Automorphism groups of monoids acting on number fields

Jannik Hess

Bachelor Thesis

October 2019

University of Stuttgart
Germany

Contents

Chapter 0

Introduction

0.1 Monoids

A monoid is a set with an associative multiplication and a neutral element, cf. Definition 1. For instance, the symmetric monoid $\mathrm{S}_n^{\mathrm{mon}}$ on n letters consists of all maps from $[1, n]$ to $[1, n]$, with composition as multiplication. By Cayley's Lemma, every finite monoid is isomorphic to a submonoid of $\mathrm{S}_n^{\mathrm{mon}}$ for a suitable n, cf. Lemma 12. For instance, in degree $n = 3$, there are 699 submonoids of $\mathrm{S}_3^{\mathrm{mon}}$, they form 160 conjugacy classes and 154 isoclasses.

0.2 Monoid algebras and field extensions

Given a finite monoid M, the monoid algebra $\mathbb{Q}M$ is the $\mathbb{Q}$-vector space with basis M and multiplication induced by the multiplication on M, cf. Definition 20. Since $\overline{\mathbb{Q}M} := \mathbb{Q}M / \operatorname{Jac}(\mathbb{Q}M)$ is semisimple, it is isomorphic to a direct product of matrix algebras over division algebras. So its center is a direct product of number fields. An automorphism σ of the monoid M induces a $\mathbb{Q}$-algebra automorphism $\sigma_{\mathbb{Q}}$ of the monoid algebra $\mathbb{Q}M$, yielding an automorphism $\overline{\sigma_{\mathbb{Q}}}$ of $\overline{\mathbb{Q}M}$. Then $\overline{\sigma_{\mathbb{Q}}}$ restricts to an automorphism of $\mathrm{Z}(\overline{\mathbb{Q}M})$. Let $1_{\mathrm{Z}(\overline{\mathbb{Q}M})} = \overline{e_1} + \cdots + \overline{e_s}$ be an orthogonal decomposition into primitive central idempotents. The automorphisms fixing a given idempotent $\overline{e_i}$ of $\mathrm{Z}(\overline{\mathbb{Q}M})$ form a subgroup $\operatorname{Aut}_{\overline{e_i}}(M)$ of the automorphism group $\operatorname{Aut}(M)$ of M. This subgroup acts on the number field $Z_i := \overline{e_i} \cdot \mathrm{Z}(\overline{\mathbb{Q}M})$. This yields the fixed field F_i under this action and the Galois extension $Z_i \,|\, F_i$, cf. Remark 21. Its Galois group is isomorphic to the factor group of $\operatorname{Aut}_{\overline{e_i}}(M)$ modulo the kernel of this action.

The Clifford-Munn-Ponizovsky-Theorem establishes a close connection from a monoid representation to a group representation for a suitable group [**2,** Th. 5.5][**3,** Th. 2.7]. Whether the endomorphisms rings of these representations are isomorphic, is not clear to me.

In our examples, the field Z_i has always been an abelian extension of $\mathbb{Q}$.

0.3 Twisted monoid algebras and field extensions

A two-cocycle is a map $\alpha : M \times M \longrightarrow \mathbb{Q}^\times$ satisfying

$$1 = (n, l)\alpha \cdot ((m \cdot n, l)\alpha)^{-1} \cdot (m, n \cdot l)\alpha \cdot ((m, n)\alpha)^{-1}$$

for m, n, $l \in M$ and

$$1 = (1_M, m)\alpha = (m, 1_M)\alpha$$

for $m \in M$; cf. Definition 22. Given a finite monoid M, the monoid algebra $\mathbb{Q}_\alpha M$ is the $\mathbb{Q}$-vector space with basis M and multiplication induced by the multiplication on M with an extra factor resulting from α, cf. Definition 23. Since $\overline{\mathbb{Q}_\alpha M} := \mathbb{Q}_\alpha M / \operatorname{Jac}(\mathbb{Q}_\alpha M)$ is semisimple, it is isomorphic to a direct product of matrix algebras over division algebras. So its center is a direct product of number fields. An automorphism σ of the monoid M that respects the two-cocycle α induces a $\mathbb{Q}$-algebra automorphism $\sigma_\mathbb{Q}$ of the twisted monoid algebra $\mathbb{Q}_\alpha M$, yielding an automorphism $\overline{\sigma_\mathbb{Q}}$ of $\overline{\mathbb{Q}_\alpha M}$. Then $\overline{\sigma_\mathbb{Q}}$ restricts to an automorphism of $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$. Let $1_{\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})} = \overline{e_1} + \cdots + \overline{e_s}$ be an orthogonal decomposition into primitive idempotents. Considering the automorphisms fixing a given idempotent $\overline{e_i}$ of $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$ we obtain a subgroup $\operatorname{Aut}_{\alpha,\overline{e_i}}(M)$ of the group $\operatorname{Aut}_\alpha(M)$ of automorphisms of M that respect α. This subgroup acts on the number field $Z_i := \overline{e_i} \cdot \mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$. This yields the fixed field F_i under this action and the Galois extension $Z_i \,|\, F_i$, cf. Remark 24. Its Galois group is isomorphic to the factor group of $\operatorname{Aut}_{\alpha,\overline{e_i}}(M)$ modulo the kernel of this action.

For instance, this method yielded the number fields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $\mathbb{Q}(\sqrt[3]{2}, \mathrm{i})$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_5)$, $\mathbb{Q}(\sqrt[3]{2}, \zeta_7)$, $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$, $\mathbb{Q}(\sqrt[3]{3}, \zeta_3)$ and $\mathbb{Q}(\sqrt[5]{3}, \zeta_3)$, none of which is contained in a cyclotomic field.

However, in all these examples, $Z_i \,|\, F_i$ is an abelian extension; so only an abelian part of $\operatorname{Aut}(M)$ acts on Z_i .

The question arises which finite groups may arise as the image of the action of $\operatorname{Aut}_{\alpha,\overline{e_i}}(M)$ on the number field Z_i and thus as $\operatorname{Gal}(Z_i \,|\, F_i)$.

Conventions

(1) Given a, $b \in \mathbb{Z}$, we write $[a, b] := \{\, z \in \mathbb{Z} \,:\, a \leqslant z \leqslant b \,\}$.

(2) Given $a \in \mathbb{Z}$, we write $\mathbb{Z}_{\geqslant a} := \{\, z \in \mathbb{Z} \,:\, a \leqslant z \,\}$, etc.

(3) We compose on the right. So given maps $X \xrightarrow{f} Y \xrightarrow{g} Z$, their composite is denoted by $X \xrightarrow{fg = f \cdot g} Z$ and maps $x \in X$ to $x(f \cdot g) = (xf)g$.

(4) Given a set X, "for $x \in X$" means "for all $x \in X$".

(5) Given a finite set X, we denote by $|X|$ its cardinality.

