_1(G)$ is the stabilizer of 1 in $G \leq S_n$.

`FirstObstructionDnr(`$G, H$`).Dnr` returns the list $[l_1, [l_2, l_3]]$ where $l_1$ is the abelian invariant of the unramified part of the denominator of the first obstruction $\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) = \Phi^G(H)/[H,H] = \langle y_1, \ldots, y_t \rangle$ with respect to $G$, $H$ as in Proposition 1.37 (iii), $l_2 = [e_1, \ldots, e_m]$ is the abelian invariant of $H^{ab} = H/[H,H] = \langle x_1, \ldots, x_m \rangle$ with $e_i = \mathrm{order}(x_i)$ and $l_3 = [l_{3,1}, \ldots, l_{3,t}]$, $l_{3,i} = [r_{i,1}, \ldots, r_{i,m}]$ is the list with $y_i = x_1^{r_{i,1}} \cdots x_m^{r_{i,m}}$ for $H \leq G \leq S_n$.

`FirstObstructionDnr(`$G$`).Dnr` returns the same as `FirstObstructionDnr(`$G, H$`).Dnr` where $H = \mathrm{Stab}_1(G)$ is the stabilizer of 1 in $G \leq S_n$.

`FirstObstructionDr(`$G, G_v, H$`).Dr` returns the list $[l_1, [l_2, l_3]]$ where $l_1$ is the abelian invariant of the ramified part of the denominator of the first obstruction $\varphi_1(\mathrm{Ker}\,\psi_2^v) = \langle y_1, \ldots, y_t \rangle$ with respect to $G$, $G_v$, $H$ as in Theorem 1.36, $l_2 = [e_1, \ldots, e_m]$ is the abelian invariant of $H^{ab} = H/[H,H] = \langle x_1, \ldots, x_m \rangle$ with $e_i = \mathrm{order}(x_i)$ and $l_3 = [l_{3,1}, \ldots, l_{3,t}]$, $l_{3,i} = [r_{i,1}, \ldots, r_{i,m}]$ is the list with $y_i = x_1^{r_{i,1}} \cdots x_m^{r_{i,m}}$ for $G_v, H \leq G \leq S_n$.

`FirstObstructionDr(`$G, G_v$`).Dr` returns the same as `FirstObstructionDr(`$G, G_v, H$`).Dr` where $H = \mathrm{Stab}_1(G)$ is the stabilizer of 1 in $G \leq S_n$.

`SchurCoverG(`$G$`).SchurCover` (resp. `SchurCoverG(`$G$`).epi`) returns one of the Schur covers $\widetilde{G}$ of $G$ (resp. the surjective map $\pi$) in a central extension $1 \to A \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $A \simeq M(G)$; Schur multiplier of $G$ (see Karpilovsky [**Kap87**, page 16]). The Schur covers $\widetilde{G}$ are stem extensions, i.e. $A \leq Z(\widetilde{G}) \cap [\widetilde{G}, \widetilde{G}]$, of the maximal size. This function is based on the built-in function `EpimorphismSchurCover` in GAP.

`MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`
(resp. `MinimalStemExtensions(`$G$`)[`$j$`].epi`) returns the $j$-th minimal stem extension $\overline{G} = \widetilde{G}/A'$, i.e. $\overline{A} \leq Z(\overline{G}) \cap [\overline{G}, \overline{G}]$, of $G$ provided by the Schur cover $\widetilde{G}$ of $G$ via `SchurCoverG(`$G$`).SchurCover` where $A'$ is the $j$-th maximal subgroup of $A = M(G)$ (resp. the surjective map $\overline{\pi}$) in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A = M(G) & \longrightarrow & \widetilde{G} & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \overline{A} = A/A' & \longrightarrow & \overline{G} = \widetilde{G}/A' & \xrightarrow{\overline{\pi}} & G & \longrightarrow & 1 \end{array}$$

(see Robinson [**Rob96**, Exercises 11.4]). This function is based on the built-in function `EpimorphismSchurCover` in GAP.

`ResolutionNormalSeries(LowerCentralSeries(`$G$`),` $n+1$`)`
(resp. `ResolutionNormalSeries(DerivedSeries (`$G$`),`$n$+1`),ResolutionFiniteGroup(`$G$`,`$n$+1`)`) returns a free resolution $RG$ of $G$ when $G$ is nilpotent (resp. solvable, finite). This function is the built-in function of HAP ([**HAP**]) in GAP ([**GAP**]) .

`ResHnZ(`$RG, RH, n$`).HnGZ` (resp. `ResHnZ(`$RG, RH, n$`).HnHZ`) returns the abelian invariants of $H^n(G, \mathbb{Z})$ (resp. $H^n(H, \mathbb{Z})$) with respect to Smith normal form, for free resolutions $RG$ and $RH$ of $G$ and $H$ respectively.

`ResHnZ(`$RG, RH, n$`).Res` returns the list $L = [l_1, \ldots, l_s]$ where $H^n(G, \mathbb{Z}) = \langle x_1, \ldots, x_s \rangle \xrightarrow{\text{res}} H^n(H, \mathbb{Z}) = \langle y_1, \ldots, y_t \rangle$, $\text{res}(x_i) = \prod_{j=1}^{t} y_j^{l_{i,j}}$ and $l_i = [l_{i,1}, \ldots, l_{i,t}]$ for free resolutions $RG$ and $RH$ of $G$ and $H$ respectively.

`ResHnZ(`$RG, RH, n$`).Ker` returns the list $L = [l_1, [l_2, l_3]]$ where $l_1$ is the abelian invariant of $\text{Ker}\{H^n(G, \mathbb{Z}) \xrightarrow{\text{res}} H^n(H, \mathbb{Z})\} = \langle y_1, \ldots, y_t \rangle$, $l_2 = [d_1, \ldots, d_s]$ is the abelian invariant of $H^n(G, \mathbb{Z}) = \langle x_1, \ldots, x_s \rangle$ with $d_i = \text{ord}(x_i)$ and $l_3 = [l_{3,1}, \ldots, l_{3,t}]$, $l_{3,j} = [r_{j,1}, \ldots, r_{j,s}]$ is the list

with $y_j = x_1^{r_{j,1}} \cdots x_s^{r_{j,s}}$ for free resolutions $RG$ and $RH$ of $G$ and $H$ respectively.

`ResHnZ(`$RG, RH, n$`).Coker` returns the list $L = [l_1, [l_2, l_3]]$ where $l_1 = [e_1, \ldots, e_t]$ is the abelian invariant of $\mathrm{Coker}\{H^n(G, \mathbb{Z}) \xrightarrow{\mathrm{res}} H^n(H, \mathbb{Z})\} = \langle \overline{y_1}, \ldots, \overline{y_t} \rangle$ with $e_j = \mathrm{ord}(\overline{y_j})$, $l_2 = [d_1, \ldots, d_s]$ is the abelian invariant of $H^n(H, \mathbb{Z}) = \langle x_1, \ldots, x_s \rangle$ with $d_i = \mathrm{ord}(x_i)$ and $l_3 = [l_{3,1}, \ldots, l_{3,t}]$, $l_{3,j} = [r_{j,1}, \ldots, r_{j,s}]$ is the list with $\overline{y_j} = \overline{x_1}^{r_{j,1}} \cdots \overline{x_s}^{r_{j,s}}$ for free resolutions $RG$ and $RH$ of $G$ and $H$ respectively.

`KerResH3Z(`$G, H$`)` returns the list $L = [l_1, [l_2, l_3]]$ where $l_1$ is the abelian invariant of $\mathrm{Ker}\{H^3(G, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = \langle y_1, \ldots, y_t \rangle$ where $H_i \leq G_i \leq G$, $H_i \leq H \cap G_i$, $[G_i : H_i] = n$ and the action of $G_i$ on $\mathbb{Z}[G_i/H_i]$ may be regarded as $nTm$ ($n \leq 15, n \neq 12$) which is not in Table 1, $l_2 = [d_1, \ldots, d_s]$ is the abelian invariant of $H^3(G, \mathbb{Z}) = \langle x_1, \ldots, x_s \rangle$ with $d_{i'} = \mathrm{ord}(x_{i'})$ and $l_3 = [l_{3,1}, \ldots, l_{3,t}]$, $l_{3,j} = [r_{j,1}, \ldots, r_{j,s}]$ is the list with $y_j = x_1^{r_{j,1}} \cdots x_s^{r_{j,s}}$ for groups $G$ and $H$ (cf. Theorem 1.40).

The functions above are available from
`https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/Norm1ToriHNP`.

*Proof of Theorem 1.18.*

Let $G = \mathrm{Gal}(L/k) = nTm \leq S_n$ be the $m$-th transitive subgroup of $S_n$ and $H = \mathrm{Gal}(L/K) \leq G$ with $[G : H] = n$. Let $V_k$ be the set of all places of $k$ and $G_v$ be the decomposition group of $G$ at $v \in V_k$.

We split the proof into the following cases:
(1) $G = 8Tm$ ($m = 2, 3, 4, 13, 14, 21, 31, 37, 38$),
(2) $G = 8Tm$ ($m = 9, 11, 15, 19, 22, 32$),
(3) $G = 9Tm$ ($m = 2, 5, 7, 9, 11, 14, 23$),
(4) $G = 10Tm$ ($m = 7, 26, 32$),
(5) $G = 14T30$,
(6) $G = 15Tm$ ($m = 9, 14$).

For the reader's convenience, we also give the GAP computations to the known cases: $G = 4T2 \simeq V_4, 4T4 \simeq A_4, 6T4 \simeq A_4, 6T12 \simeq A_5$ (see Example 6.9 and Example 6.10).

In order to prove the statement of the theorem, we may assume that $H = \mathrm{Stab}_1(G)$ is the stabilizer of 1 in $G$, i.e. $L = k(\theta_1, \ldots, \theta_n)$ and $K = L^H = k(\theta_1)$, without loss of generality

except for the cases (2) $G = 8Tm$ $(m = 9, 11, 15, 19, 22, 32)$ and $G = 10T32 \simeq S_6$ because the center $Z(G)$ and the commutator group $[G', G']$ where $G' \leq G$ is a characteristic subgroup in the statement of the theorem, are characteristic subgroups of $G$, i.e. invariants under the automorphisms of $G$.

For the cases (2) $G = 8Tm$, by the assumption of the statement of the theorem, we may assume that $H = \mathrm{Stab}_1(G)$ is the stabilizer of 1 in $G$ because (the multi-set) $\{\mathrm{Orb}_{G'}(i) \mid 1 \leq i \leq n\}$ $(G' \leq G)$ is invariant under the conjugacy actions of $G$, i.e. inner automorphisms of $G$.

For the case $G = 10T32 \simeq S_6$, there exist exactly 10 subgroups $H \leq G$ with $[G : H] = 10$ which are conjugate in $G$. Hence we may assume that $H = \mathrm{Stab}_1(G)$ without loss of generality.

By Theorem 1.2 and Theorem 1.15, it is enough to give a necessary and sufficient condition for $Ш(T) = 0$.

(1) $n = 8$: $G = 8Tm$ $(m = 2, 3, 4, 13, 14, 21, 31, 37, 38)$. Applying the functions `FirstObstructionN(G)` and `FirstObstructionDnr(G)`, we have $\mathrm{Obs}_1(L/K/k) = 1$ except for $G = 8T21 \simeq (C_2)^3 \rtimes C_4$. For $G = 8T21$, we obtain that $\mathrm{Obs}_1(L/K/k) \simeq \mathbb{Z}/2\mathbb{Z}$.

(1-1) The case $G = 8T3 \simeq (C_2)^3$. This case follows from Theorem 1.8 because $H = 1$. See also Example 1.45 and the second paragraph after Theorem 1.8.

(1-2) The case $G = 8T21 \simeq (C_2)^3 \rtimes C_4$. We have $H = H^{ab} \simeq C_2 \times C_2$. Applying `FirstObstructionN(G)` and `FirstObstructionDnr(G)`, we obtain that $\mathrm{Ker}\, \psi_1/\varphi_1(\mathrm{Ker}\, \psi_2^{\mathrm{nr}})$ $\simeq \mathbb{Z}/2\mathbb{Z}$. By Theorem 1.15, we get $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k)$ when $L/k$ is unramified (see the paragraph after Theorem 1.39). Use Theorem 1.39. Applying the function `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(G, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ and hence $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(G, \mathbb{Z})$ is surjective. It follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k)$. Applying the function `FirstObstructionDr(G,G')` for all subgroups $G' \leq G$, we find that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that $G_v = G$ (see Example 1.45).

(1-3) The case $G = 8Tm$ $(m = 2, 4, 13, 14, 37)$. Because $\mathrm{Obs}_1(K/k) = 1$, we just apply Theorem 1.40. We have the Schur multiplier $M(G) \simeq \mathbb{Z}/2\mathbb{Z}$ for $G = 8Tm$ $(m = 2, 4, 13, 14, 37)$.

(1-3-1) The case $G = 8T2 \simeq C_4 \times C_2$ (see also Theorem 1.8 because $H = 1$). Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/2\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq (C_4 \times C_2) \rtimes C_2$, $\widetilde{H} \simeq C_2$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\, \widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\, \widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ (see the paragraph after Theorem 1.39). By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $\widetilde{G}_v = \widetilde{G}$ if and only if there exists $v \in V_k$ such that $G_v = G$ (see Example 1.45).

(1-3-2) The case $G = 8T4 \simeq D_4$ (see also Theorem 1.8 because $H = 1$). Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/2\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq D_8$, $\widetilde{H} \simeq C_2$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $D_4 \leq \widetilde{G}_v$ if and only if there exists $v \in V_k$ such that $V_4 \leq G_v$ (see Example 1.45).

(1-3-3) The case $G = 8T13 \simeq A_4 \times C_2$. We have $H \simeq C_3$. Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/2\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq ((C_4 \times C_2) \rtimes C_2) \rtimes C_3$, $\widetilde{H} \simeq C_6$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $V_4 \leq G_v$ (see Example 1.45).

(1-3-4) The case $G = 8T14 \simeq S_4$. We have $H \simeq C_3$. Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/2\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq GL_2(\mathbb{F}_3)$ and $\widetilde{H} \simeq C_6$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $V_4 \leq G_v$ (see Example 1.45).

(1-3-5) The case $G = 8T37 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. We have $H \simeq C_7 \rtimes C_3$. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/2\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq \mathrm{SL}_2(\mathbb{F}_7)$, $\widetilde{H} \simeq C_2 \times (C_7 \rtimes C_3)$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $V_4 \leq G_v$ (see Example 1.45).

(1-4) The case $G = 8Tm$ $(m = 31, 38)$. Applying `FirstObstructionN(`$G$`)` and `FirstObstructionDnr(`$G$`)`, we have $\mathrm{Obs}_1(L/K/k) = 1$. For $G = 8T31$ (resp. $G = 8T38$), we have $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$ (resp. $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$). Hence we take a minimal stem extension $\overline{G} = \widetilde{G}/A'$, i.e. $\overline{A} \leq Z(\overline{G}) \cap [\overline{G}, \overline{G}]$, of $G$ in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A = M(G) & \longrightarrow & \widetilde{G} & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \overline{A} = A/A' & \longrightarrow & \overline{G} = \widetilde{G}/A' & \xrightarrow{\overline{\pi}} & G & \longrightarrow & 1 \end{array}$$

with $\overline{A} \simeq \mathbb{Z}/2\mathbb{Z}$ via the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`. Then we apply Theorem 1.39 instead of Theorem 1.40.

(1-4-1) The case $G = 8T31 \simeq ((C_2)^4 \rtimes C_2) \rtimes C_2$. We have $H \simeq (C_2)^3$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 4}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \ldots, \overline{G}_{15}$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we

see that $\mathrm{Ker}\{H^3(\overline{G}_1,\mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i,\mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j,\mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i,\mathbb{Z})\} \simeq \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{j \mid 2 \leq j \leq 15\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i,\mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_1,\mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_1/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_1$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_1, \overline{G}_1', \overline{H}_1$`)` for all subgroups $\overline{G}_1' \leq \overline{G}_1$. We find that $\mathrm{Obs}_1(\overline{L}_1/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $V_4 \cap [G,G] = 1$ (equivalently, $|\mathrm{Orb}_{V_4}(i)| = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$), (ii) $C_4 \times C_2 \leq G_v$ where $(C_4 \times C_2) \cap [G,G] \simeq C_2$ (equivalently, $C_4 \times C_2$ is transitive in $S_8$) or (iii) $(C_2)^3 \rtimes C_4 \leq G_v$ (see Details 1.42 and Example 1.45).

(1-4-2) The case $G = 8T38 \simeq (((C_2)^4 \rtimes C_2) \rtimes C_2) \rtimes C_3$. We have $H \simeq C_2 \times A_4$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \overline{G}_2, \overline{G}_3$ of $G$. Use Theorem 1.39. Applying the function `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_2,\mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i,\mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j,\mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i,\mathbb{Z})\} \simeq \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{1,3\}$. We have that $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i,\mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_2,\mathbb{Z})$ is surjective. By Theorem 1.39, $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_2/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_2$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply the function `FirstObstructionDr(`$\overline{G}_2, \overline{G}_2', \overline{H}_2$`)` for all subgroups $\overline{G}_2' \leq \overline{G}_2$. We find that $\mathrm{Obs}_1(\overline{L}_2/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $V_4 \cap [\mathrm{Syl}_2(G), \mathrm{Syl}_2(G)] = 1$ with $\mathrm{Syl}_2(G) \lhd G$ (equivalently, $|\mathrm{Orb}_{V_4}(i)| = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$), (ii) $C_4 \times C_2 \leq G_v$ where $(C_4 \times C_2) \cap [\mathrm{Syl}_2(G), \mathrm{Syl}_2(G)] \simeq C_2$ (equivalently, $C_4 \times C_2$ is transitive in $S_8$) or (iii) $(C_2)^3 \rtimes C_4 \leq G_v$ (see Details 1.42 and Example 1.45).

(2) $n = 8$: $G = 8Tm$ $(m = 9, 11, 15, 19, 22, 32)$. We assume that $H = \mathrm{Stab}_1(G)$ by the assumption. Applying `FirstObstructionN(`$G$`)`, we have $\mathrm{Obs}_1(L/K/k) = 1$. For the cases $G = 8Tm$ $(m = 9, 11, 15, 19, 22, 32)$, we also find that $(\mathbb{Z}/2\mathbb{Z})^{\oplus 2} \leq M(G) \leq (\mathbb{Z}/2\mathbb{Z})^{\oplus 5}$. Hence we take a minimal stem extension $\overline{G} = \widetilde{G}/A'$, i.e. $\overline{A} \leq Z(\overline{G}) \cap [\overline{G}, \overline{G}]$, of $G$ in the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A = M(G) & \longrightarrow & \widetilde{G} & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \overline{A} = A/A' & \longrightarrow & \overline{G} = \widetilde{G}/A' & \xrightarrow{\overline{\pi}} & G & \longrightarrow & 1 \end{array}$$

with $\overline{A} \simeq \mathbb{Z}/2\mathbb{Z}$ via the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`. Then we apply Theorem 1.39 instead of Theorem 1.40 as in the case (1-4).

(2-1) The case $G = 8T9 \simeq D_4 \times C_2$. We have $H \simeq C_2$. We obtain that the Schur multiplier $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$. By applying `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we obtain the minimal stem extensions $\overline{G}_1, \ldots, \overline{G}_7$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_2, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{1, 3, 4, 5, 6, 7\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_2, \mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_2/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_2$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. Hence $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply the function `FirstObstructionDr(`$\overline{G}_2, \overline{G}_2', \overline{H}_2$`)` for all subgroups $\overline{G}_2' \leq \overline{G}_2$. We find that $\mathrm{Obs}_1(\overline{L}_2/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $|\mathrm{Orb}_{V_4}(i)| = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap [G, G] = 1$; or (ii) $C_4 \times C_2 \leq G_v$ (see Details 1.42 and Example 1.46).

(2-2) The case $G = 8T11 \simeq (C_4 \times C_2) \rtimes C_2$. We have $H \simeq C_2$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$. Applying `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`. We get the minimal stem extensions $\overline{G}_1, \overline{G}_2, \overline{G}_3$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_2, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{1, 3\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_2, \mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_2/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_2$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_2, \overline{G}_2', \overline{H}_2$`)` for all subgroups $\overline{G}_2' \leq \overline{G}_2$. We find that $\mathrm{Obs}_1(\overline{L}_2/K/k) = 1$ if and only if there exists $v \in V_k$ such that $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is transitive in $S_8$ (see Details 1.42 and Example 1.46).

(2-3) The case $G = 8T15 \simeq C_8 \rtimes V_4$. We have $H \simeq V_4$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \overline{G}_2, \overline{G}_3$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_1, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{2, 3\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_1, \mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_1/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_1$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_1, \overline{G}_1', \overline{H}_1$`)` for all subgroups $\overline{G}_1' \leq \overline{G}_1$. We find that $\mathrm{Obs}_1(\overline{L}_1/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $|\mathrm{Orb}_{V_4}(i)| = 2$ for any $1 \leq i \leq 8$ and $V_4 \cap [G, G] = 1$

(equivalently, $|\mathrm{Orb}_{V_4}(i)| = 2$ for any $1 \leq i \leq 8$ and $V_4$ is not in $A_8$) or (ii) $C_4 \times C_2 \leq G_v$ where $(C_4 \times C_2) \cap [G, G] \simeq C_2$ (equivalently, $C_4 \times C_2$ is transitive in $S_8$) (see Details 1.42 and Example 1.46).

(2-4) The case $G = 8T19 \simeq (C_2)^3 \rtimes C_4$. We have $H \simeq C_4$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \overline{G}_2, \overline{G}_3$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_3, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{1, 2\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_3, \mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_3/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_3$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_3, \overline{G}'_3, \overline{H}_3$`)` for all subgroups $\overline{G}'_3 \leq \overline{G}_3$. We find that $\mathrm{Obs}_1(\overline{L}_3/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $V_4 \cap Z(G) = 1$ and $V_4 \cap Z^2(G) \simeq C_2$ with the upper central series $1 \leq Z(G) \leq Z^2(G) \leq G$ of $G$ (equivalently, $|\mathrm{Orb}_{V_4}(i)| = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$); or (ii) $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is not transitive in $S_8$ or $[G, G] \leq C_4 \times C_2$ (see Details 1.42 and Example 1.46).

(2-5) The case $G = 8T22 \simeq (C_2)^3 \rtimes V_4$. We have $H \simeq V_4$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 5}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \ldots, \overline{G}_{31}$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_{16}, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} \neq 0$ for $j \in J := \{j \mid 1 \leq j \leq 31, j \neq 16\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_{16}, \mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_{16}/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_{16}$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_{16}, \overline{G}'_{16}, \overline{H}_{16}$`)` for all subgroups $\overline{G}'_{16} \leq \overline{G}_{16}$. We find that $\mathrm{Obs}_1(\overline{L}_{16}/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $|\mathrm{Orb}_{V_4}(i)| = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$ or (ii) $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is transitive in $S_8$. (see Details 1.42 and Example 1.46).

(2-6) The case $G = 8T32 \simeq ((C_2)^3 \rtimes V_4) \rtimes C_3$. We have $H \simeq A_4$ and $M(G) \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 3}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \ldots, \overline{G}_7$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we see that $\mathrm{Ker}\{H^3(\overline{G}_5, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} \simeq \mathbb{Z}/2\mathbb{Z}$ for $j \in J := \{j \mid 2 \leq j \leq 7\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_5, \mathbb{Z})$ is surjective, it follows

from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_5/K/k)$. We also checked that $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_5$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_1, \overline{G}_1', \overline{H}_1$`)` for all subgroups $\overline{G}_1' \leq \overline{G}_1$. We find that $\mathrm{Obs}_1(\overline{L}_1/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $|\mathrm{Orb}_{V_4}(i)| = 4$ for any $1 \leq i \leq 8$ and $V_4 \cap Z(G) = 1$ or (ii) $C_4 \times C_2 \leq G_v$ where $C_4 \times C_2$ is transitive in $S_8$ (see Details 1.42 and Example 1.46).

(3) $n = 9$: $G = 9Tm$ $(m = 2, 5, 7, 9, 11, 14, 23)$. Applying `FirstObstructionN(`$G$`)`, we have $\mathrm{Obs}_1(L/K/k) = 1$ for each cases. We apply Theorem 1.40 for $m = 2, 5, 9, 11, 14, 23$. We see that $M(G) \simeq \mathbb{Z}/3\mathbb{Z}$ for $m = 2, 5, 9, 11, 14, 23$ and $M(G) \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ for $m = 7$. Then for $m = 7$ we apply Theorem 1.39 instead of Theorem 1.40 as in the case (2) $n = 8$.

(3-1) The case $G = 9T2 \simeq (C_3)^2$ (see also Theorem 1.8 because $H = 1$). Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/3\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq (C_3)^2 \rtimes C_3$ and $\widetilde{H} \simeq C_3$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/3\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $\widetilde{G}_v = \widetilde{G}$ if and only if there exists $v \in V_k$ such that $G_v = G$ (see Example 1.47).

(3-2) The case $G = 9T5 \simeq (C_3)^2 \rtimes C_2$. We have $H \simeq C_2$. Apply Theorem 1.40 as in the case (2) $n = 8$. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/3\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq ((C_3)^2 \rtimes C_3) \rtimes C_2$ and $\widetilde{H} \simeq C_6$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/3\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \rtimes C_3 \leq \widetilde{G}_v$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq G_v$ (see Example 1.47).

(3-3) The case $G = 9T7 \simeq (C_3)^2 \rtimes C_3$. We have $H \simeq C_3$ and $M(G) \simeq (\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$. Applying the function `MinimalStemExtensions(`$G$`)[`$j$`].MinimalStemExtension`, we get the minimal stem extensions $\overline{G}_1, \ldots, \overline{G}_4$ of $G$. Use Theorem 1.39. Applying `KerResH3Z(G,H)`, we obtain that $\mathrm{Ker}\{H^3(\overline{G}_1, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} = 0$ but $\mathrm{Ker}\{H^3(\overline{G}_j, \mathbb{Z}) \xrightarrow{\mathrm{res}} \oplus_{i=1}^{m'} H^3(G_i, \mathbb{Z})\} \simeq \mathbb{Z}/3\mathbb{Z}$ for $j \in J := \{2, 3, 4\}$. Because $\oplus_{i=1}^{m'} \widehat{H}^{-3}(G_i, \mathbb{Z}) \xrightarrow{\mathrm{cores}} \widehat{H}^{-3}(\overline{G}_1, \mathbb{Z})$ is surjective, it follows from Theorem 1.39 that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\overline{L}_1/K/k)$. We also have $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_1^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$ for $\overline{G}_1$ and $\mathrm{Ker}\,\overline{\psi}_1/\overline{\varphi}_1(\mathrm{Ker}\,\overline{\psi}_2^{\mathrm{nr}}) = 0$ for $\overline{G}_j$ $(j \in J)$. This implies that $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(\overline{L}_j/K/k)$ when $\overline{L}_j/k$ is unramified for $j \in J$. Apply `FirstObstructionDr(`$\overline{G}_1, \overline{G}_1', \overline{H}_1$`)` for all subgroups $\overline{G}_1' \leq \overline{G}_1$. We find that $\mathrm{Obs}_1(\overline{L}_1/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq \overline{G}_v$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq G_v$ (see Example 1.47).

(3-4) The case $G = 9T9 \simeq (C_3)^2 \rtimes C_4$. We have $H \simeq C_4$. Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/3\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq ((C_3)^2 \rtimes C_3) \rtimes C_4$, $\widetilde{H} \simeq C_{12}$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/3\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \rtimes C_3 \leq \widetilde{G}_v$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq G_v$ (see Example 1.47).

(3-5) The case $G = 9T11 \simeq (C_3)^2 \rtimes C_6$. We have $H \simeq C_6$. Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/3\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq ((C_3)^3 \rtimes C_3) \rtimes C_2$, $\widetilde{H} \simeq C_6 \times C_3$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/3\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq G_v$ (see Example 1.47).

(3-6) The case $G = 9T14 \simeq (C_3)^2 \rtimes Q_8$. We have $H \simeq Q_8$. Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/3\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq (((C_3)^2 \rtimes C_3) \rtimes Q_8) \rtimes C_3$, $\widetilde{H} \simeq C_3 \times \mathrm{SL}_2(\mathbb{F}_3)$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/3\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \rtimes C_3 \leq \widetilde{G}_v$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq G_v$ (see Example 1.47).

(3-7) The case $G = 9T23 \simeq ((C_3)^2 \rtimes Q_8) \rtimes C_3$. We have $H \simeq \mathrm{SL}_2(\mathbb{F}_3)$. Apply Theorem 1.40. We obtain a Schur cover $1 \to M(G) \simeq \mathbb{Z}/3\mathbb{Z} \to \widetilde{G} \xrightarrow{\pi} G \to 1$ with $\widetilde{G} \simeq (((C_3)^2 \rtimes C_3) \rtimes Q_8) \rtimes C_3$, $\widetilde{H} \simeq C_3 \times \mathrm{SL}_2(\mathbb{F}_3)$ and $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$. By Theorem 1.15, $\mathrm{Ker}\,\widetilde{\psi}_1/\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{\mathrm{nr}}) \simeq \mathbb{Z}/3\mathbb{Z}$. By applying `FirstObstructionDr(`$\widetilde{G}, \widetilde{G}', \widetilde{H}$`)` for all subgroups $\widetilde{G}' \leq \widetilde{G}$, we obtain that $\mathrm{Obs}_1(\widetilde{L}/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_3)^2 \leq G_v$ (see Example 1.47).

(4) $n = 10$: $G \simeq 10T7 \simeq A_5$, $G \simeq 10T26 \simeq A_6$ and $G \simeq 10T32 \simeq S_6$. By Theorem 1.39, we have $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k)$.

(4-1) The case $G = 10T7 \simeq A_5$. We have $H \simeq S_3$ and $H^{ab} \simeq C_2$. It follows from Theorem 1.15 that $\mathrm{Ker}\,\psi_1 \simeq \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. Apply `FirstObstructionDr(`$G, G'$`)` for all subgroups $G' \leq G$. We get that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that $V_4 \leq G_v$ (see Example 1.48).

(4-2) The case $G = 10T26 \simeq A_6$. We have $H \simeq (C_3)^2 \rtimes C_4$ and $H^{ab} \simeq C_4$. Applying `FirstObstructionN(`$G$`)` and `FirstObstructionDnr(`$G$`)`, we obtain that $\mathrm{Ker}\,\psi_1 \simeq \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. Apply `FirstObstructionDr(`$G, G'$`)` for all subgroups $G' \leq G$.

We get that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that $D_4 \leq G_v$ (see Example 1.48).

(4-3) The case $G = 10T32 \simeq S_6$. We have $H \simeq (S_3)^2 \rtimes C_2$ and $H^{ab} \simeq C_2 \times C_2$. Applying `FirstObstructionN(G)` and `FirstObstructionDnr(G)`, we obtain that $\mathrm{Ker}\,\psi_1 \simeq \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. We also apply the function `FirstObstructionDr(G,G')` for all subgroups $G' \leq G$. We obtain that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that (i) $V_4 \leq G_v$ where $N_{\widetilde{G}}(V_4) \simeq C_8 \rtimes (C_2 \times C_2)$ for the normalizer $N_{\widetilde{G}}(V_4)$ of $V_4$ in $\widetilde{G}$ with the normalizer $\widetilde{G} = N_{S_{10}}(G) \simeq \mathrm{Aut}(G)$ of $G$ in $S_{10}$ (equivalently, $|\mathrm{Orb}_{V_4}(i)| = 2$ for any $1 \leq i \leq 10$) or (ii) $D_4 \leq G_v$ where $D_4 \leq [G,G] \simeq A_6$ (see Details 1.42 and Example 1.48).

(5) $n = 14$: $G = 14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$. By Theorem 1.39, we obtain that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k)$. We have $H \simeq C_{13} \rtimes C_6$ and $H^{ab} \simeq C_6$. Applying `FirstObstructionN(G)` and `FirstObstructionDnr(G)`, we obtain that $\mathrm{Ker}\,\psi_1 \simeq \mathbb{Z}/6\mathbb{Z}$ and $\mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) \simeq \mathbb{Z}/2\mathbb{Z}$. Apply `FirstObstructionDr(G,G')` for all subgroups $G' \leq G$. We get that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that $V_4 \leq G_v$ (see Example 1.49).

(6) $n = 15$: $G = 15T9 \simeq (C_5)^2 \rtimes C_3$ and $G \simeq 15T14 \simeq (C_5)^2 \rtimes S_3$. By Theorem 1.39, we obtain that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(L/K/k)$.

(6-1) The case $G = 15T9 \simeq (C_5)^2 \rtimes C_3$. We have $H \simeq H^{ab} \simeq C_5$. Applying the functions `FirstObstructionN(G)` and `FirstObstructionDnr(G)`, we have $\mathrm{Ker}\,\psi_1 \simeq \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) \simeq \mathbb{Z}/5\mathbb{Z}$. Apply the functions `FirstObstructionDr(G,G')` for all subgroups $G' \leq G$. We get that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_5)^2 \leq G_v$ (see Example 1.50).

(6-2) The case $G = 15T14 \simeq (C_5)^2 \rtimes S_3$. We have $H \simeq H^{ab} \simeq C_{10}$. Applying the functions `FirstObstructionN(G)` and `FirstObstructionDnr(G)`, we obtain that $\mathrm{Ker}\,\psi_1 \simeq \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2^{\mathrm{nr}}) \simeq \mathbb{Z}/5\mathbb{Z}$. We apply the function `FirstObstructionDr(G,G')` for all subgroups $G' \leq G$. We get that $\mathrm{Obs}_1(L/K/k) = 1$ if and only if there exists $v \in V_k$ such that $(C_5)^2 \leq G_v$ (see Example 1.50). □

Remark 1.41. By the proof of Theorem 1.18, for $n = 8$ (resp. $n = 9$), there exists $\widetilde{L} \supset L$ with $[\widetilde{L} : L] = 2$ (resp. $[\widetilde{L} : L] = 3$) such that $\mathrm{Obs}(K/k) = \mathrm{Obs}_1(\widetilde{L}/K/k)$ although $\mathrm{Obs}(K/k) \neq \mathrm{Obs}_1(L/K/k)$ when $L/k$ is unramified and $\mathrm{Obs}_1(L/K/k) = 1$ except for the case $G = 8T21$ with $\mathrm{Obs}_1(L/K/k) \simeq \mathbb{Z}/2\mathbb{Z}$.

DETAILS 1.42 (The cases (1-4) $G = 8T31$, $8T38$, (2) $G = 8Tm$ $(m = 9, 11, 15, 19, 22, 32)$ and (4-3) $G = 10T32$ in Theorem 1.18). We take generators of $G$ and $H = \mathrm{Stab}_1(G)$ in Theorem 1.18 (Table 2) and give more details for the cases (1-4) $G = 8T31$, $8T38$, (2) $G = 8Tm$ $(m = 9, 11, 15, 19, 22, 32)$ and (4-3) $G = 10T32$.

(1-4) For $G = 8T31 \simeq ((C_2)^4 \rtimes C_2) \rtimes C_2$ and $G' = 8T38 \simeq (((C_2)^4) \rtimes C_2) \rtimes C_2) \rtimes C_3$, we take $G = \langle g_1, g_2, g_3 \rangle = \mathrm{Syl}_2(G') \lhd G' = \langle g_1, g_2, g_3' \rangle$ and $H = \mathrm{Stab}_1(G) = \langle g_1, (2,6), (3,7) \rangle \simeq (C_2)^3 \leq H' = \mathrm{Stab}_1(G') = \langle g_1, (2,6), (2,8,3)(4,7,6) \rangle \simeq C_2 \times A_4$ where $g_1 = (4,8)$, $g_2 = (1,8)(2,3)(4,5)(6,7)$, $g_3 = (1,3)(2,8)(4,6)(5,7)$, $g_3' = (1,2,3)(5,6,7)$. There exist 61 subgroups $V_4 \leq G$ and 14 of them satisfy $|\mathrm{Orb}_{V_4}(i)| = 4$ $(1 \leq i \leq 8)$:

$$V_4^{(1)} = \{1, \sigma_1, \sigma_2, \sigma_3\},\ V_4^{(2)} = \{1, \sigma_1, \sigma_6, \sigma_7\},\ V_4^{(3)} = \{1, \tau_1, \tau_2, \tau_6\},\ V_4^{(4)} = \{1, \tau_1, \sigma_4, \tau_5\},$$
$$V_4^{(5)} = \{1, \sigma_2, \tau_4, \sigma_7\},\ V_4^{(6)} = \{1, \tau_2, \sigma_4, \sigma_5)\},\ V_4^{(7)} = \{1, \sigma_3, \tau_4, \sigma_6\},\ V_4^{(8)} = \{1, \sigma_5, \tau_5, \tau_6\},$$
$$V_4^{(9)} = \{1, \sigma_1, \tau_3, \tau_4\},\ V_4^{(10)} = \{1, \tau_1, \tau_3, \sigma_5)\},\ V_4^{(11)} = \{1, \sigma_2, \tau_3, \sigma_6\},$$
$$V_4^{(12)} = \{1, \tau_2, \tau_3, \tau_5\},\ V_4^{(13)} = \{1, \sigma_3, \tau_3, \sigma_7\},\ V_4^{(14)} = \{1, \sigma_4, \tau_3, \tau_6\}$$

where $\sigma_1 = (1,2)(3,4)(5,6)(7,8)$, $\sigma_2 = (1,3)(2,4)(5,7)(6,8)$, $\sigma_3 = (1,4)(2,3)(5,8)(6,7)$,
$\sigma_4 = (1,4)(2,7)(3,6)(5,8)$, $\sigma_5 = (1,6)(2,5)(3,4)(7,8)$, $\sigma_6 = (1,7)(2,8)(3,5)(4,6)$,
$\sigma_7 = (1,8)(2,7)(3,6)(4,5)$, $\tau_1 = (1,2)(3,8)(4,7)(5,6)$, $\tau_2 = (1,3)(2,8)(4,6)(5,7)$,
$\tau_3 = (1,5)(2,6)(3,7)(4,8)$, $\tau_4 = (1,6)(2,5)(3,8)(4,7)$, $\tau_5 = (1,7)(2,4)(3,5)(6,8)$,
$\tau_6 = (1,8)(2,3)(4,5)(6,7)$. Note that $Z(G) = \langle \tau_3 \rangle \simeq C_2$ and the first 8 groups $V_4^{(i)}$ $(1 \leq i \leq 8)$ satisfy $V_4 \cap Z(G) = 1$ as appearing in Theorem 1.18 (Table 2) and the last 6 groups $V_4^{(i)}$ $(9 \leq i \leq 14)$ satisfy $V_4 \cap Z(G) \simeq C_2$. On the other hand, there exist 15 subgroups $C_4 \times C_2 \leq G$:

$$G^{(1)} = \langle (1,4,5,8)(2,3,6,7), \sigma_1, \tau_3 \rangle,$$
$$G^{(2)} = \langle (1,8,5,4)(2,3,6,7), \tau_1, \tau_3 \rangle,$$
$$G^{(3)} = \langle (1,8,5,4)(2,3,6,7), (1,2,5,6)(3,4,7,8), \tau_3 \rangle,$$
$$G^{(4)} = \langle (1,6,5,2)(3,8,7,4), \tau_6, \tau_3 \rangle,$$
$$G^{(5)} = \langle (1,4,5,8)(2,3,6,7), (1,2,5,6)(3,8,7,4), \tau_3 \rangle,$$
$$G^{(6)} = \langle (1,6,5,2)(3,4,7,8), \sigma_3, \tau_3 \rangle,$$

$$G^{(7)} = \langle (1,2)(3,8,7,4)(5,6), (1,5)(2,6), (3,7)(4,8) \rangle,$$
$$G^{(8)} = \langle (1,6,5,2)(3,8)(4,7), (1,5)(2,6), (3,7)(4,8) \rangle,$$
$$G^{(9)} = \langle (1,6,5,2)(3,8,7,4), (1,5)(2,6), (3,7)(4,8) \rangle,$$
$$G^{(10)} = \langle (1,7)(2,4,6,8)(3,5), (1,5)(3,7), (2,6)(4,8) \rangle,$$
$$G^{(11)} = \langle (1,7,5,3)(2,8)(4,6), (1,5)(3,7), (2,6)(4,8) \rangle,$$
$$G^{(12)} = \langle (1,7,5,3)(2,4,6,8), (1,5)(3,7), (2,6)(4,8) \rangle,$$
$$G^{(13)} = \langle (1,4,5,8)(2,3)(6,7), (1,5)(4,8), (2,6)(3,7) \rangle,$$
$$G^{(14)} = \langle (1,4)(2,3,6,7)(5,8), (1,5)(4,8), (2,6)(3,7) \rangle,$$
$$G^{(15)} = \langle (1,4,5,8)(2,3,6,7), (1,5)(4,8), (2,6)(3,7) \rangle.$$

Note that $[G,G] = \langle (1,5)(4,8), (2,6)(4,8), (2,6)(3,7) \rangle \simeq (C_2)^3$ and the first 6 groups $G^{(i)}$ $(1 \leq i \leq 6)$ satisfy $G^{(i)} \cap [G,G] = \langle \tau_3 \rangle \simeq C_2$ and are transitive in $S_8$ as appearing in Theorem 1.18 (Table 2) and the last 9 groups $G^{(i)}$ $(7 \leq i \leq 15)$ satisfy $G^{(i)} \cap [G,G] \simeq V_4$ and are not transitive in $S_8$. Also, there exist 3 subgroups $(C_2)^3 \rtimes V_4 \leq G$. They are all transitive in $S_8$ (see Example 1.45).

(2-1) For $G = 8T9 \simeq D_4 \times C_2$, we take $G = \langle g_1, g_2, g_3, g_4 \rangle$ and $H = \mathrm{Stab}_1(G) = \langle g_4 \rangle \simeq C_2$ where $g_1 = (1,8)(2,3)(4,5)(6,7)$, $g_2 = (1,3)(2,8)(4,6)(5,7)$, $g_3 = (1,5)(2,6)(3,7)(4,8)$, $g_4 = (4,5)(6,7)$. There exist 13 subgroups $V_4 \leq G$ and 8 of them satisfy $|\mathrm{Orb}_{V_4}(i)| = 4$ $(1 \leq i \leq 8)$:

$$V_4^{(1)} = \{1, \sigma_1, \sigma_3, \sigma_6\},\ V_4^{(2)} = \{1, \sigma_1, \sigma_4, \sigma_5\},\ V_4^{(3)} = \{1, \sigma_2, \sigma_3, \sigma_5\},\ V_4^{(4)} = \{1, \sigma_2, \sigma_4, \sigma_6\},$$
$$V_4^{(5)} = \{1, \sigma_1, \sigma_2, \tau_3\},\ V_4^{(6)} = \{1, \sigma_3, \sigma_4, \tau_3\},\ V_4^{(7)} = \{1, \sigma_5, \sigma_6, \tau_3\},\ V_4^{(8)} = \{1, \tau_1, \tau_2, \tau_3\}$$

where $\sigma_1 = (1,2)(3,8)(4,7)(5,6)$, $\sigma_2 = (1,3)(2,8)(4,6)(5,7)$, $\sigma_3 = (1,4)(2,7)(3,6)(5,8)$, $\sigma_4 = (1,5)(2,6)(3,7)(4,8)$, $\sigma_5 = \sigma_1\sigma_4 = (1,6)(2,5)(3,4)(7,8)$, $\sigma_6 = \sigma_1\sigma_3 = (1,7)(2,4)(3,5)(6,8)$, $\tau_1 = (1,2)(3,8)(4,6)(5,7)$, $\tau_2 = (1,3)(2,8)\ (4,7)(5,6)$, $\tau_3 = (1,8)(2,3)(4,5)(6,7)$. Note that $[G,G] = \langle \tau_3 \rangle \simeq C_2$ and the first half $V_4^{(i)}$ $(1 \leq i \leq 4)$ satisfy $V_4^{(i)} \cap [G,G] = 1$ as appearing in Theorem 1.18 (Table 2) although the second half $V_4^{(i)}$ $(5 \leq i \leq 8)$ satisfy $[G,G] \leq V_4^{(i)}$. On the other hand, there exists the unique subgroup $C_4 \times C_2 \leq G$ (see Example 1.46).

(2-2) For $G = 8T11 \simeq (C_4 \times C_2) \rtimes C_2$, we take $G = \langle g_1, g_2, g_3 \rangle$ and $H = \mathrm{Stab}_1(G) = \langle (2,6)(4,8) \rangle \simeq C_2$ where $g_1 = (1,5)(3,7)$, $g_2 = (1,3,5,7)(2,4,6,8)$, $g_3 = (1,4,5,8)(2,3,6,7)$.

There exist 3 subgroups $C_4 \times C_2 \leq G$:

$$G^{(1)} = \langle g_2, (1,2)(3,4)(5,6)(7,8) \rangle,$$
$$G^{(2)} = \langle g_2, (1,8)(2,3)(4,5)(6,7) \rangle,$$
$$G^{(3)} = \langle g_2, (2,6)(4,8) \rangle.$$

The first two groups $G^{(1)}$ and $G^{(2)}$ are transitive in $S_8$ as appearing in Theorem 1.18 (Table 2) although the last one $G^{(3)}$ is not transitive in $S_8$ (see Example 1.46).

(2-3) For $G = 8T15 \simeq C_8 \rtimes V_4$, we take $G = \langle g_1, g_2, g_3 \rangle$ and $H = \mathrm{Stab}_1(G) = \langle (2,8)(3,7)(4,6), (2,4)(3,7)(6,8) \rangle \simeq V_4$ where $g_1 = (1,2,3,4,5,6,7,8)$, $g_2 = (1,5)(3,7)$, $g_3 = (1,6)(2,5)(3,4)(7,8)$. There exist 15 subgroups $V_4 \leq G$ and 5 of them satisfy $|\mathrm{Orb}_{V_4}(i)| = 2$ $(1 \leq i \leq 8)$:

$$V_4^{(1)} = \{1, \sigma_1, \tau_1, \tau_2\},\ V_4^{(2)} = \{1, \sigma_2, \tau_3, \tau_4\},\ V_4^{(3)} = \{1, \sigma_2, \tau_5, \tau_6\},\ V_4^{(4)} = \{1, \sigma_1, \tau_7, \tau_8\},$$
$$V_4^{(5)} = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$$

where $\sigma_1 = (1,5)(3,7)$, $\sigma_2 = (2,6)(4,8)$, $\tau_1 = (2,4)(3,7)(6,8)$, $\tau_2 = (1,5)(2,4)(6,8)$, $\tau_3 = (1,3)(4,8)(5,7)$, $\tau_4 = (1,3)(2,6)(5,7)$, $\tau_5 = (1,7)(3,5)(4,8)$, $\tau_6 = (1,7)(2,6)(3,5)$, $\tau_7 = (2,8)(3,7)(4,6)$, $\tau_8 = (1,5)(2,8)(4,6)$. Note that $[G,G] = \langle (1,3,5,7), (2,4,6,8) \rangle \simeq C_4$ and the first four groups $V_4^{(i)}$ $(1 \leq i \leq 4)$ satisfy that $V_4^{(i)} \cap [G,G] = 1$ and $V_4$ is not in $A_8$ as appearing in Theorem 1.18 (Table 2) although the last one $V_4^{(5)}$ satisfy that $V_4^{(5)} \cap [G,G] \simeq C_2$ and $V_4$ is in $A_8$. On the other hand, there exist 3 subgroups $C_4 \times C_2 \leq G$:

$$G^{(1)} = \langle (1,3,5,7)(2,8,6,4), (1,2)(3,8)(4,7)(5,6) \rangle,$$
$$G^{(2)} = \langle (1,3,5,7)(2,8,6,4), (1,4)(2,3)(5,8)(6,7) \rangle,$$
$$G^{(3)} = \langle (1,3,5,7)(2,4,6,8), (2,6)(4,8) \rangle.$$

The first two groups $G^{(i)}$ $(i = 1,2)$ satisfy $G^{(i)} \cap [G,G] \simeq C_2$ $(i = 1,2)$ which is transitive in $S_8$ as appearing in Theorem 1.18 (Table 2) although the last one $G^{(3)}$ satisfy $G^{(i)} \cap [G,G] \simeq C_4$ which is not transitive in $S_8$ (see Example 1.46).