(6) Given a field K and given $n \in \mathbb{Z}_{\geqslant 1}$, we write the unit matrix $\mathrm{E}_n := \operatorname{diag}(1_K, \ldots, 1_K) \in K^{n \times n}$.

(7) The order of the dihedral group D_n is $2n$.

(8) The symbol %% in a comment in Magma-code refers to a function that is used in this line.

Chapter 1

Monoids

1.1 Definitions

Definition 1 A *monoid* is a set M, together with a map

$$\begin{array}{ccccc} M & \times & M & \xrightarrow{(\cdot)} & M \\ (m & , & n) & \mapsto & m \cdot n \, , \end{array}$$

called *multiplication*, such that (Mon 1–2) hold.

(Mon 1) There exists an element $e \in M$ such that $e \cdot m = m = m \cdot e$ for $m \in M$.

(Mon 2) We have $(m \cdot n) \cdot p = m \cdot (n \cdot p)$ for $m, n, p \in M$.

Often we write $M := (M, \cdot)$ to refer to this monoid.

Remark 2 *Suppose given a monoid M.*

There exists a unique element $e \in M$ such that $e \cdot m = m = m \cdot e$ for $m \in M$.

This element e is called the *neutral* element of M. It is written $1 = 1_M := e$.

Proof. We have to show uniqueness. Suppose given elements $e, e' \in M$ such that $e \cdot m = m = m \cdot e$ and $e' \cdot m = m = m \cdot e'$ for $m \in M$. Then $e = e \cdot e' = e'$. □

Remark 3 Suppose given a monoid M. If $M = \{1_M\}$ then M is called a *trivial monoid*.

Definition 4 Suppose given a monoid M.

Suppose given $m \in M$.

The element m is called *invertible* if there exists an element $m' \in M$ such that $m \cdot m' = 1$ and $m' \cdot m = 1$.

In this case, m' is uniquely determined and written $m^{-1} := m'$.

Suppose given elements $m', \widetilde{m}'$ such that $m \cdot \widetilde{m}' = 1$ and $m' \cdot m = 1$.

Then $\widetilde{m}' = (m' \cdot m) \cdot \widetilde{m}' = m' \cdot (m \cdot \widetilde{m}') = m'$.

Definition 5 Suppose given a set X.

Let the *symmetric monoid* be defined as

$$\mathrm{S}_X^{\mathrm{mon}} := \{ X \xrightarrow{f} X : f \text{ is a map} \}$$

as the set of all maps from X to X, with multiplication given by composition. Its neutral element is given by $1_{\mathrm{S}_X^{\mathrm{mon}}} = \mathrm{id}_X$.

Given $n \in \mathbf{Z}_{\geqslant 0}$, we write $\mathrm{S}_n^{\mathrm{mon}} := \mathrm{S}_{[1,n]}^{\mathrm{mon}}$. Note that $|\,\mathrm{S}_n^{\mathrm{mon}}\,| = n^n$.

Definition 6 Suppose given monoids M and M'.

A map $f : M \to M'$ is called a *monoid morphism* if the properties $(1, 2)$ hold.

(1) We have $1_M f = 1_{M'}$.

(2) We have $(m \cdot n)f = mf \cdot nf$ for $m,\, n \in M$.

A bijective monoid morphism is called a *monoid isomorphism.*

We say that the monoids M and M' are *isomorphic* if there exists a monoid isomorphism from M to M'.

An isomorphism from M to M is called an *automorphism.* The set $\mathrm{Aut}(M)$ of automorphisms of M, together with composition as multiplication, is a group.

Remark 7 Suppose given monoids M and M'.

Suppose given a monoid isomorphism $M \xrightarrow{f} M'$.

Then its inverse $M' \xrightarrow{f^{-1}} M$ is also a monoid isomorphism.

Proof. We have to show that $M' \xrightarrow{f^{-1}} M$ is also a monoid morphism.

We have $1_{M'} f^{-1} = 1_M f f^{-1} = 1_M$.

Given $m',\, n' \in M'$, we obtain

$$(m' \cdot n')f^{-1} = (m'f^{-1}f \cdot n'f^{-1}f)f^{-1} = (m'f^{-1} \cdot n'f^{-1})ff^{-1} = m'f^{-1} \cdot n'f^{-1} .$$

□

Remark 8 Suppose given a set U of monoids.

Being isomorphic is an equivalence relation on U ; cf. Remark 7.

The equivalence classes are called *isoclasses* of U.

Definition 9 Suppose given a monoid M.

A subset $N \subseteq M$ is called a *submonoid* if the properties $(1, 2)$ hold.

(1) We have $1_M \in N$.

(2) We have $m \cdot m' \in N$ for $m,\, m' \in N$.

To denote that N is a submonoid of M, we write $N \leqslant M$.

A submonoid is a monoid, with multiplication $(\cdot)|_{N\times N}^{N} : N \times N \to N$. We obtain $1_N = 1_M$.

Given a submonoid N of M, the inclusion map $N \to M : n \mapsto n$ is a monoid morphism.

Remark 10 *Suppose given monoids M and M'.*

Suppose given a monoid morphism $M \xrightarrow{f} M'$.

Then its image $Mf \;:=\; \{\, m' \in M' : \exists\, m \in M \text{ such that } mf = m' \,\}$ is a submonoid of M'.

Proof. We have to show $1_{M'} \in Mf$. We have $1_M \in M$. We obtain $1_{M'} = 1_M f \in Mf$.

We have to show $m' \cdot n' \in Mf$ for $m', n' \in Mf$. We choose $m,\, n \in M$ such that $mf = m'$ and $nf = n'$. We obtain $m' \cdot n' = mf \cdot nf = (m \cdot n)f \in Mf$. ▫

Remark 11 *Suppose given an injective monoid morphism $f : M \to M'$.*

Then $f|^{Mf}$ is a monoid isomorphism. In particular, M is isomorphic to the submonoid Mf of M' ; cf. Remark 10.

Proof. The map $f|^{Mf}$ is a monoid morphism; cf. Definition 6. By construction, $f|^{Mf}$ is bijective. So $f|^{Mf}$ is a monoid isomorphism. ▫

1.2 Cayley for monoids

Let M be a monoid.

The following lemma is the analogue of Cayley's Theorem for groups.

Lemma 12 *The map*

$$\begin{array}{rccc} \sigma : & M & \to & \mathrm{S}_M^{\mathrm{mon}} \\ & m & \mapsto & (m\sigma : x \mapsto x \cdot m) \end{array}$$

is an injective monoid morphism.

In particular, M is isomorphic to a submonoid of $\mathrm{S}_M^{\mathrm{mon}}$.

Proof. We have to show that σ is a monoid morphism.

We have to show that $1_M\sigma \overset{!}{=} 1_{\mathrm{S}_M^{\mathrm{mon}}} = \mathrm{id}_M$.

In fact, for $x \in M$, we obtain $(x)(1_M\sigma) = x \cdot 1_M = x = (x)\,\mathrm{id}_M$.

We have to show that $(m \cdot \widetilde{m})\sigma \overset{!}{=} (m)\sigma \cdot (\widetilde{m})\sigma$, for $m, \widetilde{m} \in M$.

In fact, for $x \in M$, we obtain

$$\begin{array}{rcl} (x)((m \cdot \widetilde{m})\sigma) & = & x \cdot m \cdot \widetilde{m} \\ & = & \big(x \cdot m\big)(\widetilde{m}\sigma) \\ & = & \big((x)(m\sigma)\big)(\widetilde{m}\sigma) \\ & = & (x)(m\sigma \cdot \widetilde{m}\sigma)\ . \end{array}$$

We have to show that σ is injective. Suppose given $m,\ \widetilde{m} \in M$ such that $m\sigma = \widetilde{m}\sigma$. We have to show that $m \overset{!}{=} \widetilde{m}$.

In fact, we get $m = 1_M \cdot m = (1_M)(m\sigma) = (1_M)(\widetilde{m}\sigma) = 1_M \cdot \widetilde{m} = \widetilde{m}$.

The monoid M is isomorphic to the image $M\sigma \leqslant \mathrm{S}_M^{\mathrm{mon}}$ of the injective monoid morphism σ ; cf. Remarks 10 and 11. □

Remark 13 *If M is finite, then the monoid $\mathrm{S}_M^{\mathrm{mon}}$ is isomorphic to $\mathrm{S}_n^{\mathrm{mon}}$ for $n := |M|$.*

Definition 14 Suppose given a monoid M.

Suppose given a subset $X \subseteq M$.

Let $\langle X \rangle := \bigcap_{X \subseteq N \leqslant M} N$ be the *submonoid of M generated by X.*

Remark 15 Suppose given a monoid M and a subset $X \subseteq M$.

(1) The subset $\langle X \rangle$ is in fact a submonoid of M

since $1_M \in N$ for $X \subseteq N \leqslant M$, i.e. $1_M \in \langle X \rangle$ and since given $y, \widetilde{y} \in \langle X \rangle$, we have $y \cdot \widetilde{y} \in N$ for each $X \subseteq N \leqslant M$, i.e. $y, \widetilde{y} \in \langle X \rangle$.

(2) The submonoid $\langle X \rangle$ contains X and is contained in each submonoid of M containing X. This properly characterises $\langle X \rangle$ uniquely.

Assume $Q \leqslant M$ having these properties, then Q contains X so $\langle X \rangle \leqslant Q$. On the other side Q is contained in each submonoid of M containing X so Q is also contained in the cap of all these submonoids and with that $Q \leqslant \langle X \rangle$, too.

(3) The submonoid $\langle X \rangle$ is the set of finite products in M with factors from X, the empty product being 1_M.

1.2.1 Orders of monoid elements

Suppose given a finite monoid M.

Definition 16 Suppose given an element $m \in M$.

Consider the set $P := \{(i, j) \in \mathbf{Z}_{\geqslant 0} \times \mathbf{Z}_{\geqslant 0} : i < j, m^i = m^j\}$

The set P is not empty, since M is finite.

The set P contains a unique element (a, b) such that $b \leqslant j$ for $(i, j) \in P$.

Let $\mathrm{order}(m) := (a, b)$.

So $m^a = m^b$.

Moreover, given $0 \leqslant i < j$ such that $m^i = m^j$, then either $(a, b) = (i, j)$ or $b < j$.

Remark 17 *Suppose given $m \in M$.*

We have $\mathrm{order}(m) = (0, b)$ *for some* $b \in \mathbf{Z}_{\geqslant 1}$ *if and only if* m *is invertible.*

Suppose $\mathrm{order}(m) = (0, b)$.

We have to show that m is invertible.

In fact, $m^k = 1$, so $m^{k-1} \cdot m = 1$ and $m \cdot m^{k-1} = 1$.

Suppose $\mathrm{order}(m) = (a, b)$ with $a \geqslant 1$.

We have to show that m is not invertible.

Assume m to be invertible.

We have $m^a = m^b$.

Then $m^0 = m^a \cdot (m^{-1})^a = m^b \cdot (m^{-1})^a = m^{b-a}$.

Moreover, $b \leqslant b - a$, which is a *contradiction.*

Remark 18 *Suppose given an isomorphism* $f : M \to M'$ *of monoids.*

Suppose given $m \in M$.

Then $\mathrm{order}(m) = \mathrm{order}(mf)$.

We make use of Remark 17 in an algorithmic search for isomorphisms to exclude maps in the following way.

Remark 19 *Suppose given monoids* M *and* M' *and a map* $f : M \to M'$.

If $\mathrm{order}(m) \neq \mathrm{order}(mf)$ *for some* $m \in M$, *then* f *is not an isomorphism of monoids.*

1.3 Algorithmic search for submonoids of $\mathrm{S}_n^{\mathrm{mon}}$

We use Magma [**1**] to calculate the relevant monoids.

1.3.1 First implementations of monoids

In the following programs we calculate the symmetric monoid $\mathrm{S}_n^{\mathrm{mon}}$ as mentioned in Definition 5, with the composition as its multiplication.

```
SymMon := function(n) // n: positive integer, degree of the symmetric monoid
  return [[x[i] : i in [1..n]] : x in CartesianPower([1..n],n)];
end function;
```

For example in degree $n = 3$ we receive the following list of $n^n = 27$ elements:

```
> SymMon(3);
[
    [ 1, 1, 1 ],
    [ 1, 1, 2 ],
    [ 1, 1, 3 ],
    [ 1, 2, 1 ],
    [ 1, 2, 2 ],
    [ 1, 2, 3 ],
    [ 1, 3, 1 ],
    [ 1, 3, 2 ],
    [ 1, 3, 3 ],
    [ 2, 1, 1 ],
    [ 2, 1, 2 ],
    [ 2, 1, 3 ],
    [ 2, 2, 1 ],
    [ 2, 2, 2 ],
    [ 2, 2, 3 ],
    [ 2, 3, 1 ],
    [ 2, 3, 2 ],
    [ 2, 3, 3 ],
    [ 3, 1, 1 ],
    [ 3, 1, 2 ],
    [ 3, 1, 3 ],
    [ 3, 2, 1 ],
    [ 3, 2, 2 ],
    [ 3, 2, 3 ],
    [ 3, 3, 1 ],
    [ 3, 3, 2 ],
    [ 3, 3, 3 ]
]
```