(2-4) For $G = 8T19 \simeq (C_2)^3 \rtimes C_4$, we take $G = \langle g_1, g_2, g_3, g_4 \rangle$ and $H = \mathrm{Stab}_1(G) = \langle (2,8)(4,5,6,7) \rangle \simeq C_4$ where $g_1 = (1,8)(2,3)(4,5)(6,7)$, $g_2 = (1,3)(2,8)(4,6)(5,7)$, $g_3 = (1,5)(2,6)(3,7)(4,8)$, $g_4 = (1,3)(4,5,6,7)$. There exist 13 subgroups $V_4 \leq G$ and 8 of them satisfy $|\mathrm{Orb}_{V_4}(i)| = 4$ $(1 \leq i \leq 8)$:

$$V_4^{(1)} = \{1, \sigma_1, \sigma_2, \sigma_5\},\ V_4^{(2)} = \{1, \sigma_1, \sigma_3, \sigma_4\},\ V_4^{(3)} = \{1, \sigma_2, \sigma_3, \sigma_6\},\ V_4^{(4)} = \{1, \sigma_4, \sigma_5, \sigma_6\},$$
$$V_4^{(5)} = \{1, \tau_1, \tau_2, \tau_3\},\ V_4^{(6)} = \{1, \tau_2, \sigma_1, \sigma_6\},\ V_4^{(7)} = \{1, \tau_2, \sigma_2, \sigma_4\},\ V_4^{(8)} = \{1, \tau_2, \sigma_3, \sigma_5\}$$

where $\sigma_1 = (1,2)(3,8)(4,7)(5,6)$, $\sigma_2 = (1,4)(2,7)(3,6)(5,8)$, $\sigma_3 = (1,5)(2,6)(3,7)(4,8)$,
$\sigma_4 = (1,6)(2,5)(3,4)(7,8)$, $\sigma_5 = (1,7)(2,4)(3,5)(6,8)$, $\sigma_6 = (1,8)(2,3)(4,5)(6,7)$,
$\tau_1 = (1,2)(3,8)(4,5)(6,7)$, $\tau_2 = (1,3)(2,8)(4,6)(5,7)$, $\tau_3 = (1,8)(2,3)(4,7)(5,6)$. Note that $Z(G) = \langle \tau_2 \rangle \simeq C_2$ and the first four groups $V_4^{(i)}$ $(1 \leq i \leq 4)$ satisfy $V_4^{(i)} \cap Z(G) = 1$ and $V_4^{(i)} \cap Z^2(G) \simeq C_2$ with the upper central series $1 \leq Z(G) \leq Z^2(G) \leq G$ of $G$ as appearing in Theorem 1.18 (Table 2) although the last four groups $V_4^{(i)}$ $(5 \leq i \leq 8)$ satisfy $V_4^{(i)} \cap Z(G) \simeq C_2$. On the other hand, there exist 5 subgroups $C_4 \times C_2 \leq G$:

$$
\begin{aligned}
G^{(1)} &= \langle (2,8)(4,5,6,7), (1,3)(2,8) \rangle, \\
G^{(2)} &= \langle (1,2,3,8)(5,7), (4,6)(5,7) \rangle, \\
G^{(3)} &= \langle (1,5,3,7)(2,6,8,4), (1,8)(2,3)(4,5)(6,7) \rangle, \\
G^{(4)} &= \langle (1,4,2,5)(4,6,8,7), (1,3)(2,8)(4,6)(5,7) \rangle, \\
G^{(5)} &= \langle (1,4,8,7)(2,5,3,6), (1,3)(2,8)(4,6)(5,7) \rangle.
\end{aligned}
$$

Note that $[G,G] = \langle (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) \rangle \simeq V_4$ and the first two groups $G^{(1)}$ and $G^{(2)}$ are not transitive in $S_8$ and the third one $G^{(3)}$ is transitive in $S_8$ which satisfy $[G,G] \leq G^{(3)}$ as appearing in Theorem 1.18 (Table 2) although the last two $G^{(4)}$ and $G^{(5)}$ are transitive in $S_8$ which satisfy $G^{(i)} \cap [G,G] \simeq C_2$ $(4 \leq i \leq 5)$ (see Example 1.46).

(2-5), (2-6) For $G = 8T22 \simeq (C_2)^3 \rtimes V_4$ and $G' = 8T32 \simeq ((C_2)^3 \rtimes V_4) \rtimes C_3$, we take $G = \langle g_1, g_2, g_3, g_4, g_5 \rangle$, $H = \mathrm{Stab}_1(G) = \langle g_4, g_5 \rangle \simeq V_4$, $G' = \langle g_1, g_2, g_3, g_4', g_5' \rangle$ and $H' = \mathrm{Stab}_1(G') = \langle g_5', (2,3,8)(4,7,5) \rangle \simeq A_4$ where $g_1 = (1,8)(2,3)(4,5)(6,7)$, $g_2 = (1,3)(2,8)(4,6)(5,7)$, $g_3 = (1,5)(2,6)(3,7)(4,8)$, $g_4 = (2,3)(4,5)$, $g_5 = (2,3)(6,7)$, $g_4' = (1,2,3)(4,6,5)$, $g_5' = (2,5)(3,4)$. There exist 33 subgroups $V_4 \leq G$ and 14 of them satisfy $|\mathrm{Orb}_{V_4}(i)| = 4$ $(1 \leq i \leq 8)$:

$$
\begin{aligned}
&V_4^{(1)} = \{1, \sigma_1, \sigma_3, \sigma_5\},\ V_4^{(2)} = \{1, \sigma_1, \sigma_4, \sigma_6\},\ V_4^{(3)} = \{1, \tau_1, \tau_2, \tau_5\},\ V_4^{(4)} = \{1, \tau_1, \tau_4, \sigma_5\}, \\
&V_4^{(5)} = \{1, \tau_3, \tau_2, \sigma_5\},\ V_4^{(6)} = \{1, \tau_3, \tau_4, \tau_5\},\ V_4^{(7)} = \{1, \sigma_2, \sigma_3, \sigma_6\},\ V_4^{(8)} = \{1, \sigma_2, \sigma_4, \sigma_5\}, \\
&V_4^{(9)} = \{1, \sigma_1, \sigma_2, \tau_6\},\ V_4^{(10)} = \{1, \tau_1, \tau_3, \tau_6\},\ V_4^{(11)} = \{1, \sigma_3, \sigma_4, \tau_6\}, \\
&V_4^{(12)} = \{1, \tau_2, \tau_3, \tau_6\},\ V_4^{(13)} = \{1, \sigma_5, \sigma_6, \tau_6\},\ V_4^{(14)} = \{1, \sigma_5, \tau_5, \tau_6\}
\end{aligned}
$$

where $\sigma_1 = (1,2)(3,8)(4,6)(5,7)$, $\sigma_2 = (1,3)(2,8)(4,7)(5,6)$, $\sigma_3 = (1,4)(2,6)(3,7)(5,8)$,
$\sigma_4 = (1,5)(2,7)(3,6)(4,8)$, $\sigma_5 = (1,6)(2,4)(3,5)(7,8)$, $\sigma_6 = (1,7)(2,5)(3,4)(6,8)$,
$\tau_1 = (1,2)(3,8)(4,7)(5,6)$, $\tau_2 = (1,3)(2,8)(4,6)(5,7)$ $\tau_3 = (1,4)(2,7)(3,6)(5,8)$,
$\tau_4 = (1,5)(2,6)(3,7)(4,8)$, $\tau_5 = (1,7)(2,4)(3,5)(6,8)$, $\tau_6 = (1,8)(2,3)(4,5)(6,7)$. Note that $Z(G) = \langle \tau_6 \rangle \simeq C_2$ and the first 8 groups $V_4^{(i)}$ $(1 \leq i \leq 8)$ satisfy $V_4 \cap Z(G) = 1$ as appearing

in Theorem 1.18 (Table 2) and the last 6 groups $V_4^{(i)}$ $(9 \le i \le 14)$ satisfy $V_4 \cap Z(G) \simeq C_2$. On the other hand, there exist 9 subgroups $C_4 \times C_2 \le G$:

$$G^{(1)} = \langle (1,4,8,5)(2,6,3,7), \sigma_1, \tau_6 \rangle,$$
$$G^{(2)} = \langle (1,6,8,7)(2,5,3,4), \tau_1, \tau_6 \rangle,$$
$$G^{(3)} = \langle (1,2,8,3)(4,6,5,7), \sigma_3, \tau_6 \rangle,$$
$$G^{(4)} = \langle (1,4,8,5)(2,6,3,7), (1,2,8,3)(4,6,5,7), \tau_6 \rangle,$$
$$G^{(5)} = \langle (1,2,8,3)(4,7,5,6), \tau_3, \tau_6 \rangle,$$
$$G^{(6)} = \langle (1,2,8,3)(4,7,5,6), \sigma_5, \tau_6 \rangle,$$
$$G^{(7)} = \langle (1,2,8,3)(4,6,5,7), (4,5)(6,7), \tau_6 \rangle,$$
$$G^{(8)} = \langle (1,4,8,5)(2,6,3,7), (2,3)(6,7), \tau_6 \rangle,$$
$$G^{(9)} = \langle (1,6,8,7)(2,5,3,4), (2,3)(4,5), \tau_6 \rangle.$$

The first 6 groups $G^{(i)}$ $(1 \le i \le 6)$ are transitive in $S_8$ as appearing in Theorem 1.18 (Table 2) and the last 3 groups $G^{(i)}$ $(7 \le i \le 9)$ are not transitive in $S_8$ (see Example 1.46).

(4-3) For $G = 10T32 \simeq S_6$, we take $G = \langle g_1, g_2, g_3, g_4 \rangle$ and $H = \mathrm{Stab}_1(G) = \langle g_4,$ $(3,10)(6,9)(7,8), (2,4)(3,7)\,(6,9)(8,10) \rangle \simeq (S_3)^2 \rtimes C_2$ where $g_1 = (1,2,10)(3,4,5)(6,7,8)$, $g_2 = (1,3,2,6)(4,5,8,7)$, $g_3 = (1,2)(4,7)(5,8)(9,10)$, $g_4 = (3,6)(4,7)(5,8)$. There exist 165 subgroups $V_4$ of $G$ and $45 = \binom{10}{2}$ groups $\langle (a,b)(c,d)(e,f), (a,b)(g,h)(i,j) \rangle \simeq V_4$ $(\{a,b,c,d,e,f,g,$ $h,i,j\} = \{1,2,3,4,5,6,7,8,9,10\})$ of them satisfy $N_{\widetilde{G}}(V_4) \simeq C_8 \rtimes (C_2 \times C_2)$ where $\widetilde{G} = N_{S_{10}}(G) \simeq \mathrm{Aut}(G)$ is the normalizer of $G$ in $S_{10}$ (equivalently, $|\mathrm{Orb}_{V_4}(i)| = 2$ for any $1 \le i \le 10$) as appearing in Theorem 1.18 (Table 2). There exist 180 subgroups $D_4$ of $G$ and 45 groups of them satisfy $D_4 \le [G,G] \simeq A_6$ (see Example 1.48).

Example 1.43 ($G = 4T2 \simeq V_4$ and $G = 4T4 \simeq A_4$).

Case $G = 4T2 \simeq V_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(4,2); # G=4T2=V4
E(4) = 2[x]2
gap> H:=Stabilizer(G,1); # H=1
Group(())
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [  ], [  ] ] ]
```

```
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,3), (1,2)(3,4) ]),
  epi := [ (2,3), (1,2)(3,4) ] -> [ (1,2)(3,4), (1,4)(2,3) ], Tid := [ 4, 3 ] )
gap> StructureDescription(TransitiveGroup(4,3));
"D8"
gap> tG:=ScG.SchurCover; # tG=G~=D4 is a Schur cover of G
Group([ (2,3), (1,2)(3,4) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C2
Group([ (1,4)(2,3) ])
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C2
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);
[ Group(()), Group([ (2,3) ]), Group([ (1,4) ]), Group([ (1,4)(2,3) ]),
  Group([ (1,2)(3,4) ]), Group([ (1,3)(2,4) ]), Group([ (1,4), (2,3) ]),
  Group([ (1,2)(3,4), (1,4)(2,3) ]), Group([ (1,3,4,2), (1,4)(2,3) ]),
  Group([ (1,4), (2,3), (1,2)(3,4) ]) ]
gap> List(tGs,StructureDescription);
[ "1", "C2", "C2", "C2", "C2", "C2", "C2 x C2", "C2 x C2", "C4", "D8" ]
gap> List(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]);
[ [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [ 2 ] ]
gap> List(tGs,x->StructureDescription(Image(ScG.epi,x)));
[ "1", "C2", "C2", "1", "C2", "C2", "C2", "C2", "C2", "C2 x C2" ]
```

Case $G = 4T4 \simeq A_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(4,4); # G=4T4
A4
gap> H:=Stabilizer(G,1); # H=C3
Group([ (2,3,4) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 3 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
gap> ScG:=SchurCoverG(G);
```

```
rec( SchurCover := Group([ (1,2)(3,5,7,4,6,8), (1,3,6,2,4,5)(7,8) ]),
  epi := [ (1,2)(3,5,7,4,6,8), (1,3,6,2,4,5)(7,8) ] -> [ (1,2,3), (2,3,4) ],
  Tid := [ 8, 12 ] )
gap> StructureDescription(TransitiveGroup(8,12));
"SL(2,3)"
gap> tG:=ScG.SchurCover; # tG=G~=SL(2,3) is a Schur cover of G
Group([ (1,2)(3,5,7,4,6,8), (1,3,6,2,4,5)(7,8) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C6
Group([ (1,4,6)(2,3,5), (1,2)(3,4)(5,6)(7,8) ])
gap> StructureDescription(tH);
"C6"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C2
[ [ 2 ], [ [ 6 ], [ 3 ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 6 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
15
gap> List(tGs,StructureDescription);
[ "1", "C2", "C3", "C3", "C3", "C3", "C4", "C4", "C4", "C6", "C6", "C6",
  "C6", "Q8", "SL(2,3)" ]
gap> List(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]);
[ [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ],
  [  ], [ 2 ], [ 2 ] ]
gap> List(tGs,x->StructureDescription(Image(ScG.epi,x)));
[ "1", "1", "C3", "C3", "C3", "C3", "C2", "C2", "C2", "C3",
  "C3", "C3", "C3", "C2 x C2", "A4" ]
```

EXAMPLE 1.44 ($G = 6T4 \simeq A_4$ and $G = 6T12 \simeq A_5$).

Case $G = 6T4 \simeq A_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(6,4); # G=6T4=A4
A_4(6) = [2^2]3
gap> H:=Stabilizer(G,1); # H=C2
Group([ (2,5)(3,6) ])
gap> FirstObstructionN(G).ker; # Obs1N=C2
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
```

```
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
10
gap> List(Gs,StructureDescription);
[ "1", "C2", "C2", "C2", "C3", "C3", "C3", "C3", "C2 x C2", "A4" ]
gap> List(Gs,x->FirstObstructionDr(G,x).Dr[1]);
[ [  ], [  ], [  ], [  ], [  ], [  ], [  ], [  ], [ 2 ], [ 2 ] ]
```

Case $G = 6T12 \simeq A_5$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(6,12); # G=6T12=A5
L(6) = PSL(2,5) = A_5(6)
gap> H:=Stabilizer(G,1); # H=D5
Group([ (2,4,3,6,5), (3,6)(4,5) ])
gap> StructureDescription(H);
"D10"
gap> FirstObstructionN(G).ker; # Obs1N=C2
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
59
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[]);;
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[2]);;
gap> List([GsHNPfalse,GsHNPtrue],Length);
[ 48, 11 ]                                                    ^
gap> Collected(List(GsHNPfalse,x->StructureDescription(x)));
[ [ "1", 1 ], [ "C2", 15 ], [ "C3", 10 ], [ "C5", 6 ], [ "D10", 6 ],
  [ "S3", 10 ] ]
gap> Collected(List(GsHNPtrue,x->StructureDescription(x)));
[ [ "A4", 5 ], [ "A5", 1 ], [ "C2 x C2", 5 ] ]
```

EXAMPLE 1.45 ($G = 8Tm$ ($m = 2, 3, 4, 13, 14, 21, 31, 37, 38$)).

(1-1) $G = 8T3 \simeq (C_2)^3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,3); # G=8T3=C2xC2xC2
E(8)=2[x]2[x]2
gap> H:=Stabilizer(G,1); # H=1
Group(())
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [  ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2xC2: Schur multiplier of G
[ 2, 2, 2 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,3)(4,6)(9,10)(11,13)(12,15)(14,16), (1,2)(3,5)
  (4,7)(6,8)(10,11)(12,14), (2,4)(3,6)(10,12)(11,14) ]),
  epi := [ (2,3)(4,6)(9,10)(11,13)(12,15)(14,16),
      (1,2)(3,5)(4,7)(6,8)(10,11)(12,14), (2,4)(3,6)(10,12)(11,14) ] ->
    [ (1,5)(2,6)(3,7)(4,8), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ] )
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (2,3)(4,6)(9,10)(11,13)(12,15)(14,16), (1,2)(3,5)(4,7)(6,8)(10,11)
(12,14), (2,4)(3,6)(10,12)(11,14) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C2xC2xC2
Group([ (1,5)(2,3)(4,6)(7,8)(9,13)(10,11)(12,14)(15,16), (9,15)(10,12)(11,14)
(13,16), (1,7)(2,4)(3,6)(5,8) ])
gap> IdSmallGroup(tG);
[ 64, 73 ]
gap> StructureDescription(tG);
"(C2 x C2 x D8) : C2"
gap> StructureDescription(tH);
"C2 x C2 x C2"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C2xC2xC2
[ [ 2, 2, 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 2, 2, 2 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
317
gap> Collected(List(tGs,x->FirstObstructionDr(tG,x,tH).Dr));
[ [ [ [  ], [ [ 2, 2, 2 ], [  ] ] ], 213 ],
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 0, 1 ] ] ] ], 29 ],
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 1, 0 ] ] ] ], 29 ],
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 1, 1 ] ] ] ], 5 ],
```

```
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 0 ] ] ] ], 29 ],
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 1 ] ] ] ], 5 ],
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 1, 0 ] ] ] ], 5 ],
  [ [ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 1, 1 ] ] ] ], 1 ],
  [ [ [ 2, 2, 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 0 ],
  [ 0, 1, 0 ], [ 0, 0, 1 ] ] ] ], 1 ] ]
gap> tGsHNPfalse0:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> Length(tGsHNPfalse0);
213
gap> tGsHNPtrue0:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[2,2,2]);;
gap> Length(tGsHNPtrue0);
1
gap> Collected(List(tGsHNPfalse0,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 16 ], [ "C2", 197 ] ]
gap> Collected(List(tGsHNPtrue0,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C2 x C2 x C2", 1 ] ]
```

(1-2) $G = 8T21 \simeq (C_2)^3 \rtimes C_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,21); # G=8T21=(C2xC2xC2):C4
1/2[2^4]E(4)=[1/4.dD(4)^2]2
gap> H:=Stabilizer(G,1); # H=C2xC2
Group([ (2,6)(4,8), (3,7)(4,8) ])
gap> FirstObstructionN(G).ker; # Obs1N=C2
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 0 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=1 => Obs=Obs1=C2 if unramified
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> KerResH3Z(G,H); # Obs=Obs1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
50
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x,H).Dr[1]=[]);;
gap> Length(GsHNPfalse);
49
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x,H).Dr[1]=[2]);;
gap> Length(GsHNPtrue);
1
```

```
gap> Collected(List(GsHNPfalse,StructureDescription));
[ [ "(C4 x C2) : C2", 2 ], [ "1", 1 ], [ "C2", 11 ], [ "C2 x C2", 13 ],
  [ "C2 x C2 x C2", 2 ], [ "C2 x D8", 1 ], [ "C4", 10 ], [ "C4 x C2", 5 ],
  [ "D8", 4 ] ]
gap> Collected(List(GsHNPtrue,StructureDescription));
[ [ "(C2 x C2 x C2) : C4", 1 ] ]
```

(1-3-1) $G = 8T2 \simeq C_4 \times C_2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,2); # G=8T2=C4xC2
4[x]2
gap> H:=Stabilizer(G,1); # H=1
Group(())
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [  ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,4)(3,6), (1,2,5,3)(4,7,6,8) ]),
  Tid := [ 8, 10 ], epi := [ (2,4)(3,6), (1,2,5,3)(4,7,6,8) ] ->
    [ (1,5)(2,6)(3,7)(4,8), (1,2,3,8)(4,5,6,7) ] )
gap> tG:=ScG.SchurCover; # tG=G~=(C4xC2):C2 is a Schur cover of G
Group([ (2,4)(3,6), (1,2,5,3)(4,7,6,8) ])
gap> StructureDescription(TransitiveGroup(8,10));
"(C4 x C2) : C2"
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C2
Group([ (1,8)(2,4)(3,6)(5,7) ])
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C2
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
23
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> Length(tGsHNPfalse);
22
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[2]);;
```

```
gap> Length(tGsHNPtrue);
1
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 9 ], [ "C2 x C2", 5 ], [ "C4", 6 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C4 x C2", 1 ] ]
```

(1-3-2) $G = 8T4 \simeq D_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,4); # G=8T4=D4
D_8(8)=[4]2
gap> H:=Stabilizer(G,1); # H=1
Group(())
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [  ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,3)(4,5)(6,7), (1,2,4,6,8,7,5,3) ]),
  Tid := [ 8, 6 ], epi := [ (2,3)(4,5)(6,7), (1,2,4,6,8,7,5,3) ] ->
    [ (1,6)(2,5)(3,4)(7,8), (1,2,3,8)(4,5,6,7) ] )
gap> tG:=ScG.SchurCover; # tG=G~=D8 is a Schur cover of G
Group([ (2,3)(4,5)(6,7), (1,2,4,6,8,7,5,3) ])
gap> StructureDescription(tG);
"D16"
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C2
Group([ (1,8)(2,7)(3,6)(4,5) ])
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C2
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
19
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> Length(tGsHNPfalse);
16
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[2]);;
```

```
gap> Length(tGsHNPtrue);
3
gap> Collected(List(tGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C2", 9 ], [ "C2 x C2", 4 ], [ "C4", 1 ], [ "C8", 1 ] ]
gap> Collected(List(tGsHNPtrue,StructureDescription));
[ [ "D16", 1 ], [ "D8", 2 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 13 ], [ "C4", 1 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C2 x C2", 2 ], [ "D8", 1 ] ]
```

(1-3-3) $G = 8T13 \simeq A_4 \times C_2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,13); # G=8T13=A4xC2
E(8):3=A(4)[x]2
gap> H:=Stabilizer(G,1); # H=C3
Group([ (2,3,8)(4,7,5) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 3 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (1,2,3)(4,6,7)(5,8,9)(10,14,15)(11,16,17)(12,18,19)
(13,20,21)(22,23,24), (2,4)(3,5)(6,10)(7,11)(8,12)(9,13)(15,18)(16,22)(17,20)
(19,23) ]), Tid := [ 24, 21 ],  epi := [ (1,2,3)(4,6,7)(5,8,9)(10,14,15)
(11,16,17)(12,18,19)(13,20,21)(22,23,24), (2,4)(3,5)(6,10)(7,11)(8,12)(9,13)
(15,18)(16,22)(17,20)(19,23) ] -> [ (2,8,3)(4,5,7), (1,5)(2,6)(3,7)(4,8) ] )
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (1,2,3)(4,6,7)(5,8,9)(10,14,15)(11,16,17)(12,18,19)(13,20,21)(22,23,24),
(2,4)(3,5)(6,10)(7,11)(8,12)(9,13)(15,18)(16,22)(17,20)(19,23) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C6
Group([ (1,3,2)(4,7,6)(5,9,8)(10,15,14)(11,17,16)(12,19,18)(13,21,20)(22,24,23),
(1,24)(2,22)(3,23)(4,16)(5,19)(6,17)(7,11)(8,12)(9,18)(10,20)(13,15)(14,21) ])
gap> StructureDescription(TransitiveGroup(24,21));
"((C4 x C2) : C2) : C3"
gap> StructureDescription(tH);
"C6"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C2
```

```
[ [ 2 ], [ [ 6 ], [ [ 3 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 6 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
37
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> Length(tGsHNPfalse);
30
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[2]);;
gap> Length(tGsHNPtrue);
7
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 13 ], [ "C2 x C2", 3 ], [ "C3", 8 ], [ "C6", 4 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "A4", 1 ], [ "C2 x A4", 1 ], [ "C2 x C2", 4 ], [ "C2 x C2 x C2", 1 ] ]
gap> pi:=NaturalHomomorphismByNormalSubgroup(G,Centre(G));
[ (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8),
(1,2,3)(4,6,5) ] -> [ f3, f2, f2*f3, f1*f2*f3 ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(pi,Image(ScG.epi,x)))));
[ [ "A4", 2 ], [ "C2 x C2", 5 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(pi,Image(ScG.epi,x)))));
[ [ "1", 3 ], [ "C2", 15 ], [ "C3", 12 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(pi,Image(ScG.epi,x)))));
[ [ "A4", 2 ], [ "C2 x C2", 5 ] ]
```

(1-3-4) $G = 8T14 \simeq S_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,14); # G=8T14=S4
S(4)[1/2]2=1/2(S_4[x]2)
gap> H:=Stabilizer(G,1); # H=C3
Group([ (2,8,3)(4,7,6) ])
gap> FirstObstructionN(G).ker; # Obs1N=C3
[ [ 3 ], [ [ 3 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Osb1Dr=C3
[ [ 3 ], [ [ 3 ], [ [ 1 ] ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
```

```
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,4)(3,6)(5,8), (1,2,5,7,4,3)(6,8) ]), Tid := [ 8, 23 ],
  epi := [ (2,4)(3,6)(5,8), (1,2,5,7,4,3)(6,8) ] ->
    [ (1,4)(2,6)(3,7)(5,8), (2,8,3)(4,7,6) ] )
gap> tG:=ScG.SchurCover; # tG=G~=SL(2,3) is a Schur cover of G
Group([ (2,4)(3,6)(5,8), (1,2,5,7,4,3)(6,8) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C6
Group([ (1,4,5)(2,3,7), (1,7)(2,4)(3,5)(6,8) ])
gap> StructureDescription(tG);
"GL(2,3)"
gap> StructureDescription(tH);
"C6"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C6
[ [ 6 ], [ [ 6 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=C3
[ [ 3 ], [ [ 6 ], [ [ 2 ] ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
55
gap> tGsHNPfalse1:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPfalse2:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> tGsHNPtrue1:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[2]);;
gap> tGsHNPtrue2:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[6]);;
gap> List([tGsHNPfalse1,tGsHNPfalse2,tGsHNPtrue1,tGsHNPtrue2],Length);
[ 26, 20, 7, 2 ]
gap> Sum(last);
55
gap> Collected(List(tGsHNPfalse1,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 21 ], [ "C4", 3 ] ]
gap> Collected(List(tGsHNPfalse2,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C3", 8 ], [ "S3", 12 ] ]
gap> Collected(List(tGsHNPtrue1,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C2 x C2", 4 ], [ "D8", 3 ] ]
gap> Collected(List(tGsHNPtrue2,x->StructureDescription(Image(ScG.epi,x))));
[ [ "A4", 1 ], [ "S4", 1 ] ]
```

(1-3-5) $G = 8T37 \simeq \mathrm{PSL}_3(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$.

```
gap> Read("HNP.gap");
```

```
gap> G:=TransitiveGroup(8,37); # G=8T37=PSL(3,2)=PSL(2,7)
L(8)=PSL(2,7)
gap> H:=Stabilizer(G,1); # H=C7:C3
Group([ (2,3,6)(5,8,7), (3,7,8)(4,5,6) ])
gap> StructureDescription(H);
"C7 : C3"
gap> FirstObstructionN(G).ker; # Obs1N=C3
[ [ 3 ], [ [ 3 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=C3
[ [ 3 ], [ [ 3 ], [ [ 1 ] ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2: Schur multiplier of G
[ 2 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (1,2,4,8)(3,6,9,12)(5,10,14,11)(7,13,15,16),
   (1,3,7,4,9,15)(2,5,11,8,14,10)(6,12)(13,16) ]), Tid := [ 16, 715 ],
  epi := [ (1,2,4,8)(3,6,9,12)(5,10,14,11)(7,13,15,16),
      (1,3,7,4,9,15)(2,5,11,8,14,10)(6,12)(13,16) ] ->
    [ (1,2)(3,5)(4,7)(6,8), (2,6,7)(3,5,4) ] )
gap> tG:=ScG.SchurCover; # tG=G=SL(2,7) is a Schur cover of G
Group([ (1,2,4,8)(3,6,9,12)(5,10,14,11)(7,13,15,16), (1,3,7,4,9,15)
(2,5,11,8,14,10)(6,12)(13,16) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C2x(C7:C3)
Group([ (1,11,16)(3,5,15)(4,10,13)(7,9,14), (1,13,14,4,16,5)(2,10,7,8,11,15)
(3,9)(6,12) ])
gap> StructureDescription(tG);
"SL(2,7)"
gap> StructureDescription(tH);
"C2 x (C7 : C3)"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C6
[ [ 6 ], [ [ 6 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=C3
[ [ 3 ], [ [ 6 ], [ [ 2 ] ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
224
gap> tGsHNPfalse1:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPfalse2:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> tGsHNPtrue1:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[2]);;
gap> tGsHNPtrue2:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[6]);;
```

```
gap> List([tGsHNPfalse1,tGsHNPfalse2,tGsHNPtrue1,tGsHNPtrue2],Length);
[ 60, 100, 35, 29 ]
gap> Sum(last);
224
gap> Collected(List(tGsHNPfalse1,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 21 ], [ "C4", 21 ], [ "C7", 16 ] ]
gap> Collected(List(tGsHNPfalse2,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C3", 56 ], [ "C7 : C3", 16 ], [ "S3", 28 ] ]
gap> Collected(List(tGsHNPtrue1,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C2 x C2", 14 ], [ "D8", 21 ] ]
gap> Collected(List(tGsHNPtrue2,x->StructureDescription(Image(ScG.epi,x))));
[ [ "A4", 14 ], [ "PSL(3,2)", 1 ], [ "S4", 14 ] ]
```

(1-4-1) $G = 8T31 \simeq ((C_2)^4 \rtimes C_2) \rtimes C_2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,31); # G=8T31=(C2^4:C2):C2
[2^4]E(4)
gap> GeneratorsOfGroup(G);
[ (4,8), (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7) ]
gap> H:=Stabilizer(G,1); # H=C2xC2xC2
Group([ (4,8), (2,6), (3,7) ])
gap> FirstObstructionN(G).ker; # Obs1N=C2xC2
[ [ 2, 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 1 ], [ 0, 1, 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=C2xC2
[ [ 2, 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 1 ], [ 0, 1, 1 ] ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2xC2: Schur multiplier of G
[ 2, 2, 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 15 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> od;
[ [  ], [ [ 2, 2, 2, 2, 2 ], [  ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 1, 0 ] ] ] ]
```

```
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 1, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 4 ], [ [ 0, 0, 2 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 1, 1, 1 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 2, 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
[ 2, 2 ][ 2, 2 ]
gap> cG:=cGs[1];;
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
<permutation group of size 128 with 7 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-
<permutation group of size 16 with 4 generators>
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2xC2xC2
[ [ 2, 2, 2 ],
```

```
  [ [ 2, 2, 2, 2 ], [ [ 1, 0, 1, 0 ], [ 0, 1, 1, 0 ], [ 0, 0, 0, 1 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=C2xC2
[ [ 2, 2 ], [ [ 2, 2, 2, 2 ], [ [ 1, 0, 1, 0 ], [ 0, 1, 1, 0 ] ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
896
gap> bGsHNPfalse:=Filtered(bGs,x->Filtered(FirstObstructionDr(bG,x,bH).Dr[2][2],
> y->y[4]=1)=[]);;
gap> Length(bGsHNPfalse);
855
gap> bGsHNPtrue:=Filtered(bGs,x->Filtered(FirstObstructionDr(bG,x,bH).Dr[2][2],
> y->y[4]=1)<>[]);;
gap> Length(bGsHNPtrue);
41
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C2 x C2 x C2 x C2) : C2", 19 ], [ "(C4 x C2) : C2", 45 ], [ "1", 2 ],
  [ "C2", 73 ], [ "C2 x C2", 241 ], [ "C2 x C2 x C2", 154 ],
  [ "C2 x C2 x C2 x C2", 17 ], [ "C2 x D8", 57 ], [ "C4", 54 ],
  [ "C4 x C2", 45 ], [ "D8", 146 ], [ "Q8", 2 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "((C2 x C2 x C2 x C2) : C2) : C2", 1 ],
  [ "(C2 x C2 x C2) : (C2 x C2)", 1 ], [ "(C2 x C2 x C2) : C4", 11 ],
  [ "(C4 x C2) : C2", 6 ], [ "C2 x C2", 8 ], [ "C2 x C2 x C2", 2 ],
  [ "C2 x D8", 6 ], [ "C4 x C2", 6 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
192
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
33
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (), (1,5)(2,6), (2,6)(4,8), (2,6)(3,7), (1,6)(2,5)(3,8)(4,7), (1,3)
  (2,8,6,4)(5,7) ]), Group([ (), (1,5)(2,6), (2,6)(4,8), (2,6)(3,7), (1,3)
  (2,8)(4,6)(5,7), (1,8,5,4)(2,3)(6,7) ]), Group([ (), (1,5)(2,6), (2,6)
  (4,8), (2,6)(3,7), (1,8,5,4)(2,3,6,7), (1,3)(2,8,6,4)(5,7) ]), Group([ (1,3)
  (2,4)(5,7)(6,8), (), (1,4)(2,3)(5,8)(6,7) ]), Group([ (1,7,5,3)
```

```
  (2,8,6,4), (), (1,8,5,4)(2,7,6,3), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7)
  (2,8)(3,5)(4,6), (), (1,8)(2,7)(3,6)(4,5) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,7,5,3)(2,4,6,8), (), (1,8,5,
   4)(2,3,6,7), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7)(2,4)(3,5)
  (6,8), (), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (), (1,8,
   5,4)(2,3,6,7), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7,5,3)(2,8,6,4), (), (1,
   4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (), (1,8,5,4)(2,7,6,3), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7,5,3)
  (2,4,6,8), (), (1,4)(2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)
  (2,4)(5,7)(6,8), (), (1,8)(2,7)(3,6)(4,5) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,7)(2,8)(3,5)(4,6), (), (1,4)
  (2,3)(5,8)(6,7) ]), Group([ (1,7)(2,4)(3,5)(6,8), (), (1,8)(2,3)(4,5)
  (6,7) ]) ]
gap> Length(GsHNPtrueMin);
17
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 32, 6 ], [ 32, 6 ], [ 32, 6 ], [ 4, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ],
  [ 8, 2 ], [ 4, 2 ], [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 4, 2 ],
  [ 4, 2 ], [ 4, 2 ], [ 4, 2 ] ]
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 192 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
225
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsC2xC2);
61
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
15
gap> Gs32_6:=Filtered(Gs,x->IdSmallGroup(x)=[32,6]);;
gap> Length(Gs32_6);
3
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (3,7)(4,8), (3,7) ]), Group([ (2,6)(4,8), (2,6)(4,8), (2,6) ]),
  Group([ (2,6)(3,7), (2,6)(3,7)(4,8) ]), Group([ (1,5)(4,8), (1,5)
  (4,8), (4,8) ]), Group([ (1,5)(3,7), (4,8) ]), Group([ (1,5)(2,6)
  (4,8), (1,5)(2,6) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)
  (4,8), (4,8) ]), Group([ (2,6)(3,7), (2,6)(3,7), (2,6) ]), Group([ (2,6)
```

```
  (4,8), (2,6)(4,8), (3,7) ]), Group([ (1,5)(3,7), (1,5)(3,7), (3,7) ]),
  Group([ (3,7), (1,5)(4,8) ]), Group([ (1,5)(2,6), (3,7) ]), Group([ (1,5)
  (2,6)(3,7)(4,8), (1,5)(2,6)(3,7)(4,8), (3,7) ]), Group([ (3,7)
  (4,8), (2,6) ]), Group([ (3,7)(4,8), (2,6)(3,7) ]), Group([ (1,2)(3,4)(5,6)
  (7,8), (3,7)(4,8), (3,7)(4,8) ]), Group([ (3,7)(4,8), (1,5) ]),
  Group([ (1,5)(4,8), (1,5)(4,8), (3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8), (3,7)(4,8) ]), Group([ (1,5)(2,6)(4,8), (3,7)
  (4,8) ]), Group([ (1,6)(2,5)(3,8)(4,7), (3,7)(4,8), (3,7)(4,8) ]),
  Group([ (1,5)(2,6), (1,5) ]), Group([ (1,5)(4,8), (2,6) ]), Group([ (1,5)
  (3,7), (1,5)(3,7), (2,6) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)
  (4,8), (2,6) ]), Group([ (1,3)(2,8)(4,6)(5,7), (2,6)(4,8), (2,6)(4,8) ]),
  Group([ (2,6)(4,8), (2,6)(4,8), (1,5) ]), Group([ (1,5)(4,8), (1,5)
  (4,8), (1,5)(2,6) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)
  (4,8), (2,6)(4,8) ]), Group([ (2,6)(4,8), (2,6)(4,8), (1,5)(2,6)(3,7) ]),
  Group([ (1,7)(2,4)(3,5)(6,8), (2,6)(4,8) ]), Group([ (2,6)(3,7), (1,4)(2,3)
  (5,8)(6,7) ]), Group([ (2,6)(3,7), (2,6)(3,7), (1,5) ]), Group([ (1,5)(2,6)
  (3,7)(4,8), (1,5)(4,8), (2,6)(3,7) ]), Group([ (2,6)(3,7), (2,6)(3,7), (1,5)
  (2,6) ]), Group([ (2,6)(3,7), (2,6)(3,7), (1,5)(2,6)(4,8) ]), Group([ (1,8)
  (2,3)(4,5)(6,7), (2,6)(3,7) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)
  (3,7)(4,8), (1,5) ]), Group([ (1,5)(4,8), (1,5)(4,8), (2,6)(3,7)(4,8) ]),
  Group([ (1,5)(3,7), (1,5)(3,7), (2,6)(3,7)(4,8) ]), Group([ (1,5)
  (2,6), (1,5)(2,6), (2,6)(3,7)(4,8) ]), Group([ (1,2)(3,4)(5,6)(7,8), (1,5)
  (2,6), (1,5)(2,6) ]), Group([ (1,6)(2,5)(3,8)(4,7), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,6)(2,5)(3,8)(4,7), (1,5)
  (2,6), (1,5)(2,6) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,5)
  (3,7), (1,5)(3,7) ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,5)
  (3,7), (1,5)(3,7) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,8)(2,3)(4,5)(6,7), (1,5)
  (4,8) ]), Group([ (1,8)(2,7)(3,6)(4,5), (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,5)(4,8), (1,4)(2,7)(3,6)(5,8), (1,5)(4,8) ]), Group([ (1,5)(2,6)
  (3,7)(4,8), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8) ]) ]
gap> Length(GsHNPfalseC2xC2);
53
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,3)(2,4)(5,7)(6,8), (), (1,4)(2,3)(5,8)(6,7) ]), Group([ (1,7)
  (2,8)(3,5)(4,6), (), (1,8)(2,7)(3,6)(4,5) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,7)(2,4)(3,5)(6,8), (), (1,4)
```

```
  (2,7)(3,6)(5,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (), (1,8)(2,7)(3,6)
  (4,5) ]), Group([ (1,3)(2,8)(4,6)(5,7), (), (1,4)(2,7)(3,6)(5,8) ]),
  Group([ (1,7)(2,8)(3,5)(4,6), (), (1,4)(2,3)(5,8)(6,7) ]), Group([ (1,7)
  (2,4)(3,5)(6,8), (), (1,8)(2,3)(4,5)(6,7) ]) ]
gap> Length(GsHNPtrueC2xC2);
8
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2 ], 6 ], [ [ 2, 2, 2 ], 16 ], [ [ 2, 2, 2, 2 ], 13 ],
  [ [ 2, 2, 4 ], 1 ], [ [ 2, 4, 2 ], 5 ], [ [ 4, 2, 2 ], 6 ], [ [ 4, 4 ], 6 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 8 ] ]
gap> GsHNPfalse44C2xC2:=Filtered(GsHNPfalseC2xC2,
> x->List(Orbits(x,[1..8]),Length)=[4,4]);
[ Group([ (1,6)(2,5)(3,8)(4,7), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)
  (4,8) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)
  (3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,8)(2,7)(3,6)(4,5), (1,5)(2,6)
  (3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,4)(2,7)(3,6)(5,8), (1,5)
  (2,6)(3,7)(4,8) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (1,2)(3,4)(5,6)(7,8), (1,3)(2,4)(5,7)(6,8), (1,4)(2,3)(5,8)(6,7) ],
  [ (), (1,2)(3,4)(5,6)(7,8), (1,7)(2,8)(3,5)(4,6), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,3)(2,4)(5,7)(6,8), (1,6)(2,5)(3,8)(4,7), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,6)(2,5)(3,8)(4,7), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (4,8), (3,7), (3,7)(4,8) ], [ (), (4,8), (2,6), (2,6)(4,8) ],
  [ (), (4,8), (2,6)(3,7), (2,6)(3,7)(4,8) ], [ (), (4,8), (1,5), (1,5)(4,8) ],
  [ (), (4,8), (1,5)(3,7), (1,5)(3,7)(4,8) ],
  [ (), (4,8), (1,5)(2,6), (1,5)(2,6)(4,8) ],
  [ (), (4,8), (1,5)(2,6)(3,7), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (3,7), (2,6), (2,6)(3,7) ],
  [ (), (3,7), (2,6)(4,8), (2,6)(3,7)(4,8) ],
  [ (), (3,7), (1,5), (1,5)(3,7) ],
  [ (), (3,7), (1,5)(4,8), (1,5)(3,7)(4,8) ],
```

[ (), (3,7), (1,5)(2,6), (1,5)(2,6)(3,7) ],
[ (), (3,7), (1,5)(2,6)(4,8), (1,5)(2,6)(3,7)(4,8) ],
[ (), (3,7)(4,8), (2,6), (2,6)(3,7)(4,8) ],
[ (), (3,7)(4,8), (2,6)(4,8), (2,6)(3,7) ],
[ (), (3,7)(4,8), (1,2)(3,4)(5,6)(7,8), (1,2)(3,8)(4,7)(5,6) ],
[ (), (3,7)(4,8), (1,5), (1,5)(3,7)(4,8) ],
[ (), (3,7)(4,8), (1,5)(4,8), (1,5)(3,7) ],
[ (), (3,7)(4,8), (1,5)(2,6), (1,5)(2,6)(3,7)(4,8) ],
[ (), (3,7)(4,8), (1,5)(2,6)(4,8), (1,5)(2,6)(3,7) ],
[ (), (3,7)(4,8), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,8)(4,7) ],
[ (), (2,6), (1,5), (1,5)(2,6) ],
[ (), (2,6), (1,5)(4,8), (1,5)(2,6)(4,8) ],
[ (), (2,6), (1,5)(3,7), (1,5)(2,6)(3,7) ],
[ (), (2,6), (1,5)(3,7)(4,8), (1,5)(2,6)(3,7)(4,8) ],
[ (), (2,6)(4,8), (1,3)(2,4)(5,7)(6,8), (1,3)(2,8)(4,6)(5,7) ],
[ (), (2,6)(4,8), (1,5), (1,5)(2,6)(4,8) ],
[ (), (2,6)(4,8), (1,5)(4,8), (1,5)(2,6) ],
[ (), (2,6)(4,8), (1,5)(3,7), (1,5)(2,6)(3,7)(4,8) ],
[ (), (2,6)(4,8), (1,5)(3,7)(4,8), (1,5)(2,6)(3,7) ],
[ (), (2,6)(4,8), (1,7)(2,4)(3,5)(6,8), (1,7)(2,8)(3,5)(4,6) ],
[ (), (2,6)(3,7), (1,4)(2,3)(5,8)(6,7), (1,4)(2,7)(3,6)(5,8) ],
[ (), (2,6)(3,7), (1,5), (1,5)(2,6)(3,7) ],
[ (), (2,6)(3,7), (1,5)(4,8), (1,5)(2,6)(3,7)(4,8) ],
[ (), (2,6)(3,7), (1,5)(3,7), (1,5)(2,6) ],
[ (), (2,6)(3,7), (1,5)(3,7)(4,8), (1,5)(2,6)(4,8) ],
[ (), (2,6)(3,7), (1,8)(2,3)(4,5)(6,7), (1,8)(2,7)(3,6)(4,5) ],
[ (), (2,6)(3,7)(4,8), (1,5), (1,5)(2,6)(3,7)(4,8) ],
[ (), (2,6)(3,7)(4,8), (1,5)(4,8), (1,5)(2,6)(3,7) ],
[ (), (2,6)(3,7)(4,8), (1,5)(3,7), (1,5)(2,6)(4,8) ],
[ (), (2,6)(3,7)(4,8), (1,5)(3,7)(4,8), (1,5)(2,6) ],
[ (), (1,2)(3,4)(5,6)(7,8), (1,5)(2,6), (1,6)(2,5)(3,4)(7,8) ],
[ (), (1,2)(3,4)(5,6)(7,8), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,8)(4,7) ],
[ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6), (1,6)(2,5)(3,8)(4,7) ],
[ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
[ (), (1,3)(2,4)(5,7)(6,8), (1,5)(3,7), (1,7)(2,4)(3,5)(6,8) ],
[ (), (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8), (1,7)(2,8)(3,5)(4,6) ],
[ (), (1,3)(2,8)(4,6)(5,7), (1,5)(3,7), (1,7)(2,8)(3,5)(4,6) ],
[ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ],
[ (), (1,4)(2,3)(5,8)(6,7), (1,5)(4,8), (1,8)(2,3)(4,5)(6,7) ],

```
  [ (), (1,4)(2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(4,8), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalse44C2xC2,Elements);
[ [ (), (1,2)(3,4)(5,6)(7,8), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,8)(4,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> ZG:=Centre(G);
Group([ (1,5)(2,6)(3,7)(4,8) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,ZG));
[ Group(()), Group(()), Group(()), Group(()), Group(()), Group(()),
  Group(()), Group(()) ]
gap> List(GsHNPfalse44C2xC2,x->Intersection(x,ZG));
[ Group([ (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8) ]) ]
gap> DG:=DerivedSubgroup(G);
Group([ (1,5)(4,8), (2,6)(4,8), (3,7)(4,8) ])
gap> StructureDescription(DG);
"C2 x C2 x C2"
gap> Collected(List(GsHNPfalseC2xC2,x->Order(Intersection(DG,x))));
[ [ 2, 46 ], [ 4, 7 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->Order(Intersection(DG,x))));
[ [ 1, 8 ] ]
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,2)(3,4,7,8)(5,6), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6) ]), Group([ (1,2,5,6)(3,8)(4,7), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8), (3,7)(4,8) ]), Group([ (1,2,5,6)
  (3,8,7,4), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)(4,8), (3,7)(4,8) ]),
  Group([ (1,3)(2,8,6,4)(5,7), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)
  (4,8), (2,6)(4,8) ]), Group([ (1,3,5,7)(2,4)(6,8), (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8), (1,5)(3,7) ]), Group([ (1,7,5,3)
  (2,8,6,4), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)(4,8), (2,6)(4,8) ]),
  Group([ (1,5)(2,6)(3,7)(4,8), (1,8,5,4)(2,3)(6,7), (1,5)(4,8), (2,6)
  (3,7) ]), Group([ (1,4)(2,7,6,3)(5,8), (1,5)(4,8), (2,6)(3,7) ]),
  Group([ (1,5)(4,8), (1,8,5,4)(2,3,6,7), (1,5)(2,6)(3,7)(4,8) ]) ]
```

```
gap> Length(GsHNPfalseC4xC2);
9
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,7,5,3)(2,8,6,4), (), (1,8,5,4)(2,7,6,3), (1,5)(2,6)(3,7)
  (4,8) ]), Group([ (1,7,5,3)(2,4,6,8), (), (1,8,5,4)(2,3,6,7), (1,5)(2,6)
  (3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (), (1,8,5,4)(2,3,6,7), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (1,7,5,3)(2,8,6,4), (), (1,4)(2,7)(3,6)
  (5,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (), (1,8,5,4)
  (2,7,6,3), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7,5,3)(2,4,6,8), (), (1,4)
  (2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8) ]) ]
gap> Length(GsHNPtrueC4xC2);
6
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 9 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
[ [ [ 8 ], 6 ] ]
gap> Collected(List(GsHNPfalseC4xC2,x->Order(Intersection(DG,x))));
[ [ 4, 9 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->Order(Intersection(DG,x))));
[ [ 2, 6 ] ]
```

(1-4-2) $G = 8T38 \simeq (((C_2)^4 \rtimes C_2) \rtimes C_2) \rtimes C_3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,38); # G=8T38=((C2^4:C2):C2):C3
[2^4]A(4)
gap> GeneratorsOfGroup(G);
[ (4,8), (1,8)(2,3)(4,5)(6,7), (1,2,3)(5,6,7) ]
gap> H:=Stabilizer(G,1); # H=C2xA4
Group([ (4,8), (2,6), (2,8,3)(4,7,6) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 6 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2: Schur multiplier of G
[ 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 3 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
```

```
> Print("\n");
> od;
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
[ [  ], [ [ 2, 2 ], [  ] ] ]
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[  ][  ]
[ 2 ][  ]
[  ][  ]
gap> cG:=cGs[2];;
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
<permutation group of size 384 with 8 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-
<permutation group of size 48 with 3 generators>
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 2, 6 ], [ [ 1, 0 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 2, 6 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
1002
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
951
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
51
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C2 x C2 x C2 x C2) : C2", 3 ], [ "(C4 x C2) : C2", 45 ], [ "1", 2 ],
  [ "A4", 8 ], [ "C2", 57 ], [ "C2 x A4", 36 ], [ "C2 x C2", 193 ],
  [ "C2 x C2 x A4", 20 ], [ "C2 x C2 x C2", 138 ],
  [ "C2 x C2 x C2 x C2", 17 ], [ "C2 x D8", 9 ], [ "C3", 32 ], [ "C4", 54 ],
  [ "C4 x C2", 45 ], [ "C6", 144 ], [ "C6 x C2", 80 ], [ "D8", 42 ],
```

```
  [ "Q8", 10 ], [ "SL(2,3)", 16 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "(((C2 x C2 x C2 x C2) : C2) : C2) : C3", 1 ],
  [ "((C2 x C2 x C2 x C2) : C2) : C2", 1 ],
  [ "((C2 x C2 x C2) : (C2 x C2)) : C3", 1 ],
  [ "(C2 x C2 x C2) : (C2 x C2)", 1 ], [ "(C2 x C2 x C2) : C4", 3 ],
  [ "(C4 x C2) : C2", 6 ], [ "A4", 8 ], [ "C2 x A4", 8 ], [ "C2 x C2", 8 ],
  [ "C2 x C2 x C2", 2 ], [ "C2 x D8", 6 ], [ "C4 x C2", 6 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
300
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
51
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (1,2)(3,4)(5,6)(7,8), (1,3)(2,8,6,4)(5,7), (), (2,6)(4,8), (1,5)
  (3,7), (1,5)(4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,8,5,4)(2,3)
  (6,7), (), (1,5)(4,8), (2,6)(3,7), (3,7)(4,8) ]), Group([ (1,4)(2,3)(5,8)
  (6,7), (1,2)(3,8,7,4)(5,6), (), (3,7)(4,8), (1,5)(2,6), (2,6)(4,8) ]),
  Group([ (1,3)(2,4)(5,7)(6,8), (1,4)(2,3)(5,8)(6,7), () ]), Group([ (1,2)
  (3,4)(5,6)(7,8), (1,7,5,3)(2,8,6,4), (), (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,7)(2,8)(3,5)(4,6), (1,8)(2,7)(3,6)(4,5), () ]), Group([ (1,3)
  (2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7), () ]), Group([ (1,2)(3,8)(4,7)
  (5,6), (1,7,5,3)(2,4,6,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7)(2,4)
  (3,5)(6,8), (1,4)(2,7)(3,6)(5,8), () ]), Group([ (1,3)(2,4)(5,7)
  (6,8), (1,8,5,4)(2,3,6,7), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,8)(2,3)
  (4,5)(6,7), (1,2,5,6)(3,4,7,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)
  (2,8)(4,6)(5,7), (1,4,5,8)(2,3,6,7), (), (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,4)(2,3)(5,8)(6,7), (1,2,5,6)(3,8,7,4), (), (1,5)(2,6)(3,7)
  (4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,8)(2,7)(3,6)(4,5), () ]),
  Group([ (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), () ]), Group([ (1,6)
  (2,5)(3,8)(4,7), (1,7)(2,8)(3,5)(4,6), () ]), Group([ (1,6)(2,5)(3,4)
  (7,8), (1,7)(2,4)(3,5)(6,8), () ]) ]
gap> Length(GsHNPtrueMin);
17
gap> List(GsHNPtrueMin,IdSmallGroup);
```

```
[ [ 32, 6 ], [ 32, 6 ], [ 32, 6 ], [ 4, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ],
  [ 8, 2 ], [ 4, 2 ], [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 4, 2 ],
  [ 4, 2 ], [ 4, 2 ], [ 4, 2 ] ]
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 300 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
351
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsC2xC2);
61
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
15
gap> Gs32_6:=Filtered(Gs,x->IdSmallGroup(x)=[32,6]);;
gap> Length(Gs32_6);
3
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (3,7), (4,8) ]), Group([ (2,6), (4,8) ]), Group([ (), (4,8), (2,6)
  (3,7) ]), Group([ (4,8), (1,5)(4,8) ]), Group([ (4,8), (1,5)(3,7) ]),
  Group([ (1,5)(2,6), (4,8) ]), Group([ (4,8), (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (), (2,6), (3,7) ]), Group([ (), (3,7), (2,6)(4,8) ]),
  Group([ (), (1,5), (3,7) ]), Group([ (3,7), (1,5)(4,8) ]),
  Group([ (3,7), (1,5)(2,6) ]), Group([ (), (3,7), (1,5)(2,6)(4,8) ]),
  Group([ (), (2,6), (3,7)(4,8) ]), Group([ (), (2,6)(4,8), (3,7)(4,8) ]),
  Group([ (1,2)(3,4)(5,6)(7,8), (), (3,7)(4,8) ]), Group([ (3,7)
  (4,8), (1,5) ]), Group([ (3,7)(4,8), (1,5)(4,8) ]), Group([ (), (3,7)
  (4,8), (1,5)(2,6) ]), Group([ (1,5)(2,6)(4,8), (3,7)(4,8) ]), Group([ (1,6)
  (2,5)(3,8)(4,7), (), (3,7)(4,8) ]), Group([ (), (1,5), (2,6) ]),
  Group([ (1,5)(4,8), (2,6) ]), Group([ (2,6), (1,5)(3,7) ]),
  Group([ (), (2,6), (1,5)(3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)
  (6,8), (), (2,6)(4,8) ]), Group([ (), (1,5), (2,6)(4,8) ]),
  Group([ (), (2,6)(4,8), (1,5)(2,6) ]), Group([ (), (2,6)(4,8), (1,5)
  (3,7) ]), Group([ (2,6)(4,8), (1,5)(2,6)(3,7) ]), Group([ (1,7)(2,8)(3,5)
  (4,6), (), (2,6)(4,8) ]), Group([ (1,4)(2,3)(5,8)(6,7), (), (2,6)(3,7) ]),
  Group([ (), (1,5), (2,6)(3,7) ]), Group([ (), (1,5)(4,8), (2,6)(3,7) ]),
  Group([ (), (1,5)(2,6), (2,6)(3,7) ]), Group([ (1,5)(3,7)(4,8), (2,6)
  (3,7) ]), Group([ (1,8)(2,3)(4,5)(6,7), (), (2,6)(3,7) ]), Group([ (2,6)
  (3,7)(4,8), (1,5) ]), Group([ (), (1,5)(4,8), (2,6)(3,7)(4,8) ]),
```

```
  Group([ (), (1,5)(3,7), (2,6)(3,7)(4,8) ]), Group([ (), (1,5)(2,6), (2,6)
  (3,7)(4,8) ]), Group([ (1,2)(3,4)(5,6)(7,8), (), (1,5)(2,6) ]),
  Group([ (1,2)(3,4)(5,6)(7,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,2)
  (3,8)(4,7)(5,6), (), (1,5)(2,6) ]), Group([ (1,2)(3,8)(4,7)(5,6), (), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (), (1,5)(3,7) ]),
  Group([ (1,3)(2,4)(5,7)(6,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)
  (2,8)(4,6)(5,7), (), (1,5)(3,7) ]), Group([ (1,3)(2,8)(4,6)(5,7), (), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (1,4)(2,3)(5,8)(6,7), (), (1,5)(4,8) ]),
  Group([ (1,4)(2,3)(5,8)(6,7), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,8)
  (2,7)(3,6)(4,5), (), (1,5)(4,8) ]), Group([ (1,8)(2,3)(4,5)(6,7), (), (1,5)
  (2,6)(3,7)(4,8) ]) ]
gap> Length(GsHNPfalseC2xC2);
53
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,3)(2,4)(5,7)(6,8), (1,4)(2,3)(5,8)(6,7), () ]), Group([ (1,7)
  (2,8)(3,5)(4,6), (1,8)(2,7)(3,6)(4,5), () ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (1,8)(2,3)(4,5)(6,7), () ]), Group([ (1,7)(2,4)(3,5)(6,8), (1,4)(2,7)
  (3,6)(5,8), () ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,8)(2,7)(3,6)
  (4,5), () ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), () ]),
  Group([ (1,6)(2,5)(3,8)(4,7), (1,7)(2,8)(3,5)(4,6), () ]), Group([ (1,6)
  (2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), () ]) ]
gap> Length(GsHNPtrueC2xC2);
8
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2 ], 6 ], [ [ 2, 2, 2 ], 16 ], [ [ 2, 2, 2, 2 ], 13 ],
  [ [ 2, 2, 4 ], 1 ], [ [ 2, 4, 2 ], 5 ], [ [ 4, 2, 2 ], 6 ], [ [ 4, 4 ], 6 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 8 ] ]
gap> GsHNPfalse44C2xC2:=Filtered(GsHNPfalseC2xC2,
> x->List(Orbits(x,[1..8]),Length)=[4,4]);
[ Group([ (1,2)(3,4)(5,6)(7,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,2)
  (3,8)(4,7)(5,6), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)
  (6,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (1,4)(2,3)(5,8)(6,7), (), (1,5)(2,6)(3,7)
  (4,8) ]), Group([ (1,8)(2,3)(4,5)(6,7), (), (1,5)(2,6)(3,7)(4,8) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (1,2)(3,4)(5,6)(7,8), (1,3)(2,4)(5,7)(6,8), (1,4)(2,3)(5,8)(6,7) ],
  [ (), (1,2)(3,4)(5,6)(7,8), (1,7)(2,8)(3,5)(4,6), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
```

```
  [ (), (1,2)(3,8)(4,7)(5,6), (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,3)(2,4)(5,7)(6,8), (1,6)(2,5)(3,8)(4,7), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,6)(2,5)(3,8)(4,7), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (4,8), (3,7), (3,7)(4,8) ], [ (), (4,8), (2,6), (2,6)(4,8) ],
  [ (), (4,8), (2,6)(3,7), (2,6)(3,7)(4,8) ], [ (), (4,8), (1,5), (1,5)(4,8) ],
  [ (), (4,8), (1,5)(3,7), (1,5)(3,7)(4,8) ],
  [ (), (4,8), (1,5)(2,6), (1,5)(2,6)(4,8) ],
  [ (), (4,8), (1,5)(2,6)(3,7), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (3,7), (2,6), (2,6)(3,7) ],
  [ (), (3,7), (2,6)(4,8), (2,6)(3,7)(4,8) ],
  [ (), (3,7), (1,5), (1,5)(3,7) ],
  [ (), (3,7), (1,5)(4,8), (1,5)(3,7)(4,8) ],
  [ (), (3,7), (1,5)(2,6), (1,5)(2,6)(3,7) ],
  [ (), (3,7), (1,5)(2,6)(4,8), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (3,7)(4,8), (2,6), (2,6)(3,7)(4,8) ],
  [ (), (3,7)(4,8), (2,6)(4,8), (2,6)(3,7) ],
  [ (), (3,7)(4,8), (1,2)(3,4)(5,6)(7,8), (1,2)(3,8)(4,7)(5,6) ],
  [ (), (3,7)(4,8), (1,5), (1,5)(3,7)(4,8) ],
  [ (), (3,7)(4,8), (1,5)(4,8), (1,5)(3,7) ],
  [ (), (3,7)(4,8), (1,5)(2,6), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (3,7)(4,8), (1,5)(2,6)(4,8), (1,5)(2,6)(3,7) ],
  [ (), (3,7)(4,8), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,8)(4,7) ],
  [ (), (2,6), (1,5), (1,5)(2,6) ],
  [ (), (2,6), (1,5)(4,8), (1,5)(2,6)(4,8) ],
  [ (), (2,6), (1,5)(3,7), (1,5)(2,6)(3,7) ],
  [ (), (2,6), (1,5)(3,7)(4,8), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (2,6)(4,8), (1,3)(2,4)(5,7)(6,8), (1,3)(2,8)(4,6)(5,7) ],
  [ (), (2,6)(4,8), (1,5), (1,5)(2,6)(4,8) ],
  [ (), (2,6)(4,8), (1,5)(4,8), (1,5)(2,6) ],
  [ (), (2,6)(4,8), (1,5)(3,7), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (2,6)(4,8), (1,5)(3,7)(4,8), (1,5)(2,6)(3,7) ],
  [ (), (2,6)(4,8), (1,7)(2,4)(3,5)(6,8), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (2,6)(3,7), (1,4)(2,3)(5,8)(6,7), (1,4)(2,7)(3,6)(5,8) ],
  [ (), (2,6)(3,7), (1,5), (1,5)(2,6)(3,7) ],
  [ (), (2,6)(3,7), (1,5)(4,8), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (2,6)(3,7), (1,5)(3,7), (1,5)(2,6) ],
```

```
  [ (), (2,6)(3,7), (1,5)(3,7)(4,8), (1,5)(2,6)(4,8) ],
  [ (), (2,6)(3,7), (1,8)(2,3)(4,5)(6,7), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (2,6)(3,7)(4,8), (1,5), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (2,6)(3,7)(4,8), (1,5)(4,8), (1,5)(2,6)(3,7) ],
  [ (), (2,6)(3,7)(4,8), (1,5)(3,7), (1,5)(2,6)(4,8) ],
  [ (), (2,6)(3,7)(4,8), (1,5)(3,7)(4,8), (1,5)(2,6) ],
  [ (), (1,2)(3,4)(5,6)(7,8), (1,5)(2,6), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,2)(3,4)(5,6)(7,8), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,8)(4,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6), (1,6)(2,5)(3,8)(4,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,4)(5,7)(6,8), (1,5)(3,7), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(3,7), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,5)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(4,8), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalse44C2xC2,Elements);
[ [ (), (1,2)(3,4)(5,6)(7,8), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,8)(4,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8), (1,7)(2,8)(3,5)(4,6) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)(3,6)(4,5) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> ZG:=Centre(G);
Group([ (1,5)(2,6)(3,7)(4,8) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,ZG));
[ Group(()), Group(()), Group(()), Group(()), Group(()), Group(()),
  Group(()), Group(()) ]
gap> List(GsHNPfalse44C2xC2,x->Intersection(x,ZG));
[ Group([ (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8) ]),
  Group([ (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,5)(2,6)(3,7)(4,8) ]) ]
gap> Syl2G:=SylowSubgroup(G,2);
Group([ (4,8), (1,2)(3,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7), (1,5)(2,6), (1,5)
(4,8), (1,5)(2,6)(3,7)(4,8) ])
gap> IsNormal(G,Syl2G);
true
```

```
gap> DSyl2G:=DerivedSubgroup(Syl2G);
Group([ (2,6)(3,7), (1,5)(4,8), (2,6)(4,8) ])
gap> StructureDescription(DSyl2G);
"C2 x C2 x C2"
gap> Collected(List(GsHNPfalseC2xC2,x->Order(Intersection(DSyl2G,x))));
[ [ 2, 46 ], [ 4, 7 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->Order(Intersection(DSyl2G,x))));
[ [ 1, 8 ] ]
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,2)(3,8,7,4)(5,6), (), (3,7)(4,8), (1,5)(2,6) ]),
  Group([ (1,6,5,2)(3,4)(7,8), (), (1,5)(2,6), (3,7)(4,8) ]),
  Group([ (1,6,5,2)(3,8,7,4), (), (3,7)(4,8), (1,5)(2,6) ]), Group([ (1,3)
  (2,8,6,4)(5,7), (2,6)(4,8), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,7,5,3)(2,8)
  (4,6), (1,5)(3,7), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3,5,7)
  (2,8,6,4), (), (2,6)(4,8), (1,5)(3,7) ]), Group([ (1,8,5,4)(2,3)
  (6,7), (), (1,5)(4,8), (2,6)(3,7) ]), Group([ (1,4)(2,3,6,7)(5,8), (2,6)
  (3,7), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,8,5,4)(2,7,6,3), (), (1,5)
  (4,8), (2,6)(3,7) ]) ]
gap> Length(GsHNPfalseC4xC2);
9
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,2)(3,4)(5,6)(7,8), (1,7,5,3)(2,8,6,4), (), (1,5)(2,6)(3,7)
  (4,8) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,7,5,3)(2,4,6,8), (), (1,5)(2,6)
  (3,7)(4,8) ]), Group([ (1,3)(2,4)(5,7)(6,8), (1,8,5,4)(2,3,6,7), (), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (1,8)(2,3)(4,5)(6,7), (1,2,5,6)
  (3,4,7,8), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (1,4,5,8)(2,3,6,7), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,4)(2,3)
  (5,8)(6,7), (1,2,5,6)(3,8,7,4), (), (1,5)(2,6)(3,7)(4,8) ]) ]
gap> Length(GsHNPtrueC4xC2);
6
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 9 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
[ [ [ 8 ], 6 ] ]
gap> Collected(List(GsHNPfalseC4xC2,x->Order(Intersection(DSyl2G,x))));
[ [ 4, 9 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->Order(Intersection(DSyl2G,x))));
[ [ 2, 6 ] ]
gap> Syl2G=TransitiveGroup(8,31);
```

```
true
```

EXAMPLE 1.46 ($G = 8Tm$ ($m = 9, 11, 15, 19, 22, 32$)).

(2-1) $G = 8T9 \simeq D_4 \times C_2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,9); # G=8T9=D4xC2
E(8):2=D(4)[x]2
gap> GeneratorsOfGroup(G); # H=C2
[ (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8),
  (4,5)(6,7) ]
gap> H:=Stabilizer(G,1); # H=C2
Group([ (4,5)(6,7) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2xC2: Schur multiplicer of G
[ 2, 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 7 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> Print("\n");
> od;
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 1, 1 ] ] ] ]
[ [  ], [ [ 2, 2, 2, 2 ], [  ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 0 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
```

```
[ 2 ][ 2 ]
[ 2 ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
gap> cG:=cGs[2];
rec( MinimalStemExtension := Group([ (2,3)(4,6), (1,2)(3,5)(4,7)(6,8), (2,4)
  (3,6) ]), Tid := [ 8, 18 ],
  epi := [ (2,3)(4,6), (1,2)(3,5)(4,7)(6,8), (2,4)(3,6) ] ->
    [ (4,5)(6,7), (1,5)(2,6)(3,7)(4,8), (1,3)(2,8)(4,6)(5,7) ] )
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
Group([ (2,3)(4,6), (1,2)(3,5)(4,7)(6,8), (2,4)(3,6) ])
gap> bH:=PreImage(cG.epi,H); # bH=H-
Group([ (2,3)(4,6), (1,7)(2,4)(3,6)(5,8) ])
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 2, 2 ], [ [ 0, 1 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
106
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
99
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
7
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "1", 2 ], [ "C2", 29 ], [ "C2 x C2", 41 ], [ "C2 x C2 x C2", 9 ],
  [ "C4", 6 ], [ "D8", 12 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "C2 x C2", 4 ], [ "C2 x C2 x C2", 1 ], [ "C2 x D8", 1 ], [ "C4 x C2", 1 ]
 ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
28
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
```

```
gap> Length(GsHNPtrue);
7
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (), (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,4,8,5)
  (2,7,3,6) ]), Group([ (1,2)(3,8)(4,7)(5,6), (), (1,4)(2,7)(3,6)(5,8) ]),
  Group([ (1,2)(3,8)(4,7)(5,6), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)
  (2,8)(4,6)(5,7), (), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (), (1,5)(2,6)(3,7)(4,8) ]) ]
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ] ]
gap> Length(GsHNPtrueMin);
5
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 28 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
35
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsC2xC2);
13
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
1
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,2)(3,8)(4,7)(5,6), (4,5)(6,7) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (4,5)(6,7) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (4,5)(6,7) ]),
  Group([ (1,3)(2,8)(4,6)(5,7), (1,8)(2,3) ]), Group([ (1,2)(3,8)(4,6)
  (5,7), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)
  (4,5)(6,7) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,8)(2,3) ]), Group([ (1,5)
  (2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ]), Group([ (), (1,8)(2,3)(4,5)
  (6,7), (1,7)(2,4)(3,5)(6,8) ]) ]
gap> Length(GsHNPfalseC2xC2);
9
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,2)(3,8)(4,7)(5,6), (), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,2)
  (3,8)(4,7)(5,6), (), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)
```

```
  (5,7), (), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (), (1,5)
  (2,6)(3,7)(4,8) ]) ]
gap> Length(GsHNPtrueC2xC2);
4
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2, 2 ], 1 ], [ [ 2, 2, 4 ], 2 ], [ [ 4, 2, 2 ], 2 ],
  [ [ 4, 4 ], 4 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 4 ] ]
gap> GsHNPfalse44C2xC2:=Filtered(GsHNPfalseC2xC2,x->List(Orbits(x,[1..8]),
> Length)=[4,4]);
[ Group([ (1,2)(3,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,3)(2,8)
  (4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,8)
  (2,3)(4,5)(6,7) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,7)(2,4)(3,5)
  (6,8) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (1,2)(3,8)(4,7)(5,6), (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (4,5)(6,7), (1,2)(3,8)(4,6)(5,7), (1,2)(3,8)(4,7)(5,6) ],
  [ (), (4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8)(4,7)(5,6) ],
  [ (), (4,5)(6,7), (1,8)(2,3), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,6)(5,7), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3) ],
  [ (), (1,2)(3,8)(4,6)(5,7), (1,3)(2,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,7)(5,6), (1,8)(2,3) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalse44C2xC2,Elements);
[ [ (), (1,2)(3,8)(4,6)(5,7), (1,3)(2,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> DG:=DerivedSubgroup(G);
Group([ (1,8)(2,3)(4,5)(6,7) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,DG));
[ Group(()), Group(()), Group(()), Group(()) ]
```

```
gap> List(GsHNPfalse44C2xC2,x->Intersection(x,DG));
[ Group([ (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,8)(2,3)(4,5)(6,7) ]),
  Group([ (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,8)(2,3)(4,5)(6,7) ]) ]
```

(2-2) $G = 8T11 \simeq (C_4 \times C_2) \rtimes C_2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,11); # G=8T11=(C4xC2):C2
1/2[2^3]E(4)=Q_8:2
gap> GeneratorsOfGroup(G);
[ (1,5)(3,7), (1,3,5,7)(2,4,6,8), (1,4,5,8)(2,3,6,7) ]
gap> H:=Stabilizer(G,1); # H=C2
Group([ (2,6)(4,8) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2: Schur multiplicer of G
[ 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 3 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> Print("\n");
> od;
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 0, 1 ] ] ] ]
[ [  ], [ [ 2, 2 ], [  ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 0, 1 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 2 ][ 2 ]
[ 2 ][  ]
[ 2 ][ 2 ]
gap> cG:=cGs[2];
rec( MinimalStemExtension := <permutation group of size 32 with 5 generators>,
```

```
  epi := [ (1,5,6,16)(2,9,10,22)(3,12,13,25)(4,14,15,26)(7,18,19,29)(8,20,21,
        30)(11,23,24,31)(17,27,28,32), (1,3,6,13)(2,7,10,19)(4,12,15,25)(5,11,
        16,24)(8,18,21,29)(9,17,22,28)(14,23,26,31)(20,27,30,32),
      (1,2)(3,7)(4,21)(5,22)(6,10)(8,15)(9,16)(11,28)(12,29)(13,19)(14,20)(17,
        24)(18,25)(23,27)(26,30)(31,32) ] ->
    [ (1,4,5,8)(2,3,6,7), (1,3,5,7)(2,4,6,8), (2,6)(4,8) ] )
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
<permutation group of size 32 with 5 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-
Group([ (1,2)(3,7)(4,21)(5,22)(6,10)(8,15)(9,16)(11,28)(12,29)(13,19)(14,20)
(17,24)(18,25)(23,27)(26,30)(31,32), (1,26)(2,30)(3,31)(4,5)(6,14)(7,32)(8,9)
(10,20)(11,12)(13,23)(15,16)(17,18)(19,27)(21,22)(24,25)(28,29) ])
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 2, 2 ], [ [ 0, 1 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
58
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
55
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
3
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "1", 2 ], [ "C2", 17 ], [ "C2 x C2", 11 ], [ "C4", 12 ], [ "C4 x C2", 5 ],
  [ "D8", 7 ], [ "Q8", 1 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C4 x C2) : C2", 1 ], [ "C4 x C2", 2 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
20
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
3
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
```

```
> y->IsSubgroup(x,y)))=1);
[ Group([ (), (1,5)(2,6)(3,7)(4,8), (1,4,5,8)(2,3,6,7), (1,3,5,7)
  (2,4,6,8) ]), Group([ (), (1,5)(2,6)(3,7)(4,8), (1,3,5,7)(2,4,6,8), (1,8)
  (2,3)(4,5)(6,7) ]) ]
gap> Length(GsHNPtrueMin);
2
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 8, 2 ], [ 8, 2 ] ]
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 20 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
23
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
3
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
[ Group([ (), (1,5)(2,6)(3,7)(4,8), (1,3,5,7)(2,4,6,8), (2,6)(4,8) ]) ]
gap> Length(GsHNPfalseC4xC2);
1
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (), (1,5)(2,6)(3,7)(4,8), (1,4,5,8)(2,3,6,7), (1,3,5,7)
  (2,4,6,8) ]), Group([ (), (1,5)(2,6)(3,7)(4,8), (1,3,5,7)(2,4,6,8), (1,8)
  (2,3)(4,5)(6,7) ]) ]
gap> Length(GsHNPtrueC4xC2);
2
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 1 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
[ [ [ 8 ], 2 ] ]
gap> List(GsHNPfalseC4xC2,Elements);
[ [ (), (2,6)(4,8), (1,3,5,7)(2,4,6,8), (1,3,5,7)(2,8,6,4), (1,5)(3,7),
      (1,5)(2,6)(3,7)(4,8), (1,7,5,3)(2,4,6,8), (1,7,5,3)(2,8,6,4) ] ]
gap> List(GsHNPtrueC4xC2,Elements);
[ [ (), (1,2)(3,4)(5,6)(7,8), (1,3,5,7)(2,4,6,8), (1,4,5,8)(2,3,6,7),
      (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,8)(4,7), (1,7,5,3)(2,8,6,4),
      (1,8,5,4)(2,7,6,3) ],
  [ (), (1,2,5,6)(3,4,7,8), (1,3,5,7)(2,4,6,8), (1,4)(2,7)(3,6)(5,8),
      (1,5)(2,6)(3,7)(4,8), (1,6,5,2)(3,8,7,4), (1,7,5,3)(2,8,6,4),
```

```
      (1,8)(2,3)(4,5)(6,7) ] ]
```

(2-3) $G = 8T15 \simeq C_8 \rtimes V_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,15); # G=8T15=C8:V4
[1/4.cD(4)^2]2
gap> GeneratorsOfGroup(G);
[ (1,2,3,4,5,6,7,8), (1,5)(3,7), (1,6)(2,5)(3,4)(7,8) ]
gap> H:=Stabilizer(G,1); # H=V4
Group([ (2,8)(3,7)(4,6), (2,4)(3,7)(6,8) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2: Schur multiplicer of G
[ 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 3 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> Print("\n");
> od;
[ [  ], [ [ 2, 2, 2, 2 ], [  ] ] ]
[ [ 2 ], [ [ 2, 4 ], [ [ 0, 2 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 1, 0 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 2 ][  ]
[  ][  ]
[  ][  ]
gap> cG:=cGs[1];
rec( MinimalStemExtension := <permutation group of size 64 with 3 generators>,
  epi := [ (3,4)(5,6)(7,9)(8,10)(11,13)(12,14)(15,18)(17,19)(20,23)(22,24)(25,
        27)(28,30), (1,2)(3,7)(4,9)(5,11)(6,13)(8,12)(10,14)(15,20)(16,21)(17,
```

```
        25)(18,23)(19,27)(22,28)(24,30)(26,29)(31,32),
      (1,3,8,17,26,19,10,4)(2,5,12,22,29,24,14,6)(7,15,25,31,27,18,9,16)(11,
        20,28,32,30,23,13,21) ] ->
    [ (2,8)(3,7)(4,6), (2,6)(4,8), (1,2,3,4,5,6,7,8) ] )
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
<permutation group of size 64 with 3 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-
<permutation group of size 8 with 3 generators>
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 0, 1 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 2, 2, 2 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
225
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
174
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
51
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "1", 2 ], [ "C2", 45 ], [ "C2 x C2", 55 ], [ "C4", 12 ], [ "C4 x C2", 5 ],
  [ "C8", 6 ], [ "C8 : C2", 1 ], [ "D16", 10 ], [ "D8", 35 ], [ "Q8", 1 ],
  [ "QD16", 2 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C4 x C2) : C2", 1 ], [ "C2 x C2", 20 ], [ "C2 x C2 x C2", 18 ],
  [ "C2 x D8", 9 ], [ "C4 x C2", 2 ], [ "C8 : (C2 x C2)", 1 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
47
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
11
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (1,5)(3,7), (1,5)(2,4)(6,8) ]), Group([ (2,6)(4,8), (2,6)
```

```
  (4,8), (1,3)(4,8)(5,7) ]), Group([ (2,6)(4,8), (2,6)(4,8), (1,7)(2,6)
  (3,5) ]), Group([ (1,5)(3,7), (2,8)(3,7)(4,6) ]), Group([ (1,5)(2,6)(3,7)
  (4,8), (1,2)(3,8)(4,7)(5,6), (1,3,5,7)(2,8,6,4), (1,7,5,3)(2,4,6,8) ]),
  Group([ (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)(3,6)(4,5), (1,7,5,3)
  (2,4,6,8), (1,3,5,7)(2,8,6,4) ]) ]
gap> Length(GsHNPtrueMin);
6
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 4, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ], [ 8, 2 ], [ 8, 2 ] ]
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 47 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
58
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsC2xC2);
15
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
3
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (2,6)(4,8), (2,4)(3,7)(6,8) ]), Group([ (2,4)(3,7)(6,8), (1,5)(2,8)
  (4,6) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(3,7), (2,6)(4,8) ]),
  Group([ (2,6)(4,8), (2,6)(4,8), (1,5)(2,4)(6,8) ]), Group([ (1,5)(2,6)(3,7)
  (4,8), (1,5)(2,6)(3,7)(4,8), (2,8)(3,7)(4,6) ]), Group([ (1,5)(2,6)(3,7)
  (4,8), (1,2)(3,8)(4,7)(5,6) ]), Group([ (1,5)(3,7), (1,5)(3,7), (1,3)(4,8)
  (5,7) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,7)(4,8), (1,3)(4,8)
  (5,7) ]), Group([ (1,5)(3,7), (1,5)(3,7), (1,7)(2,6)(3,5) ]), Group([ (1,5)
  (2,6)(3,7)(4,8), (1,3)(2,6)(5,7), (1,7)(3,5)(4,8) ]), Group([ (1,5)(2,6)
  (3,7)(4,8), (1,8)(2,7)(3,6)(4,5), (1,5)(2,6)(3,7)(4,8) ]) ]
gap> Length(GsHNPfalseC2xC2);
11
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,5)(3,7), (1,5)(2,4)(6,8) ]), Group([ (2,6)(4,8), (2,6)
  (4,8), (1,3)(4,8)(5,7) ]), Group([ (2,6)(4,8), (2,6)(4,8), (1,7)(2,6)
  (3,5) ]), Group([ (1,5)(3,7), (2,8)(3,7)(4,6) ]) ]
gap> Length(GsHNPtrueC2xC2);
4
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
```

```
[ [ [ 2, 2, 2, 2 ], 1 ], [ [ 2, 4 ], 1 ], [ [ 2, 4, 2 ], 2 ], [ [ 4, 2 ], 3 ],
  [ [ 4, 2, 2 ], 2 ], [ [ 4, 4 ], 2 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2, 2 ], 4 ] ]
gap> GsHNPfalse2222C2xC2:=Filtered(GsHNPfalseC2xC2,
> x->List(Orbits(x,[1..8]),Length)=[2,2,2,2]);
[ Group([ (1,5)(2,6)(3,7)(4,8), (1,5)(3,7), (2,6)(4,8) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (2,4)(3,7)(6,8), (1,5)(3,7), (1,5)(2,4)(6,8) ],
  [ (), (2,6)(4,8), (1,3)(4,8)(5,7), (1,3)(2,6)(5,7) ],
  [ (), (2,6)(4,8), (1,7)(3,5)(4,8), (1,7)(2,6)(3,5) ],
  [ (), (2,8)(3,7)(4,6), (1,5)(3,7), (1,5)(2,8)(4,6) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (2,4)(3,7)(6,8), (2,6)(4,8), (2,8)(3,7)(4,6) ],
  [ (), (2,4)(3,7)(6,8), (1,5)(2,6)(3,7)(4,8), (1,5)(2,8)(4,6) ],
  [ (), (2,6)(4,8), (1,5)(3,7), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (2,6)(4,8), (1,5)(2,4)(6,8), (1,5)(2,8)(4,6) ],
  [ (), (2,8)(3,7)(4,6), (1,5)(2,4)(6,8), (1,5)(2,6)(3,7)(4,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(4,8)(5,7), (1,5)(3,7), (1,7)(3,5)(4,8) ],
  [ (), (1,3)(4,8)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,6)(3,5) ],
  [ (), (1,3)(2,6)(5,7), (1,5)(3,7), (1,7)(2,6)(3,5) ],
  [ (), (1,3)(2,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(3,5)(4,8) ],
  [ (), (1,4)(2,3)(5,8)(6,7), (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)(3,6)(4,5) ] ]
gap> List(GsHNPfalse2222C2xC2,Elements);
[ [ (), (2,6)(4,8), (1,5)(3,7), (1,5)(2,6)(3,7)(4,8) ] ]
gap> DG:=DerivedSubgroup(G);
Group([ (1,5)(2,6)(3,7)(4,8), (1,3,5,7)(2,4,6,8) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,DG));
[ Group(()), Group(()), Group(()), Group(()) ]
gap> List(GsHNPfalse2222C2xC2,x->Intersection(x,DG));
[ Group([ (1,5)(2,6)(3,7)(4,8) ]) ]
gap> A8:=AlternatingGroup(8);
Alt( [ 1 .. 8 ] )
gap> List(GsHNPtrueC2xC2,x->IsSubgroup(A8,x));
[ false, false, false, false ]
gap> List(GsHNPfalse2222C2xC2,x->IsSubgroup(A8,x));
[ true ]
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
```

```
[ Group([ (1,5)(2,6)(3,7)(4,8), (2,6)(4,8), (1,7,5,3)(2,8,6,4) ]) ]
gap> Length(GsHNPfalseC4xC2);
1
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,5)(2,6)(3,7)(4,8), (1,2)(3,8)(4,7)(5,6), (1,3,5,7)
  (2,8,6,4), (1,7,5,3)(2,4,6,8) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,8)(2,7)
  (3,6)(4,5), (1,7,5,3)(2,4,6,8), (1,3,5,7)(2,8,6,4) ]) ]
gap> Length(GsHNPtrueC4xC2);
2
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 1 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
[ [ [ 8 ], 2 ] ]
gap> Collected(List(GsHNPfalseC4xC2,x->StructureDescription(Intersection(DG,x))));
[ [ "C4", 1 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->StructureDescription(Intersection(DG,x))));
[ [ "C2", 2 ] ]
```

(2-4) $G = 8T19 \simeq (C_2)^3 \rtimes C_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,19); # G=8T19=(C2xC2xC2):C4
E(8):4=[1/4.eD(4)^2]2
gap> GeneratorsOfGroup(G);
[ (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8),
  (1,3)(4,5,6,7) ]
gap> H:=Stabilizer(G,1); # H=C4
Group([ (2,8)(4,5,6,7) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 4 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2: Schur multiplicer of G
[ 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 3 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> Print("\n");
> od;
```

```
[ [ 2 ], [ [ 2, 4 ], [ [ 0, 2 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 0 ] ] ] ]
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[ 2 ][  ]
gap> cG:=cGs[3];
rec( MinimalStemExtension := Group([ (2,3,5,4)(6,9)(7,10)(11,13,12,14), (1,2)
  (3,6)(4,7)(5,8)(9,11)(10,12)(13,15)(14,16) ]), Tid := [ 16, 163 ],
  epi := [ (2,3,5,4)(6,9)(7,10)(11,13,12,14),
      (1,2)(3,6)(4,7)(5,8)(9,11)(10,12)(13,15)(14,16) ] ->
    [ (2,8)(4,7,6,5), (1,5)(2,6)(3,7)(4,8) ] )
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
Group([ (2,3,5,4)(6,9)(7,10)(11,13,12,14), (1,2)(3,6)(4,7)(5,8)(9,11)(10,12)
(13,15)(14,16) ])
gap> bH:=PreImage(cG.epi,H); # bH=H-
Group([ (2,4,5,3)(6,9)(7,10)(11,14,12,13), (1,15)(2,13)(3,12)(4,11)(5,14)
(6,10)(7,9)(8,16) ])
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 2, 4 ], [ [ 1, 2 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 2, 4 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
105
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
86
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
19
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
```

```
[ [ "(C4 x C2) : C2", 1 ], [ "1", 2 ], [ "C2", 25 ], [ "C2 x C2", 21 ],
  [ "C2 x C2 x C2", 1 ], [ "C4", 22 ], [ "C4 x C2", 2 ], [ "D8", 12 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C2 x C2 x C2) : C4", 1 ], [ "(C4 x C2) : C2", 1 ], [ "C2 x C2", 4 ],
  [ "C2 x C2 x C2", 1 ], [ "C2 x D8", 1 ], [ "C4 x C2", 11 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
39
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
11
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (1,3)(4,7,6,5), (1,3)(2,8)(4,6)(5,7), (4,6)(5,7) ]),
  Group([ (1,8,3,2)(5,7), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8) ]),
  Group([ (1,7,3,5)(2,4,8,6), (1,2)(3,8)(4,7)(5,6), (), (1,3)(2,8)(4,6)
  (5,7) ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,2)(3,8)(4,7)(5,6), () ]),
  Group([ (1,6)(2,5)(3,4)(7,8), (1,2)(3,8)(4,7)(5,6), () ]), Group([ (1,5)
  (2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7), () ]), Group([ (1,7)(2,4)(3,5)
  (6,8), (1,8)(2,3)(4,5)(6,7), () ]) ]
gap> Length(GsHNPtrueMin);
7
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
50
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,2)(3,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,4)(2,7)
  (3,6)(5,8), (1,2)(3,8)(4,7)(5,6) ]), Group([ (1,6)(2,5)(3,4)(7,8), (1,2)
  (3,8)(4,7)(5,6) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ]),
  Group([ (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,4)(2,7)
  (3,6)(5,8), (1,3)(2,8)(4,6)(5,7) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,3)
  (2,8)(4,6)(5,7) ]), Group([ (4,6)(5,7), (1,2)(3,8)(4,7)(5,6) ]),
  Group([ (4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,3)(2,8), (1,8)(2,3)
  (4,5)(6,7) ]), Group([ (1,3)(2,8), (1,2)(3,8)(4,7)(5,6) ]), Group([ (4,6)
  (5,7), (1,3)(2,8)(4,6)(5,7) ]), Group([ (1,8)(2,3)(4,7)(5,6), (1,3)(2,8)
```

```
  (4,6)(5,7) ]) ]
gap> Length(GsC2xC2);
13
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,2)(3,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7), (1,5,3,7)(2,6,8,4) ]),
  Group([ (2,8)(4,7,6,5), (4,6)(5,7), (1,3)(2,8)(4,6)(5,7) ]),
  Group([ (1,8,3,2)(4,6), (1,3)(2,8), (1,3)(2,8)(4,6)(5,7) ]),
  Group([ (1,4,2,5)(3,6,8,7), (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7) ]),
  Group([ (1,5,8,6)(2,4,3,7), (1,8)(2,3)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7) ]) ]
gap> Length(GsC4xC2);
5
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,2)(3,8)(4,5)(6,7), (4,6)(5,7), (4,6)(5,7) ]), Group([ (1,3)(2,8)
  (4,6)(5,7), (1,3)(2,8), (4,6)(5,7) ]), Group([ (1,8)(2,3)(4,7)(5,6), (4,6)
  (5,7), (4,6)(5,7) ]), Group([ (1,2)(3,8)(4,5)(6,7), (1,3)(2,8), (1,3)
  (2,8) ]), Group([ (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8)
  (4,6)(5,7) ]), Group([ (1,8)(2,3)(4,7)(5,6), (1,3)(2,8), (1,3)(2,8) ]),
  Group([ (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8)(4,6)
  (5,7) ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,3)(2,8)(4,6)(5,7) ]),
  Group([ (1,7)(2,4)(3,5)(6,8), (1,3)(2,8)(4,6)(5,7) ]) ]
gap> Length(GsHNPfalseC2xC2);
9
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,4)(2,7)(3,6)(5,8), (1,2)(3,8)(4,7)(5,6), () ]), Group([ (1,6)
  (2,5)(3,4)(7,8), (1,2)(3,8)(4,7)(5,6), () ]), Group([ (1,5)(2,6)(3,7)
  (4,8), (1,8)(2,3)(4,5)(6,7), () ]), Group([ (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)
  (4,5)(6,7), () ]) ]
gap> Length(GsHNPtrueC2xC2);
4
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2, 2 ], 1 ], [ [ 2, 2, 4 ], 2 ], [ [ 4, 2, 2 ], 2 ],
  [ [ 4, 4 ], 4 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 4 ] ]
gap> GsHNPfalse44C2xC2:=Filtered(GsHNPfalseC2xC2,
> x->List(Orbits(x,[1..8]),Length)=[4,4]);
[ Group([ (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8)(4,6)
  (5,7) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8)
  (4,6)(5,7) ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,3)(2,8)(4,6)(5,7) ]),
```

```
  Group([ (1,7)(2,4)(3,5)(6,8), (1,3)(2,8)(4,6)(5,7) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (1,2)(3,8)(4,7)(5,6), (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (4,6)(5,7), (1,2)(3,8)(4,5)(6,7), (1,2)(3,8)(4,7)(5,6) ],
  [ (), (4,6)(5,7), (1,3)(2,8), (1,3)(2,8)(4,6)(5,7) ],
  [ (), (4,6)(5,7), (1,8)(2,3)(4,5)(6,7), (1,8)(2,3)(4,7)(5,6) ],
  [ (), (1,2)(3,8)(4,5)(6,7), (1,3)(2,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,7)(5,6) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8), (1,8)(2,3)(4,7)(5,6) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ] ]
gap> List(GsHNPfalse44C2xC2,Elements);
[ [ (), (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,7)(5,6) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ] ]
gap> ZG:=Centre(G);
Group([ (1,3)(2,8)(4,6)(5,7) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,ZG));
[ Group(()), Group(()), Group(()), Group(()) ]
gap> List(GsHNPfalse44C2xC2,x->Intersection(x,ZG));
[ Group([ (1,3)(2,8)(4,6)(5,7) ]), Group([ (1,3)(2,8)(4,6)(5,7) ]),
  Group([ (1,3)(2,8)(4,6)(5,7) ]), Group([ (1,3)(2,8)(4,6)(5,7) ]) ]
gap> UcsG:=UpperCentralSeries(G);
[ Group([ (1,3)(2,8)(4,6)(5,7), (4,6)(5,7), (1,8)(2,3)(4,5)(6,7), (2,8)
  (4,7,6,5), (1,5)(2,6)(3,7)(4,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (4,6)
  (5,7), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,3)(2,8)(4,6)(5,7) ]), Group(()) ]
gap> Collected(List(GsHNPfalseC2xC2,x->List(UcsG,y->Order(Intersection(y,x)))));
[ [ [ 4, 2, 2, 1 ], 2 ], [ [ 4, 4, 1, 1 ], 4 ], [ [ 4, 4, 2, 1 ], 3 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(UcsG,y->Order(Intersection(y,x)))));
[ [ [ 4, 2, 1, 1 ], 4 ] ]
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,4,2,5)(3,6,8,7), (1,2)(3,8)(4,5)(6,7), (), (1,3)(2,8)(4,6)
  (5,7) ]), Group([ (1,7,8,4)(2,6,3,5), (1,8)(2,3)(4,7)(5,6), (), (1,3)(2,8)
```

```
  (4,6)(5,7) ]) ]
gap> Length(GsHNPfalseC4xC2);
2
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,3)(4,7,6,5), (1,3)(2,8)(4,6)(5,7), (4,6)(5,7) ]),
  Group([ (1,8,3,2)(5,7), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8) ]),
  Group([ (1,7,3,5)(2,4,8,6), (1,2)(3,8)(4,7)(5,6), (), (1,3)(2,8)(4,6)
  (5,7) ]) ]
gap> Length(GsHNPtrueC4xC2);
3
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 8 ], 2 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 4 ], 1 ], [ [ 4, 2, 2 ], 1 ], [ [ 8 ], 1 ] ]
gap> GsHNPtrue8C4xC2:=Filtered(GsHNPtrueC4xC2,x->List(Orbits(x,[1..8]),Length)=[8]);
[ Group([ (1,7,3,5)(2,4,8,6), (1,2)(3,8)(4,7)(5,6), (), (1,3)(2,8)(4,6)
  (5,7) ]) ]
gap> List(GsHNPfalseC4xC2,Elements);
[ [ (), (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,4,2,5)(3,6,8,7),
      (1,5,2,4)(3,7,8,6), (1,6,2,7)(3,4,8,5), (1,7,2,6)(3,5,8,4),
      (1,8)(2,3)(4,7)(5,6) ],
  [ (), (1,2)(3,8)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,4,8,7)(2,5,3,6),
      (1,5,8,6)(2,4,3,7), (1,6,8,5)(2,7,3,4), (1,7,8,4)(2,6,3,5),
      (1,8)(2,3)(4,7)(5,6) ] ]
gap> List(GsHNPtrueC4xC2,Elements);
[ [ (), (4,6)(5,7), (2,8)(4,5,6,7), (2,8)(4,7,6,5), (1,3)(4,5,6,7),
      (1,3)(4,7,6,5), (1,3)(2,8), (1,3)(2,8)(4,6)(5,7) ],
  [ (), (4,6)(5,7), (1,2,3,8)(5,7), (1,2,3,8)(4,6), (1,3)(2,8),
      (1,3)(2,8)(4,6)(5,7), (1,8,3,2)(5,7), (1,8,3,2)(4,6) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,4,3,6)(2,7,8,5),
      (1,5,3,7)(2,6,8,4), (1,6,3,4)(2,5,8,7), (1,7,3,5)(2,4,8,6),
      (1,8)(2,3)(4,5)(6,7) ] ]
gap> DG:=DerivedSubgroup(G);
Group([ (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ])
gap> List(GsHNPfalseC4xC2,x->Intersection(x,DG));
[ Group([ (1,3)(2,8)(4,6)(5,7) ]), Group([ (1,3)(2,8)(4,6)(5,7) ]) ]
gap> List(GsHNPtrue8C4xC2,x->Intersection(x,DG));
[ Group([ (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ]) ]
```

(2-5) $G = 8T22 \simeq (C_2)^3 \rtimes V_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,22); # G=8T22=(C2xC2xC2):V4
E(8):D_4=[2^3]2^2
gap> GeneratorsOfGroup(G);
[ (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8),
  (2,3)(4,5), (2,3)(6,7) ]
gap> H:=Stabilizer(G,1); # H=V4
Group([ (2,3)(4,5), (2,3)(6,7) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2^5: Schur multiplicer of G
[ 2, 2, 2, 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 31 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> Print("\n");
> od;
[ [ 2 ], [ [ 2, 2, 2, 2, 2, 2 ], [ [ 0, 0, 0, 1, 0, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 1, 0, 0, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 0, 0, 1, 1 ] ] ] ]
[ [ 2, 2 ], [ [ 2, 2, 2, 2, 4 ], [ [ 0, 0, 0, 1, 0 ], [ 0, 0, 0, 0, 2 ] ] ] ]
[ [ 2, 2, 2 ],
  [ [ 2, 2, 2, 2 ], [ [ 0, 1, 0, 0 ], [ 0, 0, 1, 0 ], [ 0, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 4 ], [ [ 1, 1, 0, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 1, 1, 0, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2, 2 ], [ [ 0, 0, 0, 1, 0, 0 ] ] ] ]
[ [ 2, 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 1, 0, 0, 0 ], [ 0, 0, 1, 0, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2, 2 ], [ [ 0, 0, 1, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 4 ], [ [ 0, 1, 0, 1, 2 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2, 2 ], [ [ 0, 0, 1, 1, 0, 1 ] ] ] ]
[ [ 2, 2 ], [ [ 2, 2, 2, 2, 4 ], [ [ 0, 0, 1, 1, 0 ], [ 0, 0, 0, 0, 2 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 1, 0, 1, 1 ] ] ] ]
[ [  ], [ [ 2, 2, 2, 2, 2 ], [  ] ] ]
```