Here, an element of a symmetric monoid S_n^{mon} is presented as the list of images of the natural numbers from 1 to n. For example, `[2,1,1]` as element in S_3^{mon} is the following map:

$$\begin{array}{rccc} f: & \{1,2,3\} & \to & \{1,2,3\} \\ & 1 & \mapsto & 2 \\ & 2 & \mapsto & 1 \\ & 3 & \mapsto & 1 \end{array}$$

```
Compose := function(f,g) // f, g: elements of the symmetric monoid
 return [g[x] : x in f];
end function;

Compose_list := function(n,f) // n: degree
// f: list or set of elements of the symmetric monoid
 prod := [i : i in [1..n]];
 for x in f do
  prod := Compose(prod,x); // %%
 end for;
 return prod;
end function;

IsCommutative := function(f,g) // f,g: elements of the symmetric monoid
 return Compose(f,g) eq Compose(g,f); // %%
end function;

IsBijective := function(f) // f: element of the symmetric monoid
 return #SequenceToSet(f) eq #f;
end function;
```

The function `BijSymMon` gives us all bijective elements of S_n^{mon}. These are exactly the elements of the symmetric group S_n.

```
BijSymMon := function(n) // n: degree of the symmetric monoid
 Bij := [];
 for x in SymMon(n) do // %%
  if IsBijective(x) then // %%
   Bij := Bij cat [x];
  end if;
 end for;
 return Bij;
end function;
```

For example, in degree $n = 3$ we receive

```
> BijSymMon(3);
[
    [ 1, 2, 3 ],
    [ 1, 3, 2 ],
    [ 2, 1, 3 ],
    [ 2, 3, 1 ],
    [ 3, 1, 2 ],
    [ 3, 2, 1 ]
]
```

The following function `Submon` calculates the set of elements of the submonoid M of $\mathrm{S}_n^{\mathrm{mon}}$ generated by a list of elements `s`.

```
Submon := function(s) // s: non-empty list of elements of the symmetric monoid
 n := #s[1];
 id := [i : i in[1..n]];
 Todo := s;
 X := {id};
 while #Todo ge 1 do
  Todo := {x : x in Todo | not x in X}; // ejecting known elements
  X join:= Todo;
  Todo := {Compose(x,y) : x in Todo, y in s}; // %% Compose is used here
 end while;
 return X;
end function;
```

For instance,

```
> Submon([[1,1,3],[2,2,3],[1,2,1],[1,2,2]]);
```

gives

```
{
    [ 1, 1, 1 ],
    [ 2, 2, 3 ],
    [ 2, 2, 2 ],
    [ 1, 2, 1 ],
    [ 2, 2, 1 ],
    [ 1, 2, 3 ],
    [ 1, 2, 2 ],
    [ 1, 1, 3 ],
    [ 1, 1, 2 ]
} .
```

For instance,

```
> Submon([[4,1,4,1],[4,2,1,1]]);
```

gives

```
{
    [ 1, 4, 1, 4 ],
    [ 4, 1, 1, 1 ],
    [ 1, 1, 4, 4 ],
    [ 4, 2, 1, 1 ],
    [ 1, 2, 4, 4 ],
    [ 4, 1, 4, 1 ],
    [ 1, 2, 3, 4 ],
    [ 4, 4, 1, 1 ],
    [ 1, 4, 4, 4 ]
} .
```

With the program `IsSubgroup` we can test if a given submonoid is also a subgroup.

```
IsSubgroup := function(X) // X: submonoid of the symmetric monoid, as list or set
 return &and[IsBijective(f) : f in X]; // %%
end function;
```

For example, the submonoids calculated above are not subgroups.

```
> IsSubgroup(Submon([[1,1,3],[2,2,3],[1,2,1],[1,2,2]]));
false
> IsSubgroup(Submon([[4,1,4,1],[4,2,1,1]]));
false
```

The program `IsAbel` decides if a given monoid is abelian.

```
IsAbel := function(M) // M: submonoid of the symmetric monoid
 return &and[Compose(i,j) eq Compose(j,i) : i, j in M]; // %%
end function;
```

For example, the submonoids calculated above are not abelian.

```
> IsAbel(Submon([[1,1,3],[2,2,3],[1,2,1],[1,2,2]]));
false
> IsAbel(Submon([[4,1,4,1],[4,2,1,1]]));
false
```

1.3.2 Orders of monoid elements

With the following program `Ord` we can calculate the order of a given element `x` of the symmetric monoid S_n^{mon} as defined in Definition 16.

```
Ord := function(x) // x: element of the symmetric monoid
 n := #x;
 id := [i : i in[1..n]];
 a := x;
 pot_list := [id];
 while not a in pot_list do
  pot_list cat:= [a];
  a := Compose(a,x); // %%
 end while;
 return <Index(pot_list,a) - 1, #pot_list>;
end function;
```

The function `Pot` returns the `k`th power of an element `m` of S_n^{mon}.

```
Pot := function(m,k) // m: element in the symmetric monoid, k: exponent
 a := [1..#m];
 for i in [1..k] do
  a := Compose(a,m); // %%
 end for;
 return a;
end function;
```

For example, `Ord([2,2,1])` gives `<2,3>`. We can verify this directly with the following calculations.

```
> Pot([2,2,1],2);
[ 2, 2, 2 ]
> Pot([2,2,1],3);
[ 2, 2, 2 ]
```

For example, `Ord([4,1,2,1])` gives `<2,4>`. We can verify this with the following calculations.

```
> Pot([4,1,2,1],2);
[ 1, 4, 1, 4 ]
> Pot([4,1,2,1],3);
[ 4, 1, 4, 1 ]
> Pot([4,1,2,1],4);
[ 1, 4, 1, 4 ]
```

With the following function we sort and subdivide the elements of a given monoid `X` via their orders in a lexicographic way.

```
SortedSubmon := function(X) // X: submonoid of the symmetric monoid
 n := #X;
 list := [];
 X_red := SetToSequence(X);
 for i in [0..(n-1)] do // first index of order
  for j in [(i+1)..n] do // second index of order
   list_red := [];
   for x in X_red do
    if Ord(x) eq <i,j> then // %% Ord is used here
     list_red := list_red cat [x];
     X_red := [y : y in X_red | not y eq x];
    end if;
   end for;
   if not #list_red eq 0 then
    list := list cat [list_red];
   end if;
  end for;
 end for;
 return list;
end function;
```

For instance,

```
> SortedSubmon(Submon([[1,1,3],[2,2,3],[1,2,1],[1,2,2]]));
```

gives

```
[
    [
        [ 1, 2, 3 ]                 // Ord([1,2,3]) = <0,1>
    ],
    [
        [ 1, 1, 1 ],                // Ord([1,1,1]) = <1,2>
        [ 2, 2, 3 ],                // Ord([2,2,3]) = <1,2>
        [ 2, 2, 2 ],                // Ord([2,2,2]) = <1,2>
        [ 1, 2, 1 ],                // Ord([1,2,1]) = <1,2>
        [ 1, 2, 2 ],                // Ord([1,2,2]) = <1,2>
        [ 1, 1, 3 ]                 // Ord([1,1,3]) = <1,2>
    ],
    [
        [ 2, 2, 1 ],                // Ord([2,2,1]) = <2,3>
        [ 1, 1, 2 ]                 // Ord([1,1,2]) = <2,3>
    ]
] .
```