```
[ [ 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 0, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 1, 0, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 0, 0, 1 ] ] ] ]
[ [ 2, 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 1, 0, 0, 0 ], [ 0, 0, 0, 1, 0 ] ] ] ]
[ [ 2, 2, 2 ],
  [ [ 2, 2, 4, 4 ], [ [ 1, 0, 0, 0 ], [ 0, 0, 2, 0 ], [ 0, 0, 0, 2 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 4 ], [ [ 0, 0, 1, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 1, 0, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 1, 0, 0, 0 ] ] ] ]
[ [ 2, 2 ], [ [ 2, 2, 2, 2 ], [ [ 1, 0, 0, 0 ], [ 0, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 1, 0, 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 1, 0, 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2, 2 ], [ [ 0, 0, 0, 1, 0, 1 ] ] ] ]
[ [ 2, 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 0, 1, 0, 1 ], [ 0, 0, 0, 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2, 2 ], [ [ 0, 0, 1, 0, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2, 2, 2 ], [ [ 0, 1, 1, 0 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][  ]
```

```
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[ 2 ][ 2 ]
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
gap> cG:=cGs[16];;
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
<permutation group of size 64 with 6 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-
<permutation group of size 8 with 3 generators>
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 2, 2, 2 ], [ [ 0, 0, 1 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 2, 2, 2 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
321
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
292
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
29
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "1", 2 ], [ "C2", 49 ], [ "C2 x C2", 101 ], [ "C2 x C2 x C2", 28 ],
  [ "C2 x D8", 19 ], [ "C4", 18 ], [ "C4 x C2", 15 ], [ "D8", 58 ],
  [ "Q8", 2 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C2 x C2 x C2) : (C2 x C2)", 1 ], [ "(C4 x C2) : C2", 6 ],
```

```
  [ "C2 x C2", 8 ], [ "C2 x C2 x C2", 2 ], [ "C2 x D8", 6 ],
  [ "C4 x C2", 6 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
81
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
29
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,6)(5,7), (1,4,8,5)
  (2,6,3,7) ]), Group([ (1,4)(2,6)(3,7)(5,8), (1,6)(2,4)(3,5)(7,8), () ]),
  Group([ (1,5)(2,7)(3,6)(4,8), (1,7)(2,5)(3,4)(6,8), () ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,6,8,7)(2,5,3,4), (1,2)(3,8)(4,7)
  (5,6) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,7)(2,4)(3,5)(6,8), () ]),
  Group([ (1,2)(3,8)(4,7)(5,6), (1,6)(2,5)(3,4)(7,8), () ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,4)(2,6)(3,7)(5,8), (1,2,8,3)
  (4,6,5,7) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,4,8,5)(2,6,3,7), (1,2,8,
   3)(4,6,5,7) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2,8,3)
  (4,7,5,6), (1,4)(2,7)(3,6)(5,8) ]), Group([ (), (1,8)(2,3)(4,5)
  (6,7), (1,2,8,3)(4,7,5,6), (1,6)(2,4)(3,5)(7,8) ]), Group([ (1,3)(2,8)(4,6)
  (5,7), (1,6)(2,5)(3,4)(7,8), () ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,7)
  (2,4)(3,5)(6,8), () ]), Group([ (1,4)(2,6)(3,7)(5,8), (1,7)(2,5)(3,4)
  (6,8), () ]), Group([ (1,5)(2,7)(3,6)(4,8), (1,6)(2,4)(3,5)(7,8), () ]) ]
gap> Length(GsHNPtrueMin);
14
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 8, 2 ],
  [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ] ]
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 81 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
110
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsC2xC2);
33
```

```
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
9
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (4,5)(6,7), (2,3)(4,5) ]), Group([ (4,5)(6,7), (1,2)(3,8)(4,7)
  (5,6) ]), Group([ (4,5)(6,7), (1,3)(2,8)(4,6)(5,7), () ]), Group([ (4,5)
  (6,7), (1,8)(6,7), () ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (4,5)(6,7) ]),
  Group([ (1,4)(2,6)(3,7)(5,8), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,5)(2,7)
  (3,6)(4,8), (1,5)(2,6)(3,7)(4,8), () ]), Group([ (1,8)(2,3), (1,8)
  (6,7) ]), Group([ (2,3)(6,7), (1,8)(2,3)(4,5)(6,7) ]), Group([ (2,3)
  (4,5), (1,6)(2,5)(3,4)(7,8), () ]), Group([ (2,3)(4,5), (1,7)(2,4)(3,5)
  (6,8), () ]), Group([ (2,3)(4,5), (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,8)
  (2,3), (2,3)(4,5) ]), Group([ (1,8)(2,3), (1,3)(2,8)(4,6)(5,7), () ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,6)(5,7) ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,7)(5,6) ]), Group([ (1,8)
  (2,3), (1,2)(3,8)(4,7)(5,6), () ]), Group([ (1,4)(2,6)(3,7)(5,8), (1,5)
  (2,6)(3,7)(4,8) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,4)(2,6)(3,7)
  (5,8) ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,8)(2,3)(4,5)(6,7) ]),
  Group([ (1,5)(2,7)(3,6)(4,8), (1,4)(2,7)(3,6)(5,8) ]), Group([ (1,8)
  (6,7), (1,7)(2,4)(3,5)(6,8), () ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,6)
  (2,4)(3,5)(7,8) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,6)(2,5)(3,4)
  (7,8) ]), Group([ (1,8)(6,7), (1,6)(2,5)(3,4)(7,8), () ]) ]
gap> Length(GsHNPfalseC2xC2);
25
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,4)(2,6)(3,7)(5,8), (1,6)(2,4)(3,5)(7,8), () ]), Group([ (1,5)
  (2,7)(3,6)(4,8), (1,7)(2,5)(3,4)(6,8), () ]), Group([ (1,2)(3,8)(4,7)
  (5,6), (1,7)(2,4)(3,5)(6,8), () ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,6)
  (2,5)(3,4)(7,8), () ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,6)(2,5)(3,4)
  (7,8), () ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,7)(2,4)(3,5)(6,8), () ]),
  Group([ (1,4)(2,6)(3,7)(5,8), (1,7)(2,5)(3,4)(6,8), () ]), Group([ (1,5)
  (2,7)(3,6)(4,8), (1,6)(2,4)(3,5)(7,8), () ]) ]
gap> Length(GsHNPtrueC2xC2);
8
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2 ], 4 ], [ [ 2, 2, 2, 2 ], 3 ], [ [ 2, 2, 4 ], 2 ],
  [ [ 2, 4, 2 ], 4 ], [ [ 4, 2, 2 ], 6 ], [ [ 4, 4 ], 6 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 8 ] ]
```

```
gap> GsHNPfalse44C2xC2:=Filtered(GsHNPfalseC2xC2,
> x->List(Orbits(x,[1..8]),Length)=[4,4]);
[ Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,6)(5,7) ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,7)(5,6) ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,4)(2,6)(3,7)(5,8) ]), Group([ (1,4)
  (2,7)(3,6)(5,8), (1,8)(2,3)(4,5)(6,7) ]), Group([ (), (1,8)(2,3)(4,5)
  (6,7), (1,6)(2,4)(3,5)(7,8) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,6)
  (2,5)(3,4)(7,8) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (1,2)(3,8)(4,6)(5,7), (1,4)(2,6)(3,7)(5,8), (1,6)(2,4)(3,5)(7,8) ],
  [ (), (1,2)(3,8)(4,6)(5,7), (1,5)(2,7)(3,6)(4,8), (1,7)(2,5)(3,4)(6,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,3)(2,8)(4,7)(5,6), (1,4)(2,6)(3,7)(5,8), (1,7)(2,5)(3,4)(6,8) ],
  [ (), (1,3)(2,8)(4,7)(5,6), (1,5)(2,7)(3,6)(4,8), (1,6)(2,4)(3,5)(7,8) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (4,5)(6,7), (2,3)(6,7), (2,3)(4,5) ],
  [ (), (4,5)(6,7), (1,2)(3,8)(4,6)(5,7), (1,2)(3,8)(4,7)(5,6) ],
  [ (), (4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,3)(2,8)(4,7)(5,6) ],
  [ (), (4,5)(6,7), (1,8)(6,7), (1,8)(4,5) ],
  [ (), (4,5)(6,7), (1,8)(2,3), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (2,3)(6,7), (1,4)(2,6)(3,7)(5,8), (1,4)(2,7)(3,6)(5,8) ],
  [ (), (2,3)(6,7), (1,5)(2,6)(3,7)(4,8), (1,5)(2,7)(3,6)(4,8) ],
  [ (), (2,3)(6,7), (1,8)(6,7), (1,8)(2,3) ],
  [ (), (2,3)(6,7), (1,8)(4,5), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (2,3)(4,5), (1,6)(2,4)(3,5)(7,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (2,3)(4,5), (1,7)(2,4)(3,5)(6,8), (1,7)(2,5)(3,4)(6,8) ],
  [ (), (2,3)(4,5), (1,8)(6,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (2,3)(4,5), (1,8)(4,5), (1,8)(2,3) ],
  [ (), (1,2)(3,8)(4,6)(5,7), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3) ],
  [ (), (1,2)(3,8)(4,6)(5,7), (1,3)(2,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,7)(5,6), (1,8)(2,3) ],
  [ (), (1,4)(2,6)(3,7)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(4,5) ],
  [ (), (1,4)(2,6)(3,7)(5,8), (1,5)(2,7)(3,6)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,7)(3,6)(4,8), (1,8)(4,5) ],
```

```
  [ (), (1,6)(2,4)(3,5)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(6,7) ],
  [ (), (1,6)(2,4)(3,5)(7,8), (1,7)(2,5)(3,4)(6,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,5)(3,4)(6,8), (1,8)(6,7) ] ]
gap> List(GsHNPfalse44C2xC2,Elements);
[ [ (), (1,2)(3,8)(4,6)(5,7), (1,3)(2,8)(4,7)(5,6), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,6)(3,7)(5,8), (1,5)(2,7)(3,6)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,4)(3,5)(7,8), (1,7)(2,5)(3,4)(6,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> ZG:=Centre(G);
Group([ (1,8)(2,3)(4,5)(6,7) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,ZG));
[ Group(()), Group(()), Group(()), Group(()), Group(()), Group(()),
  Group(()), Group(()) ]
gap> List(GsHNPfalse44C2xC2,x->Intersection(x,ZG));
[ Group([ (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,8)(2,3)(4,5)(6,7) ]),
  Group([ (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,8)(2,3)(4,5)(6,7) ]),
  Group([ (1,8)(2,3)(4,5)(6,7) ]), Group([ (1,8)(2,3)(4,5)(6,7) ]) ]
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
[ Group([ (), (1,8)(2,3)(4,5)(6,7), (4,5)(6,7), (1,2,8,3)(4,6,5,7) ]),
  Group([ (2,3)(6,7), (1,4,8,5)(2,6,3,7), (1,8)(2,3)(4,5)(6,7) ]),
  Group([ (), (1,8)(2,3)(4,5)(6,7), (1,6,8,7)(2,5,3,4), (2,3)(4,5) ]) ]
gap> Length(GsHNPfalseC4xC2);
3
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (), (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,6)(5,7), (1,4,8,5)
  (2,6,3,7) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,6,8,7)(2,5,3,4), (1,2)
  (3,8)(4,7)(5,6) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,4)(2,6)(3,7)
  (5,8), (1,2,8,3)(4,6,5,7) ]), Group([ (), (1,8)(2,3)(4,5)(6,7), (1,4,8,5)
  (2,6,3,7), (1,2,8,3)(4,6,5,7) ]), Group([ (), (1,8)(2,3)(4,5)
  (6,7), (1,2,8,3)(4,7,5,6), (1,4)(2,7)(3,6)(5,8) ]), Group([ (), (1,8)(2,3)
  (4,5)(6,7), (1,2,8,3)(4,7,5,6), (1,6)(2,4)(3,5)(7,8) ]) ]
gap> Length(GsHNPtrueC4xC2);
6
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 3 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
```

```
[ [ [ 8 ], 6 ] ]
```

(2-6) $G' = 8T32 \simeq ((C_2)^3 \rtimes V_4) \rtimes C_3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(8,32); # G=8T32=(C2^3:V4):C3
[2^3]A(4)
gap> GeneratorsOfGroup(G);
[ (1,8)(2,3)(4,5)(6,7), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8),
  (1,2,3)(4,6,5), (2,5)(3,4) ]
gap> H:=Stabilizer(G,1); # H=A4
Group([ (2,5)(3,4), (2,3,8)(4,7,5) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 3 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C2xC2xC2: Schur multiplier of G
[ 2, 2, 2 ]
gap> cGs:=MinimalStemExtensions(G);; # 7 minimal stem extensions
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(KerResH3Z(bG,bH));
> Print("\n");
> od;
[ [  ], [ [ 2, 2 ], [  ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 0, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 0 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 1 ] ] ] ]
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 1 ] ] ] ]
gap> for cG in cGs do
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 2 ][  ]
[ 2 ][ 2 ]
```

```
[ 2 ][ 2 ]
[  ][  ]
[  ][  ]
[  ][  ]
[  ][  ]
gap> cG:=cGs[1];;
gap> bG:=cG.MinimalStemExtension; # bG=G- is a minimal stem extension of G
<permutation group of size 192 with 7 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-
<permutation group of size 24 with 3 generators>
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C2
[ [ 2 ], [ [ 6 ], [ [ 3 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 6 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
326
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
gap> Length(bGsHNPfalse);
280
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[2]);;
gap> Length(bGsHNPtrue);
46
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "1", 2 ], [ "A4", 8 ], [ "C2", 33 ], [ "C2 x A4", 12 ], [ "C2 x C2", 53 ],
  [ "C2 x C2 x C2", 12 ], [ "C2 x D8", 3 ], [ "C3", 32 ], [ "C4", 18 ],
  [ "C4 x C2", 15 ], [ "C6", 48 ], [ "D8", 18 ], [ "Q8", 10 ],
  [ "SL(2,3)", 16 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "((C2 x C2 x C2) : (C2 x C2)) : C3", 1 ],
  [ "(C2 x C2 x C2) : (C2 x C2)", 1 ], [ "(C4 x C2) : C2", 6 ], [ "A4", 8 ],
  [ "C2 x A4", 8 ], [ "C2 x C2", 8 ], [ "C2 x C2 x C2", 2 ], [ "C2 x D8", 6 ],
  [ "C4 x C2", 6 ] ]
gap> GsHNPfalse:=Set(bGsHNPfalse,x->Image(cG.epi,x));;
gap> Length(GsHNPfalse);
129
gap> GsHNPtrue:=Set(bGsHNPtrue,x->Image(cG.epi,x));;
gap> Length(GsHNPtrue);
46
```

```
gap> Intersection(GsHNPfalse,GsHNPtrue);
[  ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);
[ Group([ (1,7)(2,3)(4,5)(6,8), (1,2)(3,7)(4,8)(5,6), () ]), Group([ (1,3,6,4)
  (2,7,5,8), (1,8,6,7)(2,4,5,3), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)
  (7,8) ]), Group([ (1,4)(2,8)(3,6)(5,7), (1,8)(2,4)(3,5)(6,7), () ]),
  Group([ (1,8)(2,3)(4,5)(6,7), (1,2)(3,8)(4,7)(5,6), () ]), Group([ (1,7,6,8)
  (2,4,5,3), (1,2)(3,8)(4,7)(5,6), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)
  (7,8) ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8), () ]),
  Group([ (1,7,6,8)(2,4,5,3), (1,2,6,5)(3,7,4,8), (1,6)(2,5)(3,4)(7,8), (1,6)
  (2,5)(3,4)(7,8) ]), Group([ (1,3,6,4)(2,7,5,8), (1,7)(2,4)(3,5)(6,8), (1,6)
  (2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,5,6,2)(3,7,4,8), (1,3)
  (2,8)(4,6)(5,7), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]),
  Group([ (1,5,6,2)(3,7,4,8), (1,3,6,4)(2,8,5,7), (1,6)(2,5)(3,4)(7,8), (1,6)
  (2,5)(3,4)(7,8) ]), Group([ (1,8)(2,4)(3,5)(6,7), (1,5)(2,6)(3,8)
  (4,7), () ]), Group([ (1,7)(2,4)(3,5)(6,8), (1,5)(2,6)(3,7)(4,8), () ]),
  Group([ (1,8)(2,3)(4,5)(6,7), (1,5)(2,6)(3,7)(4,8), () ]), Group([ (1,7)
  (2,3)(4,5)(6,8), (1,5)(2,6)(3,8)(4,7), () ]) ]
gap> Length(GsHNPtrueMin);
14
gap> List(GsHNPtrueMin,IdSmallGroup);
[ [ 4, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 8, 2 ], [ 4, 2 ], [ 8, 2 ],
  [ 8, 2 ], [ 8, 2 ], [ 8, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ], [ 4, 2 ] ]
gap> Collected(List(GsHNPfalse,x->Filtered(GsHNPtrueMin,y->IsSubgroup(x,y))));
[ [ [  ], 129 ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
175
gap> GsC2xC2:=Filtered(Gs,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsC2xC2);
33
gap> GsC4xC2:=Filtered(Gs,x->IdSmallGroup(x)=[8,2]);;
gap> Length(GsC4xC2);
9
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);
[ Group([ (3,4)(7,8), (2,5)(7,8) ]), Group([ (1,2)(3,8)(4,7)(5,6), (3,4)
  (7,8), (3,4)(7,8) ]), Group([ (1,5)(2,6)(3,7)(4,8), (3,4)(7,8), (3,4)
  (7,8) ]), Group([ (1,6)(3,4), (3,4)(7,8), (1,6)(7,8) ]), Group([ (3,4)
```

```
  (7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (2,5)
  (7,8), (2,5)(7,8) ]), Group([ (1,4)(2,7)(3,6)(5,8), (2,5)(7,8), (2,5)
  (7,8) ]), Group([ (2,5)(7,8), (1,6)(2,5), (1,6)(7,8) ]), Group([ (1,6)
  (3,4), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,6)(2,5)(3,4)(7,8), (2,5)
  (3,4), (1,6)(7,8) ]), Group([ (2,5)(3,4), (1,6)(2,5) ]), Group([ (1,7)(2,4)
  (3,5)(6,8), (2,5)(3,4), (2,5)(3,4) ]), Group([ (1,8)(2,3)(4,5)(6,7), (2,5)
  (3,4), (2,5)(3,4) ]), Group([ (1,5)(2,6)(3,7)(4,8), (1,6)(2,5), (1,6)
  (2,5) ]), Group([ (1,5)(2,6)(3,8)(4,7), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)
  (3,4)(7,8) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,6)(2,5)(3,4)(7,8), (1,6)
  (2,5)(3,4)(7,8) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,6)(2,5), (1,6)
  (2,5) ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,6)(3,4), (1,6)(3,4) ]),
  Group([ (1,3)(2,7)(4,6)(5,8), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)
  (7,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)
  (3,4)(7,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,6)(3,4), (1,6)(3,4) ]),
  Group([ (1,8)(2,3)(4,5)(6,7), (1,6)(7,8), (1,6)(7,8) ]), Group([ (1,7)(2,4)
  (3,5)(6,8), (1,6)(7,8), (1,6)(7,8) ]), Group([ (1,8)(2,4)(3,5)(6,7), (1,6)
  (2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,7)(2,4)(3,5)
  (6,8), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]) ]
gap> Length(GsHNPfalseC2xC2);
25
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);
[ Group([ (1,7)(2,3)(4,5)(6,8), (1,2)(3,7)(4,8)(5,6), () ]), Group([ (1,4)
  (2,8)(3,6)(5,7), (1,8)(2,4)(3,5)(6,7), () ]), Group([ (1,8)(2,3)(4,5)
  (6,7), (1,2)(3,8)(4,7)(5,6), () ]), Group([ (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)
  (3,5)(6,8), () ]), Group([ (1,8)(2,4)(3,5)(6,7), (1,5)(2,6)(3,8)
  (4,7), () ]), Group([ (1,7)(2,4)(3,5)(6,8), (1,5)(2,6)(3,7)(4,8), () ]),
  Group([ (1,8)(2,3)(4,5)(6,7), (1,5)(2,6)(3,7)(4,8), () ]), Group([ (1,7)
  (2,3)(4,5)(6,8), (1,5)(2,6)(3,8)(4,7), () ]) ]
gap> Length(GsHNPtrueC2xC2);
8
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2 ], 4 ], [ [ 2, 2, 2, 2 ], 3 ], [ [ 2, 2, 4 ], 1 ],
  [ [ 2, 4, 2 ], 5 ], [ [ 4, 2, 2 ], 6 ], [ [ 4, 4 ], 6 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 8 ] ]
gap> GsHNPfalse44C2xC2:=Filtered(GsHNPfalseC2xC2,
> x->List(Orbits(x,[1..8]),Length)=[4,4]);
[ Group([ (1,5)(2,6)(3,8)(4,7), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)
  (7,8) ]), Group([ (1,2)(3,8)(4,7)(5,6), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)
```

```
  (3,4)(7,8) ]), Group([ (1,3)(2,7)(4,6)(5,8), (1,6)(2,5)(3,4)(7,8), (1,6)
  (2,5)(3,4)(7,8) ]), Group([ (1,3)(2,8)(4,6)(5,7), (1,6)(2,5)(3,4)
  (7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,8)(2,4)(3,5)(6,7), (1,6)(2,5)
  (3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,7)(2,4)(3,5)(6,8), (1,6)
  (2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]) ]
gap> List(GsHNPtrueC2xC2,Elements);
[ [ (), (1,2)(3,7)(4,8)(5,6), (1,3)(2,7)(4,6)(5,8), (1,7)(2,3)(4,5)(6,8) ],
  [ (), (1,2)(3,7)(4,8)(5,6), (1,4)(2,8)(3,6)(5,7), (1,8)(2,4)(3,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,3)(2,8)(4,6)(5,7), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,4)(2,7)(3,6)(5,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,3)(2,7)(4,6)(5,8), (1,5)(2,6)(3,8)(4,7), (1,8)(2,4)(3,5)(6,7) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,5)(2,6)(3,7)(4,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (1,4)(2,7)(3,6)(5,8), (1,5)(2,6)(3,7)(4,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,4)(2,8)(3,6)(5,7), (1,5)(2,6)(3,8)(4,7), (1,7)(2,3)(4,5)(6,8) ] ]
gap> List(GsHNPfalseC2xC2,Elements);
[ [ (), (3,4)(7,8), (2,5)(7,8), (2,5)(3,4) ],
  [ (), (3,4)(7,8), (1,2)(3,7)(4,8)(5,6), (1,2)(3,8)(4,7)(5,6) ],
  [ (), (3,4)(7,8), (1,5)(2,6)(3,7)(4,8), (1,5)(2,6)(3,8)(4,7) ],
  [ (), (3,4)(7,8), (1,6)(7,8), (1,6)(3,4) ],
  [ (), (3,4)(7,8), (1,6)(2,5), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (2,5)(7,8), (1,3)(2,7)(4,6)(5,8), (1,3)(2,8)(4,6)(5,7) ],
  [ (), (2,5)(7,8), (1,4)(2,7)(3,6)(5,8), (1,4)(2,8)(3,6)(5,7) ],
  [ (), (2,5)(7,8), (1,6)(7,8), (1,6)(2,5) ],
  [ (), (2,5)(7,8), (1,6)(3,4), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (2,5)(3,4), (1,6)(7,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (2,5)(3,4), (1,6)(3,4), (1,6)(2,5) ],
  [ (), (2,5)(3,4), (1,7)(2,3)(4,5)(6,8), (1,7)(2,4)(3,5)(6,8) ],
  [ (), (2,5)(3,4), (1,8)(2,3)(4,5)(6,7), (1,8)(2,4)(3,5)(6,7) ],
  [ (), (1,2)(3,7)(4,8)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5) ],
  [ (), (1,2)(3,7)(4,8)(5,6), (1,5)(2,6)(3,8)(4,7), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,8)(4,7), (1,6)(2,5) ],
  [ (), (1,3)(2,7)(4,6)(5,8), (1,4)(2,7)(3,6)(5,8), (1,6)(3,4) ],
  [ (), (1,3)(2,7)(4,6)(5,8), (1,4)(2,8)(3,6)(5,7), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,8)(3,6)(5,7), (1,6)(3,4) ],
  [ (), (1,6)(7,8), (1,7)(2,3)(4,5)(6,8), (1,8)(2,3)(4,5)(6,7) ],
  [ (), (1,6)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,4)(3,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,3)(4,5)(6,8), (1,8)(2,4)(3,5)(6,7) ],
```

```
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> List(GsHNPfalse44C2xC2,Elements);
[ [ (), (1,2)(3,7)(4,8)(5,6), (1,5)(2,6)(3,8)(4,7), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,2)(3,8)(4,7)(5,6), (1,5)(2,6)(3,7)(4,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,7)(4,6)(5,8), (1,4)(2,8)(3,6)(5,7), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,3)(2,8)(4,6)(5,7), (1,4)(2,7)(3,6)(5,8), (1,6)(2,5)(3,4)(7,8) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,3)(4,5)(6,8), (1,8)(2,4)(3,5)(6,7) ],
  [ (), (1,6)(2,5)(3,4)(7,8), (1,7)(2,4)(3,5)(6,8), (1,8)(2,3)(4,5)(6,7) ] ]
gap> ZG:=Centre(G);
Group([ (1,6)(2,5)(3,4)(7,8) ])
gap> List(GsHNPtrueC2xC2,x->Intersection(x,ZG));
[ Group(()), Group(()), Group(()), Group(()), Group(()), Group(()),
  Group(()), Group(()) ]
gap> List(GsHNPfalse44C2xC2,x->Intersection(x,ZG));
[ Group([ (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,6)(2,5)(3,4)(7,8) ]),
  Group([ (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,6)(2,5)(3,4)(7,8) ]),
  Group([ (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,6)(2,5)(3,4)(7,8) ]) ]
gap> GsHNPfalseC4xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,2,6,5)(3,8,4,7), (1,6)(2,5)(3,4)(7,8), (3,4)(7,8) ]),
  Group([ (1,3,6,4)(2,7,5,8), (1,6)(2,5)(3,4)(7,8), (1,6)(3,4), (2,5)
  (7,8) ]), Group([ (1,7,6,8)(2,4,5,3), (1,6)(2,5)(3,4)(7,8), (2,5)(3,4) ]) ]
gap> Length(GsHNPfalseC4xC2);
3
gap> GsHNPtrueC4xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,2]);
[ Group([ (1,3,6,4)(2,7,5,8), (1,8,6,7)(2,4,5,3), (1,6)(2,5)(3,4)(7,8), (1,6)
  (2,5)(3,4)(7,8) ]), Group([ (1,7,6,8)(2,4,5,3), (1,2)(3,8)(4,7)(5,6), (1,6)
  (2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,7,6,8)(2,4,5,3), (1,2,
   6,5)(3,7,4,8), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]),
  Group([ (1,3,6,4)(2,7,5,8), (1,7)(2,4)(3,5)(6,8), (1,6)(2,5)(3,4)
  (7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,5,6,2)(3,7,4,8), (1,3)(2,8)(4,6)
  (5,7), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)(7,8) ]), Group([ (1,5,6,2)
  (3,7,4,8), (1,3,6,4)(2,8,5,7), (1,6)(2,5)(3,4)(7,8), (1,6)(2,5)(3,4)
  (7,8) ]) ]
gap> Length(GsHNPtrueC4xC2);
6
gap> Collected(List(GsHNPfalseC4xC2,x->List(Orbits(x),Length)));
[ [ [ 4, 4 ], 3 ] ]
gap> Collected(List(GsHNPtrueC4xC2,x->List(Orbits(x),Length)));
[ [ [ 8 ], 6 ] ]
```

```
gap> Syl2G:=SylowSubgroup(G,2);
Group([ (2,5)(3,4), (2,5)(7,8), (1,2)(3,8)(4,7)(5,6), (1,8)(2,3)(4,5)
(6,7), (1,6)(2,5)(3,4)(7,8) ])
gap> IsNormal(G,Syl2G);
true
gap> IsConjugate(SymmetricGroup(8),Syl2G,TransitiveGroup(8,22));
true
```

EXAMPLE 1.47 ($G = 9Tm$ $(m = 2, 5, 7, 9, 11, 14, 23)$).

(3-1) $G = 9T2 \simeq (C_3)^2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,2); # G=9T2=C3xC3
E(9)=3[x]3
gap> H:=Stabilizer(G,1); # H=1
Group(())
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [  ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3: Schur multiplier of G
[ 3 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,4,5)(3,6,7), (1,2,3)(4,7,8)(5,6,9) ]),
  epi := [ (2,4,5)(3,6,7), (1,2,3)(4,7,8)(5,6,9) ] ->
    [ (1,4,7)(2,5,8)(3,6,9), (1,2,9)(3,4,5)(6,7,8) ], Tid := [ 9, 7 ] )
gap> StructureDescription(TransitiveGroup(9,7));
"(C3 x C3) : C3"
gap> tG:=ScG.SchurCover; # tG=G~=(C3xC3):C3 is a Schur cover of G
Group([ (2,4,5)(3,6,7), (1,2,3)(4,7,8)(5,6,9) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C3
Group([ (1,9,8)(2,5,4)(3,6,7) ])
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C3
[ [ 3 ], [ [ 3 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 3 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
19
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
```

```
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> List([tGsHNPfalse,tGsHNPtrue],Length);
[ 18, 1 ]
gap> Collected(List(tGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C3", 13 ], [ "C3 x C3", 4 ] ]
gap> Collected(List(tGsHNPtrue,StructureDescription));
[ [ "(C3 x C3) : C3", 1 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C3", 16 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "C3 x C3", 1 ] ]
```

(3-2) $G = 9T5 \simeq (C_3)^2 \rtimes C_2$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,5); # G=9T5=(C3xC3):C2
S(3)[1/2]S(3)=3^2:2
gap> H:=Stabilizer(G,1); # H=C2
Group([ (2,9)(3,8)(4,7)(5,6) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3: Schur multiplier of G
[ 3 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,3)(4,7)(5,6), (1,2,3)(4,7,8)(5,6,9), (2,4,5)
  (3,6,7) ]), Tid := [ 9, 12 ],
  epi := [ (2,3)(4,7)(5,6), (1,2,3)(4,7,8)(5,6,9), (2,4,5)(3,6,7) ] ->
    [ (2,9)(3,8)(4,7)(5,6), (1,4,7)(2,5,8)(3,6,9), (1,2,9)(3,4,5)(6,7,8) ] )
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (2,3)(4,7)(5,6), (1,2,3)(4,7,8)(5,6,9), (2,4,5)(3,6,7) ])
gap> StructureDescription(tG);
"((C3 x C3) : C3) : C2"
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C6
Group([ (2,3)(4,7)(5,6), (1,8,9)(2,4,5)(3,7,6) ])
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C3
[ [ 3 ], [ [ 6 ], [ 2 ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 6 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
```

```
gap> Length(tGs);
62
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> List([tGsHNPfalse,tGsHNPtrue],Length);
[ 60, 2 ]
gap> Collected(List(tGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C2", 9 ], [ "C3", 13 ], [ "C3 x C3", 4 ], [ "C3 x S3", 12 ],
  [ "C6", 9 ], [ "S3", 12 ] ]
gap> Collected(List(tGsHNPtrue,StructureDescription));
[ [ "((C3 x C3) : C3) : C2", 1 ], [ "(C3 x C3) : C3", 1 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 18 ], [ "C3", 16 ], [ "S3", 24 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "(C3 x C3) : C2", 1 ], [ "C3 x C3", 1 ] ]
```

(3-3) $G = 9T7 \simeq (C_3)^2 \rtimes C_3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,7); # G=9T7=(C3xC3):C3
E(9):3=[3^2]3
gap> H:=Stabilizer(G,1); # H=C3
Group([ (3,4,5)(6,8,7) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 3 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3xC3: Schur multiplier of G
[ 3, 3 ]
gap> cGs:=MinimalStemExtensions(G);;
gap> for cG in cGs do
> tG:=cG.MinimalStemExtension;
> tH:=PreImage(cG.epi,H);
> Print(KerResH3Z(tG,tH));
> Print("\n");
> od;
[ [  ], [ [ 3 ], [  ] ] ]
[ [ 3 ], [ [ 3 ], [ [ 1 ] ] ] ]
[ [ 3 ], [ [ 3, 3 ], [ [ 0, 1 ] ] ] ]
[ [ 3 ], [ [ 3, 3 ], [ [ 0, 1 ] ] ] ]
gap> for cG in cGs do
```

```
> bG:=cG.MinimalStemExtension;
> bH:=PreImage(cG.epi,H);
> Print(FirstObstructionN(bG,bH).ker[1]);
> Print(FirstObstructionDnr(bG,bH).Dnr[1]);
> Print("\n");
> od;
[ 3 ][  ]
[ 3 ][ 3 ]
[ 3 ][ 3 ]
[ 3 ][ 3 ]
gap> cG:=cGs[1];
rec( MinimalStemExtension := <permutation group of size 81 with 4 generators>,
  epi := [ (1,5,15)(2,9,24)(3,12,29)(4,14,31)(6,18,37)(7,21,42)(8,23,44)(10,
        26,47)(11,28,49)(13,30,50)(16,34,55)(17,36,57)(19,39,60)(20,41,62)(22,
        43,63)(25,46,65)(27,48,66)(32,52,69)(33,54,71)(35,56,72)(38,59,74)(40,
        61,75)(45,64,76)(51,68,78)(53,70,79)(58,73,80)(67,77,81),
      (1,2,6)(3,22,51)(4,40,32)(5,23,34)(7,35,25)(8,53,10)(9,36,12)(11,20,
        33)(13,38,16)(14,21,18)(15,63,69)(17,27,19)(24,72,47)(26,43,77)(28,61,
        68)(29,44,71)(30,73,52)(31,62,55)(37,50,60)(39,56,64)(41,70,46)(42,57,
        49)(45,58,67)(48,59,54)(65,75,81)(66,80,78)(74,79,76),
      (1,3,10)(2,7,19)(4,11,25)(5,12,26)(6,16,32)(8,20,38)(9,21,39)(13,27,
        45)(14,28,46)(15,29,47)(17,33,51)(18,34,52)(22,40,58)(23,41,59)(24,42,
        60)(30,48,64)(31,49,65)(35,53,67)(36,54,68)(37,55,69)(43,61,73)(44,62,
        74)(50,66,76)(56,70,77)(57,71,78)(63,75,80)(72,79,81) ] ->
    [ (3,4,5)(6,8,7), (1,4,7)(2,5,8)(3,6,9), (1,2,9)(3,4,5)(6,7,8) ] )
gap> bG:=cG.MinimalStemExtension;
<permutation group of size 81 with 4 generators>
gap> bH:=PreImage(cG.epi,H); # bH=H-=C3xC3
<permutation group of size 9 with 2 generators>
gap> KerResH3Z(bG,bH);
[ [  ], [ [ 3 ], [  ] ] ]
gap> FirstObstructionN(bG,bH).ker; # Obs1N-=C3
[ [ 3 ], [ [ 3, 3 ], [ [ 0, 1 ] ] ] ]
gap> FirstObstructionDnr(bG,bH).Dnr; # Obs1Dnr-=1
[ [  ], [ [ 3, 3 ], [  ] ] ]
gap> bGs:=AllSubgroups(bG);;
gap> Length(bGs);
50
gap> bGsHNPfalse:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[]);;
```

```
gap> Length(bGsHNPfalse);
36
gap> bGsHNPtrue:=Filtered(bGs,x->FirstObstructionDr(bG,x,bH).Dr[1]=[3]);;
gap> Length(bGsHNPtrue);
14
gap> Collected(List(bGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C3", 22 ], [ "C3 x C3", 7 ], [ "C9", 6 ] ]
gap> Collected(List(bGsHNPtrue,StructureDescription));
[ [ "(C3 x C3 x C3) : C3", 1 ], [ "(C3 x C3) : C3", 1 ], [ "C3 x C3", 9 ],
  [ "C3 x C3 x C3", 1 ], [ "C9 : C3", 2 ] ]
gap> Collected(List(bGsHNPfalse,x->StructureDescription(Image(cG.epi,x))));
[ [ "1", 2 ], [ "C3", 34 ] ]
gap> Collected(List(bGsHNPtrue,x->StructureDescription(Image(cG.epi,x))));
[ [ "(C3 x C3) : C3", 1 ], [ "C3 x C3", 13 ] ]
```

(3-4) $G = 9T9 \simeq (C_3)^2 \rtimes C_4$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,9); # G=9T9=(C3xC3):C4
E(9):4
gap> H:=Stabilizer(G,1); # H=C4
Group([ (2,5,9,6)(3,4,8,7) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 4 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3: Schur multiplier of G
[ 3 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (1,2)(3,5,4,6)(7,11,10,12)(8,13,9,14)(15,17)
  (16,18), (2,3,4)(5,7,8)(6,9,10)(11,15,12)(13,16,14) ]), Tid := [ 18, 49 ],
  epi := [ (1,2)(3,5,4,6)(7,11,10,12)(8,13,9,14)(15,17)(16,18),
      (2,3,4)(5,7,8)(6,9,10)(11,15,12)(13,16,14) ] ->
    [ (2,6,9,5)(3,7,8,4), (1,6,5)(2,7,3)(4,9,8) ] )
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (1,2)(3,5,4,6)(7,11,10,12)(8,13,9,14)(15,17)(16,18), (2,3,4)(5,7,8)
(6,9,10)(11,15,12)(13,16,14) ])
gap> StructureDescription(tG);
"((C3 x C3) : C3) : C4"
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C12
Group([ (1,2)(3,6,4,5)(7,12,10,11)(8,14,9,13)(15,17)(16,18), (1,17,18)
```

```
(2,15,16)(3,12,14)(4,11,13)(5,7,8)(6,10,9) ])
gap> StructureDescription(tH);
"C12"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C3
[ [ 3 ], [ [ 12 ], [ 4 ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 12 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
81
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> List([tGsHNPfalse,tGsHNPtrue],Length);
[ 78, 3 ]
gap> Collected(List(tGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C12", 9 ], [ "C2", 9 ], [ "C3", 13 ], [ "C3 x C3", 4 ],
  [ "C3 x S3", 12 ], [ "C4", 9 ], [ "C6", 9 ], [ "S3", 12 ] ]
gap> Collected(List(tGsHNPtrue,StructureDescription));
[ [ "((C3 x C3) : C3) : C2", 1 ], [ "((C3 x C3) : C3) : C4", 1 ],
  [ "(C3 x C3) : C3", 1 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 18 ], [ "C3", 16 ], [ "C4", 18 ], [ "S3", 24 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "(C3 x C3) : C2", 1 ], [ "(C3 x C3) : C4", 1 ], [ "C3 x C3", 1 ] ]
```

### (3-5) $G = 9T11 \simeq (C_3)^2 \rtimes C_6$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,11); # G=9T11=(C3xC3):C6
E(9):6=1/2[3^2:2]S(3)
gap> H:=Stabilizer(G,1); # H=C6
Group([ (3,4,5)(6,8,7), (2,9)(3,8)(4,7)(5,6) ])
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 6 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3: Schur multiplier of G
[ 3 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (1,2)(3,5)(4,6)(7,8)(9,11)(10,12)(13,14)(15,17)
  (16,18), (1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18), (1,4,5)(2,3,6)
```

```
  (7,10,17)(8,15,12)(9,18,14)(11,13,16) ]), Tid := [ 18, 86 ],
  epi := [ (1,2)(3,5)(4,6)(7,8)(9,11)(10,12)(13,14)(15,17)(16,18),
      (1,7,13)(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18),
      (1,4,5)(2,3,6)(7,10,17)(8,15,12)(9,18,14)(11,13,16) ] ->
    [ (2,9)(3,8)(4,7)(5,6), (3,4,5)(6,8,7), (1,4,7)(2,5,8)(3,6,9) ] )
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (1,2)(3,5)(4,6)(7,8)(9,11)(10,12)(13,14)(15,17)(16,18), (1,7,13)
(2,8,14)(3,9,15)(4,10,16)(5,11,17)(6,12,18), (1,4,5)(2,3,6)(7,10,17)(8,15,12)
(9,18,14)(11,13,16) ])
gap> StructureDescription(tG);
"((C3 x C3 x C3) : C3) : C2"
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C6xC3
Group([ (1,2)(3,5)(4,6)(7,8)(9,11)(10,12)(13,14)(15,17)(16,18), (3,15,9)
(5,17,11), (1,7,13)(2,8,14)(3,15,9)(4,10,16)(5,17,11)(6,12,18) ])
gap> StructureDescription(tH);
"C6 x C3"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C3
[ [ 3 ], [ [ 3, 6 ], [ [ 1, 4 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 3, 6 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
142
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> List([tGsHNPfalse,tGsHNPtrue],Length);
[ 114, 28 ]
gap> Collected(List(tGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C2", 9 ], [ "C3", 22 ], [ "C3 x C3", 7 ], [ "C3 x S3", 12 ],
  [ "C6", 36 ], [ "C6 x C3", 9 ], [ "C9", 6 ], [ "S3", 12 ] ]
gap> Collected(List(tGsHNPtrue,StructureDescription));
[ [ "((C3 x C3 x C3) : C3) : C2", 1 ], [ "((C3 x C3) : C3) : C2", 1 ],
  [ "(C3 x C3 x C3) : C3", 1 ], [ "(C3 x C3) : C3", 1 ], [ "C3 x C3", 9 ],
  [ "C3 x C3 x C3", 1 ], [ "C3 x C3 x S3", 3 ], [ "C3 x S3", 9 ],
  [ "C9 : C3", 2 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 18 ], [ "C3", 34 ], [ "C6", 36 ], [ "S3", 24 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "(C3 x C3) : C2", 1 ], [ "(C3 x C3) : C3", 1 ], [ "(C3 x C3) : C6", 1 ],
```

```
  [ "C3 x C3", 13 ], [ "C3 x S3", 12 ] ]
```

(3-6) $G = 9T14 \simeq (C_3)^2 \rtimes Q_8$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,14); # G=9T14=(C3xC3):Q8
M(9)=E(9):Q_8
gap> H:=Stabilizer(G,1); # H=Q8
Group([ (2,8,9,3)(4,6,7,5), (2,5,9,6)(3,4,8,7) ])
gap> StructureDescription(H);
"Q8"
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3: Schur multiplier of G
[ 3 ]
gap> ScG:=SchurCoverG(G);
rec( SchurCover := Group([ (2,4,3,5)(6,9,7,8)(10,20,13,19)(11,14,12,17)
  (15,24,16,25)(18,22,21,23), (2,6,3,7)(4,8,5,9)(10,16,13,15)(11,22,12,23)
  (14,18,17,21)(19,25,20,24), (1,2,3)(4,10,11)(5,12,13)(6,14,15)(7,16,17)
  (8,18,19)(9,20,21)(22,23,26)(24,25,27) ]), Tid := [ 27, 83 ],
  epi := [ (2,4,3,5)(6,9,7,8)(10,20,13,19)(11,14,12,17)(15,24,16,25)(18,22,21,
        23), (2,6,3,7)(4,8,5,9)(10,16,13,15)(11,22,12,23)(14,18,17,21)(19,25,
        20,24), (1,2,3)(4,10,11)(5,12,13)(6,14,15)(7,16,17)(8,18,19)(9,20,
        21)(22,23,26)(24,25,27) ] ->
    [ (2,8,9,3)(4,6,7,5), (2,6,9,5)(3,7,8,4), (1,6,5)(2,7,3)(4,9,8) ] )
gap> StructureDescription(TransitiveGroup(27,83));
"((C3 x C3) : C3) : Q8"
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (2,4,3,5)(6,9,7,8)(10,20,13,19)(11,14,12,17)(15,24,16,25)
(18,22,21,23), (2,6,3,7)(4,8,5,9)(10,16,13,15)(11,22,12,23)(14,18,17,21)
(19,25,20,24), (1,2,3)(4,10,11)(5,12,13)(6,14,15)(7,16,17)(8,18,19)(9,20,21)
(22,23,26)(24,25,27) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C3xQ8
Group([ (2,4,3,5)(6,9,7,8)(10,20,13,19)(11,14,12,17)(15,24,16,25)
(18,22,21,23), (2,7,3,6)(4,9,5,8)(10,15,13,16)(11,23,12,22)(14,21,17,18)
(19,24,20,25), (1,27,26)(2,24,22)(3,25,23)(4,16,21)(5,15,18)(6,19,12)(7,20,11)
(8,13,14)(9,10,17) ])
gap> StructureDescription(tH);
"C3 x Q8"
```

```
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C3
[ [ 3 ], [ [ 2, 6 ], [ [ 0, 2 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 2, 6 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
138
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> List([tGsHNPfalse,tGsHNPtrue],Length);
[ 132, 6 ]
gap> Collected(List(tGsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C12", 27 ], [ "C2", 9 ], [ "C3", 13 ], [ "C3 x C3", 4 ],
  [ "C3 x Q8", 9 ], [ "C3 x S3", 12 ], [ "C4", 27 ], [ "C6", 9 ],
  [ "Q8", 9 ], [ "S3", 12 ] ]
gap> Collected(List(tGsHNPtrue,StructureDescription));
[ [ "((C3 x C3) : C3) : C2", 1 ], [ "((C3 x C3) : C3) : C4", 3 ],
  [ "((C3 x C3) : C3) : Q8", 1 ], [ "(C3 x C3) : C3", 1 ] ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 18 ], [ "C3", 16 ], [ "C4", 54 ], [ "Q8", 18 ],
  [ "S3", 24 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "(C3 x C3) : C2", 1 ], [ "(C3 x C3) : C4", 3 ], [ "(C3 x C3) : Q8", 1 ],
  [ "C3 x C3", 1 ] ]
```

(3-7) $G = 9T23 \simeq ((C_3)^2 \rtimes Q_8) \rtimes C_3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(9,23); # G=9T23=((C3xC3):Q8):C3
E(9):2A_4
gap> H:=Stabilizer(G,1); # H=SL(2,3)
Group([ (3,4,5)(6,8,7), (2,4,6)(5,9,7) ])
gap> StructureDescription(H);
"SL(2,3)"
gap> FirstObstructionN(G).ker; # Obs1N=1
[ [  ], [ [ 3 ], [  ] ] ]
gap> SchurMultPcpGroup(G); # M(G)=C3: Schur multiplier of G
[ 3 ]
gap> ScG:=SchurCoverG(G);
```

```
rec( SchurCover := Group([ (2,4,5)(3,7,6)(10,22,21)(12,19,24)(15,20,25)
  (17,23,18), (2,5,3,6)(4,8,7,9)(10,23,17,22)(11,12,16,15)(13,18,14,21)
  (19,25,20,24), (1,2,3)(4,10,11)(5,12,13)(6,14,15)(7,16,17)(8,18,19)(9,20,21)
  (22,26,23)(24,27,25) ]), Tid := [ 27, 212 ],
  epi := [ (2,4,5)(3,7,6)(10,22,21)(12,19,24)(15,20,25)(17,23,18),
      (2,5,3,6)(4,8,7,9)(10,23,17,22)(11,12,16,15)(13,18,14,21)(19,25,20,24),
      (1,2,3)(4,10,11)(5,12,13)(6,14,15)(7,16,17)(8,18,19)(9,20,21)(22,26,
        23)(24,27,25) ] -> [ (3,4,5)(6,8,7), (2,8,9,3)(4,6,7,5),
      (1,6,5)(2,7,3)(4,9,8) ] )
gap> StructureDescription(TransitiveGroup(27,212));
"(((C3 x C3) : C3) : Q8) : C3"
gap> tG:=ScG.SchurCover; # tG=G~ is a Schur cover of G
Group([ (2,4,5)(3,7,6)(10,22,21)(12,19,24)(15,20,25)(17,23,18), (2,5,3,6)
(4,8,7,9)(10,23,17,22)(11,12,16,15)(13,18,14,21)(19,25,20,24), (1,2,3)
(4,10,11)(5,12,13)(6,14,15)(7,16,17)(8,18,19)(9,20,21)(22,26,23)(24,27,25) ])
gap> tH:=PreImage(ScG.epi,H); # tH=H~=C3xSL(2,3)
Group([ (1,27,26)(2,15,17)(3,12,10)(4,20,23)(5,25,18)(6,24,21)(7,19,22)
(8,11,14)(9,16,13), (1,26,27)(2,13,19)(3,14,20)(4,18,15)(5,22,11)(6,23,16)
(7,21,12)(8,17,24)(9,10,25), (1,26,27)(2,23,25)(3,22,24)(4,18,15)(5,17,20)
(6,10,19)(7,21,12)(8,14,11)(9,13,16) ])
gap> StructureDescription(tH);
"C3 x SL(2,3)"
gap> FirstObstructionN(tG,tH).ker; # Obs1N~=C3
[ [ 3 ], [ [ 3, 3 ], [ [ 1, 2 ] ] ] ]
gap> FirstObstructionDnr(tG,tH).Dnr; # Obs1Dnr~=1
[ [  ], [ [ 3, 3 ], [  ] ] ]
gap> tGs:=AllSubgroups(tG);;
gap> Length(tGs);
495
gap> tGsHNPfalse:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[]);;
gap> tGsHNPtrue:=Filtered(tGs,x->FirstObstructionDr(tG,x,tH).Dr[1]=[3]);;
gap> List([tGsHNPfalse,tGsHNPtrue],Length);
[ 384, 111 ]
gap> Collected(List(tGsHNPfalse,x->StructureDescription(Image(ScG.epi,x))));
[ [ "1", 2 ], [ "C2", 18 ], [ "C3", 88 ], [ "C4", 54 ], [ "C6", 144 ],
  [ "Q8", 18 ], [ "S3", 24 ], [ "SL(2,3)", 36 ] ]
gap> Collected(List(tGsHNPtrue,x->StructureDescription(Image(ScG.epi,x))));
[ [ "((C3 x C3) : Q8) : C3", 1 ], [ "(C3 x C3) : C2", 1 ],
  [ "(C3 x C3) : C3", 4 ], [ "(C3 x C3) : C4", 3 ], [ "(C3 x C3) : C6", 4 ],
```