For instance,

```
> SortedSubmon(Submon([[4,1,4,1],[4,2,1,1]]));
```

gives

```
[
    [
        [ 1, 2, 3, 4 ]              // Ord([1,2,3,4]) = <0,1>
    ],
    [
        [ 1, 4, 1, 4 ],             // Ord([1,4,1,4]) = <1,2>
        [ 1, 1, 4, 4 ],             // Ord([1,1,4,4]) = <1,2>
        [ 1, 2, 4, 4 ],             // Ord([1,2,4,4]) = <1,2>
        [ 1, 4, 4, 4 ]              // Ord([1,4,4,4]) = <1,2>
    ],
    [
        [ 4, 1, 1, 1 ],             // Ord([4,1,1,1]) = <1,3>
        [ 4, 2, 1, 1 ],             // Ord([4,2,1,1]) = <1,3>
        [ 4, 1, 4, 1 ],             // Ord([4,1,4,1]) = <1,3>
        [ 4, 4, 1, 1 ]              // Ord([4,4,1,1]) = <1,3>
    ]
]
```

1.3.3 Listing submonoids

1.3.3.1 The list of submonoids

We want to list submonoids of $\mathrm{S}_n^{\mathrm{mon}}$ in a given degree n with the following function ListOfSubmonoids_capped. We cap the orders of the submonoids to be listed by m. The cap is useful to obtain partial results in cases where the complete list exceeds the computer capacities. Setting $m := n^n$, we obtain the complete list of submonoids.

With each submonoid, we also return a list of generators.

```
ListOfSubmonoids_capped := function(n, m) // n: degree of the symmetric monoid
                                          // m: cap for order of submonoids
 S := SymMon(n); // %%
 id := [i : i in[1..n]];
 Todo := { <{id},[id]> }; // pairs of submonoid and its generators
 Todo_red := { {id} }; // just submonoids without the generators,
                       // first entries of Todo
 X_red := {}; // just submonoids without the generators
 i := 0; // counter_1
 while #Todo ge 1 do
  i +:= 1; // counter_1
```

```
  print "counter_1 i =", i;
  Todo     := { x : x in Todo | not x[1] in X_red}; // ejecting known elements
  Todo_red := { x[1] : x in Todo };
  X_red join:= Todo_red;
  j := 0; // counter_2
  for x in Todo do
   j +:= 1; // counter_2
   if j mod 100 eq 0 then
    print "counter_2 j =", j;
   end if;
   for s in S do
    if not s in x[1] then
     list_gen := x[2] cat [s];
     M := Submon(list_gen); // %%
     if #M le m then
      if not M in Todo_red then
       Todo     join:= { <M, list_gen> };
       Todo_red join:= { M             };
      end if;
     end if;
    end if;
   end for;
  end for;
 end while;
 print "Info: #X_red = ", #X_red;
 return SetToSequence(X_red);
end function;
```

For example,

```
> [<i,#ListOfSubmonoids_capped(i,i^i)> : i in [1..3]];
```

yields

```
[ <1, 1>, <2, 6>, <3, 699> ].
```

So there are 6 different submonoids of the symmetric monoid $\mathrm{S}_2^{\mathrm{mon}}$ in degree $n = 2$, and there are 699 different submonoids of the symmetric monoid $\mathrm{S}_3^{\mathrm{mon}}$ in degree $n = 3$.

In the following table, we list the 6 submonoids of $\mathrm{S}_2^{\mathrm{mon}}$.

$M_1 = \langle\ \rangle = \{\mathrm{id}_{\{1,2\}}\}$, abelian, subgroup	$M_2 = \langle$`[2,1]`$\rangle$, abelian, subgroup
$M_3 = \langle$`[2,1], [1,1]`$\rangle$	$M_4 = \langle$`[1,1], [2,2]`$\rangle$
$M_5 = \langle$`[1,1]`$\rangle$, abelian	$M_6 = \langle$`[2,2]`$\rangle$, abelian

In particular, we have $M_3 = \mathrm{S}_2^{\mathrm{mon}}$.

The list of occurring orders of submonoids of $\mathrm{S}_3^{\mathrm{mon}}$ is

```
[ <1, 1>, <2, 12>, <3, 37>, <4, 55>, <5, 87>, <6, 119>, <7, 96>,
  <8, 96>, <9, 64>, <10, 48>, <11, 24>, <12, 30>, <13, 6>, <14, 3>,
  <15, 3>, <16, 6>, <17,6>, <22, 1>, <23, 3>, <24, 1>, <27, 1> ] .
```

For example, the entry `<5,87>` means that there are 87 submonoids of S_3^{mon} of order 5.

For example, the entry `<27,1>` means that there is just one monoid with 27 elements. This is the symmetric monoid S_3^{mon}.

1.3.3.2 The list of submonoids up to conjugacy

Then function `Inverse` gives us the inverse of an element `f` of the symmetric group S_n. The element `f` is given as the list of its images.

```
Inverse := function(f) // f: element of the symmetric group,
                       // i.e. f has to be bijective
 n := #f;
 return &cat[[Index(f,i) : i in [1..n]]];
end function;
```

The we can conjugate an element `x` of the symmetric monoid S_n^{mon} with an element `s` from the symmetric group S_n as follows.

```
Conjugate := function(x,s) // x: element of the symmetric monoid
                           // s: element of the symmetric group
 return Compose(Compose(Inverse(s),x),s); // %%
end function;
```

We want to list representatives of conjugacy classes of submonoids on S_n^{mon} in a given degree n with the following function `ListOfSubmonoids_up_to_conj_with_gen_and_capped`. We cap the number of generators of the submonoids to be listed by c. Moreover, we cap their orders by m. Setting $c := n^n$ and $m := n^n$, we obtain a complete list of representatives of conjugacy classes of our submonoids.

```
ListOfSubmonoids_up_to_conj_with_gen_and_capped := function(n,c,m)
// n: degree of the symmetric monoid
// c: cap for the number of generators
// m : cap for the orders of the submonoids of the symmetric monoid
 S := SymMon(n); // %%
 id := [i : i in[1..n]];
 Todo := { <{id},[]> }; // pairs of submonoid and its generators
 X     := { <{id},[]> }; // pairs of submonoid and its generators
 X_red_conj := { {id} }; // just submonoids without the generators
 i := 0; // counter_1
 while #Todo ge 1 do
  i +:= 1; // counter_1
```

```
  if i eq c+1 then // quit if exceeding cap
   break;
  end if;
  print "counter_1 i =", i;
  Todo_new          := {};
  Todo_new_red_conj := {};
  j := 0; // counter_2
  for x in Todo do
   j +:= 1; // counter_2
   if j mod 10 eq 0 then
    print "counter_2 j =", j;
   end if;
   for s in S do
    if not s in x[1] then
     list_gen := x[2] cat [s];
     M := Submon(list_gen); // %%
     if #M le m then
      if not M in X_red_conj and not M in Todo_new_red_conj then
       Todo_new          join:= { <M, list_gen> };
       Todo_new_red_conj join:= {{Conjugate(x,s) : x in M} :
                                s in S | IsBijective(s)};
       // %% Conjugate and IsBijective are used here
      end if;
     end if;
    end if;
   end for;
  end for;
  Todo           := Todo_new;
  X          join:= Todo_new;
  X_red_conj join:= Todo_new_red_conj;
  print "Info_1: #Todo = ", #Todo;
  print "Info_2: #X = ", #X;
  print "Info_3: #X_red_conj = ", #X_red_conj;
 end while;
 return SetToSequence(X);
end function;
```

In the following table, we list representatives of the 5 conjugacy classes of submonoids of $\mathrm{S}_2^{\mathrm{mon}}$, as can be obtained via `ListOfSubmonoids_up_to_conj_with_gen_and_capped(2,4,4)`.