```
  [ "(C3 x C3) : Q8", 1 ], [ "C3 x C3", 49 ], [ "C3 x S3", 48 ] ]
```

EXAMPLE 1.48 ($G = 10T7 \simeq A_5$, $G = 10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9) \simeq A_6$ and $G = 10T32 \simeq S_6$).

(4-1) $G = 10T7 \simeq A_5$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(10,7); # G=10T7=A5
A_5(10)
gap> H:=Stabilizer(G,1); # H=S3
Group([ (2,8)(3,6)(4,7)(5,10), (2,10)(3,9)(4,8)(5,7) ])
gap> StructureDescription(H);
"S3"
gap> FirstObstructionN(G).ker; # Obs1N=C2
[ [ 2 ], [ [ 2 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=1
[ [  ], [ [ 2 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
59
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[]);;
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[2]);;
gap> List([GsHNPfalse,GsHNPtrue],Length);
[ 48 , 11 ]
gap> Collected(List(GsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C2", 15 ], [ "C3", 10 ], [ "C5", 6 ], [ "D10", 6 ],
  [ "S3", 10 ] ]
gap> Collected(List(GsHNPtrue,StructureDescription));
[ [ "A4", 5 ], [ "A5", 1 ], [ "C2 x C2", 5 ] ]
```

(4-2) $G = 10T26 \simeq \mathrm{PSL}_2(\mathbb{F}_9) \simeq A_6$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(10,26); # G=10T26=SPL(2,9)=A6
L(10)=PSL(2,9)
gap> H:=Stabilizer(G,1); # H=(C3xC3):C4
Group([ (3,9,6,10)(4,8,5,7), (2,4)(3,7)(6,9)(8,10) ])
gap> StructureDescription(H);
"(C3 x C3) : C4"
gap> FirstObstructionN(G).ker; # Obs1N=C4
```

```
[ [ 4 ], [ [ 4 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # ObsDnr=C2
[ [ 2 ], [ [ 4 ], [ [ 2 ] ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
501
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]<>[4]);;
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[4]);;
gap> List([GsHNPfalse,GsHNPtrue],Length);
[ 425, 76 ]
gap> Collected(List(GsHNPfalse,StructureDescription));
[ [ "(C3 x C3) : C2", 10 ], [ "(C3 x C3) : C4", 10 ], [ "1", 1 ],
  [ "A4", 30 ], [ "A5", 12 ], [ "C2", 45 ], [ "C2 x C2", 30 ],
  [ "C3", 40 ], [ "C3 x C3", 10 ], [ "C4", 45 ], [ "C5", 36 ],
  [ "D10", 36 ], [ "S3", 120 ] ]
gap> Collected(List(GsHNPtrue,StructureDescription));
[ [ "A6", 1 ], [ "D8", 45 ], [ "S4", 30 ] ]
```

(4-3) $G = 10T32 \simeq S_6$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(10,32); # G=10T32=S6
S_6(10)=L(10):2
gap> GeneratorsOfGroup(G);
[ (1,2,10)(3,4,5)(6,7,8), (1,3,2,6)(4,5,8,7), (1,2)(4,7)(5,8)(9,10),
  (3,6)(4,7)(5,8) ]
gap> H:=Stabilizer(G,1); # H=(S3xS3):C2
Group([ (3,6)(4,7)(5,8), (3,10)(6,9)(7,8), (2,4)(3,7)(6,9)(8,10) ])
gap> FirstObstructionN(G).ker; # Obs1N=C2
[ [ 2 ], [ [ 2, 2 ], [ [ 1, 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # Obs1Dnr=1
[ [  ], [ [ 2, 2 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
1455
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[]);;
gap> Length(GsHNPfalse);
1153
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[2]);;
```

```
gap> Length(GsHNPtrue);
302
gap> Collected(List(GsHNPfalse,StructureDescription));
[ [ "(C3 x C3) : C2", 10 ], [ "(C3 x C3) : C4", 10 ],
  [ "(S3 x S3) : C2", 10 ], [ "1", 1 ], [ "A4", 30 ], [ "A5", 12 ],
  [ "C2", 75 ], [ "C2 x C2", 120 ], [ "C3", 40 ], [ "C3 x C3", 10 ],
  [ "C3 x S3", 40 ], [ "C4", 90 ], [ "C5", 36 ], [ "C5 : C4", 36 ],
  [ "C6", 120 ], [ "D10", 36 ], [ "D12", 120 ], [ "D8", 135 ], [ "S3", 160 ],
  [ "S3 x S3", 20 ], [ "S4", 30 ], [ "S5", 12 ] ]
gap> Collected(List(GsHNPtrue,StructureDescription));
[ [ "A6", 1 ], [ "C2 x A4", 30 ], [ "C2 x C2", 45 ], [ "C2 x C2 x C2", 30 ],
  [ "C2 x D8", 45 ], [ "C2 x S4", 30 ], [ "C4 x C2", 45 ], [ "D8", 45 ],
  [ "S4", 30 ], [ "S6", 1 ] ]
gap> GsHNPtrueMin:=Filtered(GsHNPtrue,x->Length(Filtered(GsHNPtrue,
> y->IsSubgroup(x,y)))=1);;
gap> Collected(List(GsHNPtrueMin,StructureDescription));
[ [ "C2 x C2", 45 ], [ "D8", 45 ] ]
gap> GsHNPfalseC2xC2:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsHNPfalseC2xC2);
120
gap> GsHNPtrueC2xC2:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[4,2]);;
gap> Length(GsHNPtrueC2xC2); # there exist 45 minimal true cases
45
gap> Collected(List(GsHNPfalseC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2, 4 ], 3 ], [ [ 2, 2, 4 ], 15 ], [ [ 2, 2, 4, 2 ], 6 ],
  [ [ 2, 4, 2 ], 30 ], [ [ 2, 4, 2, 2 ], 9 ], [ [ 4, 2, 2 ], 45 ],
  [ [ 4, 2, 2, 2 ], 12 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->List(Orbits(x),Length)));
[ [ [ 2, 2, 2, 2, 2 ], 45 ] ]
gap> Collected(List(GsHNPfalseC2xC2,x->Collected(List(x,
> y->List(Orbits(Group(y)),Length)))));
[ [ [ [ [  ], 1 ], [ [ 2, 2, 2 ], 2 ], [ [ 2, 2, 2, 2 ], 1 ] ], 90 ],
  [ [ [ [  ], 1 ], [ [ 2, 2, 2, 2 ], 3 ] ], 30 ] ]
gap> Collected(List(GsHNPtrueC2xC2,x->Collected(List(x,
> y->List(Orbits(Group(y)),Length)))));
[ [ [ [ [  ], 1 ], [ [ 2, 2, 2 ], 2 ], [ [ 2, 2, 2, 2 ], 1 ] ], 45 ] ]
gap> S10:=SymmetricGroup(10);
Sym( [ 1 .. 10 ] )
gap> NS10G:=Normalizer(S10,G);
```

```
Group([ (1,8,4)(2,7,5)(3,9,10), (1,5,8,10)(2,7,9,3), (1,8)(2,3)(4,6)
(7,9), (2,3)(5,10)(7,9), (2,10,7,5)(3,4,9,6) ])
gap> StructureDescription(NS10G);
"(A6 : C2) : C2"
gap> CS10G:=Centralizer(S10,G);
Group(())
gap> StructureDescription(NS10G/CS10G); # Aut(G)=NS10G/CS10G<=S10
"(A6 : C2) : C2"
gap> Collected(List(GsHNPfalseC2xC2,
> x->StructureDescription(Normalizer(NS10G,x))));
[ [ "C2 x D8", 90 ], [ "C2 x S4", 30 ] ]
gap> Collected(List(GsHNPtrueC2xC2,
> x->StructureDescription(Normalizer(NS10G,x))));
[ [ "C8 : (C2 x C2)", 45 ] ]
gap> ChG:=CharacteristicSubgroups(G);
[ Group(()), Group([ (1,8,3)(2,6,4)(5,10,7), (1,10)(2,9)(3,6)(4,7), (1,2)(3,6)
  (4,8)(5,7) ]), S_6(10)=L(10):2 ]
gap> List(ChG,StructureDescription);
[ "1", "A6", "S6" ]
gap> GsHNPfalseD4:=Filtered(GsHNPfalse,x->IdSmallGroup(x)=[8,3]);;
gap> Length(GsHNPfalseD4);
135
gap> GsHNPtrueD4:=Filtered(GsHNPtrue,x->IdSmallGroup(x)=[8,3]);;
gap> Length(GsHNPtrueD4);
45
gap> A6:=DerivedSubgroup(G);
Group([ (1,8,3)(2,6,4)(5,10,7), (1,10)(2,9)(3,6)(4,7), (1,2)(3,6)(4,8)(5,7) ])
gap> Collected(List(GsHNPfalseD4,x->StructureDescription(Intersection(A6,x))));
[ [ "C2 x C2", 90 ], [ "C4", 45 ] ]
gap> Collected(List(GsHNPtrueD4,x->StructureDescription(Intersection(A6,x))));
[ [ "D8", 45 ] ]
```

EXAMPLE 1.49 ($G = 14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$).

(5) $G = 14T30 \simeq \mathrm{PSL}_2(\mathbb{F}_{13})$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(14,30); # G=14T30=PSL(2,13)
L(14)=PSL(2,13)
```

```
gap> H:=Stabilizer(G,1); # H=C13:C6
Group([ (2,12,11,5,9,3)(4,6,7,8,10,13), (2,6)(3,8)(4,13)(5,14)(9,11)(10,12) ])
gap> StructureDescription(H);
"C13 : C6"
gap> FirstObstructionN(G).ker; # Obs1N=C6
[ [ 6 ], [ [ 6 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # ObsDnr=C3
[ [ 3 ], [ [ 6 ], [ [ 2 ] ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
942
gap> GsHNPfalse1:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[]);;
gap> GsHNPfalse2:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[3]);;
gap> GsHNPtrue1:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[2]);;
gap> GsHNPtrue2:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[6]);;
gap> List([GsHNPfalse1,GsHNPfalse2,GsHNPtrue1,GsHNPtrue2],Length);
[ 276, 392, 91, 183 ]
gap> Sum(last);
942
gap> Collected(List(GsHNPfalse1,StructureDescription));
[ [ "1", 1 ], [ "C13", 14 ], [ "C2", 91 ], [ "C7", 78 ], [ "D14", 78 ],
  [ "D26", 14 ] ]
gap> Collected(List(GsHNPfalse2,StructureDescription));
[ [ "C13 : C3", 14 ], [ "C13 : C6", 14 ], [ "C3", 91 ], [ "C6", 91 ],
  [ "S3", 182 ] ]
gap> Collected(List(GsHNPtrue1,StructureDescription));
[ [ "C2 x C2", 91 ] ]
gap> Collected(List(GsHNPtrue2,StructureDescription));
[ [ "A4", 91 ], [ "D12", 91 ], [ "PSL(2,13)", 1 ] ]
```

EXAMPLE 1.50 ($G = 15T9 \simeq (C_5)^2 \rtimes C_3$ and $G = 15T14 \simeq (C_5)^2 \rtimes S_3$).

(6-1) $G = 15T9 \simeq (C_5)^2 \rtimes C_3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(15,9); # G=15T9=(C5xC5):C3
[5^2]3
gap> H:=Stabilizer(G,1); # H=C5
Group([ (2,5,8,11,14)(3,15,12,9,6) ])
```

```
gap> StructureDescription(H);
"C5"
gap> FirstObstructionN(G).ker; # Obs1N=C5
[ [ 5 ], [ [ 5 ], [ [ 1 ] ] ] ]
gap> FirstObstructionDnr(G).Dnr; # ObsDnr=1
[ [  ], [ [ 5 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
34
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[]);;
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[5]);;
gap> List([GsHNPfalse,GsHNPtrue],Length);
[ 32, 2 ]
gap> Collected(List(GsHNPfalse,StructureDescription));
[ [ "1", 1 ], [ "C3", 25 ], [ "C5", 6 ] ]
gap> Collected(List(GsHNPtrue,StructureDescription));
[ [ "(C5 x C5) : C3", 1 ], [ "C5 x C5", 1 ] ]
```

(6-2) $G = 15T14 \simeq (C_5)^2 \rtimes S_3$.

```
gap> Read("HNP.gap");
gap> G:=TransitiveGroup(15,14); # G=15T14=(C5xC5):S3
5^2:2[1/2]S(3)
gap> H:=Stabilizer(G,1); # H=C10
Group([ (2,5,8,11,14)(3,15,12,9,6), (2,12)(3,11)(4,13)(5,9)(6,8)(7,10)(14,15) ])
gap> StructureDescription(H);
"C10"
gap> FirstObstructionN(G).ker; # Obs1N=C5
[ [ 5 ], [ [ 10 ], [ 2 ] ] ]
gap> FirstObstructionDnr(G).Dnr; # ObsDnr=1
[ [  ], [ [ 10 ], [  ] ] ]
gap> Gs:=AllSubgroups(G);;
gap> Length(Gs);
96
gap> GsHNPfalse:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[]);;
gap> GsHNPtrue:=Filtered(Gs,x->FirstObstructionDr(G,x).Dr[1]=[5]);;
gap> List([GsHNPfalse,GsHNPtrue],Length);
[ 90, 6 ]
gap> Collected(List(GsHNPfalse,StructureDescription));
```

```
[ [ "1", 1 ], [ "C10", 15 ], [ "C2", 15 ], [ "C3", 25 ], [ "C5", 6 ],
  [ "D10", 3 ], [ "S3", 25 ] ]
gap> Collected(List(GsHNPtrue,StructureDescription));
[ [ "(C5 x C5) : C3", 1 ], [ "(C5 x C5) : S3", 1 ], [ "C5 x C5", 1 ],
  [ "C5 x D10", 3 ] ]
```

## 7. Application 1: $R$-equivalence in algebraic $k$-tori

DEFINITION 1.51. Let $k$ be a field and $T$ be an algebraic $k$-torus. A exact sequence of algebraic $k$-tori

$$1 \to S \to Q \to T \to 1$$

is called *flabby resolution* of $T$ if

$$0 \to \widehat{T} \to \widehat{Q} \to \widehat{S} \to 0$$

is a flabby resolution of $G$-lattice $\widehat{T}$.

DEFINITION 1.52 (Manin [**Man74**, II. §14]). We say that a rational map of $k$-varieties $f : Z \to X$ *covers a point* $x \in X(k)$ if there exists a point $z \in Z(k)$ such that $f$ is defined at $z$ and $f(z) = x$. Two points $x, y \in X(k)$ are called *$R$-equivalent* if there exist a finite sequence of points $x = x_1, \ldots, x_r = y$ and rational maps $f_i : \mathbb{P}^1 \to X$ $(1 \leq i \leq r-1)$ such that $f_i$ covers $x_i$, $x_{i+1}$.

THEOREM 1.53 (Colliot-Thélène and Sansuc [**CTS77**, Theorem 2, page 199], see also [**Vos98**, Section 17.1]). *Let $k$ be a field, $T$ be an algebraic $k$-torus and $1 \to S \to Q \to T \to 1$ be a flabby resolution of $T$. Then the connecting homomorphism*

$$T(k) \to H^1(k, S)$$

*induces an isomorphism*

$$T(k)/R \simeq H^1(k, S).$$

THEOREM 1.54 (Colliot-Thélène and Sansuc [**CTS77**, Corollary 5, page 201], see also [**Vos98**, Section 17.2]). *Let $k$ be a field and $T$ be an algebraic $k$-torus which splits over finite Galois extension $K$ of $k$ with $G = \mathrm{Gal}(K/k)$. Let $1 \to S \to Q \to T \to 1$ be a flabby resolution of $T$. Then*

(i) *If $k = \mathbb{F}_q$ or a field of cohomological dimension $\mathrm{cd}(k) \leq 1$, then*

$$T(k)/R = 0;$$

(ii) *If $k$ is a local field, then*

$$T(k)/R \simeq H^1(G, \widehat{S})^\vee;$$

(iii) *If $k$ is a global field, then there exists an exact sequence*

$$0 \to Ш^2(G, \widehat{S})^\vee \to T(k)/R \to \quad \text{Ч}^1(G, \widehat{S})^\vee \to 0$$

*where*

$$Ш^2(G, \widehat{S}) = \mathrm{Ker}\{H^2(G, \widehat{S}) \xrightarrow{\mathrm{res}} \bigoplus_{v \in V_k} H^2(G_v, \widehat{S})\},$$
$$\text{Ч}^1(G, \widehat{S}) = \mathrm{Coker}\{H^1(G, \widehat{S}) \xrightarrow{\mathrm{res}} \bigoplus_{v \in V_k} H^1(G_v, \widehat{S})\}.$$

When $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ and $K/k$ is a finite Galois extension, we have $\widehat{T} = J_G$ and $H^1(k, \widehat{S}) \simeq H^3(G, \mathbb{Z})$. Hence Theorem 1.54 can be stated as follows:

THEOREM 1.55 (Colliot-Thélène and Sansuc [**CTS77**, Corollary 1, page 207], see also [**Vos98**, Section 17.2]). *Let $k$ be a field and $K/k$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/k)$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus defined by $K/k$. Then*
(i) *If $k = \mathbb{F}_q$ or a field of cohomological dimension $\mathrm{cd}(k) \leq 1$, then*

$$T(k)/R = 0;$$

(ii) *If $k$ is a local field, then*

$$T(k)/R \simeq H^3(G, \mathbb{Z})^\vee;$$

(iii) *If $k$ is a global field, then there exists an exact sequence*

$$0 \to Ш^4(G, \mathbb{Z})^\vee \to T(k)/R \to \quad \text{Ч}^3(G, \mathbb{Z})^\vee \to 0.$$

When $k$ is a local field, Voskresenskii's theorem ([**Vos67**]), Kunyavskii's theorem (Theorem 1.4), Theorem 1.27 and Theorem 1.28 enable us to get $T(k)/R$ for algebraic $k$-tori $T$ of dimension $\leq 5$. We also refer to Merkurjev [**Mer08**] for algebraic $k$-tori $T$ of dimension 3.

THEOREM 1.56. *Let $k$ be a local field and $T$ be an algebraic $k$-torus of dimension $n \leq 5$. Then*

$$T(k)/R \leq \begin{cases} 0 & (n = 1, 2), \\ \mathbb{Z}/2\mathbb{Z} & (n = 3), \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} & (n = 4, 5) \end{cases}$$

*and* $T(k)/R \simeq H^1(G, [\widehat{T}]^{fl})$ *is given as in Theorem 1.4* ($n = 3$)*, Theorem 1.27* ($n = 4$) *and Theorem 1.28* ($n = 5$).

Also, Theorem 1.15 enables us to obtain $T(k)/R \simeq H^1(k, \operatorname{Pic}\overline{X}) \simeq H^1(G, [J_{G/H}]^{fl})$ for norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ where $k$ is a local field and $[K : k] = n \leq 15$ and $n \neq 12$.

THEOREM 1.57. *Let* $2 \leq n \leq 15$ *be an integer with* $n \neq 12$*. Let* $k$ *be a local field,* $K/k$ *be a separable field extension of degree* $n$ *and* $L/k$ *be the Galois closure of* $K/k$*. Assume that* $G = \operatorname{Gal}(L/k) = nTm$ *is a transitive subgroup of* $S_n$ *and* $H = \operatorname{Gal}(L/K)$ *with* $[G : H] = n$*. Let* $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ *be the norm one torus of* $K/k$ *of dimension* $n - 1$*. Then*

$$T(k)/R \simeq H^1(G, [J_{G/H}]^{fl}) \leq \begin{cases} 0 & (n = 2, 3, 5, 7, 11, 13) \\ \mathbb{Z}/2\mathbb{Z} & (n = 4, 6, 10, 14), \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 3} & (n = 8), \\ \mathbb{Z}/3\mathbb{Z} & (n = 9), \\ \mathbb{Z}/5\mathbb{Z} & (n = 15) \end{cases}$$

*and* $T(k)/R \neq 0$ *if and only if* $G$ *is given as in Table* 1*.*

## 8. Application 2: Tamagawa number $\tau(T)$

By Theorem 1.18, we obtain the Tamagawa number $\tau(T)$ of algebraic $k$-tori $T$ (see Ono [**Ono63**], [**Ono65**] and Voskresenskii [**Vos98**, Chapter 5]).

THEOREM 1.58 (Ono [**Ono63**, Main theorem, page 68], see also [**Vos98**, Theorem 2, page 146]). *Let* $k$ *be a global field,* $T$ *be an algebraic* $k$*-torus and* $\tau(T)$ *be the Tamagawa number of* $T$*. Then*

$$\tau(T) = \frac{|H^1(k, \widehat{T})|}{|Ш(T)|}.$$

*In particular, if* $T$ *is retract* $k$*-rational, then* $\tau(T) = |H^1(k, \widehat{T})|$*.*

For the last assertion, see Theorem 1.26. As a consequence of Theorem 1.1, Theorem 1.27 and Theorem 1.28 (Theorem 1.5 and Theorem 1.6), we have:

THEOREM 1.59. *Let* $k$ *be a global field and* $T$ *be an algebraic* $k$*-torus of dimension* 4 (*resp.* 5)*. Among* 710 (*reps.* 6079) *cases of algebraic* $k$*-tori* $T$*, if* $T$ *is one of the* 688 (*resp.* 5805) *cases with* $H^1(k, \operatorname{Pic}\overline{X}) = 0$*, then* $\tau(T) = |H^1(k, \widehat{T})|$*.*

When $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ and $K/k$ is a finite Galois extension, i.e. $\widehat{T} = J_G$, it follows from Endo and Miyata [**EM75**, Theorem 1.5] that if all the Sylow subgroups of $G = \mathrm{Gal}(K/k)$ are cyclic, then $|Ш(T)| = 1$ and hence $\tau(T) = |H^1(G, J_G)| = |H^2(G, \mathbb{Z})| = |H^1(G, \mathbb{Q}/\mathbb{Z})| = |G^{ab}|$. For norm one tori $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ with $[K : k] = n \leq 15$ and $n \neq 12$, Kunyavskii's theorem (Theorem 1.13), Drakokhrust and Platonov's theorem (Theorem 1.14) and Theorem 1.18 enable us to get the Tamagawa number $\tau(T)$:

THEOREM 1.60. *Let $2 \leq n \leq 15$ be an integer with $n \neq 12$. Let $k$ be a number field, $K/k$ be a field extension of degree $n$ and $L/k$ be the Galois closure of $K/k$. Assume that $G = \mathrm{Gal}(L/k) = nTm$ is a transitive subgroup of $S_n$ and $H = \mathrm{Gal}(L/K)$ with $[G : H] = n$. Let $T = R^{(1)}_{K/k}(\mathbb{G}_m)$ be the norm one torus of $K/k$ of dimension $n-1$. Then $\tau(T) = |H^1(G, J_{G/H})|$ except for the cases in Table* 1. *For the cases in Table* 1, *we have $\tau(T) = |H^1(G, J_{G/H})|/|Ш(T)|$ where $H^1(G, J_{G/H})$ is given as in Section 9 and $Ш(T)$ is given as in Theorem 1.18.*

We give GAP computations of $H^1(G, J_{G/H})$ for $G = \mathrm{Gal}(L/k) = nTm$ $(n \leq 15)$ in Section 9 as the appendix of this chapter.

## 9. Appendix: Computation of $H^1(G, J_{G/H})$ for $G = \mathrm{Gal}(L/k) = nTm$ $(n \leq 15)$

```
gap> Read("FlabbyResolutionFromBase.gap");
gap> for n in [2..15] do for m in [1..NrTransitiveGroups(n)] do
> Print([[n,m],Filtered(H1(Norm1TorusJ(n,m)),x->x>1)],"\n");od;Print("\n");od;
[ [ 2, 1 ], [ 2 ] ]

[ [ 3, 1 ], [ 3 ] ]
[ [ 3, 2 ], [  ] ]

[ [ 4, 1 ], [ 4 ] ]
[ [ 4, 2 ], [ 2, 2 ] ]
[ [ 4, 3 ], [ 2 ] ]
[ [ 4, 4 ], [  ] ]
[ [ 4, 5 ], [  ] ]

[ [ 5, 1 ], [ 5 ] ]
[ [ 5, 2 ], [  ] ]
[ [ 5, 3 ], [  ] ]
[ [ 5, 4 ], [  ] ]
```

```
[ [ 5, 5 ], [  ] ]

[ [ 6, 1 ], [ 6 ] ]
[ [ 6, 2 ], [ 2 ] ]
[ [ 6, 3 ], [ 2 ] ]
[ [ 6, 4 ], [ 3 ] ]
[ [ 6, 5 ], [ 2 ] ]
[ [ 6, 6 ], [ 3 ] ]
[ [ 6, 7 ], [  ] ]
[ [ 6, 8 ], [  ] ]
[ [ 6, 9 ], [ 2 ] ]
[ [ 6, 10 ], [ 2 ] ]
[ [ 6, 11 ], [  ] ]
[ [ 6, 12 ], [  ] ]
[ [ 6, 13 ], [ 2 ] ]
[ [ 6, 14 ], [  ] ]
[ [ 6, 15 ], [  ] ]
[ [ 6, 16 ], [  ] ]

[ [ 7, 1 ], [ 7 ] ]
[ [ 7, 2 ], [  ] ]
[ [ 7, 3 ], [  ] ]
[ [ 7, 4 ], [  ] ]
[ [ 7, 5 ], [  ] ]
[ [ 7, 6 ], [  ] ]
[ [ 7, 7 ], [  ] ]

[ [ 8, 1 ], [ 8 ] ]
[ [ 8, 2 ], [ 2, 4 ] ]
[ [ 8, 3 ], [ 2, 2, 2 ] ]
[ [ 8, 4 ], [ 2, 2 ] ]
[ [ 8, 5 ], [ 2, 2 ] ]
[ [ 8, 6 ], [ 2 ] ]
[ [ 8, 7 ], [ 4 ] ]
[ [ 8, 8 ], [ 2 ] ]
[ [ 8, 9 ], [ 2, 2 ] ]
[ [ 8, 10 ], [ 4 ] ]
[ [ 8, 11 ], [ 2, 2 ] ]
[ [ 8, 12 ], [  ] ]
```

```
[ [ 8, 13 ], [ 2 ] ]
[ [ 8, 14 ], [ 2 ] ]
[ [ 8, 15 ], [ 2 ] ]
[ [ 8, 16 ], [ 4 ] ]
[ [ 8, 17 ], [ 2 ] ]
[ [ 8, 18 ], [ 2 ] ]
[ [ 8, 19 ], [ 2 ] ]
[ [ 8, 20 ], [ 4 ] ]
[ [ 8, 21 ], [ 2, 2 ] ]
[ [ 8, 22 ], [ 2, 2 ] ]
[ [ 8, 23 ], [  ] ]
[ [ 8, 24 ], [ 2 ] ]
[ [ 8, 25 ], [  ] ]
[ [ 8, 26 ], [ 2 ] ]
[ [ 8, 27 ], [ 4 ] ]
[ [ 8, 28 ], [ 2 ] ]
[ [ 8, 29 ], [ 2 ] ]
[ [ 8, 30 ], [ 2 ] ]
[ [ 8, 31 ], [ 2, 2 ] ]
[ [ 8, 32 ], [  ] ]
[ [ 8, 33 ], [ 2 ] ]
[ [ 8, 34 ], [ 2 ] ]
[ [ 8, 35 ], [ 2 ] ]
[ [ 8, 36 ], [  ] ]
[ [ 8, 37 ], [  ] ]
[ [ 8, 38 ], [  ] ]
[ [ 8, 39 ], [  ] ]
[ [ 8, 40 ], [  ] ]
[ [ 8, 41 ], [ 2 ] ]
[ [ 8, 42 ], [ 2 ] ]
[ [ 8, 43 ], [  ] ]
[ [ 8, 44 ], [  ] ]
[ [ 8, 45 ], [ 2 ] ]
[ [ 8, 46 ], [ 2 ] ]
[ [ 8, 47 ], [ 2 ] ]
[ [ 8, 48 ], [  ] ]
[ [ 8, 49 ], [  ] ]
[ [ 8, 50 ], [  ] ]
```

```
[ [ 9, 1 ], [ 9 ] ]
[ [ 9, 2 ], [ 3, 3 ] ]
[ [ 9, 3 ], [  ] ]
[ [ 9, 4 ], [ 3 ] ]
[ [ 9, 5 ], [  ] ]
[ [ 9, 6 ], [ 3 ] ]
[ [ 9, 7 ], [ 3 ] ]
[ [ 9, 8 ], [  ] ]
[ [ 9, 9 ], [  ] ]
[ [ 9, 10 ], [  ] ]
[ [ 9, 11 ], [  ] ]
[ [ 9, 12 ], [  ] ]
[ [ 9, 13 ], [ 3 ] ]
[ [ 9, 14 ], [  ] ]
[ [ 9, 15 ], [  ] ]
[ [ 9, 16 ], [  ] ]
[ [ 9, 17 ], [ 3 ] ]
[ [ 9, 18 ], [  ] ]
[ [ 9, 19 ], [  ] ]
[ [ 9, 20 ], [  ] ]
[ [ 9, 21 ], [  ] ]
[ [ 9, 22 ], [ 3 ] ]
[ [ 9, 23 ], [  ] ]
[ [ 9, 24 ], [  ] ]
[ [ 9, 25 ], [ 3 ] ]
[ [ 9, 26 ], [  ] ]
[ [ 9, 27 ], [  ] ]
[ [ 9, 28 ], [ 3 ] ]
[ [ 9, 29 ], [  ] ]
[ [ 9, 30 ], [  ] ]
[ [ 9, 31 ], [  ] ]
[ [ 9, 32 ], [  ] ]
[ [ 9, 33 ], [  ] ]
[ [ 9, 34 ], [  ] ]

[ [ 10, 1 ], [ 10 ] ]
[ [ 10, 2 ], [ 2 ] ]
[ [ 10, 3 ], [ 2 ] ]
[ [ 10, 4 ], [ 2 ] ]
```

[ [ 10, 5 ], [ 2 ] ]
[ [ 10, 6 ], [ 2 ] ]
[ [ 10, 7 ], [  ] ]
[ [ 10, 8 ], [ 5 ] ]
[ [ 10, 9 ], [ 2 ] ]
[ [ 10, 10 ], [ 2 ] ]
[ [ 10, 11 ], [ 2 ] ]
[ [ 10, 12 ], [ 2 ] ]
[ [ 10, 13 ], [  ] ]
[ [ 10, 14 ], [ 5 ] ]
[ [ 10, 15 ], [  ] ]
[ [ 10, 16 ], [  ] ]
[ [ 10, 17 ], [ 2 ] ]
[ [ 10, 18 ], [ 2 ] ]
[ [ 10, 19 ], [ 2 ] ]
[ [ 10, 20 ], [ 2 ] ]
[ [ 10, 21 ], [ 2 ] ]
[ [ 10, 22 ], [ 2 ] ]
[ [ 10, 23 ], [  ] ]
[ [ 10, 24 ], [  ] ]
[ [ 10, 25 ], [  ] ]
[ [ 10, 26 ], [  ] ]
[ [ 10, 27 ], [ 2 ] ]
[ [ 10, 28 ], [ 2 ] ]
[ [ 10, 29 ], [  ] ]
[ [ 10, 30 ], [  ] ]
[ [ 10, 31 ], [  ] ]
[ [ 10, 32 ], [  ] ]
[ [ 10, 33 ], [ 2 ] ]
[ [ 10, 34 ], [  ] ]
[ [ 10, 35 ], [  ] ]
[ [ 10, 36 ], [  ] ]
[ [ 10, 37 ], [  ] ]
[ [ 10, 38 ], [  ] ]
[ [ 10, 39 ], [  ] ]
[ [ 10, 40 ], [ 2 ] ]
[ [ 10, 41 ], [ 2 ] ]
[ [ 10, 42 ], [ 2 ] ]
[ [ 10, 43 ], [ 2 ] ]

```
[ [ 10, 44 ], [  ] ]
[ [ 10, 45 ], [  ] ]

[ [ 11, 1 ], [ 11 ] ]
[ [ 11, 2 ], [  ] ]
[ [ 11, 3 ], [  ] ]
[ [ 11, 4 ], [  ] ]
[ [ 11, 5 ], [  ] ]
[ [ 11, 6 ], [  ] ]
[ [ 11, 7 ], [  ] ]
[ [ 11, 8 ], [  ] ]

[ [ 12, 1 ], [ 12 ] ]
[ [ 12, 2 ], [ 2, 6 ] ]
[ [ 12, 3 ], [ 2, 2 ] ]
[ [ 12, 4 ], [ 3 ] ]
[ [ 12, 5 ], [ 4 ] ]
[ [ 12, 6 ], [ 3 ] ]
[ [ 12, 7 ], [ 6 ] ]
[ [ 12, 8 ], [  ] ]
[ [ 12, 9 ], [ 2 ] ]
[ [ 12, 10 ], [ 2, 2 ] ]
[ [ 12, 11 ], [ 4 ] ]
[ [ 12, 12 ], [ 2 ] ]
[ [ 12, 13 ], [ 2 ] ]
[ [ 12, 14 ], [ 6 ] ]
[ [ 12, 15 ], [ 2 ] ]
[ [ 12, 16 ], [ 2, 2 ] ]
[ [ 12, 17 ], [ 4 ] ]
[ [ 12, 18 ], [ 2, 2 ] ]
[ [ 12, 19 ], [ 4 ] ]
[ [ 12, 20 ], [ 3 ] ]
[ [ 12, 21 ], [ 2 ] ]
[ [ 12, 22 ], [  ] ]
[ [ 12, 23 ], [ 2 ] ]
[ [ 12, 24 ], [ 2 ] ]
[ [ 12, 25 ], [ 6 ] ]
[ [ 12, 26 ], [ 3 ] ]
[ [ 12, 27 ], [  ] ]
```

[ [ 12, 28 ], [ 2 ] ]
[ [ 12, 29 ], [ 6 ] ]
[ [ 12, 30 ], [ 2 ] ]
[ [ 12, 31 ], [ 3 ] ]
[ [ 12, 32 ], [ 3 ] ]
[ [ 12, 33 ], [  ] ]
[ [ 12, 34 ], [ 2, 2 ] ]
[ [ 12, 35 ], [ 2 ] ]
[ [ 12, 36 ], [ 2 ] ]
[ [ 12, 37 ], [ 2, 2 ] ]
[ [ 12, 38 ], [ 2 ] ]
[ [ 12, 39 ], [ 4 ] ]
[ [ 12, 40 ], [ 2, 2 ] ]
[ [ 12, 41 ], [ 4 ] ]
[ [ 12, 42 ], [ 2 ] ]
[ [ 12, 43 ], [  ] ]
[ [ 12, 44 ], [  ] ]
[ [ 12, 45 ], [ 3 ] ]
[ [ 12, 46 ], [ 4 ] ]
[ [ 12, 47 ], [ 2, 2 ] ]
[ [ 12, 48 ], [ 2 ] ]
[ [ 12, 49 ], [  ] ]
[ [ 12, 50 ], [ 2 ] ]
[ [ 12, 51 ], [ 6 ] ]
[ [ 12, 52 ], [ 2 ] ]
[ [ 12, 53 ], [ 2 ] ]
[ [ 12, 54 ], [ 2 ] ]
[ [ 12, 55 ], [ 3 ] ]
[ [ 12, 56 ], [ 3 ] ]
[ [ 12, 57 ], [ 3 ] ]
[ [ 12, 58 ], [ 6 ] ]
[ [ 12, 59 ], [ 3 ] ]
[ [ 12, 60 ], [ 3 ] ]
[ [ 12, 61 ], [ 3 ] ]
[ [ 12, 62 ], [  ] ]
[ [ 12, 63 ], [  ] ]
[ [ 12, 64 ], [  ] ]
[ [ 12, 65 ], [  ] ]
[ [ 12, 66 ], [  ] ]

```
[ [ 12, 67 ], [  ] ]
[ [ 12, 68 ], [  ] ]
[ [ 12, 69 ], [ 2 ] ]
[ [ 12, 70 ], [ 2, 2 ] ]
[ [ 12, 71 ], [ 2, 2 ] ]
[ [ 12, 72 ], [ 4 ] ]
[ [ 12, 73 ], [ 4 ] ]
[ [ 12, 74 ], [ 2 ] ]
[ [ 12, 75 ], [ 2 ] ]
[ [ 12, 76 ], [  ] ]
[ [ 12, 77 ], [ 2, 2 ] ]
[ [ 12, 78 ], [ 2 ] ]
[ [ 12, 79 ], [ 4 ] ]
[ [ 12, 80 ], [ 2 ] ]
[ [ 12, 81 ], [ 2 ] ]
[ [ 12, 82 ], [ 2 ] ]
[ [ 12, 83 ], [  ] ]
[ [ 12, 84 ], [ 2 ] ]
[ [ 12, 85 ], [ 3 ] ]
[ [ 12, 86 ], [ 2 ] ]
[ [ 12, 87 ], [ 6 ] ]
[ [ 12, 88 ], [ 3 ] ]
[ [ 12, 89 ], [ 3 ] ]
[ [ 12, 90 ], [ 3 ] ]
[ [ 12, 91 ], [ 3 ] ]
[ [ 12, 92 ], [ 3 ] ]
[ [ 12, 93 ], [ 3 ] ]
[ [ 12, 94 ], [ 3 ] ]
[ [ 12, 95 ], [  ] ]
[ [ 12, 96 ], [  ] ]
[ [ 12, 97 ], [  ] ]
[ [ 12, 98 ], [  ] ]
[ [ 12, 99 ], [ 3 ] ]
[ [ 12, 100 ], [  ] ]
[ [ 12, 101 ], [  ] ]
[ [ 12, 102 ], [  ] ]
[ [ 12, 103 ], [  ] ]
[ [ 12, 104 ], [ 3 ] ]
[ [ 12, 105 ], [ 6 ] ]
```

[ [ 12, 106 ], [ 2 ] ]
[ [ 12, 107 ], [ 2 ] ]
[ [ 12, 108 ], [ 2 ] ]
[ [ 12, 109 ], [ 2 ] ]
[ [ 12, 110 ], [  ] ]
[ [ 12, 111 ], [  ] ]
[ [ 12, 112 ], [  ] ]
[ [ 12, 113 ], [  ] ]
[ [ 12, 114 ], [  ] ]
[ [ 12, 115 ], [  ] ]
[ [ 12, 116 ], [ 2 ] ]
[ [ 12, 117 ], [ 2, 2 ] ]
[ [ 12, 118 ], [ 2 ] ]
[ [ 12, 119 ], [ 4 ] ]
[ [ 12, 120 ], [ 2 ] ]
[ [ 12, 121 ], [ 2 ] ]
[ [ 12, 122 ], [  ] ]
[ [ 12, 123 ], [ 2 ] ]
[ [ 12, 124 ], [  ] ]
[ [ 12, 125 ], [ 2 ] ]
[ [ 12, 126 ], [ 2 ] ]
[ [ 12, 127 ], [  ] ]
[ [ 12, 128 ], [  ] ]
[ [ 12, 129 ], [ 3 ] ]
[ [ 12, 130 ], [ 2, 2 ] ]
[ [ 12, 131 ], [ 4 ] ]
[ [ 12, 132 ], [  ] ]
[ [ 12, 133 ], [  ] ]
[ [ 12, 134 ], [ 6 ] ]
[ [ 12, 135 ], [ 2 ] ]
[ [ 12, 136 ], [ 2 ] ]
[ [ 12, 137 ], [  ] ]
[ [ 12, 138 ], [  ] ]
[ [ 12, 139 ], [  ] ]
[ [ 12, 140 ], [  ] ]
[ [ 12, 141 ], [ 3 ] ]
[ [ 12, 142 ], [ 3 ] ]
[ [ 12, 143 ], [ 3 ] ]
[ [ 12, 144 ], [ 3 ] ]

```
[ [ 12, 145 ], [ 2 ] ]
[ [ 12, 146 ], [  ] ]
[ [ 12, 147 ], [  ] ]
[ [ 12, 148 ], [  ] ]
[ [ 12, 149 ], [  ] ]
[ [ 12, 150 ], [  ] ]
[ [ 12, 151 ], [  ] ]
[ [ 12, 152 ], [  ] ]
[ [ 12, 153 ], [  ] ]
[ [ 12, 154 ], [ 2 ] ]
[ [ 12, 155 ], [ 2 ] ]
[ [ 12, 156 ], [ 2 ] ]
[ [ 12, 157 ], [  ] ]
[ [ 12, 158 ], [ 2 ] ]
[ [ 12, 159 ], [ 2 ] ]
[ [ 12, 160 ], [ 2 ] ]
[ [ 12, 161 ], [ 2 ] ]
[ [ 12, 162 ], [ 2 ] ]
[ [ 12, 163 ], [ 2 ] ]
[ [ 12, 164 ], [ 3 ] ]
[ [ 12, 165 ], [  ] ]
[ [ 12, 166 ], [ 3 ] ]
[ [ 12, 167 ], [ 2 ] ]
[ [ 12, 168 ], [ 2, 2 ] ]
[ [ 12, 169 ], [ 2 ] ]
[ [ 12, 170 ], [ 4 ] ]
[ [ 12, 171 ], [ 2, 2 ] ]
[ [ 12, 172 ], [ 2, 2 ] ]
[ [ 12, 173 ], [ 4 ] ]
[ [ 12, 174 ], [ 2, 2 ] ]
[ [ 12, 175 ], [  ] ]
[ [ 12, 176 ], [  ] ]
[ [ 12, 177 ], [  ] ]
[ [ 12, 178 ], [  ] ]
[ [ 12, 179 ], [  ] ]
[ [ 12, 180 ], [ 2 ] ]
[ [ 12, 181 ], [ 2 ] ]
[ [ 12, 182 ], [ 2 ] ]
[ [ 12, 183 ], [ 2 ] ]
```

[ [ 12, 184 ], [  ] ]
[ [ 12, 185 ], [  ] ]
[ [ 12, 186 ], [  ] ]
[ [ 12, 187 ], [ 3 ] ]
[ [ 12, 188 ], [ 3 ] ]
[ [ 12, 189 ], [ 3 ] ]
[ [ 12, 190 ], [  ] ]
[ [ 12, 191 ], [  ] ]
[ [ 12, 192 ], [  ] ]
[ [ 12, 193 ], [ 2 ] ]
[ [ 12, 194 ], [  ] ]
[ [ 12, 195 ], [ 2 ] ]
[ [ 12, 196 ], [ 2 ] ]
[ [ 12, 197 ], [ 2 ] ]
[ [ 12, 198 ], [ 2 ] ]
[ [ 12, 199 ], [ 2 ] ]
[ [ 12, 200 ], [ 2 ] ]
[ [ 12, 201 ], [ 2 ] ]
[ [ 12, 202 ], [ 2 ] ]
[ [ 12, 203 ], [ 2 ] ]
[ [ 12, 204 ], [  ] ]
[ [ 12, 205 ], [ 3 ] ]
[ [ 12, 206 ], [  ] ]
[ [ 12, 207 ], [  ] ]
[ [ 12, 208 ], [ 2 ] ]
[ [ 12, 209 ], [ 2 ] ]
[ [ 12, 210 ], [ 2, 2 ] ]
[ [ 12, 211 ], [ 4 ] ]
[ [ 12, 212 ], [ 2 ] ]
[ [ 12, 213 ], [  ] ]
[ [ 12, 214 ], [ 2, 2 ] ]
[ [ 12, 215 ], [ 4 ] ]
[ [ 12, 216 ], [ 2 ] ]
[ [ 12, 217 ], [ 2 ] ]
[ [ 12, 218 ], [  ] ]
[ [ 12, 219 ], [ 2 ] ]
[ [ 12, 220 ], [ 2 ] ]
[ [ 12, 221 ], [  ] ]
[ [ 12, 222 ], [ 3 ] ]

[ [ 12, 223 ], [  ] ]
[ [ 12, 224 ], [  ] ]
[ [ 12, 225 ], [  ] ]
[ [ 12, 226 ], [  ] ]
[ [ 12, 227 ], [  ] ]
[ [ 12, 228 ], [ 3 ] ]
[ [ 12, 229 ], [ 3 ] ]
[ [ 12, 230 ], [  ] ]
[ [ 12, 231 ], [  ] ]
[ [ 12, 232 ], [  ] ]
[ [ 12, 233 ], [  ] ]
[ [ 12, 234 ], [  ] ]
[ [ 12, 235 ], [ 2 ] ]
[ [ 12, 236 ], [ 2 ] ]
[ [ 12, 237 ], [ 2 ] ]
[ [ 12, 238 ], [ 2 ] ]
[ [ 12, 239 ], [  ] ]
[ [ 12, 240 ], [ 2 ] ]
[ [ 12, 241 ], [ 2 ] ]
[ [ 12, 242 ], [ 2, 2 ] ]
[ [ 12, 243 ], [ 2 ] ]
[ [ 12, 244 ], [ 4 ] ]
[ [ 12, 245 ], [ 4 ] ]
[ [ 12, 246 ], [ 2, 2 ] ]
[ [ 12, 247 ], [ 2 ] ]
[ [ 12, 248 ], [ 2 ] ]
[ [ 12, 249 ], [ 2 ] ]
[ [ 12, 250 ], [  ] ]
[ [ 12, 251 ], [  ] ]
[ [ 12, 252 ], [  ] ]
[ [ 12, 253 ], [ 3 ] ]
[ [ 12, 254 ], [  ] ]
[ [ 12, 255 ], [  ] ]
[ [ 12, 256 ], [  ] ]
[ [ 12, 257 ], [  ] ]
[ [ 12, 258 ], [  ] ]
[ [ 12, 259 ], [  ] ]
[ [ 12, 260 ], [ 2 ] ]
[ [ 12, 261 ], [ 2, 2 ] ]

[ [ 12, 262 ], [ 2 ] ]
[ [ 12, 263 ], [ 2 ] ]
[ [ 12, 264 ], [ 4 ] ]
[ [ 12, 265 ], [ 3 ] ]
[ [ 12, 266 ], [ 2 ] ]
[ [ 12, 267 ], [ 2 ] ]
[ [ 12, 268 ], [  ] ]
[ [ 12, 269 ], [ 2 ] ]
[ [ 12, 270 ], [  ] ]
[ [ 12, 271 ], [  ] ]
[ [ 12, 272 ], [  ] ]
[ [ 12, 273 ], [ 3 ] ]
[ [ 12, 274 ], [ 2 ] ]
[ [ 12, 275 ], [  ] ]
[ [ 12, 276 ], [  ] ]
[ [ 12, 277 ], [  ] ]
[ [ 12, 278 ], [ 2 ] ]
[ [ 12, 279 ], [ 2 ] ]
[ [ 12, 280 ], [  ] ]
[ [ 12, 281 ], [  ] ]
[ [ 12, 282 ], [  ] ]
[ [ 12, 283 ], [  ] ]
[ [ 12, 284 ], [ 3 ] ]
[ [ 12, 285 ], [  ] ]
[ [ 12, 286 ], [  ] ]
[ [ 12, 287 ], [  ] ]
[ [ 12, 288 ], [ 2 ] ]
[ [ 12, 289 ], [  ] ]
[ [ 12, 290 ], [  ] ]
[ [ 12, 291 ], [  ] ]
[ [ 12, 292 ], [ 3 ] ]
[ [ 12, 293 ], [  ] ]
[ [ 12, 294 ], [  ] ]
[ [ 12, 295 ], [  ] ]
[ [ 12, 296 ], [ 2 ] ]
[ [ 12, 297 ], [ 2 ] ]
[ [ 12, 298 ], [ 2 ] ]
[ [ 12, 299 ], [ 2 ] ]
[ [ 12, 300 ], [  ] ]

```
[ [ 12, 301 ], [  ] ]

[ [ 13, 1 ], [ 13 ] ]
[ [ 13, 2 ], [  ] ]
[ [ 13, 3 ], [  ] ]
[ [ 13, 4 ], [  ] ]
[ [ 13, 5 ], [  ] ]
[ [ 13, 6 ], [  ] ]
[ [ 13, 7 ], [  ] ]
[ [ 13, 8 ], [  ] ]
[ [ 13, 9 ], [  ] ]

[ [ 14, 1 ], [ 14 ] ]
[ [ 14, 2 ], [ 2 ] ]
[ [ 14, 3 ], [ 2 ] ]
[ [ 14, 4 ], [ 2 ] ]
[ [ 14, 5 ], [ 2 ] ]
[ [ 14, 6 ], [ 7 ] ]
[ [ 14, 7 ], [ 2 ] ]
[ [ 14, 8 ], [ 2 ] ]
[ [ 14, 9 ], [ 7 ] ]
[ [ 14, 10 ], [  ] ]
[ [ 14, 11 ], [  ] ]
[ [ 14, 12 ], [ 2 ] ]
[ [ 14, 13 ], [ 2 ] ]
[ [ 14, 14 ], [ 2 ] ]
[ [ 14, 15 ], [ 2 ] ]
[ [ 14, 16 ], [ 2 ] ]
[ [ 14, 17 ], [  ] ]
[ [ 14, 18 ], [  ] ]
[ [ 14, 19 ], [ 2 ] ]
[ [ 14, 20 ], [ 2 ] ]
[ [ 14, 21 ], [ 7 ] ]
[ [ 14, 22 ], [ 2 ] ]
[ [ 14, 23 ], [ 2 ] ]
[ [ 14, 24 ], [ 2 ] ]
[ [ 14, 25 ], [ 2 ] ]
[ [ 14, 26 ], [ 2 ] ]
[ [ 14, 27 ], [  ] ]
```

```
[ [ 14, 28 ], [  ] ]
[ [ 14, 29 ], [ 7 ] ]
[ [ 14, 30 ], [  ] ]
[ [ 14, 31 ], [ 2 ] ]
[ [ 14, 32 ], [ 2 ] ]
[ [ 14, 33 ], [  ] ]
[ [ 14, 34 ], [  ] ]
[ [ 14, 35 ], [  ] ]
[ [ 14, 36 ], [ 2 ] ]
[ [ 14, 37 ], [ 2 ] ]
[ [ 14, 38 ], [  ] ]
[ [ 14, 39 ], [  ] ]
[ [ 14, 40 ], [  ] ]
[ [ 14, 41 ], [  ] ]
[ [ 14, 42 ], [  ] ]
[ [ 14, 43 ], [  ] ]
[ [ 14, 44 ], [  ] ]
[ [ 14, 45 ], [ 2 ] ]
[ [ 14, 46 ], [ 2 ] ]
[ [ 14, 47 ], [ 2 ] ]
[ [ 14, 48 ], [  ] ]
[ [ 14, 49 ], [ 2 ] ]
[ [ 14, 50 ], [  ] ]
[ [ 14, 51 ], [  ] ]
[ [ 14, 52 ], [ 2 ] ]
[ [ 14, 53 ], [  ] ]
[ [ 14, 54 ], [  ] ]
[ [ 14, 55 ], [  ] ]
[ [ 14, 56 ], [  ] ]
[ [ 14, 57 ], [  ] ]
[ [ 14, 58 ], [ 2 ] ]
[ [ 14, 59 ], [ 2 ] ]
[ [ 14, 60 ], [ 2 ] ]
[ [ 14, 61 ], [ 2 ] ]
[ [ 14, 62 ], [  ] ]
[ [ 14, 63 ], [  ] ]

[ [ 15, 1 ], [ 15 ] ]
[ [ 15, 2 ], [  ] ]
```

```
[ [ 15, 3 ], [ 3 ] ]
[ [ 15, 4 ], [ 5 ] ]
[ [ 15, 5 ], [  ] ]
[ [ 15, 6 ], [  ] ]
[ [ 15, 7 ], [  ] ]
[ [ 15, 8 ], [ 3 ] ]
[ [ 15, 9 ], [ 3 ] ]
[ [ 15, 10 ], [  ] ]
[ [ 15, 11 ], [  ] ]
[ [ 15, 12 ], [ 3 ] ]
[ [ 15, 13 ], [  ] ]
[ [ 15, 14 ], [  ] ]
[ [ 15, 15 ], [  ] ]
[ [ 15, 16 ], [ 3 ] ]
[ [ 15, 17 ], [  ] ]
[ [ 15, 18 ], [  ] ]
[ [ 15, 19 ], [ 3 ] ]
[ [ 15, 20 ], [  ] ]
[ [ 15, 21 ], [  ] ]
[ [ 15, 22 ], [  ] ]
[ [ 15, 23 ], [  ] ]
[ [ 15, 24 ], [ 3 ] ]
[ [ 15, 25 ], [ 3 ] ]
[ [ 15, 26 ], [ 5 ] ]
[ [ 15, 27 ], [  ] ]
[ [ 15, 28 ], [  ] ]
[ [ 15, 29 ], [  ] ]
[ [ 15, 30 ], [ 3 ] ]
[ [ 15, 31 ], [  ] ]
[ [ 15, 32 ], [  ] ]
[ [ 15, 33 ], [ 5 ] ]
[ [ 15, 34 ], [  ] ]
[ [ 15, 35 ], [  ] ]
[ [ 15, 36 ], [ 5 ] ]
[ [ 15, 37 ], [  ] ]
[ [ 15, 38 ], [ 3 ] ]
[ [ 15, 39 ], [ 3 ] ]
[ [ 15, 40 ], [  ] ]
[ [ 15, 41 ], [  ] ]
```

[ [ 15, 42 ], [  ] ]
[ [ 15, 43 ], [  ] ]
[ [ 15, 44 ], [ 5 ] ]
[ [ 15, 45 ], [  ] ]
[ [ 15, 46 ], [  ] ]
[ [ 15, 47 ], [  ] ]
[ [ 15, 48 ], [  ] ]
[ [ 15, 49 ], [  ] ]
[ [ 15, 50 ], [ 3 ] ]
[ [ 15, 51 ], [  ] ]
[ [ 15, 52 ], [  ] ]
[ [ 15, 53 ], [  ] ]
[ [ 15, 54 ], [  ] ]
[ [ 15, 55 ], [  ] ]
[ [ 15, 56 ], [  ] ]
[ [ 15, 57 ], [ 3 ] ]
[ [ 15, 58 ], [  ] ]
[ [ 15, 59 ], [ 3 ] ]
[ [ 15, 60 ], [  ] ]
[ [ 15, 61 ], [  ] ]
[ [ 15, 62 ], [  ] ]
[ [ 15, 63 ], [  ] ]
[ [ 15, 64 ], [  ] ]
[ [ 15, 65 ], [  ] ]
[ [ 15, 66 ], [  ] ]
[ [ 15, 67 ], [ 3 ] ]
[ [ 15, 68 ], [  ] ]
[ [ 15, 69 ], [  ] ]
[ [ 15, 70 ], [  ] ]
[ [ 15, 71 ], [ 5 ] ]
[ [ 15, 72 ], [  ] ]
[ [ 15, 73 ], [  ] ]
[ [ 15, 74 ], [  ] ]
[ [ 15, 75 ], [ 3 ] ]
[ [ 15, 76 ], [  ] ]
[ [ 15, 77 ], [  ] ]
[ [ 15, 78 ], [  ] ]
[ [ 15, 79 ], [  ] ]
[ [ 15, 80 ], [  ] ]

```
[ [ 15, 81 ], [ 5 ] ]
[ [ 15, 82 ], [  ] ]
[ [ 15, 83 ], [  ] ]
[ [ 15, 84 ], [  ] ]
[ [ 15, 85 ], [  ] ]
[ [ 15, 86 ], [  ] ]
[ [ 15, 87 ], [  ] ]
[ [ 15, 88 ], [  ] ]
[ [ 15, 89 ], [  ] ]
[ [ 15, 90 ], [  ] ]
[ [ 15, 91 ], [  ] ]
[ [ 15, 92 ], [ 3 ] ]
[ [ 15, 93 ], [  ] ]
[ [ 15, 94 ], [  ] ]
[ [ 15, 95 ], [ 3 ] ]
[ [ 15, 96 ], [  ] ]
[ [ 15, 97 ], [  ] ]
[ [ 15, 98 ], [ 3 ] ]
[ [ 15, 99 ], [  ] ]
[ [ 15, 100 ], [  ] ]
[ [ 15, 101 ], [ 3 ] ]
[ [ 15, 102 ], [  ] ]
[ [ 15, 103 ], [  ] ]
[ [ 15, 104 ], [  ] ]
```

## 10. GAP algorithms

We give GAP algorithms for computing the total obstruction $\mathrm{Obs}(K/k)$ and the first obstruction $\mathrm{Obs}_1(L/K/k)$ as in Section 6. The functions which are provided in this section are available from
https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/Norm1ToriHNP/.

```
LoadPackage("HAP");


Norm1TorusJ :=function(d,n)
    local I,M1,M2,M,f,Sn,T;
    I:=IdentityMat(d-1);
    Sn:=SymmetricGroup(d);
    T:=TransitiveGroup(d,n);
```

```
    M1:=Concatenation(List([2..d-1],x->I[x]),[-List([1..d-1],One)]);
    if d=2 then
        M:=[M1];
    else
        M2:=Concatenation([I[2],I[1]],List([3..d-1],x->I[x]));
        M:=[M1,M2];
    fi;
    f:=GroupHomomorphismByImages(Sn,Group(M),GeneratorsOfGroup(Sn),M);
    return Image(f,T);
end;

AbelianInvariantsSNF := function(G)
  local n,m,s,l;
  if Order(G)=1 then
    return [];
  fi;
  n:=AbelianInvariants(G);
  m:=DiagonalMat(n);
  s:=SmithNormalFormIntegerMat(m);
  return Filtered(DiagonalOfMat(s),x -> x>1);
end;

AbelianizationGen:= function(G)
    local Gab,pi,inv,A,iso,gen,genrep;
    Reset(GlobalMersenneTwister);
    Reset(GlobalRandomSource);
    pi:=NaturalHomomorphismByNormalSubgroup(G,DerivedSubgroup(G));
    Gab:=Image(pi);
    inv:=AbelianInvariantsSNF(Gab);
    A:=AbelianGroup(inv);
    iso:=IsomorphismGroups(A,Gab);
    gen:=List(GeneratorsOfGroup(A),x->Image(iso,x));
    genrep:=List(gen,x->PreImagesRepresentative(pi,x));
    return rec(Gab:=Gab, gen:=gen, genrep:=genrep, inv:=inv, pi:=pi);
end;

FindGenFiniteAbelian:= function(g)
    local e,a,ga,iso;
    e:=AbelianInvariants(g);
```

```
    if Length(e)>1 then
        e:=SmithNormalFormIntegerMat(DiagonalMat(e));
        e:=List([1..Length(e)],x->e[x][x]);
        e:=Filtered(e,x->x>1);
    fi;
    a:=AbelianGroup(e);
    ga:=GeneratorsOfGroup(a);
    iso:=IsomorphismGroups(a,g);
    return List(ga,x->Image(iso,x));
end;

EltFiniteAbelian:= function(arg)
    local g,c,gg,F,gF,hom,cF,e;
    g:=arg[1];
    c:=arg[2];
    if Length(arg)=3 then
        gg:=arg[3];
    else
        gg:=GeneratorsOfGroup(g);
    fi;
    F:=FreeGroup(Length(gg));
    gF:=GeneratorsOfGroup(F);
    hom:=GroupHomomorphismByImages(F,g,gF,gg);
    cF:=PreImagesRepresentative(hom,c);
    e:=List(gF,x->ExponentSumWord(cF,x));
    return e;
end;

FirstObstructionN:= function(arg)
    local G,H,Gab,Hab,K,Kinv,mat,v,Habbase,ker1;
    G:=arg[1];
    if Length(arg)=1 then
        H:=Stabilizer(G,1);
    else
        H:=arg[2];
    fi;
    Gab:=AbelianizationGen(G);
    Hab:=AbelianizationGen(H);
    Hab.Hab:=Hab.Gab;
```

```
    Unbind(Hab.Gab);
    if DerivedSubgroup(H)=H then
        return rec(ker:=[[],[],[]]], Hab:=Hab, Gab:=Gab, psi:=[]);
    fi;
    if DerivedSubgroup(G)=G then
        return rec(ker:=[Hab.inv,[Hab.inv,IdentityMat(Length(Hab.inv))]],
            Hab:=Hab, Gab:=Gab, psi:=List(Hab.inv,x->[]));
    fi;
    K:=Image(Hab.pi,Intersection(H,DerivedSubgroup(G)));
    Kinv:=AbelianInvariantsSNF(K);
    mat:=[];
    for v in Hab.genrep do
        Add(mat,EltFiniteAbelian(Gab.Gab,Image(Gab.pi,v),Gab.gen));
    od;
    Habbase:=DiagonalMat(Hab.inv);
    ker1:=List(GeneratorsOfGroup(K),x->EltFiniteAbelian(Hab.Hab,x,Hab.gen));
    ker1:=LatticeBasis(Concatenation(Habbase,ker1));
    ker1:=LatticeBasis(Difference(ker1,Habbase));
    return rec(ker:=[Kinv,[Hab.inv,ker1]],
        Hab:=Hab, Gab:=Gab, psi:=mat);;
end;

FirstObstructionDnr:= function(arg)
    local G,H,Gab,Hab,HG,HGrep,Dnrgen,h,x,Dnr,Dnrinv,Habbase,Dnrmat;
    G:=arg[1];
    if Length(arg)=1 then
        H:=Stabilizer(G,1);
    else
        H:=arg[2];
    fi;
    Gab:=AbelianizationGen(G);
    Hab:=AbelianizationGen(H);
    Hab.Hab:=Hab.Gab;
    Unbind(Hab.Gab);
    if DerivedSubgroup(H)=H then
        return rec(Dnr:=[[],[],[]]], Hab:=Hab, Gab:=Gab);
    fi;
    Reset(GlobalMersenneTwister);
    Reset(GlobalRandomSource);
```

```
    HG:=RightCosets(G,H);
    HGrep:=List(HG,Representative);
    Dnrgen:=[];
    for x in HGrep do
        for h in GeneratorsOfGroup(Intersection(H,H^x)) do
            Add(Dnrgen,Image(Hab.pi,Comm(h,x^-1)));
        od;
    od;
    Dnr:=Group(Dnrgen,Identity(Hab.Hab));
    Dnrinv:=AbelianInvariantsSNF(Dnr);
    Habbase:=DiagonalMat(Hab.inv);
    Dnrmat:=List(Dnrgen,x->EltFiniteAbelian(Hab.Hab,x,Hab.gen));
    Dnrmat:=LatticeBasis(Concatenation(Habbase,Dnrmat));
    Dnrmat:=LatticeBasis(Difference(Dnrmat,Habbase));
    return rec(Dnr:=[Dnrinv,[Hab.inv,Dnrmat]],
        Hab:=Hab, Gab:=Gab);
end;

FirstObstructionDr:= function(arg)
    local G,Gv,H,Gab,Hab,HGGv,HGGvrep,Hwi,Hwiab,Gvab,psi2i,i,psi2iimage,Hw,
          psi2,ker,phi1i,phi1iimage,phi1,Dr,Drinv,Habbase,Drmat;
    G:=arg[1];
    Gv:=arg[2];
    if Length(arg)=2 then
        H:=Stabilizer(G,1);
    else
        H:=arg[3];
    fi;
    Gab:=AbelianizationGen(G);
    Hab:=AbelianizationGen(H);
    Hab.Hab:=Hab.Gab;
    Unbind(Hab.Gab);
    if DerivedSubgroup(H)=H then
        return rec(Dr:=[[],[[],[]]], Hab:=Hab, Gab:=Gab);
    fi;
    HGGv:=DoubleCosets(G,H,Gv);
    HGGvrep:=List(HGGv,Representative);
    Hwi:=List(HGGvrep,x->Intersection(Gv^(x^(-1)),H));
    Hwiab:=List(Hwi,AbelianizationGen);
```

```
    Gvab:=AbelianizationGen(Gv);
    psi2i:=[];
    for i in [1..Length(HGGv)] do
        psi2iimage:=List(Hwiab[i].genrep,x->x^HGGvrep[i]);
        psi2iimage:=List(psi2iimage,x->Image(Gvab.pi,x));
        Add(psi2i,GroupHomomorphismByImages(Hwiab[i].Gab,Gvab.Gab,Hwiab[i].gen,
            psi2iimage));
    od;
    Hw:=DirectProduct(List(Hwiab,x->x.Gab));
    psi2:=GroupHomomorphismByFunction(Hw,Gvab.Gab,x->
     Product([1..Length(HGGv)],i->Image(psi2i[i],Image(Projection(Hw,i),x))));
    ker:=Kernel(psi2);
    phi1i:=[];
    for i in [1..Length(HGGv)] do
        phi1iimage:=List(Hwiab[i].genrep,x->Image(Hab.pi,x));
        Add(phi1i,GroupHomomorphismByImages(Hwiab[i].Gab,Hab.Hab,Hwiab[i].gen,
            phi1iimage));
    od;
    phi1:=GroupHomomorphismByFunction(Hw,Hab.Hab,x->
     Product([1..Length(HGGv)],i->Image(phi1i[i],Image(Projection(Hw,i),x))));
    Dr:=Image(phi1,ker);
    Drinv:=AbelianInvariantsSNF(Dr);
    Habbase:=DiagonalMat(Hab.inv);
    Drmat:=List(GeneratorsOfGroup(Dr),x->EltFiniteAbelian(Hab.Hab,x,Hab.gen));
    Drmat:=LatticeBasis(Concatenation(Habbase,Drmat));
    Drmat:=LatticeBasis(Difference(Drmat,Habbase));
    return rec(Dr:=[Drinv,[Hab.inv,Drmat]],
        Hab:=Hab, Gab:=Gab);
end;

MaximalSubgroups2:= function(G)
    Reset(GlobalMersenneTwister);
    Reset(GlobalRandomSource);
    return SortedList(MaximalSubgroups(G));
end;

SchurCoverG:= function(G)
    local epi,iso,ScG,ScGg,GG,GGg,Gg,n,i,id;
    Reset(GlobalMersenneTwister);
```

```
    Reset(GlobalRandomSource);
    epi:=EpimorphismSchurCover(G);
    iso:=IsomorphismPermGroup(Source(epi));
    ScG:=Source(epi);
    ScGg:=GeneratorsOfGroup(ScG);
    GG:=Range(iso);
    GGg:=List(ScGg,x->Image(iso,x));
    Gg:=List(ScGg,x->Image(epi,x));
    epi:=GroupHomomorphismByImages(GG,G,GGg,Gg);
    n:=NrMovedPoints(Source(epi));
    if n>=2 and n<=30 and IsTransitive(Source(epi),[1..n]) then
        for i in [1..NrTransitiveGroups(n)] do
            if Order(TransitiveGroup(n,i))=Order(Source(epi)) and
             IsConjugate(SymmetricGroup(n),
              TransitiveGroup(n,i),Source(epi)) then
                id:=[n,i];
                break;
            fi;
        od;
        return rec(SchurCover:=Source(epi), epi:=epi, Tid:=id);
    else
        return rec(SchurCover:=Source(epi), epi:=epi);
    fi;
end;

MinimalStemExtensions:= function(G)
    local ScG,ScGg,K,MK,ans,m,pi,cG,cGg,iso,GG,GGg,Gg,epi,n,i,id;
    ScG:=SchurCoverG(G);
    ScGg:=GeneratorsOfGroup(ScG.SchurCover);
    K:=Kernel(ScG.epi);
    MK:=MaximalSubgroups2(K);
    ans:=[];
    for m in MK do
        pi:=NaturalHomomorphismByNormalSubgroup(ScG.SchurCover,m);
        cG:=Range(pi);
        cGg:=List(ScGg,x->Image(pi,x));
        iso:=IsomorphismPermGroup(Range(pi));
        GG:=Range(iso);
        GGg:=List(cGg,x->Image(iso,x));
```

```
        Gg:=List(ScGg,x->Image(ScG.epi,x));
        epi:=GroupHomomorphismByImages(GG,G,GGg,Gg);
        n:=NrMovedPoints(Source(epi));
        if n>=2 and n<=30 and IsTransitive(Source(epi),[1..n]) then
            for i in [1..NrTransitiveGroups(n)] do
                if Order(TransitiveGroup(n,i))=Order(Source(epi)) and
                 IsConjugate(SymmetricGroup(n),
                  TransitiveGroup(n,i),Source(epi)) then
                    id:=[n,i];
                    break;
                fi;
            od;
            Add(ans,rec(MinimalStemExtension:=Source(epi), epi:=epi, Tid:=id));
        else
            Add(ans,rec(MinimalStemExtension:=Source(epi), epi:=epi));
        fi;
    od;
    return ans;
end;

ResHnZ:= function(arg)
    local RG,RH,n,G,H,inj,map,mapZ,CRGn,CRHn,HnG,HnH,m,res,null,ker,Hng,Hnggen,
          Hnh,Hnhgen,resHnggen,torbase,im,coker,hom,cokergen,cokergen1;
    RG:=arg[1];
    RH:=arg[2];
    n:=arg[3];
    G:=RG!.group;
    H:=RH!.group;
    inj:=GroupHomomorphismByFunction(H,G,x->x);
    map:=EquivariantChainMap(RH,RG,inj);
    mapZ:=HomToIntegers(map);
    if Length(arg)>=4 then
        CRGn:=arg[4];
    else
        CRGn:=CR_CocyclesAndCoboundaries(RG,n,true);
    fi;
    if Length(arg)=5 then
        CRHn:=arg[5];
    else
```

```
    CRHn:=CR_CocyclesAndCoboundaries(RH,n,true);
fi;
HnG:=CRGn.torsionCoefficients;
HnH:=CRHn.torsionCoefficients;
if HnG=[] then
    if HnH=[] then
        return rec(HnGZ:=[],HnHZ:=HnH,Res:=[],Ker:=[[],[[],[]]],
                   Coker:=[[],[[],[]]]);
    else
        return rec(HnGZ:=[],HnHZ:=HnH,Res:=[],Ker:=[[],[[],[]]],
                   Coker:=[HnH,[HnH,IdentityMat(Length(HnH))]]);
    fi;
fi;
if HnH=[] then
    return rec(HnGZ:=HnG,HnHZ:=[],
        Res:=List(HnG,x->[]),Ker:=[HnG,[HnG,IdentityMat(Length(HnG))]],
                  Coker:=[[],[[],[]]]);
fi;
m:=List(IdentityMat(Length(HnG)),x->
        CRHn.cocycleToClass(mapZ!.mapping(CRGn.classToCocycle(x),n)));
null:=NullspaceIntMat(m);
Hng:=AbelianGroup(HnG);
Hnggen:=GeneratorsOfGroup(Hng);
Hnh:=AbelianGroup(HnH);
Hnhgen:=GeneratorsOfGroup(Hnh);
resHnggen:=List(m,x->Product([1..Length(Hnhgen)],y->Hnhgen[y]^x[y]));
res:=GroupHomomorphismByImages(Hng,Hnh,Hnggen,resHnggen);
ker:=Kernel(res);
im:=Image(res);
null:=List(GeneratorsOfGroup(ker),x->EltFiniteAbelian(Hng,x,Hnggen));
torbase:=DiagonalMat(HnG);
null:=LatticeBasis(Concatenation(torbase,null));
null:=LatticeBasis(Difference(null,torbase));
hom:=NaturalHomomorphismByNormalSubgroup(Hnh,im);
coker:=Image(hom);
if Order(coker)=1 then
    return rec(HnGZ:=HnG,HnHZ:=HnH,Res:=m,
        Ker:=[AbelianInvariantsSNF(ker),[HnG,null]],Coker:=[[],[HnH,[]]]);
fi;
```

```
    cokergen:=FindGenFiniteAbelian(coker);
    cokergen1:=List(cokergen,x->Representative(PreImages(hom,x)));
    cokergen1:=List(cokergen1,x->EltFiniteAbelian(Hnh,x,Hnhgen));
    return rec(HnGZ:=HnG,HnHZ:=HnH,Res:=m,
        Ker:=[AbelianInvariantsSNF(ker),[HnG,null]],
              Coker:=[AbelianInvariants(coker),[HnH,cokergen1]]);
end;

CosetRepresentationTid:= function(G,H)
    local Gg,HG,HGg,HGgr,n,i,id;
    Gg:=GeneratorsOfGroup(G);
    HG:=RightCosets(G,H);
    HGg:=List(Gg,x->Permutation(x,HG,OnRight));
    HGgr:=Group(HGg,());
    n:=Index(G,H);
    if n=1 then
        id:=[1,1];
    elif n<=30 then
        for i in [1..NrTransitiveGroups(n)] do
            if Order(TransitiveGroup(n,i))=Order(HGgr) and
              IsConjugate(SymmetricGroup(n),TransitiveGroup(n,i),HGgr) then
                id:=[n,i];
                break;
            fi;
        od;
    else
        id:=fail;
    fi;
    return id;
end;

AlwaysHNPholds:= function(Tid)
    local n,i,tbl,tbl4,tbl6,tbl8,tbl9,tbl10,tbl14,tbl15;
    tbl4:=[2,4];
    tbl6:=[4,12];
    tbl8:=[2,3,4,9,11,13,14,15,19,21,22,31,32,37,38];
    tbl9:=[2,5,7,9,11,14,23];
    tbl10:=[7,26,32];
    tbl14:=[30];
```

```
    tbl15:=[9,14];
    tbl:=[[],[],[],tbl4,[],tbl6,[],tbl8,tbl9,tbl10,[],[],[],tbl14,tbl15];
    if Tid=fail then
        return fail;
    fi;
    n:=Tid[1];
    i:=Tid[2];
    if IsPrime(n) or n=1 then
        return true;
    elif n=12 or n>15 then
        return fail;
    elif i in tbl[n] then
        return false;
    else
        return true;
    fi;
end;

IsMetacyclic:= function(G)
    local p;
    if Order(G)=1 then
        return true;
    fi;
    for p in Set(Factors(Order(G))) do
        if not IsCyclic(SylowSubgroup(G,p)) then
            return false;
        fi;
    od;
    return true;
end;

ChooseGi:= function(bG,bH)
    local bGs,Gicandidates,Gis,cGi,Gi,His,Hi,flag;
    bGs:=ConjugacyClassesSubgroups(bG);
    Gicandidates:=Filtered(bGs,x->not IsMetacyclic(Representative(x)));
    Gis:=[];
    for cGi in Gicandidates do
        for Gi in Elements(cGi) do
            His:=Reversed(List(ConjugacyClassesSubgroups(Intersection(Gi,bH)),
```

```
             Representative));
            flag:=false;
            for Hi in His do
                if AlwaysHNPholds(CosetRepresentationTid(Gi,Hi))=true then
                    Add(Gis,Gi);
                    flag:=true;
                    break;
                fi;
            od;
            if flag=true then
                break;
            fi;
        od;
    od;
    return Gis;
end;

KerResH3Z:= function(G,H)
    local RG,CRG3,H3Z,torbase,kerbase,Gis,Gi,RGi,ker,H3,H3g,K;
    if IsNilpotent(G) then
        RG:=ResolutionNormalSeries(LowerCentralSeries(G),4);
    elif IsSolvable(G) then
        RG:=ResolutionNormalSeries(DerivedSeries(G),4);
    else
        RG:=ResolutionFiniteGroup(G,4);
    fi;
    CRG3:=CR_CocyclesAndCoboundaries(RG,3,true);
    H3Z:=CRG3.torsionCoefficients;
    if H3Z=[] then
        return [[],[[],[]]];
    fi;
    torbase:=DiagonalMat(H3Z);
    kerbase:=IdentityMat(Length(H3Z));
    Gis:=ChooseGi(G,H);
    for Gi in Gis do
        if IsNilpotent(Gi) then
            RGi:=ResolutionNormalSeries(LowerCentralSeries(Gi),4);
        elif IsSolvable(Gi) then
            RGi:=ResolutionNormalSeries(DerivedSeries(Gi),4);
```

```
        else
            RGi:=ResolutionFiniteGroup(Gi,4);
        fi;
        ker:=ResHnZ(RG,RGi,3,CRG3).Ker;
        kerbase:=LatticeIntersection(kerbase,Union(ker[2][2],torbase));
        kerbase:=LatticeBasis(kerbase);
    od;
    kerbase:=LatticeBasis(Difference(kerbase,torbase));
    H3:=AbelianGroup(H3Z);
    H3g:=GeneratorsOfGroup(H3);
    K:=Group(List(kerbase,x->Product([1..Length(x)],y->H3g[y]^x[y])),Identity(H3));
    return [AbelianInvariantsSNF(K),[H3Z,kerbase]];
end;
```

# Bibliography to Chapter 1


[Bar81a] H.-J. Bartels, *Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen*, J. Algebra **70** (1981) 179–199.

[Bar81b] H.-J. Bartels, *Zur Arithmetik von Diedergruppenerweiterungen*, Math. Ann. **256** (1981) 465–473.

[BT82] F. R. Beyl, J. Tappe, *Group extensions, representations, and the Schur multiplicator*, Lecture Notes in Mathematics, 958. Springer-Verlag, Berlin-New York, 1982.

[But93] G. Butler, *The transitive groups of degree fourteen and fifteen*, J. Symbolic Comput. **16** (1993) 413–422.

[BM83] G. Butler, J. McKay, *The transitive groups of degree up to eleven*, Comm. Algebra **11** (1983) 863–911.

[CT07] J.-L. Colliot-Thélène, *Lectures on Linear Algebraic Groups*, Beijing lectures, Moning side centre, April 2007, https://www.math.u-psud.fr/~colliot/BeijingLectures2Juin07.pdf.

[CTHS05] J.-L. Colliot-Thélène, D. Harari, A. N. Skorobogatov, *Compactification équivariante d'un tore (d'après Brylinski et Künnemann)*, Expo. Math. **23** (2005) 161–170.

[CTS77] J.-L. Colliot-Thélène, J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. École Norm. Sup. (4) **10** (1977) 175–229.

[CTS87] J.-L. Colliot-Thélène, J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: Applications*, J. Algebra **106** (1987) 148–205.

[CTS07] J.-L. Colliot-Thélène, J.-J. Sansuc, *The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group)*, Algebraic groups and homogeneous spaces, 113–186, Tata Inst. Fund. Res. Stud. Math., 19, Tata Inst. Fund. Res., Mumbai, 2007.

[CK00] A. Cortella, B. Kunyavskii, *Rationality problem for generic tori in simple groups*, J. Algebra **225** (2000) 771–793.

[DM96] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996. xii+346 pp.

[Dra89] Yu. A. Drakokhrust, *On the complete obstruction to the Hasse principle*, (Russian) Dokl. Akad. Nauk BSSR **30** (1986) 5–8; translation in Amer. Math. Soc. Transl. (2) **143** (1989) 29–34.

[DP87] Yu. A. Drakokhrust, V. P. Platonov, *The Hasse norm principle for algebraic number fields*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986) 946–968; translation in Math. USSR-Izv. **29** (1987) 299–322.

[End11] S. Endo, *The rationality problem for norm one tori*, Nagoya Math. J. **202** (2011) 83–106.

[EK17] S. Endo, M. Kang, *Function fields of algebraic tori revisited*, Asian J. Math. **21** (2017) 197–224.

[EM73] S. Endo, T. Miyata, *Invariants of finite abelian groups*, J. Math. Soc. Japan **25** (1973) 7–26.

[EM75] S. Endo, T. Miyata, *On a classification of the function fields of algebraic tori*, Nagoya Math. J. **56** (1975) 85–104. Corrigenda: Nagoya Math. J. **79** (1980) 187–190.

[Flo] M. Florence, *Non rationality of some norm-one tori*, preprint (2006).

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.9.3; 2018. (http://www.gap-system.org).

[Ger77] F. Gerth III, *The Hasse norm principle in metacyclic extensions of number fields*, J. London Math. Soc. (2) **16** (1977) 203–208.

[Ger78] F. Gerth III, *The Hasse norm principle in cyclotomic number fields*, J. Reine Angew. Math. **303/304** (1978) 249–252.

[GLS98] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups*, Number 3, Part I, Chapter A: Almost simple $\mathcal{K}$-groups, Mathematical Surveys and Monographs, 40.3, American Mathematical Society, Providence, RI, 1998, xvi+419 pp.

[Gur78a] S. Gurak, *On the Hasse norm principle*, J. Reine Angew. Math. **299/300** (1978) 16–27.

[Gur78b] S. Gurak, *The Hasse norm principle in non-abelian extensions*, J. Reine Angew. Math. **303/304** (1978) 314–318.

[Gur80] S. Gurak, *The Hasse norm principle in a compositum of radical extensions*, J. London Math. Soc. (2) **22** (1980) 385–397.

[HAP] G. Ellis, The GAP package HAP, version 1.12.6, available from http://www.gap-system.org/Packages/hap.html.

[HHY20] S. Hasegawa, A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori in small dimensions*, Math. Comp. **89** (2020) 923–940.

[Has31] H. Hasse, *Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1931) 64–69.

[Hir64] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II.*, Ann. of Math. (2) **79** (1964) 109–203; 205–326.

[HKY] A. Hoshi, K. Kanai, A. Yamasaki, *Norm one tori and Hasse norm principle*, arXiv:1910.01469, to appear in Mathematics of Computation.

[HY17] A. Hoshi, A. Yamasaki, *Rationality problem for algebraic tori*, Mem. Amer. Math. Soc. **248** (2017) no. 1176, v+215 pp.

[HY21] A. Hoshi, A. Yamasaki, *Rationality problem for norm one tori*, Israel J. Math. **241** (2021) 849–867.

[Hür84] W. Hürlimann, *On algebraic tori of norm type*, Comment. Math. Helv. **59** (1984) 539–549.

[Jeh79] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. **311/312** (1979) 215–254.

[Kan12] M. Kang, *Retract rational fields*, J. Algebra **349** (2012) 22–37.

[Mer08] A. Merkurjev, *R-equivalence on three-dimensional tori and zero-cycles*, Algebra Number Theory **2** (2008) 69–89.

[Kap87] G. Karpilovsky, *The Schur multiplier*, London Mathematical Society Monographs. New Series, 2. The Clarendon Press, Oxford University Press, New York, 1987.

[KMRT98] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, 44, American Mathematical Society, Providence, RI, 1998, xxii+593 pp.

[Kun84] B. E. Kunyavskii, *Arithmetic properties of three-dimensional algebraic tori*, (Russian) Integral lattices and finite linear groups, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **116** (1982) 102–107, 163; translation in J. Soviet Math. **26** (1984) 1898–1901.

[Kun90] B. E. Kunyavskii, *Three-dimensional algebraic tori*, Selecta Math. Soviet. **9** (1990) 1–21.

[Kun07] B. E. Kunyavskii, *Algebraic tori — thirty years after*, Vestnik Samara State Univ. (2007) 198–214.

[LL00] N. Lemire, M. Lorenz, *On certain lattices associated with generic division algebras*, J. Group Theory **3** (2000) 385–405.

[LPR06] N. Lemire, V. L. Popov, Z. Reichstein, *Cayley groups*, J. Amer. Math. Soc. **19** (2006) 921–967.

[LeB95] L. Le Bruyn, *Generic norm one tori*, Nieuw Arch. Wisk. (4) **13** (1995) 401–407.

[Len74] H. W. Lenstra, Jr., *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974) 299–325.

[Lor05] M. Lorenz, *Multiplicative invariant theory*, Encyclopaedia Math. Sci., vol. 135, Springer-Verlag, Berlin, 2005.

[Mac20] A. Macedo, *The Hasse norm principle for $A_n$-extensions*, J. Number Theory **211** (2020) 500–512.

[Mac] A. Macedo, *On the obstruction to the Hasse principle for multinorm equations*, arXiv:1912.11941.

[MN] A. Macedo, R. Newton, *Explicit methods for the Hasse norm principle and applications to $A_n$ and $S_n$ extensions*, arXiv:1906.03730.

[Man74] Yu. I. Manin, *Cubic forms: algebra, geometry, arithmetic*, North-Holland Mathematical Library 4, North-Holland, Amsterdam, 1974.

[Maz82] P. Mazet, *Sur les multiplicateurs de Schur des groupes de Mathieu*, (French) J. Algebra **77** (1982) 552–576.

[Ono61] T. Ono, *Arithmetic of algebraic tori*, Ann. of Math. (2) **74** (1961) 101–139.

[Ono63] T. Ono, *On the Tamagawa number of algebraic tori*, Ann. of Math. (2) **78** (1963) 47–73.

[Ono65] T. Ono, *On the relative theory of Tamagawa numbers*, Ann. of Math. (2) **82** (1965) 88–111.

[Opo80] H. Opolka, *Zur Auflösung zahlentheoretischer Knoten*, Math. Z. **173** (1980) 95–103.

[Pla82] V. P. Platonov, *Arithmetic theory of algebraic groups*, (Russian) Uspekhi Mat. Nauk **37** (1982) 3–54; translation in Russian Math. Surveys **37** (1982) 1–62.

[PD85a] V. P. Platonov, Yu. A. Drakokhrust, *On the Hasse principle for algebraic number fields*, (Russian) Dokl. Akad. Nauk SSSR **281** (1985) 793–797; translation in Soviet Math. Dokl. **31** (1985) 349–353.

[PD85b] V. P. Platonov, Yu. A. Drakokhrust, *The Hasse norm principle for primary extensions of algebraic number fields*, (Russian) Dokl. Akad. Nauk SSSR **285** (1985) 812–815; translation in Soviet Math. Dokl. **32** (1985) 789–792.

[PR94] V. P. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Translated from the 1991 Russian original by Rachel Rowen, Pure and applied mathematics, 139, Academic Press, 1994.

[Rob96] D. J. S. Robinson, *A course in the theory of groups*, Second edition. Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[Roy87] G. F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987) 255–268.

[Sal84] D. J. Saltman, *Retract rational fields and cyclic Galois extensions*, Israel J. Math. **47** (1984) 165–215.

[Sal99] D. J. Saltman, *Lectures on division algebras*, CBMS Regional Conference Series in Mathematics, 94, Published by American Mathematical Society, Providence, RI; on behalf of Conference Board of the Mathematical Sciences, Washington, DC, 1999. viii+120 pp.

[San81] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, (French) J. Reine Angew. Math. **327** (1981) 12–80.

[Sch36] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen I*, J. Reine Angew. Math. **175** (1936) 100–107.

[Sch40] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen II*, J. Reine Angew. Math. **182** (1940) 217–234.

[Swa83] R. G. Swan, *Noether's problem in Galois theory*, Emmy Noether in Bryn Mawr (Bryn Mawr, Pa., 1982), 21–40, Springer, New York-Berlin, 1983.

[Swa10] R. G. Swan, *The flabby class group of a finite cyclic group*, Fourth International Congress of Chinese Mathematicians, 259–269, AMS/IP Stud. Adv. Math., 48, Amer. Math. Soc., Providence, RI, 2010.

[Tat67] J. Tate, *Global class field theory*, Algebraic Number Theory, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union, Edited by J. W. S. Cassels and A. Fröhlich, 162–203, Academic Press, London; Thompson Book Co., Inc., Washington, D.C. 1967.

[Vos67] V. E. Voskresenskii, *On two-dimensional algebraic tori II*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **31** (1967) 711–716; translation in Math. USSR-Izv. **1** (1967) 691–696.

[Vos69] V. E. Voskresenskii, *The birational equivalence of linear algebraic groups*, (Russian) Dokl. Akad. Nauk SSSR **188** (1969) 978–981; erratum, ibid. 191 1969 nos., 1, 2, 3, vii; translation in Soviet Math. Dokl. **10** (1969) 1212–1215.

[Vos70] V. E. Voskresenskii, *Birational properties of linear algebraic groups*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **34** (1970) 3–19; translation in Math. USSR-Izv. **4** (1970) 1–17.

[Vos74] V. E. Voskresenskii, *Stable equivalence of algebraic tori*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974) 3–10; translation in Math. USSR-Izv. **8** (1974) 1–7.

[Vos83] V. E. Voskresenskii, *Projective invariant Demazure models*, (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982) 195–210, 431; translation in Math USSR-Izv. **20** (1983) 189–202.

[Vos88] V. E. Voskresenskii, *Maximal tori without affect in semisimple algebraic groups*, (Russian) Mat. Zametki 44 (1988) 309–318; translation in Math. Notes **44** (1988) 651–655.

[Vos98] V. E. Voskresenskii, *Algebraic groups and their birational invariants*, Translated from the Russian manuscript by Boris Kunyavskii, Translations of Mathematical Monographs, 179. American Mathematical Society, Providence, RI, 1998.

[VK84] V. E. Voskresenskii, B. E. Kunyavskii, *Maximal tori in semisimple algebraic groups*, Kuibyshev State Inst., Kuibyshev (1984). Deposited in VINITI March 5, 1984, No. 1269-84 Dep. (Ref. Zh. Mat. (1984), 7A405 Dep.).

[Yam12] A. Yamasaki, *Negative solutions to three-dimensional monomial Noether problem*, J. Algebra **370** (2012) 46–78.

CHAPTER 2

# Davenport-Hasse lifting theorem


## Abstract

Let $e \geq 2$ be an integer, $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$ and $\eta_r(i)$ be Gaussian periods of degree $e$ for $\mathbb{F}_{p^r}$. By the dual form of Davenport and Hasse's lifting theorem on Gauss sums, we establish lifts of the multiplication matrices of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ which are defined by F. Thaine. We also give some examples of the explicit lifts for prime degree $e$ with $3 \leq e \leq 23$ which also illustrate relations among lifts of Jacobi sums, Gaussian periods and multiplication matrices of Gaussian periods. This chapter is based on [**HK**].


## 1. Introduction

Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. Write $p^r = ef + 1$. Let $\mathbb{F}_{p^r}$ be the finite field of $p^r$ elements and $\gamma$ be a fixed generator of $\mathbb{F}_{p^r}^\times = \mathbb{F}_{p^r} \setminus \{0\}$. Let $\zeta_n = e^{2\pi i/n}$ be an $n$-th root of unity. For $0 \leq i \leq e-1$, *Gaussian periods $\eta_r(i)$ of degree $e$ for* $\mathbb{F}_{p^r}$ are defined by

$$\eta_r(i) := \sum_{j=0}^{f-1} \zeta_p^{\mathrm{Tr}(\gamma^{ej+i})}$$

where Tr is the trace map $\mathrm{Tr} : \mathbb{F}_{p^r} \to \mathbb{F}_p$, and *the period polynomial $P_{e,r}(X)$ of degree $e$ for $\mathbb{F}_{p^r}$* is defined by $P_{e,r}(X) = \prod_{i=0}^{e-1} (X - \eta_r(i)) \in \mathbb{Z}[X]$. Note that $\eta_r(i)$ depends on the choice of $\gamma$.

We recall notion of Jacobi sums, Gauss sums and cyclotomic numbers and their relations (see Berndt, Evans and Williams [**BEW98**]). For a nontrivial character $\psi$ on $\mathbb{F}_{p^r}^\times$ and the trivial character $\varepsilon$ on $\mathbb{F}_{p^r}^\times$, we extend them to $\mathbb{F}_{p^r}$ by setting $\psi(0) = 0$ and $\varepsilon(0) = 1$. Let $\psi_1$, $\psi_2$ be characters on $\mathbb{F}_{p^r}$. *Jacobi sums $J_r(\psi_1, \psi_2)$ and $J_r^*(\psi_1, \psi_2)$ for $\mathbb{F}_{p^r}$* are defined by

$$J_r(\psi_1, \psi_2) := \sum_{\alpha \in \mathbb{F}_{p^r}} \psi_1(\alpha)\psi_2(1-\alpha) \quad \text{and} \quad J_r^*(\psi_1, \psi_2) := \sum_{\substack{\alpha \in \mathbb{F}_{p^r} \\ \alpha \neq 0,1}} \psi_1(\alpha)\psi_2(1-\alpha).$$

If $\psi_1, \psi_2 \neq \varepsilon$, then $J_r(\psi_1, \psi_2) = J_r^*(\psi_1, \psi_2)$ although $J_r(\varepsilon, \psi_2) = J_r(\psi_1, \varepsilon) = 0$, $J_r(\varepsilon, \varepsilon) = p^r$ and $J_r^*(\varepsilon, \psi_2) = J_r^*(\psi_1, \varepsilon) = -1$, $J_r^*(\varepsilon, \varepsilon) = p^r - 2$. *Gauss sums $G_r(\psi_1)$ and $G_r^*(\psi_1)$ for $\mathbb{F}_{p^r}$* are

defined to be

$$G_r(\psi_1) := \sum_{\alpha\in\mathbb{F}_{p^r}} \psi_1(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)} \quad \text{and} \quad G_r^*(\psi_1) := \sum_{\alpha\in\mathbb{F}_{p^r}^\times} \psi_1(\alpha)\zeta_p^{\mathrm{Tr}(\alpha)}.$$

If $\psi_1 \neq \varepsilon$, then $G_r(\psi_1) = G_r^*(\psi_1)$ although $G_r(\varepsilon) = 0$ and $G_r^*(\varepsilon) = -1$. We have the well-known relations

$$J_r(\psi_1,\psi_2) = \frac{G_r(\psi_1)G_r(\psi_2)}{G_r(\psi_1\psi_2)} \quad \text{and} \quad J_r^*(\psi_1,\psi_2) = \frac{G_r^*(\psi_1)G_r^*(\psi_2)}{G_r^*(\psi_1\psi_2)}$$

whenever $\psi_1\psi_2 \neq \varepsilon$.

The following theorem is the Davenport and Hasse's lifting theorem (see also Weil [**Wei49**, pages 503–505], [**BEW98**, page 360, Theorem 11.5.2]):

THEOREM 2.1 (Davenport and Hasse [**DH35**, Relation (0.8)]). *Let $e \geq 2$ be an integer, $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$ and $\psi$ be a nontrivial character on $\mathbb{F}_{p^r}$. Then, for any integer $n \geq 1$, we have*

$$G_{nr}(\psi') = (-1)^{n-1}G_r(\psi)^n$$

*where $\psi'$ is the lift of $\psi$ from $\mathbb{F}_{p^r}$ to $\mathbb{F}_{p^{nr}}$ defined by $\psi'(\alpha) = \psi(\mathrm{Nr}(\alpha))$ and* Nr *is the norm map. In particular, if $\psi_1$, $\psi_2$ and $\psi_1\psi_2$ are nontrivial characters on $\mathbb{F}_{p^r}$, then we have*

$$J_{nr}(\psi_1',\psi_2') = (-1)^{n-1}J_r(\psi_1,\psi_2)^n.$$

From now on, we take the character $\chi$ of order $e$ on $\mathbb{F}_{p^r}$ with $\chi(\gamma) = \zeta_e$ and $\chi(0) = 0$ where $\langle\gamma\rangle = \mathbb{F}_{p^r}^\times$. For $0 \leq i,j \leq e-1$, we simply write

$$J_r(i,j) := J_r(\chi^i,\chi^j) \quad \text{and} \quad J_r^*(i,j) := J_r^*(\chi^i,\chi^j).$$

We have

$$J_r(i,j) = J_r^*(i,j) + \delta_{i,0} + \delta_{0,j}$$

where $\delta_{i,j}$ is Kronecker's delta.

REMARK 2.2. (1) If we adopt the another manner $\varepsilon(0) = 0$, then we have $J_r(i,j) = J_r^*(i,j)$ (e.g. Myerson [**Mye81**], Parnami, Agrawal and Rajwade [**PAR82**], Katre and Rajwade [**KR85a**]).

(2) We may take another Jacobi sum

$$J_r'(i,j) = \sum_{\alpha\in\mathbb{F}_{p^r}} \chi^i(\alpha)\chi^j(1+\alpha)$$

which satisfies $J_r'(i,j) = \chi(-1)^i J_r(i,j) = (-1)^{fi}J_r(i,j)$ (see e.g. [**PAR82**], [**KR85a**]).

For $0 \leq i, j \leq e-1$, *cyclotomic numbers* $\mathrm{Cyc}_r(i,j)$ *of order* $e$ *for* $\mathbb{F}_{p^r}$ are defined by

$$\mathrm{Cyc}_r(i,j) := \#\{(v_1, v_2) \mid 0 \leq v_1, v_2 \leq f-1,\ 1+\gamma^{ev_1+i} \equiv \gamma^{ev_2+j} \pmod{p^r}\}.$$

We have the following well-known relations between cyclotomic numbers $\mathrm{Cyc}_r(a,b)$ and Jacobi sums $J_r^*(i,j)$ (see [**BEW98**, page 79, Theorem 2.5.1]):

$$\sum_{i=0}^{e-1}\sum_{j=0}^{e-1}(-1)^{fi}\zeta_e^{-(ai+bj)}J_r^*(i,j) = e^2\mathrm{Cyc}_r(a,b)$$

and

$$(-1)^{fi}\sum_{a=0}^{e-1}\sum_{b=0}^{e-1}\mathrm{Cyc}_r(a,b)\zeta_e^{ai+bj} = J_r^*(i,j).$$

Note that both $\mathrm{Cyc}_r(a,b)$ and $J_r^*(i,j)$ depend on the choice of the fixed generator $\gamma$ of $\mathbb{F}_{p^r}^{\times}$.