$M_1 = \langle\rangle = \{\mathrm{id}_{\{1,2\}}\}$, abelian, subgroup	$M_2 = \langle$`[2,1]`$\rangle$, abelian, subgroup
$M_3 = \langle$`[2,1], [1,1]`$\rangle$	$M_4 = \langle$`[1,1], [2,2]`$\rangle$
$M_5 = \langle$`[1,1]`$\rangle$, abelian	

In particular, we have $M_3 = \mathrm{S}_2^{\mathrm{mon}}$.

The list of occurring orders of representatives of conjugacy classes of submonoids of S_3^{mon}, is

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

1.4 Isomorphisms between monoids

We want to list representatives of isoclasses of submonoids of S_n^{mon} in a given degree n.

1.4.1 The list of submonoids up to isomorphism

In the following function we calculate the `Tree` of a submonoid `X` of the symmetric monoid S_n^{mon}. The `Tree` gives us a list of pairs. In such a pair, the first entry is an element of the submonoid `X` . The second entry is a list containing indices of the generators, such that the product of these generators yield the first entry. Each element of the submonoids occurs once.

```
Tree := function(X) // X : submonoid of the symmetric monoid with generators
 n := #Random(X[1]);
 id := [i : i in[1..n]];
 treelist := [<id,[]>];
 j := 0;
 todo := treelist;
 while #todo ge 1 do
  for x in todo do
   for s in X[2] do
    elt := Compose(x[1],s); // %%
    if not elt in {y[1] : y in treelist} then
     treelist cat:= [<elt,x[2] cat [Index(X[2],s)]>];
    end if;
   end for;
  end for;
  j +:= 1;
  todo := [x : x in treelist | #x[2] eq j];
 end while;
 return treelist;
end function;
```

For example, let

```
> list_gen := [[1,1,3],[2,2,3],[1,2,1],[1,2,2]];
> M := <Submon(list_gen),list_gen>;
```

Now

```
> Tree(M);
```

gives

```
[
    <[ 1, 2, 3 ], []>,
    <[ 1, 1, 3 ], [ 1 ]>,
    <[ 2, 2, 3 ], [ 2 ]>,
    <[ 1, 2, 1 ], [ 3 ]>,
    <[ 1, 2, 2 ], [ 4 ]>,
    <[ 1, 1, 1 ], [ 1, 3 ]>,
    <[ 1, 1, 2 ], [ 1, 4 ]>,
    <[ 2, 2, 1 ], [ 2, 3 ]>,
    <[ 2, 2, 2 ], [ 2, 4 ]>
].
```

For example, the pair `<[ 2, 2, 1 ], [ 2, 3 ]>` shows that the element `[ 2, 2, 1 ]` of the submonoid can be obtained as follows.

```
> Compose_list(3,[list_gen[2],list_gen[3]]);
```

gives

```
[ 2, 2, 1 ].
```

For example, let

```
> list_gen := [[1,4,1,4],[4,2,1,1]];
> N := <Submon(list_gen),list_gen>;
```

Now

```
> Tree(N);
```

gives

```
[
    <[ 1, 2, 3, 4 ], []>,
    <[ 1, 4, 1, 4 ], [ 1 ]>,
    <[ 4, 2, 1, 1 ], [ 2 ]>,
    <[ 4, 1, 4, 1 ], [ 1, 2 ]>,
    <[ 4, 4, 1, 1 ], [ 2, 1 ]>,
    <[ 1, 2, 4, 4 ], [ 2, 2 ]>,
    <[ 1, 1, 4, 4 ], [ 2, 1, 2 ]>,
    <[ 1, 4, 4, 4 ], [ 2, 2, 1 ]>,
    <[ 4, 1, 1, 1 ], [ 2, 2, 1, 2 ]>
].
```

For example, the pair `<[ 4, 1, 1, 1 ], [ 2, 2, 1, 2 ]>` shows that the element `[ 4, 1, 1, 1 ]` of the submonoid can be obtained as follows.

```
> Compose_list(4,[list_gen[2],list_gen[2],list_gen[1],list_gen[2]]);
```

gives

```
[ 4, 1, 1, 1 ].
```

Suppose given `X`, `Y` submonoids of the symmetric monoid, with generators. If `{*Ord(x) : x in X[1]*}` and `{*Ord(y) : y in Y[1]*}` are not equal, X and Y can not be isomorphic. If they are equal, then we can test with the function `IsIso` if `X` and `Y` are isomorphic. We first compute all candidates for isomorphisms between the two submonoids `X` and `Y`. Then, we verify if the candidate is in fact an isomorphism. We terminate the function `IsIso` if we have found an isomorphism and return the information that the submonoids `X` and `Y` are isomorphic.

For finding candidates for isomorphisms we use `SortedSubmon` to sort the monoid into lists of elements with the same order. Isomorphisms have to respect these lists. So we first have to send each generator of `X` to an element of the same order.

Using `Tree`, we extend this map to a map from `X` to `Y`, mapping products of generators as stored in `Tree` to the respective products of the images of the generators. Then we test the resulting map on bijectivity and on compatibility with the monoid multipliction. If these tests are successful our map is an isomorphism of monoids from `X` to `Y`. Conversly, any isomorphism of monoids from `X` to `Y` can be found in this way.