We see that the product of the Gaussian periods is represented by a linear combination of the Gaussian periods again and these coefficients are given in terms of the cyclotomic numbers (see [**BEW98**, page 328, Lemma 10.10.2, page 437, Exercises 12.23]):

$$\eta_r(m)\eta_r(m+i) = \sum_{j=0}^{e-1}(\mathrm{Cyc}_r(i,j) - D_i f)\eta_r(m+j) \tag{2}$$

where $D_i = \delta_{0,i}$ (resp. $\delta_{e/2,i}$) if $f$ is even (resp. odd). It follows that the Gaussian periods are the eigenvalues of the $e \times e$ matrix $C_r := [\mathrm{Cyc}_r(i,j) - D_i f]_{0 \leq i,j \leq e-1}$ called *the multiplication matrix of* $\eta_r(0), \ldots, \eta_r(e-1)$ (see Section 2). Hence the period polynomial $P_{e,r}(X)$ can be obtained as the characteristic polynomial $\mathrm{Char}_X(C_r)$ of the multiplication matrix $C_r$.

F. Thaine investigated various properties and characterizations of Gaussian periods, cyclotomic numbers and Jacobi sums with applications to the construction of cyclic polynomials in the series of the papers [**Tha96**], [**Tha99**], [**Tha00**], [**Tha01**], [**Tha04**], [**Tha08**] (see also Lehmer [**Leh88**], Schoof and Washington [**SW88**], Hashimoto and Hoshi [**HH05a**], [**HH05b**]).

According to Thaine [**Tha04**, Section 2], for two $e \times e$ matrices $A = [a_{i,j}]_{0 \leq i,j \leq e-1}$, $B = [b_{i,j}]_{0 \leq i,j \leq e-1}$ and $d \in (\mathbb{Z}/e\mathbb{Z}) \setminus \{0\}$, we define *the d-composition* $A \overset{d}{*} B$ *of* $A$ *and* $B$ as

$$A \overset{d}{*} B := \left[\sum_{s=0}^{e-1}\sum_{t=0}^{e-1} a_{s,t}b_{ds+i,dt+j}\right]_{0 \leq i,j \leq e-1}.$$

For the multiplication matrix $C_1$ (resp. $C_1'$) of Gaussian periods $\eta_1(0), \ldots, \eta_1(e-1)$ (resp. $\eta_1'(0), \ldots, \eta_1'(e-1)$) of degree $e$ for $\mathbb{F}_{p^1}$, the $d$-composition $C_1 \overset{d}{*} C_1'$ gives the multiplication matrix of $\theta_{d,0}, \ldots, \theta_{d,e-1}$ where $\theta_{d,i} = \sum_{s=0}^{e-1}\eta_1(s)\eta_1'(ds+i)$. Hence we obtain the cyclic polynomial $\mathrm{Char}_X(C_1 \overset{d}{*} C_1')$ which gives an intermediate cyclic field $\mathbb{Q}(\theta_{d,i})$ of degree $e$ in the composite bicyclic field $\mathbb{Q}(\eta_1(0), \eta_1'(0)) \subset \mathbb{Q}(\zeta_p, \zeta_q)$ with $p \neq q$ (see Section 2 and Section 3).

In Section 4, we regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the function $\eta_r : \mathbb{Z}/e\mathbb{Z} \to \mathbb{C}$, $i \mapsto \eta_r(i)$ and the Gauss sums $G_r^*(\chi)$ for $\mathbb{F}_{p^r}$ as the function $G_r^* : \widehat{\mathbb{Z}/e\mathbb{Z}} \to \mathbb{C}$, $\chi \mapsto G_r^*(\chi)$. Then we find that they are each other's finite Fourier transform with some twist (see Lemma 2.11 in Section 4) and we have:

THEOREM 2.3 (Davenport and Hasse's lifting theorem: the dual form). *Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. We regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the function $\eta_r : \mathbb{Z}/e\mathbb{Z} \to \mathbb{C}$, $i \mapsto \eta_r(i)$. Then, for any integer $n \geq 1$, we have*

$$\eta_{nr}(i) = (-1)^{n-1}\eta_r^{(n)}(i) \quad \textit{for} \quad 0 \leq i \leq e-1$$

*where*

$$\eta_r^{(n)}(i) = \sum_{\substack{k_1+\cdots+k_n \equiv i \,(\mathrm{mod}\, e) \\ 0 \leq k_1,\ldots,k_n \leq e-1}} \eta_r(k_1)\cdots\eta_r(k_n)$$

*is the $n$-fold product of $\eta_r$ with respect to the convolution product.*

By using Theorem 2.3, we get our main theorem which gives lifts of the multiplication matrix $C_r$ of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$ via Thaine's $(-1)$-composition $\overset{-1}{*}$:

THEOREM 2.4. *Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. Let $C_r = [\mathrm{Cyc}_r(i,j) - D_i f]_{0 \leq i,j \leq e-1}$ be the multiplication matrix of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$. Then, for any integer $n \geq 1$, we have*

$$C_{nr} = (-1)^{n-1}C_r^{(n)}$$

*where $C_r^{(n)}$ is the $n$-fold product of $C_r$ with respect to the $(-1)$-composition $\overset{-1}{*}$. In particular, we have $P_{e,nr}(X) = \mathrm{Char}_X((-1)^{n-1}C_r^{(n)})$.*

We organize Chapter 2 as follows. In Section 2, we review Thaine's results on the $d$-composition of the multiplication matrices based on [**Tha04**]. In Section 3, we study the $d$-compositions of matrices and functions in the general situations. This enables us to consider the $d$-compositions of the multiplication matrices $C_r$ of the Gaussian periods and also the $d$-compositions of the Gaussian periods $\eta_r(i)$ without linear independence. In Section 4, we recall a Fourier transform on finite abelian groups and show that Gaussian periods $\eta_r(i)$ and Gauss sums $G_r^*(\chi)$ are each other's finite Fourier transform (with some twist). Using this, we give a proof of Theorem 2.3. We will give some examples of Theorem 2.3 in Section 5. In

Section 6, the proof of Theorem 2.4 will be given. In Section 7, we give some examples of Theorem 2.4 for prime degree $e$ with $3 \leq e \leq 23$ which also illustrate relations among lifts of Jacobi sums, Gaussian periods and multiplication matrices of Gaussian periods as in Theorem 2.1, Theorem 2.3 and Theorem 2.4 respectively.

## 2. Thaine's results: compositions of multiplication matrices of Gaussian periods

We review Thaine's results on the $d$-composition of the multiplication matrices based on [**Tha04**, Section 1 and Section 2].

**2.1. Multiplication matrices of roots.** Thaine [**Tha04**, Section 1] defined the multiplication matrix $A$ of $\theta_0, \ldots, \theta_{e-1}$ as follows.

Let $D$ be an integrally closed domain with $\mathrm{char}\ D = 0$ and $K$ be the quotient field of $D$. Let $e \geq 2$ be an integer and $P(X) = \sum_{k=0}^{e} c_k X^k = \prod_{i=0}^{e-1}(X - \theta_i) \in D[X]$ be a cyclic polynomial, i.e. an irreducible polynomial with cyclic Galois group over $K$. Then $K(\theta_i)/K$ is a cyclic extension of degree $e$ with $\mathrm{Gal}(K(\theta_i)/K) = \langle\tau\rangle$. We may assume that $\tau(\theta_i) = \theta_{i+1}$ where we regard the subscripts modulo $e$. We also assume that the discriminant $\mathrm{disc}_{K(\theta_i)/K}(\theta_0, \ldots \theta_{e-1}) = (\det[\tau^j(\theta_i)]_{0\leq i,j\leq e-1})^2 \neq 0$. Then $\{\theta_0, \ldots, \theta_{e-1}\}$ is a vector space basis of $K(\theta_i)$.

Let $M_e(K)$ be the algebra of $e \times e$ matrices over $K$. Define the matrix $A = [a_{i,j}]_{0\leq i,j\leq e-1} \in M_e(K)$ by $\theta_0\theta_i = \sum_{j=0}^{e-1} a_{i,j}\theta_j$ which is called *the multiplication matrix of* $\theta_0, \ldots, \theta_{e-1}$. Note that the $\theta_i$'s are eigenvalues of $A$ and hence $P(X) = \mathrm{Char}_X(A)$; the characteristic polynomial of $A$.

Thaine [**Tha04**, Proposition 1] showed that
(i) $a_{i,j} = a_{-i,j-i}$ for $0 \leq i, j \leq e-1$;
(ii) $A(\mathcal{K}^{-i}A\mathcal{K}^i) = (\mathcal{K}^{-i}A\mathcal{K}^i)A$ for $0 \leq i \leq e-1$ where $\mathcal{K} = [\delta_{i+1,j}]_{0\leq i,j\leq e-1}$ is the $e \times e$ circulant matrix

$$\mathcal{K} = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{pmatrix}.$$

Conversely, if $A' = [a'_{i,j}]_{0\leq i,j\leq e-1} \in M_e(K)$ satisfies (i) and (ii) and $P'(X) = \mathrm{Char}_X(A')$ is irreducible over $K$ with roots $\theta'_0, \ldots, \theta'_{e-1}$, then the Galois group of $P'(X)$ over $K$ is cyclic and $A'$ is the multiplication matrix of $\theta'_0, \ldots, \theta'_{e-1}$ with $\mathrm{disc}_{K(\theta_i)/K}(\theta'_0, \ldots, \theta'_{e-1}) \neq 0$.

**2.2. The $d$-compositions of multiplication matrices.** Thaine [**Tha04**, Section 2] defined the $d$-composition $A \overset{d}{*} A'$ of the multiplication matrices $A$ and $A'$ as follows.

Let $P(X) = \prod_{i=0}^{e-1}(X - \theta_i), P'(X) = \prod_{i=0}^{e-1}(X - \theta'_i) \in D[X]$ be cyclic polynomials of degree $e$. Then $L = K(\theta_i)$ and $L' = K(\theta'_i)$ are cyclic extensions of $K$ of degree $e$ with $\mathrm{Gal}(L/K) = \langle\tau\rangle$, $\tau(\theta_i) = \theta_{i+1}$ and $\mathrm{Gal}(L'/K) = \langle\tau'\rangle$, $\tau'(\theta'_i) = \theta'_{i+1}$ where we regard the subscripts modulo $e$.

We assume that $L \cap L' = K$. We also assume that $\{\theta_0, \ldots, \theta_{e-1}\}$ and $\{\theta'_0, \ldots, \theta'_{e-1}\}$ are linearly independent over $K$. Then $[LL' : K] = e^2$ with $G = \mathrm{Gal}(LL'/K) \simeq \langle\tau\rangle \times \langle\tau'\rangle$ and $\{\theta_i\theta'_j \mid 0 \le i, j \le e-1\}$ becomes a vector space basis of $LL'$ over $K$. We make indentifications $\tau = (\tau, 1)$ and $\tau' = (1, \tau')$. For $1 \le d \le e-1$, we have an intermediate field $L_d = (LL')^{\langle\tau\tau'^d\rangle} = K(\theta_{d,i})$ which is a cyclic extension of $K$ of degree $e$ with a normal basis $\{\theta_{d,0}, \ldots, \theta_{d,e-1}\}$ where $\theta_{d,i} = \sum_{s=0}^{e-1} \theta_s\theta'_{ds+i}$.

Thaine [**Tha04**, Proposition 6] (see also [**Tha04**, Example 4]) proved that the multiplication matrix $A_d$ of $\theta_{d,0}, \ldots, \theta_{d,e-1}$ is given by

$$A_d = A \overset{d}{*} A'$$

where $A = [a_{i,j}]_{0 \le i,j \le e-1}$ and $A' = [a'_{i,j}]_{0 \le i,j \le e-1}$ are the multiplication matrices of $\theta_0, \ldots, \theta_{e-1}$ and $\theta'_0, \ldots, \theta'_{e-1}$ respectively and the $d$-composition $A \overset{d}{*} A'$ of the matrices $A$ and $A'$ is defined by

$$A \overset{d}{*} A' := \left[\sum_{s=0}^{e-1}\sum_{t=0}^{e-1} a_{s,t}a'_{ds+i,dt+j}\right]_{0 \le i,j \le e-1}.$$

**2.3. Multiplication matrices of Gaussian periods.** The simplest example of the multiplication matrix is that of Gaussian periods $\eta_1(0), \ldots, \eta_1(e-1)$ for $\mathbb{F}_{p^1}$ (see Section 1).

Let $p$ be a prime with $p \equiv 1 \pmod{e}$ and $\eta_1(0), \ldots, \eta_1(e-1)$ be the Gaussian periods of degree $e$ for $\mathbb{F}_{p^1}$. Then $\eta_1(0), \ldots, \eta_1(e-1)$ are linearly independent over $\mathbb{Q}$ and $A = [\mathrm{Cyc}_1(i, j) - D_i f]_{0 \le i,j \le e-1}$ becomes the multiplication matrix of $\eta_1(0), \ldots, \eta_1(e-1)$ with $P_{e,1}(X) = \mathrm{Char}_X(A)$ (see the equation (1) in Section 1).

However, in the general case with $r \ge 2$, Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$ are not necessarily linearly independent over $\mathbb{Q}$. Myerson [**Mye81**] showed that $P_{e,r}(X)$ splits over $\mathbb{Q}$ into $\delta = \gcd(e, (p^r - 1)/(p - 1))$ factors. For example, $P_{e,e}(X)$ splits completely over $\mathbb{Q}$, i.e. $\eta_e(0), \ldots, \eta_e(e-1) \in \mathbb{Q}$.

In the next section, we study the $d$-compositions of matrices and the $d$-compositions of functions for more general situations. This enables us to consider the $d$-compositions of the multiplication matrices $C_r$ of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ and also the $d$-compositions of the Gaussian periods $\eta_r(i)$ without linear independence.

## 3. The $d$-compositions

**3.1. The $d$-compositions of matrices.** Let $K$ be a field with $\mathrm{char}\, K = 0$. Let $e \geq 2$ be an integer and $M_e(K)$ be the algebra of $e \times e$ matrices over $K$.

According to Thaine [**Tha04**] (see Subsection 2.2), for $A = [a_{i,j}]_{0 \leq i,j \leq e-1}$, $B = [b_{i,j}]_{0 \leq i,j \leq e-1} \in M_e(K)$ and $d \in (\mathbb{Z}/e\mathbb{Z}) \setminus \{0\}$, we define *the $d$-composition $A \overset{d}{*} B$ of $A$ and $B$* as

$$A \overset{d}{*} B := \left[ \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} a_{s,t} b_{ds+i,dt+j} \right]_{0 \leq i,j \leq e-1}.$$

We see that the $d$-composition $\overset{d}{*}$ and the ordinary addition $+$ satisfy the distributive law, i.e.

$$A \overset{d}{*} (B + C) = (A \overset{d}{*} B) + (A \overset{d}{*} C), \ (A + B) \overset{d}{*} C = (A \overset{d}{*} C) + (B \overset{d}{*} C),$$

although it does not satisfy the cancellation law, i.e. there exist matrices $A, B, C$ such that $A \overset{d}{*} C = B \overset{d}{*} C$ and $A \neq B$.

PROPOSITION 2.5. *Let $A = [a_{i,j}]_{0 \leq i,j \leq e-1}$, $B = [b_{i,j}]_{0 \leq i,j \leq e-1} \in M_e(K)$. We write $A[i,j] = a_{i,j}$ for convenience. For $d \in (\mathbb{Z}/e\mathbb{Z})^\times$, we have*

$$(B \overset{d}{*} A)[i,j] = (A \overset{d^{-1}}{*} B)[-d^{-1}i, -d^{-1}j].$$

*In particular, we get*

$$A \overset{-1}{*} B = B \overset{-1}{*} A.$$

PROOF. Putting $s' := ds + i$ and $t' := dt + j$, we have

$$\begin{aligned}
(B \overset{d}{*} A)[i,j] &= \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} B[s,t] A[ds+i, dt+j] \\
&= \sum_{s'=0}^{e-1} \sum_{t'=0}^{e-1} B[d^{-1}(s'-i), d^{-1}(t'-i)] A[s',t'] \\
&= \sum_{s'=0}^{e-1} \sum_{t'=0}^{e-1} A[s',t'] B[d^{-1}s' + (-d^{-1}i), d^{-1}t' + (-d^{-1}i)] \\
&= (A \overset{d^{-1}}{*} B)[-d^{-1}i, -d^{-1}j].
\end{aligned}$$

□

COROLLARY 2.6. *We have* $\mathrm{Char}_X(B \overset{d}{*} A) = \mathrm{Char}_X(A \overset{d^{-1}}{*} B)$ *where* $\mathrm{Char}_X(A)$ *stands for the characteristic polynomial of* $A$.

PROOF. By Proposition 2.5, we see that there exists an invertible matrix $P \in M_e(K)$ such that

$$B \overset{d}{*} A = P^{-1}(A \overset{d^{-1}}{*} B)P.$$

Hence the assertion follows. □

LEMMA 2.7. *Let* $A = [a_{i,j}]_{0 \le i,j \le e-1}$, $B = [b_{i,j}]_{0 \le i,j \le e-1} \in M_e(K)$. *Let* $\mathcal{K} = [\delta_{i+1,j}]_{0 \le i,j \le e-1} \in M_e(K)$ *be a circulant matrix. For* $0 \le l \le e-1$, *we have*
(i) $\mathcal{K}^l(A \overset{d}{*} B) = A \overset{d}{*} (\mathcal{K}^l B) = (\mathcal{K}^{-d^{-1}l} A) \overset{d}{*} B$,
(ii) $(A \overset{d}{*} B)\mathcal{K}^l = A \overset{d}{*} (B\mathcal{K}^l) = (A\mathcal{K}^{-d^{-1}l}) \overset{d}{*} B$.

PROOF. Write $A[i,j] = a_{i,j}$. We first see that

$$(\mathcal{K}^l A)[i,j] = A[i+l, j], \ (A\mathcal{K}^l)[i,j] = A[i, j-l].$$

(i) The first equality follows from

$$\begin{aligned}
(\mathcal{K}^l(A \overset{d}{*} B))[i,j] &= (A \overset{d}{*} B)[i+l, j] \\
&= \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t] B[ds + (i+l), dt + j] \\
&= \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t] (\mathcal{K}^l B)[ds + i, dt + j] \\
&= (A \overset{d}{*} (\mathcal{K}^l B))[i,j].
\end{aligned}$$

By substituting $s' := s + d^{-1}l$, the second equality follows from

$$\begin{aligned}
(A \overset{d}{*} (\mathcal{K}^l B))[i,j] &= \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t] \mathcal{K}^l B[ds + i, dt + j] \\
&= \sum_{s'=0}^{e-1} \sum_{t=0}^{e-1} A[s' - d^{-1}l, t] B[ds' + i, dt + j] \\
&= \sum_{s'=0}^{e-1} \sum_{t=0}^{e-1} (\mathcal{K}^{-d^{-1}l}) A[s', t] B[ds' + i, dt + j] \\
&= ((\mathcal{K}^{-d^{-1}l} A) \overset{d}{*} B)[i,j].
\end{aligned}$$

(ii) can be proved in the similar way, and we omit the proof. □

PROPOSITION 2.8. *For $A, B, C \in M_e(K)$ and $d_1, d_2 \in (\mathbb{Z}/e\mathbb{Z})^\times$, we have*

$$A \overset{d_1}{*} (B \overset{d_2}{*} C) = (A \overset{-d_2^{-1}d_1}{*} B) \overset{d_2}{*} C.$$

*In particular, we get*

$$A \overset{d_1}{*} (B \overset{-1}{*} C) = (A \overset{d_1}{*} B) \overset{-1}{*} C$$

*and hence the $(-1)$-composition $\overset{-1}{*}$ satisfies the associative law.*

PROOF. For $A = [a_{i,j}]_{0 \le i,j \le e-1} \in M_e(K)$, we write $A[i,j] = a_{i,j}$. We obtain the following expression of $A \overset{d}{*} B$ by using the circulant matrix $\mathcal{K} = [\delta_{i+1,j}]_{0 \le i,j \le e-1} \in M_e(K)$:

$$A \overset{d}{*} B = \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t]\, \mathcal{K}^{ds} B \mathcal{K}^{-dt}.$$

Then it follows from Lemma 2.7 that

$$\begin{aligned}
A \overset{d_1}{*} (B \overset{d_2}{*} C) &= -\sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t]\, \mathcal{K}^{d_1 s} (B \overset{d_2}{*} C) \mathcal{K}^{-d_1 t} \\
&= \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t] \left( (\mathcal{K}^{-d_2^{-1}d_1 s} B \mathcal{K}^{d_2^{-1}d_1 t}) \overset{d_2}{*} C \right) \\
&= \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t] \left( \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} \mathcal{K}^{-d_2^{-1}d_1 s} B \mathcal{K}^{d_2^{-1}d_1 t} [u,v]\, \mathcal{K}^{d_2 u} C \mathcal{K}^{d_2 v} \right) \\
&= \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} \left( \sum_{s=0}^{e-1} \sum_{t=0}^{e-1} A[s,t] \mathcal{K}^{-d_2^{-1}d_1 s} B \mathcal{K}^{d_2^{-1}d_1 t} \right) [u,v]\, \mathcal{K}^{d_2 u} C \mathcal{K}^{d_2 v} \\
&= \sum_{u=0}^{e-1} \sum_{v=0}^{e-1} (A \overset{-d_2^{-1}d_1}{*} B)[u,v]\, \mathcal{K}^{d_2 u} C \mathcal{K}^{d_2 v} \\
&= (A \overset{-d_2^{-1}d_1}{*} B) \overset{d_2}{*} C.
\end{aligned}$$

The last assertion follows if we take $d_2 = -1$. □

By the last statement of Proposition 2.8, we can define the $n$-fold product $A^{(n)}$ as

$$A^{(n)} := A \overset{-1}{*} \cdots \overset{-1}{*} A \quad (n\text{-fold}).$$

**3.2. The $d$-compositions of functions.** Let $e \ge 2$ be an integer and $P(X) = \sum_{k=0}^{e-1} c_k X^k = \prod_{i=0}^{e-1} (X - \theta_i) \in D[X]$ be a cyclic polynomial. Let $L^2(\mathbb{Z}/e\mathbb{Z})$ be the vector space of all $\mathbb{C}$-valued functions on $\mathbb{Z}/e\mathbb{Z}$. We may regard $\theta_i = \theta(i)$ as the function $\theta : \mathbb{Z}/e\mathbb{Z} \to \mathbb{C}$, i.e. $\theta \in$

$L^2(\mathbb{Z}/e\mathbb{Z})$. Based on the results in Subsection 3.1, for $f, g \in L^2(\mathbb{Z}/e\mathbb{Z})$ and $d \in (\mathbb{Z}/e\mathbb{Z}) \setminus \{0\}$, we define *the d-composition* $f \overset{d}{*} g$ *of* $f$ *and* $g$ by

$$(f \overset{d}{*} g)(i) := \sum_{s=0}^{e-1} f(s)g(ds+i).$$

In particular, we get

$$(f \overset{-1}{*} g)(i) = \sum_{\substack{k_1+k_2 \equiv i \,(\mathrm{mode}) \\ 0 \le k_1, k_2 \le e-1}} f(k_1)g(k_2) = (f * g)(i)$$

where $*$ is the (usual) convolution of $L^2(\mathbb{Z}/e\mathbb{Z})$ (see also Section 4). Hence the $(-1)$-composition $\overset{-1}{*}$ satisfies the commutative and the associative laws, and we can define the $n$-fold product of $f$ with respect to $\overset{-1}{*}$ as

$$f^{(n)}(i) := (f \overset{-1}{*} \cdots \overset{-1}{*} f)(i) \quad (n\text{-fold}).$$

By the definition, we get

$$f^{(n)}(i) = \sum_{\substack{k_1+\cdots+k_n \equiv i \,(\mathrm{mode}) \\ 0 \le k_1, \ldots, k_n \le e-1}} f(k_1) \cdots f(k_n).$$

In order to prove Theorem 2.4, we need the following proposition which gives the relation between $A \overset{d}{*} B$ and $f \overset{d}{*} g$:

PROPOSITION 2.9. *Let* $K$ *be a field with* $\mathrm{char}\ K = 0$. *For* $f, g \in L^2(\mathbb{Z}/e\mathbb{Z})$, *we assume that there exist* $A = [a_{i,j}]_{0 \le i,j \le e-1}$, $B = [b_{i,j}]_{0 \le i,j \le e-1} \in M_e(K)$ *such that*

$$f(i)\, f(j) = \sum_{k=0}^{e-1} a_{j-i,k-i}\, f(k) \text{ and } g(i)\, g(j) = \sum_{k=0}^{e-1} b_{j-i,k-i}\, g(k).$$

*Then we have*

$$(f \overset{d}{*} g)(i)\, (f \overset{d}{*} g)(j) = \sum_{k=0}^{e-1} (A \overset{d}{*} B)[j-i, k-i]\, (f \overset{d}{*} g)(k)$$

*where we write* $A[i,j] = a_{i,j}$. *In particular,*

$$f^{(n)}(i)\, f^{(n)}(j) = \sum_{j=0}^{e-1} A^{(n)}[j-i, k-i]\, f^{(n)}(j)$$

*where* $A^{(n)}$ *is the n-fold product of* $A$ *with respect to the* $(-1)$*-composition* $\overset{-1}{*}$.

PROOF. By substituting $k := v - du$, $s := n - m$, $t := u - m$, we have

$$\begin{aligned}
&(f \overset{d}{*} g)(i)(f \overset{d}{*} g)(j) \\
&= \left(\sum_{m=0}^{e-1} f(m)g(dm+i)\right)\left(\sum_{n=0}^{e-1} f(n)g(dn+j)\right) \\
&= \sum_{m,n=0}^{e-1} (f(m)f(n))(g(dm+i)g(dn+j)) \\
&= \sum_{m,n=0}^{e-1} \left(\sum_{u=0}^{e-1} A[n-m, u-m]f(u)\right)\left(\sum_{v=0}^{e-1} B[d(n-m)+j-i, v-(dm+i)]g(v)\right) \\
&= \sum_{m,n,u,k=0}^{e-1} A[n-m, u-m]B[d(n-m)+j-i, d(u-n)+k-i]f(u)g(du+k) \\
&= \sum_{s,t,u,k=0}^{e-1} A[s,t]B[ds+j-i, dt+k-i]f(u)g(du+k) \\
&= \sum_{k=0}^{e-1} \left(\sum_{s,t=0}^{e-1} A[s,t]B[ds+(j-i), dt+(k-i)]\right)\left(\sum_{u=0}^{e-1} f(u)g(du+k)\right) \\
&= \sum_{k=0}^{e-1} (A \overset{d}{*} B)[j-i, k-i](f \overset{d}{*} g)(k).
\end{aligned}$$

□

Applying Proposition 2.9 for Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ and $\eta'_s(i)$ for $\mathbb{F}_{q^s}$ with $p^r, q^s \equiv 1 \pmod{e}$ (we may apply the both cases $p \neq q$ and $p = q$) and their multiplication matrices, we get:

COROLLARY 2.10. *Let $e \geq 2$ be an integer and $p^r$ (resp. $q^s$) be prime power with $p^r \equiv 1 \pmod{e}$ (resp. $q^s \equiv 1 \pmod{e}$). (We may take $p^r$, $q^s$ in the both cases $p \neq q$ and $p = q$.) We regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the functions from $\mathbb{Z}/e\mathbb{Z}$ to $\mathbb{C}$, i.e. $\eta_r \in L^2(\mathbb{Z}/e\mathbb{Z})$. Let $C$ (resp. $C'$) be the multiplication matrix of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$ (resp. $\eta'_s(0), \ldots, \eta'_s(e-1)$ of degree $e$ for $\mathbb{F}_{q^s}$). Then we have*

$$(\eta_r \overset{d}{*} \eta'_s)(i)\,(\eta_r \overset{d}{*} \eta'_s)(j) = \sum_{k=0}^{e-1} (C \overset{d}{*} C')[j-i, k-i]\,(\eta_r \overset{d}{*} \eta'_s)(k).$$

For the case $p \neq q$, we can find examples of $C \overset{d}{*} C'$ in Thaine [**Tha04**, Example 4, page 259]. We will treat the case $p = q$ in the remaining part of this chapter.

## 4. Proof of Theorem 2.3

We recall a Fourier transform on finite abelian groups (see Terras [**Ter99**, Chapter 10]). Let $G$ be a finite abelian group and

$$L^2(G) = \{f : G \to \mathbb{C}\}$$

be the vector space of all $\mathbb{C}$-valued functions on $G$ with the inner product $\langle f, g\rangle = \sum_{x\in G} f(x)\overline{g(x)}$. Let $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^\times)$ be the dual of $G$. For $f \in L^2(G)$, *the finite Fourier transform* $\mathscr{F}(f) = \widehat{f} \in L^2(\widehat{G})$ *of* $f$ is defined to be

$$(\mathscr{F}(f))(\chi) = \widehat{f}(\chi) = \sum_{x\in G} f(x)\overline{\chi(x)} = \langle f, \chi\rangle.$$

Then $\mathscr{F} : L^2(G) \to L^2(\widehat{G})$ becomes a bijective linear transformation with the inverse

$$(\mathscr{F}^{-1}(\widehat{f}))(x) = f(x) = \frac{1}{\#G}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\chi(x) = \frac{1}{\#G}\sum_{\chi\in\widehat{G}} \langle f, \chi\rangle\chi(x).$$

For $f, g \in L^2(G)$, we define *the convolution* $f * g \in L^2(G)$ *of* $f$ *and* $g$ by

$$(f * g)(x) = \sum_{y\in G} f(y)g(x - y).$$

Then the space $L^2(G)$ with the convolution $*$ is isomorphic to the group ring $\mathbb{C}[G]$ (with the usual convolution product) as a commutative $\mathbb{C}$-algebra by $L^2(G) \ni f \mapsto \sum_{x\in G} f(x)x \in \mathbb{C}[G]$. We also have the compatibility of the convolution $*$ and the finite Fourier transform $\mathscr{F}(f) = \widehat{f}$:

$$\widehat{(f * g)}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi) \tag{3}$$

(see Terras [**Ter99**, page 168, Theorem 2]).

In order to show Theorem 2.3, we prepare the following fundamental lemma:

LEMMA 2.11. *Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. Let $\gamma$ be a fixed generator of $\mathbb{F}_{p^r}^\times$ and $\chi$ be the character on $\mathbb{F}_{p^r}$ with $\chi(\gamma) = \zeta_e$ and $\chi(0) = 0$. We regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the functions from $\mathbb{Z}/e\mathbb{Z}$ to $\mathbb{C}$, i.e. $\eta_r \in L^2(\mathbb{Z}/e\mathbb{Z})$, and the Gauss sum $G_r^*(\chi^j)$ for $\mathbb{F}_{p^r}$ as the functions from $\widehat{\mathbb{Z}/e\mathbb{Z}}$ to $\mathbb{C}$, i.e. $G_r^* \in L^2(\widehat{\mathbb{Z}/e\mathbb{Z}})$. Then the finite Fourier transform $\mathscr{F}(\eta_r)$ of $\eta_r$ is given by*

$$(\mathscr{F}(\eta_r))(\chi^j) = G_r^*(\chi^{-j})$$

*and we also have*

$$(\mathscr{F}^{-1}(G_r^*))(i) = \eta_r(-i).$$

PROOF. Because $\mathbb{F}_{p^r}^\times$ is a cyclic group of order $p^r - 1 = ef$ and $\chi \in \widehat{\mathbb{F}_{p^r}^\times}$ is of order $e$, the Gauss sum $G_r^*(\chi^j)$ can be regarded as the function from $\widehat{\mathbb{Z}/e\mathbb{Z}}$ to $\mathbb{C}$ via factors through $G_r^* : \widehat{\mathbb{F}_{p^r}^\times} \to \widehat{\mathbb{F}_{p^r}^\times}/H \to \mathbb{C}$ where $H$ is the group of $e$-th powers of $\widehat{\mathbb{F}_{p^r}^\times}$ with $\widehat{\mathbb{F}_{p^r}^\times}/H \simeq \widehat{\mathbb{Z}/e\mathbb{Z}}$. Note that $\{\chi^j H \mid 0 \le j \le e-1\}$ gives a set of complete representatives for $\widehat{\mathbb{F}_{p^r}^\times}/H \simeq \widehat{\mathbb{Z}/e\mathbb{Z}}$.

We have the following well-known relations between the Gauss sums $G_r^*(\chi^j)$ and the Gaussian periods $\eta_r(i)$:

$$G_r^*(\chi^j) = \sum_{i=0}^{e-1} \zeta_e^{ij} \eta_r(i), \quad \eta_r(i) = \frac{1}{e} \sum_{j=0}^{e-1} \zeta_e^{-ij} G_r^*(\chi^j)$$

(see [**Mye81**, Proposition 1 (f)]). Then it follows that

$$(\mathscr{F}(\eta_r))(\chi^j) = \sum_{x \in \mathbb{Z}/e\mathbb{Z}} \eta_r(x) \overline{\chi^j}(x) = \sum_{i=0}^{e-1} \zeta_e^{-ij} \eta_r(i) = G_r^*(\chi^{-j})$$

and

$$\begin{aligned}(\mathscr{F}^{-1}(G_r^*))(i) &= \frac{1}{\#(\mathbb{Z}/e\mathbb{Z})} \sum_{\psi \in \widehat{\mathbb{Z}/e\mathbb{Z}}} G_r^*(\psi)\psi(i) \\ &= \frac{1}{e} \sum_{j=0}^{e-1} G_r^*(\chi^j)\chi^j(i) = \frac{1}{e} \sum_{j=0}^{e-1} \zeta_e^{ij} G_r^*(\chi^j) = \eta_r(-i).\end{aligned}$$

□

Now, we give the proof of Theorem 2.3.

THEOREM 2.3 (Davenport and Hasse's lifting theorem: the dual form). *Let $e \ge 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. We regard the Gaussian periods $\eta_r(i)$ of degree $e$ for $\mathbb{F}_{p^r}$ as the function $\eta_r : \mathbb{Z}/e\mathbb{Z} \to \mathbb{C}$, $i \mapsto \eta_r(i)$. Then, for any integer $n \ge 1$, we have*

$$\eta_{nr}(i) = (-1)^{n-1} \eta_r^{(n)}(i) \quad \textit{for} \quad 0 \le i \le e-1$$

*where*

$$\eta_r^{(n)}(i) = \sum_{\substack{k_1 + \cdots + k_n \equiv i \,(\mathrm{mod}\, e) \\ 0 \le k_1, \ldots, k_n \le e-1}} \eta_r(k_1) \cdots \eta_r(k_n)$$

*is the $n$-fold product of $\eta_r$ with respect to the convolution product.*

PROOF. By Theorem 2.1, the equation (3) and Lemma 2.11, we have

$$\widehat{\eta_r^{(n)}}(\chi^i) = (\widehat{\eta_r}(\chi^i))^n = (G_r^*(\chi^{-i}))^n = (-1)^{n-1} G_{nr}^*(\chi^{-i}) = (-1)^{n-1} \widehat{\eta_{nr}}(\chi^i).$$

We get $\widehat{\eta_r^{(n)}} = (-1)^{n-1}\widehat{\eta_{nr}}$ and hence $\eta_r^{(n)} = (-1)^{n-1}\eta_{nr}$. □

## 5. Examples of Theorem 2.3

*Exponential Gauss sums* $g_r(b,e)$ $(b \in \mathbb{F}_{p^r})$ *of degree* $e$ *for* $\mathbb{F}_{p^r}$ are defined by

$$g_r(b,e) := \sum_{\alpha \in \mathbb{F}_{p^r}} \zeta_p^{\mathrm{Tr}(b\alpha^e)}.$$

We write $g_r(e) := g_r(1,e)$. We also define *the reduced Gaussian periods* $\eta_r^*(i)$ of order $e$ for $\mathbb{F}_{p^r}$ as

$$\eta_r^*(i) := e\eta_r(i) + 1 = g_r(\gamma^i, e)$$

for $0 \le i \le e-1$ (see [**BEW98**, page 327]). Let $\chi$ be the character on $\mathbb{F}_{p^r}$ with $\chi(\gamma) = \zeta_e$ and $\chi(0) = 0$ where $\langle\gamma\rangle = \mathbb{F}_{p^r}^\times$ as before. We see that the Gauss sums $G_r^*(\chi^j)$ and the reduced Gaussian periods $\eta_r^*(i)$ satisfy the following relations

$$G_r^*(\chi^j) = \begin{cases} \dfrac{1}{e}\displaystyle\sum_{i=0}^{e-1} \zeta_e^{ij}\eta_r^*(i) & \text{if} \quad 1 \le j \le e-1 \\ -1 & \text{if} \quad j = 0, \end{cases}$$

$$\eta_r^*(i) = \sum_{j=1}^{e-1} \zeta_e^{-ij} G_r^*(\chi^j)$$

(see [**Mye81**, Proposition 1 (g)], [**BEW98**, page 332, Theorem 10.10.8], cf. the proof of Lemma 2.11). In particular, we have

$$g_r(e) = \eta_r^*(0) = \sum_{j=1}^{e-1} G_r^*(\chi^j) = \sum_{j=1}^{e-1} G_r(\chi^j).$$

We also use *the reduced period polynomial* $P_{e,r}^*(X) := \prod_{i=0}^{e-1}(X - \eta_r^*(i))$ of degree $e$ for $\mathbb{F}_{p^r}$ with the coefficient of $X^{e-1}$ zero. An explicit determination of the factors of $P_{e,r}^*(X)$ is important because the exponential Gauss sum $g_r(e) = \eta_r^*(0)$ becomes a root of $P_{e,r}^*(X)$. For further applications to the coding theory, see e.g. McEliece and Rumsey [**MR72**] and [**BEW98**, Section 11.7].

By applying Theorem 2.3, we can obtain the reduced Gaussian periods $\eta_e^*(i)$ $(i = 0, \ldots, e-1)$ of order $e$ for $\mathbb{F}_{p^e}$ as follows (we take the generator $\gamma$ of $\mathbb{F}_p^\times = \langle\gamma\rangle$ as the smallest one):

(1) $e = 3$. We take $p = 7 = ef + 1$ with $f = 2$ and $\gamma = 3$. Then $\eta_3^*(i)$ $(i = 0, 1, 2)$ are given by 7, $-35$, 28 (in this order).

(2) $e = 5$. We take $p = 11 = ef + 1$ with $f = 2$ and $\gamma = 2$. Then $\eta_5^*(i)$ $(i = 0, \ldots, 4)$ are given by $-979$, $-649$, 1276, $-99$, 451.

(3) $e = 7$. We take $p = 29 = ef + 1$ with $f = 4$ and $\gamma = 2$. Then $\eta_7^*(i)$ $(i = 0, \ldots, 6)$ are given by $-317869$, $-259405$, $-324771$, 442569, 233682, $-182671$, 408465.

(4) $e = 11$. We take $p = 23 = ef + 1$ with $f = 2$ and $\gamma = 5$. Then $\eta_{11}^*(i)$ $(i = 0, \ldots, 10)$ are given by 52918009, 3199967, $-202694722$, $-64390754$, 142959444, $-23093817$, 166665038, $-19592803$, 47121273, $-58652208$, $-44439427$.

(5) $e = 13$. We take $p = 53 = ef + 1$ with $f = 4$ and $\gamma = 2$. Then $\eta_{13}^*(i)$ $(i = 0, \ldots, 12)$ are given by 782475795674, 338244988654, $-245670171356$, 83828569254, $-740552966334$, $-910543059425$, 117899008800, 664438112586, $-186980700750$, $-238169301889$, $-277653262665$, 1040615291340, $-427932303889$.

(6) $e = 17$. We take $p = 103 = ef + 1$ with $f = 6$ and $\gamma = 5$. Then $\eta_{17}^*(i)$ $(i = 0, \ldots, 16)$ are given by $-651513206543247755$, 670088231006862759, $-373934090375919493$, 587253242462231659, $-243310155546790559$, 163898849457734107, $-197783211402587952$, $-1253189038565026183$, 35922811461007315, 356621718684896633, $-478731856802195967$, $-289516205265127375$, 461908111585063663, 464742031061114921, 670357206530506901, 282238003107978403, $-205052440856501077$.

We give GAP ([**GAP**]) computations for (6) $e = 17$, $p = 103$ and $\gamma = 5$. The cases (1)–(5) can be obtained by the similar manner.

```
gap> etaf:=function(e,p,i)
> local g;
> g:=PrimitiveRootMod(p);
> if i<0 then i:=i mod e;
> fi;
> return Sum([1..(p-1)/e],j->E(p)^(g^(e*j+i)));
> end;
function( e, p, i ) ... end
gap> e:=17;;p:=103;;PrimitiveRootMod(p); # e=17, p=103, g=5
5
gap> eta:=function(i)
> return(etaf(e,p,i));
> end;
function( i ) ... end
gap> p2:=function(i)
```

```
> return Sum([0..e-1],k1->eta(k1)*eta(-k1+i));
> end;
function( i ) ... end
gap> p4:=function(i)
> return Sum([0..e-1],k1->p2(k1)*p2(-k1+i));
> end;
function( i ) ... end
gap> p8:=function(i)
> return Sum([0..e-1],k1->p4(k1)*p4(-k1+i));
> end;
function( i ) ... end
gap> p9:=function(i)
> return Sum([0..e-1],k1->p8(k1)*eta(-k1+i));
> end;
function( i ) ... end
gap> p17:=function(i)
> return Sum([0..e-1],k1->p9(k1)*p8(-k1+i));
> end;
function( i ) ... end
gap> L:=List([0..e-1],i->p17(i)); # Gaussian periods eta_{e,i}: i=0,...16
[ -38324306267249868, 39416954765109574, -21996122963289382,
  34544308380131274, -14312362090987680, 9641108791631418,
  -11634306553093409, -73717002268530952, 2113106556529842,
  20977748157935096, -28160697458952704, -17030365015595728,
  27171065387356686, 27337766533006760, 39432776854735700,
  16602235476939906, -12061908285676534 ]
gap> 17*L+1; # reduced Gaussian periods eta^*_{e,i}: i=0,...16
[ -651513206543247755, 670088231006862759, -373934090375919493,
  587253242462231659, -243310155546790559, 163898849457734107,
  -197783211402587952, -1253189038565026183, 35922811461007315,
  356621718684896633, -478731856802195967, -289516205265127375,
  461908111585063663, 464742031061114921, 670357206530506901,
  282238003107978403, -205052440856501077 ]
```

## 6. Proof of Theorem 2.4

For $A = [a_{i,j}]_{0 \le i,j \le e-1} \in M_e(K)$, we write $A[i,j] = a_{i,j}$ for convenience. We give the proof of Theorem 2.4.

THEOREM 2.4. *Let $e \geq 2$ be an integer and $p^r$ be a prime power with $p^r \equiv 1 \pmod{e}$. Let $C_r = [\mathrm{Cyc}_r(i,j) - D_i f]_{0 \leq i,j \leq e-1}$ be the multiplication matrix of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$. Then, for any integer $n \geq 1$, we have*

$$C_{nr} = (-1)^{n-1} C_r^{(n)}$$

*where $C_r^{(n)}$ is the $n$-fold product of $C_r$ with respect to the $(-1)$-composition $\overset{-1}{*}$. In particular, we have $P_{e,nr}(X) = \mathrm{Char}_X((-1)^{n-1} C_r^{(n)})$.*

PROOF. By the definition, for the multiplication matrix $C_{nr}$ of Gaussian periods $\eta_{nr}(0), \ldots, \eta_{nr}(e-1)$, we have

$$\eta_{nr}(i)\eta_{nr}(j) = \sum_{k=0}^{e-1} C_{nr}[j-i, k-i]\eta_{nr}(k).$$

By Theorem 2.3 (the dual form of Davenport and Hasse's lifting theorem), we obtain

$$\eta_r^{(n)}(i)\eta_r^{(n)}(j) = \sum_{k=0}^{e-1} (-1)^{n-1} C_{nr}[j-i, k-i]\eta_r^{(n)}(k).$$

By setting $l := j - i$ and $m := k - i$, we get

$$\eta_r^{(n)}(i)\eta_{r,i}^{(n)}(l) = \sum_{m=0}^{e-1} (-1)^{n-1} C_{nr}[l, m]\eta_r^{(n)}(i+m). \tag{4}$$

On the other hand, by Proposition 2.9, we have

$$\eta_r^{(n)}(i)\eta_r^{(n)}(j) = \sum_{k=0}^{e-1} C_r^{(n)}[j-i, k-i]\eta_r^{(n)}(k).$$

By setting $l := j - i$ and $m := k - i$ also, we obtain

$$\eta_r^{(n)}(i)\eta_r^{(n)}(i+l) = \sum_{m=0}^{e-1} C_r^{(n)}[l, m]\eta_r^{(n)}(i+m). \tag{5}$$

Equations (4) and (5) imply that $(-1)^{n-1} C_{nr}$ and $C_r^{(n)}$ have the same eigenvalues $\eta_r^{(n)}(i)$ $(0 \leq i \leq e-1)$ and the same eigenvector

$$T_i = (\eta_r^{(n)}(i), \eta_r^{(n)}(i+1), \ldots, \eta_r^{(n)}(0), \eta_r^{(n)}(1), \ldots, \eta_r^{(n)}(i-1))^t$$

with respect to $\eta_r^{(n)}(i)$ where $t$ stands for the transposed vector.

We take the circulant matrix $P := (T_0, \ldots, T_{e-1})$ with determinant $\prod_{j=0}^{e-1} f(\zeta_e^j)$ where $f(x) = \sum_{i=0}^{e-1} \eta_r^{(n)}(i) x^i$. We see that the matrix $P$ is invertible because there exist at least

two distinct $\eta_r^{(n)}(i) = (-1)^{n-1}\eta_{nr}(i)$ by Baumert, Mills and Ward [**BMW82**, Lemma 2 and the proof of Lemma 3]. Hence the both $(-1)^{n-1}C_{nr}$ and $C_r^{(n)}$ are diagonalized by the same $P$:

$$P^{-1}(-1)^{n-1}C_{nr}P = \begin{pmatrix} \eta_r^{(n)}(0) & & \\ & \ddots & \\ & & \eta_r^{(n)}(e-1) \end{pmatrix} = P^{-1}C_r^{(n)}P.$$

This implies that $(-1)^{n-1}C_{nr} = C_r^{(n)}$. □

## 7. Examples of Theorem 2.4

We give some examples of Theorem 2.4 when $e = l$ is an odd prime which also illustrate relations among lifts of Jacobi sums, Gaussian periods and multiplication matrices of Gaussian periods as in Theorem 2.1, Theorem 2.3 and Theorem 2.4 respectively.

Let $p$ be a prime with $p \equiv 1 \pmod{l}$. Katre and Rajwade [**KR85a**, Main theorem, page 186] gave some system of Diophantine equations whose unique solution gives the coefficient $a_1(n), \ldots, a_{l-1}(n)$ of the Jacobi sums $J_r(1,n) = \sum_{i=1}^{l-1} a_i(n)\zeta_l^i \in \mathbb{Z}[\zeta_l]$ $(1 \le n \le l-2)$ and the cyclotomic numbers $\mathrm{Cyc}_r(i,j)$ of order $l$ are obtained in terms of $a_1(n), \ldots, a_{l-1}(n)$ $(1 \le n \le l-2)$ as

$$l^2\mathrm{Cyc}_r(0,0) = p^r - 3l + 1 - \sum_{n=1}^{l-2}\sum_{k=1}^{l-1} a_k(n),$$

$$l^2\mathrm{Cyc}_r(i,j) = l\left(\delta_{i,0} + \delta_{0,j} + \delta_{i,j} + \sum_{n=1}^{l-2} a_{in+j}(n)\right) + l^2\mathrm{Cyc}_r(0,0)$$

where the subscripts in $a_{in+j}(n)$ are considered modulo $l$. See also van Wamelen [**Wam02**] for general cases where $e \ge 3$ and $p^r \equiv 1 \pmod{e}$. Recall that $C_r = [\mathrm{Cyc}_r(i,j) - D_i f]_{0 \le i,j \le e-1}$ is the multiplication matrix of the Gaussian periods $\eta_r(0), \ldots, \eta_r(e-1)$ of degree $e$ for $\mathbb{F}_{p^r}$. Hence Theorem 2.4 gives explicit lifts of not only the multiplication matrix $C_r$ but also of cyclotomic numbers $\mathrm{Cyc}_r(i,j)$ and of Jacobi sums $J_r(i,j)$ from $\mathbb{F}_{p^r}$ to $\mathbb{F}_{p^{nr}}$. Recall also that the Jacobi sum $J_r(i,j) = J_r(\chi^i, \chi^j) = \sum_{\alpha \in \mathbb{F}_{p^r}} \chi^i(\alpha)\chi^j(1-\alpha)$ where $\chi$ is a character of order $e$ on $\mathbb{F}_{p^r}$ with $\chi(\gamma) = \zeta_e$, $\mathbb{F}_{p^r}^\times = \langle\gamma\rangle$ and $\chi(0) = 0$.

We give examples of Theorem 2.4 for prime degree $e = l$ with $3 \le l \le 23$.