Note that the extension from the map from the generators of `X` to `Y` to a map from `X` to `Y` only ensures compatibility with products occurring in `Tree`, but not necessarily with the monoid multiplication as a whole.

```
IsIso := function(X,Y) // X, Y: Submonoids with generators
                              // X, Y have to have the same multiset of orders
 // {*Ord(x) : x in X[1]*} eq {*Ord(y) : y in Y[1]*} has to result true
 XS := SortedSubmon(X[1]); // %%
 XSS := &cat XS;
 n := #XSS[1]; // n: degree
 id := [1..n]; // id: identity
 YS := SortedSubmon(Y[1]); // %%
 YSS := &cat YS;
 if #X[2] eq 0 then // intercept error: in the case if X is the trivial monoid
                    // cf. Remark 3 we have to set the identity as generator
  X[2] := [id];
 end if;
 if #Y[2] eq 0 then
  Y[2] := [id];
 end if;
```

```
 RegionGen := [Index([s in b : b in XS],true) : s in X[2]];
 list := [j : j in CartesianProduct([{1..#XS[t]} : t in RegionGen])];
 list := [j : j in list | #{<RegionGen[k],j[k]> : k in [1..#X[2]]} eq #X[2]];
 // ejecting candidates that give no bijection at all
 // print "Info_1: list = ", list;
 T := Tree(X); // %%
 bij_list := [];
 for j in list do
  im_gen := [YS[RegionGen[k]][j[k]] : k in [1..#X[2]]];
  // print "Info_2: im_gen = ", im_gen;
  bij := [];
  for k in [1..#XSS] do
   elt_list := T[Index([y[1] : y in T],XSS[k])][2];
   bij cat:= [Index(YSS,Compose_list(n,[im_gen[k] : k in elt_list]))];
   // %% Compose_list is used here
  end for;
  // print "Info_3: bij = ", bij;
  if #{i : i in bij} eq #bij then
   bij_list cat:= [bij];
  end if;
 end for;
 isiso := false;
 for f in bij_list do
  if &and[YSS[f[Index(XSS,Compose(x,xx))]] eq Compose(YSS[f[Index(XSS,x)]],
     YSS[f[Index(XSS,xx)]]) : x in XSS, xx in X[2] | &and[not x eq id,
     not xx eq id]] // %% Compose is used here
  then
   isiso := true;
   break f;
  end if;
 end for;
 return isiso;
end function;
```

With the function `IsoRepresentatives` we can list the isoclasses of monoids of a given list `L` of submonoids of $\mathrm{S}_n^{\mathrm{mon}}$.

```
IsoRepresentatives := function(L) // L: non-empty list of submonoids of the
                                  // symmetric monoid with their generators
 n := #Random(L[1][1]); // n: degree of the symmetric monoid
 id := [i : i in[1..n]];
 IsoRep := [];
 k := 0; // counter
 for X in L do
  k +:= 1; // counter
  if k mod 100 eq 0 then // counter
   print "counter k =", k;
```

```
  end if;
  isiso := false;
  for Y in IsoRep do // now we test if the monoid X under consideration is
                     // isomorphic to a monoid in an isoclass we already have
   if #Y[1] eq #X[1] then
    if {* Ord(x) : x in X[1] *} eq {* Ord(y) : y in Y[1] *} then
    // %% Ord is used here
     if IsIso(X,Y) then // %% IsIso is used here
      isiso := true;
      break Y;
     end if;
    end if;
   end if;
  end for;
  if not isiso then
   IsoRep cat:= [X];
  end if;
 end for;
 return IsoRep;
end function;
```

The function `Isomorphisms` is built in a way like the program `IsIso` except for the fact that we check all candidates for isomorphisms and return all isomorphisms between the two submonoids `X` and `Y`. The input submonoids `X` and `Y` have to have the same multisets of orders and additionally they have to be sent through the function `SortedSubmon`.
The output `iso_list` is the list of isomorphisms f between the two submonoids `X` and `Y`. For example see 1.4.2.

```
Isomorphisms := function(X,Y) // X,Y: submonoids with generators, but first
// entry X[1] resp Y[1] is already divided into sublists of elements with
// the same order
 XS := X[1];
 XSS := &cat XS;
 n := #XSS[1]; // n: degree
 id := [1..n]; // id: identity
 YS := Y[1];
 YSS := &cat YS;
 if #X[2] eq 0 then // intercept error: in the case if X is the trivial monoid
                    // cf. Remark 3 we have to set the identity as generator
  X[2] := [id];
 end if;
 if #Y[2] eq 0 then // intercept error: in the case if X is the trivial monoid
                    // cf. Remark 3 we have to set the identity as generator
  Y[2] := [id];
 end if;
 RegionGen := [Index([s in b : b in XS],true) : s in X[2]];
 list := [j : j in CartesianProduct([{1..#XS[t]} : t in RegionGen])];
```

```
 list := [j : j in list | #{<RegionGen[k],j[k]> : k in [1..#X[2]]}
 eq #SequenceToSet(X[2])]; // ejecting candidates that give no bijection
                           // at all
 T := Tree(<SequenceToSet(&cat(X[1])),X[2]>); // %%
 // X: now back into form <set,list>
 bij_list := [];
 for j in list do
  im_gen := [YS[RegionGen[k]][j[k]] : k in [1..#X[2]]];
  bij := [];
  for k in [1..#XSS] do
   elt_list := T[Index([y[1] : y in T],XSS[k])][2];
   bij cat:= [Index(YSS,Compose_list(n,[im_gen[k] : k in elt_list]))];
   // %% Compose_list is used here
  end for;
  // print "Info: bij = ", bij;
  if #{i : i in bij} eq #bij then
   bij_list cat:= [bij];
  end if;
 end for;
 iso_list := [];
 for f in bij_list do
  if &and[YSS[f[Index(XSS,Compose(x,xx))]] eq Compose(YSS[f[Index(XSS,x)]],
  YSS[f[Index(XSS,xx)]]) : x in XSS, xx in X[2] | &and[not x eq id, not xx eq id]]
  // %% Compose is used here
  then
   iso_list cat:= [f];
  end if;
 end for;
 return iso_list;
end function;
```

1.4.2 The automorphism group of a submonoid

To compute the automorphism group of a submonoid M of the symmetric monoid $\mathrm{S}_n^{\mathrm{mon}}$, the function `Autom` just searches for isomorphisms between M and M.

```
Autom := function(M) // M: monoid with generators, but first entry M[1]
                     // is already sent through SortedSubmon
 return Isomorphisms(M,M); // %%
end function;
```

For example, with

```
> s := [[1,1,3],[2,2,3],[1,2,1],[1,2,2]];
> M := <SortedSubmon(Submon(s)),s>;
```

we get

```
> Autom(M);
[
    [ 1, 4, 7, 2, 6, 5, 3, 9, 8 ],
    [ 1, 2, 3, 4, 5, 6, 7, 8, 9 ]
] .
```

And with

```
> s := [[1,4,1,4],[4,2,1,1]];
> M := <SortedSubmon(Submon(s)),s>;
```

we get the trivial automorphism group

```
> Autom(M);
[
    [ 1, 2, 3, 4, 5, 6, 7, 8, 9 ]
]
```

1.5 Resulting lists

1.5.1 The list of submonoids of $\mathrm{S}_2^{\mathrm{mon}}$ up to isomorphism

In the following table, we list representatives of the 5 isoclasses of submonoids of $\mathrm{S}_2^{\mathrm{mon}}$.