(1) $e = 3$ (cf. Gauss [**Gau01**, Setion 358], Katre and Rajwade [**KR85a**, Proposition 1], [**BEW98**, Section 3.1, Section 10.10]). Let $p$ be a prime with $p \equiv 1 \pmod{3}$. The Jacobi sum

$J_r(1,1)$ is given by

$$J_r(1,1) = J(c,d) = \frac{c+3d}{2} + 3d\zeta_3$$

where $c, d \in \mathbb{Z}$ are given as the integer solutions of the Diophantine equation

$$\begin{cases} 4p^r = c^2 + 27d^2, \\ c \equiv 1 \pmod 3, \ p \nmid c. \end{cases} \tag{6}$$

The equations have two solutions $(c, \pm d)$ and the sign of $d$ depends on the choice of $\gamma$. The unique solution with respect to $\gamma$ can be determined by

$$\gamma^{(p^r-1)/3} \equiv \frac{c+9d}{c-9d} \pmod p$$

(see Katre and Rajwade [**KR85a**, Proposition 1], [**BEW98**, Section 3.1]). The multiplication matrix $C_r$ of the Gaussian periods $\eta_r(0), \eta_r(1), \eta_r(2)$ of degree 3 for $\mathbb{F}_{p^r}$ is given by

$$C_r = C_r(p,c,d) = \begin{pmatrix} A-f & B-f & C-f \\ B & C & D \\ C & D & B \end{pmatrix}$$

where

$$A = \mathrm{Cyc}_r(0,0) = \frac{1}{9}(p^r + c - 8), \qquad B = \mathrm{Cyc}_r(0,1) = \frac{1}{18}(2p^r - c + 9d - 4),$$
$$C = \mathrm{Cyc}_r(0,2) = \frac{1}{18}(2p^r - c - 9d - 4), \qquad D = \mathrm{Cyc}_r(1,2) = \frac{1}{9}(p^r + c + 1)$$

(see [**BEW98**, Section 2.3]). Then we have

$$P_{3,r}(X) = \mathrm{Char}_X(C_r(p,c,d)),$$
$$P^*_{3,r}(X) = P^*_{3,r}(p,c,d;X) = 3^3 P_{3,r}((X-1)/3) = X^3 - 3p^r X - p^r c.$$

By Theorem 2.4, we get

$$C_{2r} = C_{2r}(p,c,d) = -C_r(p,c,d)^{(2)} = C_r(p^2, c^{(2)}, d^{(2)}),$$
$$C_{3r} = C_{3r}(p,c,d) = C_r(p,c,d)^{(3)} = C_r(p^3, c^{(3)}, d^{(3)})$$

where

$$c^{(2)} = \frac{1}{2}(-c^2 + 27d^2), \ d^{(2)} = -cd,$$
$$c^{(3)} = \frac{1}{4}c(c+9d)(c-9d), \ d^{(3)} = \frac{3}{4}d(c+3d)(c-3d).$$

Hence we obtain that

$$J_{2r}(1,1) = J(c^{(2)}, d^{(2)}), \qquad J_{3r}(1,1) = J(c^{(3)}, d^{(3)}),$$
$$P_{3,2r}(X) = \mathrm{Char}_X(C_r(p^2, c^{(2)}, d^{(2)})), \qquad P_{3,3r}(X) = \mathrm{Char}_X(C_r(p^3, c^{(3)}, d^{(3)}))$$

and

$$\begin{aligned} P^*_{3,2r}(X) = P^*_{3,r}(p^2, c^{(2)}, d^{(2)}) &= X^3 - 3p^{2r}X - p^{2r}c^{(2)} \\ &= X^3 - 3p^{2r}X - \frac{1}{2}p^{2r}(-c^2 + 27d^2), \\ P^*_{3,3r}(X) = P^*_{3,r}(p^3, c^{(3)}, d^{(3)}) &= X^3 - 3p^{3r}X - p^{3r}c^{(3)} \\ &= X^3 - \frac{3}{4}p^{2r}(c^2 + 27d^2)X - \frac{1}{4}\left(p^{3r}c(c+9d)(c-9d)\right) \\ &= (X - p^r c)\left(X + p^r\,\frac{c+9d}{2}\right)\left(X + p^r\,\frac{c-9d}{2}\right) \end{aligned}$$

(see [**BEW98**, Section 12.10]). The exponential cubic Gauss sum $g_{3r}(3) = \eta^*_{3r}(0)$ is one of the roots of $P^*_{3,3r}(X)$. Indeed, we see that

$$g_{3r}(3) = p^r c.$$

By repeating this procedure using Theorem 2.4, we get

$$\begin{aligned} J_{nr}(1,1) &= J(c^{(n)}, d^{(n)}), \\ P_{3,nr}(X) &= \mathrm{Char}_X(C_r(p^n, c^{(n)}, d^{(n)})), \\ P^*_{3,nr}(X) &= P^*_{3,r}(p^n, c^{(n)}, d^{(n)}), \\ g_{3mr}(3) &= p^r c^{(m)}. \end{aligned}$$

Note that the integers $c^{(n)}$, $d^{(n)}$ satisfy the equation (6) with respect to $p^{nr}$ again. In particular, we get

$$p^{nr} = \left(\frac{c^2 + 27d^2}{4}\right)^n = \frac{(c^{(n)})^2 + 27(d^{(n)})^2}{4}.$$

(2) $e = 5$ (cf. Lehmer [**Leh51**, Equation (10)], Berndt and Evans [**BE81**, Section 5], Katre and Rajwade [**KR85b**], [**BEW98**, Section 3.7], Hoshi [**Hos03**, Section 5], [**Hos06**, Section 3]). Let $p$ be a prime with $p \equiv 1 \pmod 5$. The Jacobi sum $J_r(1,1)$ is given by

$$J_r(1,1) = J(x,w,v,u) = \frac{1}{4}\left(Z\zeta_5 + \sigma^3(Z)\zeta_5^2 + \sigma(Z)\zeta_5^3 + \sigma^2(Z)\zeta_5^4\right)$$

where $Z = -x + 5w + 4v + 2u$, $\sigma(x, w, v, u) = (x, -w, -u, v)$ and $x, w, v, u \in \mathbb{Z}$ are obtained as the integer solutions of the system of Diophantine equations

$$\begin{cases} 16p^r = x^2 + 125w^2 + 50v^2 + 50u^2, \\ xw = v^2 - 4vu - u^2, \\ x \equiv 1 \pmod 5,\ p \nmid x^2 - 125w^2. \end{cases} \tag{7}$$

The equations have four solutions $\sigma^i(x, w, v, u)$ $(i = 0, 1, 2, 3)$ which depend on the choice of $\gamma$. The unique solution with respect to $\gamma$ can be determined by

$$\gamma^{(p^r-1)/5} \equiv \frac{x^2 - 125w^2 - 10(2xu - xv - 25wv)}{x^2 - 125w^2 + 10(2xu - xv - 25wv)} \pmod p$$

(see Katre and Rajwade [**KR85b**, Theorem 1]). The multiplication matrix of $C_r$ of the Gaussian periods $\eta_r(0), \ldots, \eta_r(4)$ of order 5 for $\mathbb{F}_{p^r}$ is given by

$$C_r = C_r(p, x, u, v, w) = \begin{pmatrix} A - f & B - f & C - f & D - f & E - f \\ B & E & F & G & F \\ C & F & D & G & G \\ D & G & G & C & F \\ E & F & G & F & B \end{pmatrix}$$

where

$$\begin{aligned} A &= \frac{1}{25}(p^r + 3x - 14), \\ B &= \frac{1}{100}(4p^r - 3x + 25w + 50v - 16), & C &= \frac{1}{100}(4p^r - 3x - 25w + 50u - 16), \\ D &= \frac{1}{100}(4p^r - 3x - 25w - 50u - 16), & E &= \frac{1}{100}(4p^r - 3x + 25w - 50v - 16), \\ F &= \frac{1}{50}(2p^r + x - 25w + 2), & G &= \frac{1}{50}(2p^r + x + 25w + 2). \end{aligned}$$

Then we have

$$\begin{aligned} P_{5,r}(X) &= \mathrm{Char}_X(C_r(p, x, u, v, w)), \\ P^*_{5,r}(X) &= P^*_{5,r}(p, x, w, v, u; X) = 5^5 P_{5,r}((X - 1)/5) \\ &= X^5 - 10p^r X^3 - 5p^r x X^2 + \frac{5}{4}p^r(4p^r - x^2 + 125w^2)X \\ &\quad + \frac{1}{8}p^r(-x^3 + 8p^r x + 625w(v^2 - u^2)). \end{aligned}$$

(see [**Leh51**, Equation (10)], [**BE81**, Section 5], [**Hos06**, Section 3]).

By Theorem 2.4, we get

$$C_{2r} = C_{2r}(p, x, w, v, u) = -C_r(p, x, w, v, u)^{(2)} = C_r(p^2, x^{(2)}, w^{(2)}, v^{(2)}, u^{(2)})$$

where

$$\begin{aligned}
x^{(2)} &= \frac{1}{4}(-x^2 - 125w^2 + 50v^2 + 50u^2),\\
w^{(2)} &= \frac{1}{2}(-xw - v^2 + 4vu + u^2),\\
v^{(2)} &= \frac{1}{2}(-xv - 10wu + 5vw),\\
u^{(2)} &= \frac{1}{2}(-xu - 10wv - 5uw).
\end{aligned}$$

Hence we get

$$\begin{aligned}
J_{2r}(1,1) &= J(x^{(2)}, w^{(2)}, v^{(2)}, u^{(2)}),\\
P_{5,2r}(X) &= \mathrm{Char}_X(C_r(p^2, x^{(2)}, w^{(2)}, v^{(2)}, u^{(2)})),\\
P^*_{5,2r}(X) &= P^*_{5,r}(p^2, p^2, x^{(2)}, w^{(2)}, v^{(2)}, u^{(2)}; X).
\end{aligned}$$

Continuing the argument, by Theorem 2.4, we also get $P_{5,5r}(X) = \mathrm{Char}_X(C_r^{(5)})$ and

$$P^*_{5,5r}(X) = \left(X - \frac{p^r}{16}L\right)\prod_{l=0}^{3}\left(X - \frac{p^r}{64}\sigma^l(M)\right)$$

where

$$\begin{aligned}
L = L(x, w, v, u) &= x^3 - 50(v^2 + u^2)w - 125(11v^2 - 4vu - 11u^2),\\
M = M(x, w, v, u) &= -x^3 + 25x\,(2ux + (7v - u)(v + 3u))\\
&\quad + 125w\left(25w^2 + 10(4v - 3u)w + (7v - u)(v + 3u)\right)\\
&\quad + 500(-2v^3 - 3v^2u + 6vu^2 + u^3).
\end{aligned}$$

The exponential quintic Gauss sum $g_{5r}(5)$ is a root of $P^*_{5,5r}(X)$ and indeed we see that

$$g_{5r}(5) = \frac{p^r}{16}L(x, w, v, u).$$

(see [**Hos06**, Theorem 1]).

By repeating this procedure using Theorem 2.4, we also get

$$\begin{aligned}
J_{nr}(1,1) &= J(x^{(n)}, w^{(n)}, v^{(n)}, u^{(n)}),\\
P_{5,nr}(X) &= \mathrm{Char}_X(C_r(p^n, x^{(n)}, w^{(n)}, v^{(n)}, u^{(n)})),\\
P^*_{5,nr}(X) &= P^*_{5,r}(p^n, x^{(n)}, w^{(n)}, v^{(n)}, u^{(n)}; X),\\
g_{5mr}(5) &= \frac{p^r}{16} L(x^{(m)}, w^{(m)}, v^{(m)}, u^{(m)}).
\end{aligned}$$

Note that the integers $x^{(n)}, w^{(n)}, v^{(n)}, u^{(n)}$ satisfy the equation (7) with respect to $p^{nr}$. In particular, we have

$$p^{nr} = \left(\frac{x^2+125w^2+50v^2+50u^2}{16}\right)^n = \frac{(x^{(n)})^2+125(w^{(n)})^2+50(v^{(n)})^2+50(u^{(n)})^2}{16},$$
$$x^{(n)}w^{(n)} = (v^{(n)})^2 - 4v^{(n)}u^{(n)} - (u^{(n)})^2.$$

For example, we take $p = 11$ and $r = 1$. Then we have $g_5(5) = \eta^*_5(0) = \frac{11}{16}L(1,1,1,0) = -979 = -11 \cdot 89$. Indeed, we may check that $g_5(5) = 13751 \cdot \zeta_{11}^0 + 14730 \cdot \sum_{i=1}^{10} \zeta_{11}^i = 13751 - 14730 = -979$ by the definition using a computer (cf. Section 5 (2) $e = 5$).

(3) $e = 7$ (cf. Leonard and Williams [**LW75**], [**BEW98**, Section 3.9]). Let $p$ be a prime with $p \equiv 1 \pmod 7$. The Jacobi sums $J_r(1,1)$ and $J_r(1,2)$ are given by

$$\begin{aligned}
J_r(1,1) &= J(x_1,x_2,x_3,x_4,x_5,x_6)\\
&= \frac{1}{12}\left(Z\zeta_7 + \sigma^4(Z)\zeta_7^2 + \sigma^5(Z)\zeta_7^3 + \sigma^2(Z)\zeta_7^4 + \sigma(Z)\zeta_7^5 + \sigma^3(Z)\zeta_7^6\right),\\
J_r(1,2) &= J'(t,u) = -t + u\sqrt{-7}
\end{aligned}$$

where $Z = -2x_1+6x_2+7x_5+21x_6$, $\sigma(x_1,x_2,x_3,x_4,x_5,x_6) = (x_1, -x_3, x_4, x_2, (-x_5-3x_6)/2, (x_5-x_6)/2)$ and $x_1,x_2,x_3,x_4,x_5,x_6,t,u \in \mathbb{Z}$ are obtained as the integer solutions of the system of Diophantine equations

$$(8)\quad \begin{cases}
72p^r = 2x_1^2 + 42x_2^2 + 42x_3^2 + 42x_4^2 + 343x_5^2 + 1029x_6^2,\\
12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0,\\
12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 + 28x_1x_6 + 48x_2x_3 + 24x_2x_4 + 24x_3x_4\\
+490x_5x_6 = 0,\\
x_1 \equiv 1 \pmod 7,\ (x_5,x_6) \neq (0,0),\\
p^r = t^2 + 7u^2,\ t \equiv 1 \pmod 7,\ u \equiv 3x_2 + 2x_3 \pmod 7.
\end{cases}$$

The equations has six solutions $\sigma^i(x_1, x_2, x_3, x_4, x_5, x_6)$ $(i = 0, 1, 2, 3, 4, 5)$ which depend on the choice of $\gamma$. The multiplication matrix $C_r$ of the Gaussian periods $\eta_r(0), \ldots, \eta_r(6)$ of order 7 for $\mathbb{F}_{p^r}$ is given by

$$
\begin{aligned}
C_r &= C_r(p, x_1, x_2, x_3, x_4, x_5, x_6, t, u) \\
&= \begin{pmatrix}
A-f & B-f & C-f & D-f & E-f & F-f & G-f \\
B & G & H & I & J & K & H \\
C & H & F & K & L & L & I \\
D & I & K & E & J & L & J \\
E & J & L & J & D & I & K \\
F & K & L & L & I & C & H \\
G & H & I & J & K & H & B
\end{pmatrix}
\end{aligned}
$$

where

$$
\begin{aligned}
A &= \frac{1}{49}(p^r + 3x_1 - 12t - 20), \\
B &= \frac{1}{196}(4p^r - 2x_1 + 28x_2 - 14x_3 + 49x_5 + 49x_6 + 8t + 56u - 24), \\
C &= \frac{1}{98}(2p^r - x_1 + 14x_3 + 7x_4 - 49x_6 + 4t + 28u - 12), \\
D &= \frac{1}{196}(4p^r - 2x_1 + 14x_2 + 28x_4 - 49x_5 + 49x_6 + 8t - 56u - 24), \\
E &= \frac{1}{196}(4p^r - 2x_1 - 14x_2 - 28x_4 - 49x_5 + 49x_6 + 8t + 56u - 24), \\
F &= \frac{1}{98}(2p^r - x_1 - 14x_3 - 7x_4 - 49x_6 + 4t - 28u - 12), \\
G &= \frac{1}{196}(4p^r - 2x_1 - 28x_2 + 14x_3 + 49x_5 + 49x_6 + 8t - 56u - 24), \\
H &= \frac{1}{147}(3p^r + 2x_1 - 49x_5 + 6t + 3), \\
I &= \frac{1}{98}(2p^r - x_1 + 7x_2 + 7x_3 - 7x_4 - 10t - 14u + 2), \\
J &= \frac{1}{294}(6p^r + 4x_1 + 49x_5 - 147x_6 + 12t + 6), \\
K &= \frac{1}{98}(2p^r - x_1 - 7x_2 - 7x_3 + 7x_4 - 10t + 14u + 2), \\
L &= \frac{1}{294}(6p^r + 4x_1 + 49x_5 + 147x_6 + 12t + 6)
\end{aligned}
$$

(see [**LW75**, Theorem] with a typo for $B$ ($147x_4$ should be $147x_5$)). Then we have

$$\begin{aligned}
P_{7,r}(X) &= \mathrm{Char}_X(C_r(p, x_1, x_2, x_3, x_4, x_5, x_6, t, u)),\\
P^*_{7,r}(X) &= P^*_{7,r}(p, x_1, x_2, x_3, x_4, x_5, x_6, t, u; X) = 7^7 P_{7,r}((X-1)/7)\\
&= X^7 - 21p^r X^5 + a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0
\end{aligned}$$

where $a_i = a_i(p, x_1, x_2, x_3, x_4, x_5, x_6, t, u)$ $(0 \le i \le 4)$ can be obtained explicitly (we omit the display here).

By Theorem 2.4, we get

$$C_{2r} = -C_r(p, x_1, x_2, x_3, x_4, x_5, x_6, t, u)^{(2)} = C_r(p^2, x_1^{(2)}, x_2^{(2)}, x_3^{(2)}, x_4^{(2)}, x_5^{(2)}, x_6^{(2)}, t^{(2)}, u^{(2)})$$

where

$$\begin{aligned}
x_1^{(2)} &= \frac{1}{12}(-2x_1^2 + 42x_2^2 + 42x_3^2 + 42x_4^2 - 343x_5^2 - 1029x_6^2),\\
x_2^{(2)} &= \frac{1}{12}(-4x_1x_2 + 14x_2x_5 - 42x_3x_5 - 42x_4x_5 - 42x_2x_6 - 42x_3x_6 + 42x_4x_6),\\
x_3^{(2)} &= \frac{1}{12}(-4x_1x_3 - 42x_2x_5 - 28x_3x_5 - 42x_2x_6 - 84x_4x_6),\\
x_4^{(2)} &= \frac{1}{12}(-4x_1x_4 - 42x_2x_5 + 14x_4x_5 + 42x_2x_6 - 84x_3x_6 + 42x_4x_6),\\
x_5^{(2)} &= \frac{1}{168}(-12x_2^2 + 72x_2x_3 + 24x_3^2 + 72x_2x_4 - 12x_4^2 - 56x_1x_5 + 49x_5^2 - 882x_5x_6 - 147x_6^2),\\
x_6^{(2)} &= \frac{1}{168}(12x_2^2 + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 - 12x_4^2 - 147x_5^2 - 56x_1x_6 - 98x_5x_6 + 441x_6^2),\\
t^{(2)} &= t^2 - 7u^2,\\
u^{(2)} &= 2tu.
\end{aligned}$$

By repeating this procedure using Theorem 2.4, we also get

$$\begin{aligned}
J_{nr}(1,1) &= J(x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, x_4^{(n)}, x_5^{(n)}, x_6^{(n)}),\\
J_{nr}(1,2) &= J'(t^{(n)}, u^{(n)}),\\
P_{7,nr}(X) &= \mathrm{Char}_X(C_r(p^n, x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, x_4^{(n)}, x_5^{(n)}, x_6^{(n)}, t^{(n)}, u^{(n)})),\\
P^*_{7,nr}(X) &= P^*_{7,r}(p^n, x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, x_4^{(n)}, x_5^{(n)}, x_6^{(n)}, t^{(n)}, u^{(n)}; X).
\end{aligned}$$

Note that the integers $x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, x_4^{(n)}, x_5^{(n)}, x_6^{(n)}, t^{(n)}, u^{(n)}$ satisfy the equation (8) with respect to $p^{nr}$. In particular, we have

$$\begin{aligned} p^{nr} &= \left(\frac{2x_1^2 + 42x_2^2 + 42x_3^2 + 42x_4^2 + 343x_5^2 + 1029x_6^2}{72}\right)^n \\ &= \frac{2(x_1^{(n)})^2 + 42(x_2^{(n)})^2 + 42(x_3^{(n)})^2 + 42(x_4^{(n)})^2 + 343(x_5^{(n)})^2 + 1029(x_6^{(n)})^2}{72}, \\ p^{nr} &= (t^2 + 7u^2)^n = (t^{(n)})^2 + 7(u^{(n)})^2. \end{aligned}$$

For example, we take $p = 29 = ef + 1$ with $f = 4$. Then we get

$$\begin{aligned} P_{7,7}^*(X) = (X - 442569)(X - 408465)(X - 233682)(X + 182671) \\ \cdot (X + 259405)(X + 317869)(X + 324771). \end{aligned}$$

Indeed, we may check that $g_7(7) = 594516413 \cdot \zeta_{29}^0 + 594834282 \cdot \sum_{i=1}^{28} \zeta_{29}^i = 594516413 - 594834282 = -317869 = -29 \cdot 97 \cdot 113$ by the definition using a computer (cf. Section 5 (3) $e = 7$).

(4) $e = 11$, $e = 13$ and $e = 17$. By using Thaine's formula [**Tha04**, page 259], we can obtain the multiplication matrix $C_1$ of the Gaussian periods $\eta_1(0), \ldots, \eta_1(e-1)$ of degree $e$ for $\mathbb{F}_{p^1}$. By using Theorem 2.4 as in the case of $e = 7$, we get $C_e = C_1^{(e)}$, $P_{e,e}(X) = \mathrm{Char}_X(C_1^{(e)})$ and the explicit factorization of $P_{e,e}^*(X)$ into $e$ linear factors. For example, we take $p = 23 = ef + 1$ with $e = 11$ and $f = 2$. Then, we get $C_{11} = C_1^{(11)}$, $P_{11,11}(X) = \mathrm{Char}_X(C_1^{(11)})$ and

$$\begin{aligned} P_{11,11}^*(X) = (X - 166665038)(X - 142959444)(X - 52918009)(X - 47121273) \\ \cdot (X - 3199967)(X + 19592803)(X + 23093817)(X + 44439427) \\ \cdot (X + 58652208)(X + 64390754)(X + 202694722) \end{aligned}$$

with a root $g_{11}(11) = \eta_{11}^*(0) = 52918009 = 23 \cdot 53 \cdot 43441$ (cf. Section 5 (4) $e = 11$). Similarly, by using Theorem 2.4, we can obtain for $p = 53 = ef + 1$ with $e = 13$ and $f = 4$, $P_{13,13}^*(X)$ with a root $g_{13}(13) = \eta_{13}^*(0) = 782475795674 = 2 \cdot 53 \cdot 7381847129$ and for $p = 103 = ef + 1$ with $e = 17$ and $f = 6$, $P_{17,17}^*(X)$ with a root $g_{17}(17) = \eta_{17}^*(0) = -651513206543247755 = -5 \cdot 7 \cdot 103 \cdot 172709 \cdot 1046412659$ (cf. Section 5 (5) $e = 13$, (6) $e = 17$).

(5) $e = 19$ and $e = 23$. We take $p = 191 = ef + 1$ with $e = 19$ and $f = 10$. As in the case (4), we can get $C_{19} = C_1^{(19)}$, $P_{19,19}(X) = \mathrm{Char}_X(C_1^{(19)})$ and the explicit factorization of $P_{19,19}^*(X)$ into 19 linear factors. We see that $\eta_{19}^*(i) = p\,\xi_i$ and the $\xi_i$'s ($i \neq 0$) are permuted

under the action $\zeta_p \mapsto \zeta_p^{\gamma}$ with $\mathbb{F}_p^{\times} = \langle\gamma\rangle$ (which depends on the choice of $\gamma$). Because we see that $\xi_0 \in \mathbb{F}_{191}^{\times}$ is of order 10 and $\xi_i \in \mathbb{F}_{191}^{\times}$ $(1 \leq i \leq 18)$ is of order 190, we can find $p\,\xi_0 = g_{19}(19) = \eta_{19}^*(0) = 2801935824159299141695 = 5 \cdot 191 \cdot 509 \cdot 26374987 \cdot 218546963$. Similarly, for $p = 47 = ef + 1$ with $e = 23$ and $f = 2$, we get $P_{23,23}^*(X)$ with a root $g_{23}(23) = \eta_{23}^*(0) = -492643134044787602 = -2 \cdot 17 \cdot 43 \cdot 47 \cdot 7169472509893$.

We give GAP ([**GAP**]) computations for examples above. The function `MultMat`$(e, p, \gamma)$ returns the multiplication matrix $C_1$ of the Gaussian periods $\eta_1(0), \ldots, \eta_1(e-1)$ of degree $e$ for $\mathbb{F}_{p^1}$ with respect to the generator $\gamma$ of $\mathbb{F}_p^{\times}$ using Thaine's formula [**Tha04**, page 259]. The function `dComp`$(A, B, d)$ returns the $d$-composition $A \overset{d}{*} B$ for two matrices $A$ and $B$.

```
MultMat:=function(e,p,g)
  local f,mat,j;
  f:=(p-1)/e;
  mat:=List([0..e-1],i->List([0..e-1],j->(-1/e^2)*Sum([0..e-1],
    l->Sum([0..e],k->Binomial(f*k,f*l)*g^(f*(l*i-k*j)))) mod p));
  if IsEvenInt(f) then for j in [1..e] do mat[1,j]:=mat[1,j]-f;od;
    else for j in [1..e] do mat[e/2+1,j]:=mat[e/2+1,j]-f;od;
  fi;
  return mat;
end;

Mode:=function(a,e)
  if a mod e = 0 then return e; else return a mod e;fi;
end;

dComp:=function(A,B,d)
  local s,t,i,j,e,mat;
  if Size(A)=Size(B) then e:=Size(A); else return "Input error";
  fi;
  mat:=List([0..e-1],i->List([0..e-1],j->Sum([0..e-1],
    s->Sum([0..e-1],t->A[s+1,t+1]*B[Mode(d*s+i+1,e),Mode(d*t+j+1,e)])))));
  return mat;
end;

gap> PrimitiveRootMod(7); # g=3
3
```

```
gap> C:=MultMat(3,7,3); # Multiplication matrix C1 for e=3, p=7, g=3
[ [ -2, -2, -1 ],
  [ 0, 1, 1 ],
  [ 1, 1, 0 ] ]
gap> C2:=dComp(C,C,-1); # C2=C^(2)
[ [ 10, 11, 12 ],
  [ -5, -4, -7 ],
  [ -4, -7, -5 ] ]
gap> C3:=dComp(C2,C,-1); # C3=C^(3)
[ [ -79, -72, -78 ],
  [ 42, 36, 36 ],
  [ 36, 36, 42 ] ]
gap> P3:=CharacteristicPolynomial(C3); # P3 is the priod polynomial for r=3
x_1^3+x_1^2-114*x_1+216
gap> R3:=RootsOfPolynomial(P3); # roots of P3
[ 9, 2, -12 ]
gap> L3:=List(R3,x->3*x+1); # roots of the reduced period polynomial P3^*
[ 28, 7, -35 ]
gap> X3:=L3/7;
[ 4, 1, -5 ]
gap> List(X3,x->x mod 7); # X3[2]=1 mod 7
[ 4, 1, 2 ]
gap> List(X3,x->x^2 mod 7);
[ 2, 1, 4 ]
gap> List(X3,x->x^3 mod 7); # X3[i] (i<>2) is of order 3 in F7^x
[ 1, 1, 1 ]
gap> L3[2]; # L3[2] is the exponential Gauss sum g_3(3)
7

gap> PrimitiveRootMod(11); # g=2
2
gap> C:=MultMat(5,11,2); # Multiplication matrix C1 for e=5, p=11, g=2
[ [ -2, -1, -2, -2, -2 ],
  [ 1, 0, 0, 1, 0 ],
  [ 0, 0, 0, 1, 1 ],
  [ 0, 1, 1, 0, 0 ],
  [ 0, 0, 1, 0, 1 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
```

```
gap> C5:=dComp(C4,C,-1); # C5=C^(5)
[ [ -25721, -25790, -25680, -25830, -25820 ],
  [ 6420, 6390, 6500, 6400, 6500 ],
  [ 6530, 6500, 6380, 6400, 6400 ],
  [ 6380, 6400, 6400, 6530, 6500 ],
  [ 6390, 6500, 6400, 6500, 6420 ] ]
gap> P5:=CharacteristicPolynomial(C5); # P5 is the priod polynomial for r=5
x_1^5+x_1^4-64420*x_1^3-2589700*x_1^2+558588000*x_1+11695320000
gap> R5:=RootsOfPolynomial(P5); # roots of P5
[ 255, 90, -20, -130, -196 ]
gap> L5:=List(R5,x->5*x+1); # roots of the reduced period polynomial P5^*
[ 1276, 451, -99, -649, -979 ]
gap> X5:=L5/11;
[ 116, 41, -9, -59, -89 ]
gap> List(X5,x->x mod 11); # X5[5]=-1 mod 11
[ 6, 8, 2, 7, 10 ]
gap> List(X5,x->x^2 mod 11);
[ 3, 9, 4, 5, 1 ]
gap> List(X5,x->x^5 mod 11); # X5[i] (i<>5) is of order 10 in F11^x
[ 10, 10, 10, 10, 10 ]
gap> L5[5]; # L5[5] is the exponential Gauss sum g_5(5)
-979
gap> Factors(L5[5]);
[ -11, 89 ]

gap> PrimitiveRootMod(29); # g=2
2
gap> C:=MultMat(7,29,2); # Multiplication matrix C1 for e=7, p=29, g=2
[ [ -4, -3, -4, -4, -2, -4, -4 ],
  [ 1, 0, 1, 0, 0, 1, 1 ],
  [ 0, 1, 0, 1, 1, 1, 0 ],
  [ 0, 0, 1, 2, 0, 1, 0 ],
  [ 2, 0, 1, 0, 0, 0, 1 ],
  [ 0, 1, 1, 1, 0, 0, 1 ],
  [ 0, 1, 0, 0, 1, 1, 1 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
gap> C3:=dComp(C2,C,-1);; # C3=C^(3)
gap> C7:=dComp(C4,C3,-1);; # C7=C^(7)
```

```
gap> P7:=CharacteristicPolynomial(C7);; # P7 is the priod polynomial for r=7
gap> R7:=RootsOfPolynomial(P7);; # roots of P7
gap> L7:=List(R7,x->7*x+1); # roots of the reduced period polynomial P7^*
[ 442569, 408465, 233682, -182671, -259405, -317869, -324771 ]
gap> X7:=L7/29;
[ 15261, 14085, 8058, -6299, -8945, -10961, -11199 ]
gap> List(X7,x->x mod 29); # X7[6]=1 mod 29
[ 7, 20, 25, 23, 16, 1, 24 ]
gap> List(X7,x->x^2 mod 29);
[ 20, 23, 16, 7, 24, 1, 25 ]
gap> List(X7,x->x^4 mod 29);
[ 23, 7, 24, 20, 25, 1, 16 ]
gap> List(X7,x->x^7 mod 29); # X7[i] (i<>6) is of order 7 in F29^x
[ 1, 1, 1, 1, 1, 1, 1 ]
gap> L7[6]; # L7[6] is the exponential Gauss sum g_7(7)
-317869
gap> Factors(L7[6]);
[ -29, 97, 113 ]

gap> PrimitiveRootMod(23); # g=5
5
gap> C:=MultMat(11,23,5); # Multiplication matrix C1 for e=11, p=23, g=5
[ [ -2, -2, -1, -2, -2, -2, -2, -2, -2, -2, -2 ],
  [ 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0 ],
  [ 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1 ],
  [ 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0 ],
  [ 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1 ],
  [ 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0 ],
  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0 ],
  [ 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
gap> C8:=dComp(C4,C4,-1);; # C8=C^(8)
gap> C3:=dComp(C2,C,-1);; # C3=C^(3)
gap> C11:=dComp(C8,C3,-1);; # C11=C^(11)
gap> P11:=CharacteristicPolynomial(C11);; # P11 is the priod polynomial for r=11
```

```
gap> R11:=RootsOfPolynomial(P11);; # roots of P11
gap> L11:=List(R11,x->11*x+1); # roots of the reduced period polynomial P11^*
[ 166665038, 142959444, 52918009, 47121273, 3199967, -19592803,
  -23093817, -44439427, -58652208, -64390754, -202694722 ]
gap> X11:=L11/23;;
gap> List(X11,x->x mod 23); # X11[3]=1 mod 23
[ 18, 16, 1, 3, 2, 13, 9, 12, 6, 8, 4 ]
gap> List(X11,x->x^2 mod 23);
[ 2, 3, 1, 9, 4, 8, 12, 6, 13, 18, 16 ]
gap> List(X11,x->x^11 mod 23); # X13[i] (i<>3) is of order 11 in F23^x
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
gap> L11[3]; # L11[3] is the exponential Gauss sum g_{11}(11)
52918009
gap> Factors(L11[3]);
[ 23, 53, 43411 ]

gap> PrimitiveRootMod(53); # g=2
2
gap> C:=MultMat(13,53,2); # Multiplication matrix C1 for e=13, p=53, g=2
[ [ -4, -3, -4, -4, -4, -4, -4, -2, -4, -4, -4, -4, -4 ],
  [ 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1 ],
  [ 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1 ],
  [ 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1 ],
  [ 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 2, 0, 0, 1, 0, 1, 0 ],
  [ 2, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0 ],
  [ 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0 ],
  [ 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 0 ],
  [ 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
gap> C8:=dComp(C4,C4,-1);; # C8=C^(8)
gap> C5:=dComp(C4,C,-1);; # C5=C^(5)
gap> C13:=dComp(C8,C5,-1);; # C13=C^(13)
gap> P13:=CharacteristicPolynomial(C13);; # P13 is the priod polynomial for r=13
gap> R13:=RootsOfPolynomial(P13) # roots of P13
```

```
gap> L13:=List(R13,x->13*x+1); # roots of the reduced period polynomial P13^*
[ 1040615291340, 782475795674, 664438112586, 338244988654, 117899008800,
  83828569254, -186980700750, -238169301889, -245670171356, -277653262665,
  -427932303889, -740552966334, -910543059425 ]
gap> X13:=L13/53;;
gap> List(X13,x->x mod 53); # X13[2]=1 mod 53
[ 47, 1, 49, 16, 13, 15, 42, 36, 44, 46, 10, 28, 24 ]
gap> List(X13,x->x^2 mod 53);
[ 36, 1, 16, 44, 10, 13, 15, 24, 28, 49, 47, 42, 46 ]
gap> List(X13,x->x^4 mod 53);
[ 24, 1, 44, 28, 47, 10, 13, 46, 42, 16, 36, 15, 49 ]
gap> List(X13,x->x^13 mod 53); # X13[i] (i<>2) is of order 13 in F53^x
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
gap> L13[2]; # L13[2] is the exponential Gauss sum g_{13}(13)
782475795674
gap> Factors(L13[2]);
[ 2, 53, 7381847129 ]

gap> PrimitiveRootMod(103); # g=5
5
gap> C:=MultMat(17,103,5); # Multiplication matrix C1 for e=17, p=103, g=5
[ [ -4, -6, -6, -6, -6, -6, -6, -6, -6, -6, -5, -4, -6, -6, -6, -6, -6 ],
  [ 0, 0, 1, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 1, 1 ],
  [ 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1 ],
  [ 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0 ],
  [ 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0 ],
  [ 0, 0, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 1, 0, 2 ],
  [ 0, 2, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0 ],
  [ 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0 ],
  [ 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0 ],
  [ 1, 0, 0, 0, 0, 1, 0, 0, 1, 0, 0, 2, 0, 1, 0, 0, 0 ],
  [ 2, 0, 0, 0, 0, 0, 0, 0, 1, 0, 2, 0, 0, 1, 0, 0, 0 ],
  [ 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0 ],
  [ 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0 ],
  [ 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1 ],
  [ 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1 ],
  [ 0, 1, 1, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
```

```
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
gap> C8:=dComp(C4,C4,-1);; # C8=C^(8)
gap> C16:=dComp(C8,C8,-1);; # C16=C^(16)
gap> C17:=dComp(C16,C,-1);; # C17=C^(17)
gap> P17:=CharacteristicPolynomial(C17);; # P17 is the priod polynomial for r=17
gap> R17:=RootsOfPolynomial(P17);; # roots of P17
gap> L17:=List(R17,x->17*x+1); # roots of the reduced period polynomial P17^*
[ 670357206530506901, 670088231006862759, 587253242462231659,
  464742031061114921, 461908111585063663, 356621718684896633,
  282238003107978403, 163898849457734107, 35922811461007315,
  -197783211402587952, -205052440856501077, -243310155546790559,
  -289516205265127375, -373934090375919493, -478731856802195967,
  -651513206543247755, -1253189038565026183 ]
gap> X17:=L17/103;;
gap> List(X17,x->x mod 103); # X17[16]=-1 mod 103
[ 73, 31, 24, 94, 90, 22, 3, 95, 89, 42, 10, 80, 27, 69, 39, 102, 37 ]
gap> List(X17,x->x^2 mod 103);
[ 76, 34, 61, 81, 66, 72, 9, 64, 93, 13, 100, 14, 8, 23, 79, 1, 30 ]
gap> List(X17,x->x^3 mod 103);
[ 89, 24, 22, 95, 69, 39, 27, 3, 37, 31, 73, 90, 10, 42, 94, 102, 80 ]
gap> List(X17,x->x^17 mod 103); # X17[i] (i<>16) is of order 34 in F103^x
[ 102, 102, 102, 102, 102, 102, 102, 102, 102, 102,
  102, 102, 102, 102, 102, 102, 102 ]
gap> L17[16]; # L17[16] is the exponential Gauss sum g_{17}(17)
-651513206543247755
gap> Factors(L17[16]);
[ -5, 7, 103, 172709, 1046412659 ]

gap> PrimitiveRootMod(191); # g=19
19
gap> C:=MultMat(19,191,19); # Multiplication matrix C1 for e=19, p=191, g=19
[ [ -10, -10, -10, -10, -10, -10, -9, -8, -8, -10,
    -10, -8, -10, -10, -10, -10, -10, -10, -8 ],
  [ 0, 2, 0, 1, 2, 2, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 2, 0, 0, 1, 1, 0, 1 ],
  [ 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 2, 1, 0, 1, 0, 1, 0, 1, 2 ],
  [ 0, 2, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 2 ],
  [ 0, 2, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0 ],
  [ 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0 ],
```

```
  [ 2, 0, 1, 0, 1, 0, 0, 0, 0, 2, 0, 0, 0, 1, 0, 1, 2, 0, 0 ],
  [ 2, 0, 1, 0, 0, 0, 0, 0, 2, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0 ],
  [ 0, 0, 0, 0, 0, 0, 1, 2, 0, 0, 1, 1, 2, 1, 1, 0, 0, 0, 1 ],
  [ 0, 1, 1, 2, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 2, 0 ],
  [ 2, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 2, 0, 1, 0, 0, 0, 0, 0 ],
  [ 0, 0, 2, 0, 0, 0, 1, 0, 1, 2, 0, 0, 2, 0, 1, 0, 1, 0, 0 ],
  [ 0, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, 1 ],
  [ 0, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 2, 1, 1, 1 ],
  [ 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 2, 0, 2, 0, 0 ],
  [ 0, 0, 1, 0, 0, 0, 0, 2, 1, 0, 1, 0, 1, 0, 1, 2, 0, 1, 0 ],
  [ 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 2, 0, 0, 1, 1, 0, 1, 0, 0 ],
  [ 2, 0, 1, 2, 2, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0, 0 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
gap> C8:=dComp(C4,C4,-1);; # C8=C^(8)
gap> C16:=dComp(C8,C8,-1);; # C16=C^(16)
gap> C3:=dComp(C2,C,-1);; # C3=C^(3)
gap> C19:=dComp(C16,C3,-1);; # C19=C^(19)
gap> P19:=CharacteristicPolynomial(C19);; # P19 is the priod polynomial for r=19
gap> R19:=RootsOfPolynomial(P19);; # roots of P19
gap> L19:=List(R19,x->19*x+1); # roots of the reduced period polynomial P19^*
[ 55891098112086637001228, 21343147495425176673226, 16127550524178031129657,
  14355859672843887131634, 10195021892556248415182, 777734271088664497713l,
  577633811959984735062l, 508051386374073968346l, 280193582415929914169l,
  85941359850926610557l, -196783169381560744866l, -204250013609128033507l,
  -55993895385997956308l, -110602827743399434685l, -141175367125961717113l,
  -199502291828313888976l, -272508920796453753571l, -281872662315144737708l,
  -300322934645517409793l ]
gap> X19:=List(L19,x->x/191);;
gap> List(X19,x->x mod 191);
[ 58, 182, 157, 178, 94, 21, 126, 151, 142, 57,
  99, 113, 146, 88, 112, 143, 105, 137, 183 ]
gap> List(X19,x->x^10 mod 191); # X19[9]^10=1 mod 191
[ 52, 136, 107, 121, 125, 30, 25, 154, 1, 32,
  36, 69, 6, 160, 5, 150, 153, 177, 180 ]
gap> List(X19,x->x^2 mod 191);
[ 117, 81, 10, 169, 50, 59, 23, 72, 109, 2,
  60, 163, 115, 104, 129, 12, 138, 51, 64 ]
gap> List(X19,x->x^5 mod 191); # X19[9] is of order 10 in F191^x
```

```
[ 166, 161, 38, 11, 70, 139, 186, 66, 190, 37,
  185, 159, 31, 55, 14, 155, 41, 122, 84 ]
gap> List(X19,x->x^19 mod 191); # X19[i] (i<>9) is of order 190 in F191^x
[ 152, 152, 152, 152, 152, 152, 152, 152, 152, 152,
  152, 152, 152, 152, 152, 152, 152, 152, 152 ]
gap> L19[9]; # L19[9] is the exponential Gauss sum g_{19}(19)
2801935824159299141695
gap> Factors(L19[9]);
[ 5, 191, 509, 26374987, 218546963 ]

gap> PrimitiveRootMod(47); # g=5
5
gap> C:=MultMat(23,47,5);  # Multiplication matrix C1 for e=23, p=47, g=5
[ [ -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2,
    -2, -2, -2, -2, -2, -2, -1, -2, -2, -2, -2 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0 ],
  [ 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1 ],
  [ 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1 ],
  [ 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0 ],
  [ 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0 ],
  [ 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 ],
  [ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0 ] ]
gap> C2:=dComp(C,C,-1);; # C2=C^(2)
gap> C4:=dComp(C2,C2,-1);; # C4=C^(4)
```

```
gap> C8:=dComp(C4,C4,-1);; # C8=C^(8)
gap> C16:=dComp(C8,C8,-1);; # C16=C^(16)
gap> C3:=dComp(C2,C,-1);; # C3=C^(3)
gap> C7:=dComp(C4,C3,-1);; # C7=C^(7)
gap> C23:=dComp(C16,C7,-1);; # C23=C^(23)
gap> P23:=CharacteristicPolynomial(C23);; # P23 is the priod polynomial for r=23
gap> R23:=RootsOfPolynomial(P23);; # roots of P23
gap> L23:=List(R23,x->23*x+1); # roots of the reduced period polynomial P23^*
[ 142339874433137221525, 118065170266710759348, 90401156916499269233,
  55373954393947818396, 55099193646218848063, 42654144441633168738,
  42378310496086559486, 36268843595424974262, 35660322726333362220,
  34760976326466677323, 28446187386897694871, 17050560055492972666,
  -492643134044787602, -9055501540645768832, -16107397702852877550,
  -31331987537967805455, -36858108220907188977, -38922282154313258582,
  -39922556198217904917, -67269172064831016965, -90222434992270940059,
  -151942428479066503710, -216374182659731273482 ]
gap> X23:=L23/47;;
gap> List(X23,x->x mod 47); # X23[13]=1 mod 47
[ 9, 32, 24, 4, 17, 12, 8, 2, 3, 37, 14, 18,
  1, 21, 36, 16, 25, 28, 42, 27, 34, 6, 7 ]
gap> List(X23,x->x^2 mod 47);
[ 34, 37, 12, 16, 7, 3, 17, 4, 9, 6, 8, 42,
  1, 18, 27, 21, 14, 32, 25, 24, 28, 36, 2 ]
gap> List(X23,x->x^23 mod 47); # X23[i] (i<>13) is of order 23 in F47^x
[ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 ]
gap> L23[13]; # L23[13] is the exponential Gauss sum g_{23}(23)
-492643134044787602
gap> Factors(L23[13]);
[ -2, 17, 43, 47, 7169472509893 ]
```

# Bibliography to Chapter 2


[BE81] B. C. Berndt, R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981) 107–129.

[BEW98] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Wiley, New York, 1998.

[BMW82] L. D. Baumert, W. H. Mills, R. L. Ward, *Uniform cyclotomy*, J. Number Theory **14** (1982) 67–82.

[DH35] H. Davenport, H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, (German) J. Reine Angew. Math. **172** (1935) 151–182.

[Dic35] L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935) 391–424.

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1; 2021. (http://www.gap-system.org).

[Gau01] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801.

[HH05a] K. Hashimoto, A. Hoshi, *Families of cyclic polynomials obtained from geometric generalization of Gaussian period relations*, Math. Comp. **74** (2005) 1519–1530.

[HH05b] K. Hashimoto, A. Hoshi, *Geometric generalization of Gaussian period relations with application to Noether's problem for meta-cyclic groups*, Tokyo J. Math. **28** (2005) 13–32.

[Hos03] A. Hoshi, *Multiplicative quadratic forms on algebraic varieties*, Proc. Japan Acad. Ser. A Math. Sci. **79** (2003) 71–75.

[Hos06] A. Hoshi, *Explicit lifts of quintic Jacobi sums and period polynomials for* $\mathbb{F}_q$, Proc. Japan Acad. Ser. A Math. Sci. **82** (2006) 87–92.

[HK] A. Hoshi, K. Kanai, *Davenport and Hasse's theorems and lifts of multiplication matrices of Gaussian periods*, arXiv:2105.14872.

[KR85a] S. A. Katre, A. R. Rajwade, *Complete solution of the cyclotomic problem in* $\mathbb{F}_q^*$ *for any prime modulus* $l$, $q = p^\alpha$, $p \equiv 1 \pmod{l}$, Acta Arith. **45** (1985) 183–199.

[KR85b] S. A. Katre, A. R. Rajwade, *Unique determination of cyclotomic numbers of order five*, Manuscripta Math. **53** (1985) 65–75.

[Leh51] E. Lehmer, *The quintic character of* 2 *and* 3, Duke Math. J. **18** (1951) 11–18.

[Leh88] E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988) 535–541.

[LW75] P. A. Leonard, K. S. Williams, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc. **51** (1975) 295–300.

[MR72] R. J. McEliece, H. Rumsey, Jr, *Euler products, cyclotomy, and coding*, J. Number Theory **4** (1972) 302–311.

[Mye81] G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith. **39** (1981) 251–264.

[PAR82] J. C. Parnami, M. K. Agrawal, A. R. Rajwade, *Jacobi sums and cyclotomic numbers for a finite field*, Acta Arith. **41** (1982) 1–13.

[SW88] R. Schoof, L. C. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988) 543–556.

[Ter99] A. Terras, *Fourier analysis on finite groups and applications*, London Mathematical Society Student Texts, 43, Cambridge University Press, Cambridge, 1999, x+442 pp.

[Tha96] F. Thaine, *Properties that characterize Gaussian periods and cyclotomic numbers*, Proc. Amer. Math. Soc. **124** (1996) 35–45.

[Tha99] F. Thaine, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Trans. Amer. Math. Soc. **351** (1999) 4769–4790.

[Tha00] F. Thaine, *Families of irreducible polynomials of Gaussian periods and matrices of cyclotomicnumbers*, Math. Comp. **69** (2000) 1653–1666.

[Tha01] F. Thaine, *Jacobi sums and new families of irreducible polynomials of Gaussian periods*, Math. Comp. **70** (2001) 1617–1640.

[Tha04] F. Thaine, *Cyclic polynomials and the multiplication matrices of their roots*, J. Pure Appl. Algebra **188** (2004) 247–286.

[Tha08] F. Thaine, *On the construction of families of cyclic polynomials whose roots are units*, Experiment. Math. **17** (2008) 315–331.

[Wam02] P. van Wamelen, *Jacobi sums over finite fields*, Acta Arith. **102** (2002) 1–20.

[Wei49] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949) 497–508.

# List of papers by Kazuki Kanai

1. *Norm one tori and Hasse norm principle*,
   to appear in Mathematics of Computation,
   with Akinari Hoshi, Aiichi Yamasaki.