$M_1 = \langle\ \rangle = \{\mathrm{id}_{\{1,2\}}\}$, abelian, subgroup $\mathrm{Aut}(M_1) \simeq 1$	$M_2 = \langle$`[2,1]`$\rangle$, abelian, subgroup $\mathrm{Aut}(M_2) \simeq 1$
$M_3 = \langle$`[2,1], [1,1]`$\rangle$ $\mathrm{Aut}(M_3) \simeq \mathrm{C}_2$	$M_4 = \langle$`[1,1], [2,2]`$\rangle$ $\mathrm{Aut}(M_4) \simeq \mathrm{C}_2$
$M_5 = \langle$`[1,1]`$\rangle$, abelian $\mathrm{Aut}(M_5) \simeq 1$	

In particular, we have $M_3 = \mathrm{S}_2^{\mathrm{mon}}$.

1.5.2 The list of submonoids of $\mathrm{S}_3^{\mathrm{mon}}$ up to isomorphism

In the following table, we give a complete list of representatives of the 154 isoclasses of submonoids of $\mathrm{S}_3^{\mathrm{mon}}$.

$M_1 = \langle\ \rangle = \{\mathrm{id}_{\{1,2,3\}}\}$, abelian, subgroup $\mathrm{Aut}(M_1) \simeq 1$	$M_2 = \langle$[1,1,3]$\rangle$, abelian $\mathrm{Aut}(M_2) \simeq 1$
$M_3 = \langle$[1,3,2]$\rangle$, abelian, subgroup $\mathrm{Aut}(M_3) \simeq 1$	$M_4 = \langle$[1,1,2]$\rangle$, abelian $\mathrm{Aut}(M_4) \simeq 1$
$M_5 = \langle$[2,1,1]$\rangle$, abelian $\mathrm{Aut}(M_5) \simeq 1$	$M_6 = \langle$[2,3,1]$\rangle$, abelian, subgroup $\mathrm{Aut}(M_6) \simeq \mathrm{C}_2$
$M_7 = \langle$[1,1,3],[2,2,1]$\rangle$ $\mathrm{Aut}(M_7) \simeq 1$	$M_8 = \langle$[1,1,3],[2,2,2]$\rangle$ $\mathrm{Aut}(M_8) \simeq 1$
$M_9 = \langle$[1,1,3],[3,3,3]$\rangle$, abelian $\mathrm{Aut}(M_9) \simeq 1$	$M_{10} = \langle$[1,1,3],[3,2,2]$\rangle$ $\mathrm{Aut}(M_{10}) \simeq 1$
$M_{11} = \langle$[1,1,3],[2,3,3]$\rangle$ $\mathrm{Aut}(M_{11}) \simeq 1$	$M_{12} = \langle$[1,1,1],[1,3,2]$\rangle$, abelian $\mathrm{Aut}(M_{12}) \simeq 1$
$M_{13} = \langle$[1,1,3],[1,2,2]$\rangle$ $\mathrm{Aut}(M_{13}) \simeq 1$	$M_{14} = \langle$[1,1,3],[2,3,2]$\rangle$ $\mathrm{Aut}(M_{14}) \simeq 1$
$M_{15} = \langle$[2,1,1],[2,3,2]$\rangle$ $\mathrm{Aut}(M_{15}) \simeq 1$	$M_{16} = \langle$[1,1,1],[2,3,3]$\rangle$ $\mathrm{Aut}(M_{16}) \simeq 1$
$M_{17} = \langle$[1,1,3],[3,1,3]$\rangle$ $\mathrm{Aut}(M_{17}) \simeq 1$	$M_{18} = \langle$[2,1,1],[2,3,3]$\rangle$ $\mathrm{Aut}(M_{18}) \simeq 1$
$M_{19} = \langle$[1,1,1],[2,2,1]$\rangle$ $\mathrm{Aut}(M_{19}) \simeq 1$	$M_{20} = \langle$[1,1,1],[2,3,2]$\rangle$ $\mathrm{Aut}(M_{20}) \simeq 1$
$M_{21} = \langle$[1,1,3],[2,1,2]$\rangle$ $\mathrm{Aut}(M_{21}) \simeq 1$	$M_{22} = \langle$[1,1,3],[1,1,2]$\rangle$ $\mathrm{Aut}(M_{22}) \simeq 1$
$M_{23} = \langle$[1,1,3],[2,1,1]$\rangle$ $\mathrm{Aut}(M_{23}) \simeq 1$	$M_{24} = \langle$[1,1,3],[1,2,1]$\rangle$, abelian $\mathrm{Aut}(M_{24}) \simeq \mathrm{C}_2$
$M_{25} = \langle$[1,1,3],[3,1,1]$\rangle$ $\mathrm{Aut}(M_{25}) \simeq \mathrm{C}_2$	$M_{26} = \langle$[1,1,3],[3,3,2]$\rangle$ $\mathrm{Aut}(M_{26}) \simeq \mathrm{C}_2$
$M_{27} = \langle$[2,1,1],[1,3,2]$\rangle$ $\mathrm{Aut}(M_{27}) \simeq \mathrm{C}_2$	$M_{28} = \langle$[1,1,2],[1,3,1]$\rangle$ $\mathrm{Aut}(M_{28}) \simeq \mathrm{C}_2$
$M_{29} = \langle$[1,1,3],[1,3,3]$\rangle$ $\mathrm{Aut}(M_{29}) \simeq \mathrm{C}_2$	$M_{30} = \langle$[1,1,1],[2,2,2]$\rangle$ $\mathrm{Aut}(M_{30}) \simeq \mathrm{C}_2$
$M_{31} = \langle$[1,1,1],[2,1,3]$\rangle$ $\mathrm{Aut}(M_{31}) \simeq \mathrm{C}_2$	$M_{32} = \langle$[1,1,3],[1,3,2]$\rangle$ $\mathrm{Aut}(M_{32}) \simeq \mathrm{C}_2$
$M_{33} = \langle$[1,1,3],[3,2,1]$\rangle$ $\mathrm{Aut}(M_{33}) \simeq \mathrm{C}_2$	$M_{34} = \langle$[1,1,2],[2,3,3]$\rangle$ $\mathrm{Aut}(M_{34}) \simeq \mathrm{C}_2$
$M_{35} = \langle$[1,1,1],[2,1,1]$\rangle$ $\mathrm{Aut}(M_{35}) \simeq \mathrm{C}_2$	$M_{36} = \langle$[1,1,2],[3,1,3]$\rangle$ $\mathrm{Aut}(M_{36}) \simeq \mathrm{C}_2$
$M_{37} = \langle$[2,1,1],[3,3,2]$\rangle$ $\mathrm{Aut}(M_{37}) \simeq \mathrm{C}_2$	$M_{38} = \langle$[1,1,2],[2,1,1]$\rangle$ $\mathrm{Aut}(M_{38}) \simeq \mathrm{C}_2$
$M_{39} = \langle$[2,1,1],[3,2,1]$\rangle$ $\mathrm{Aut}(M_{39}) \simeq \mathrm{C}_2$	$M_{40} = \langle$[2,1,1],[1,1,2]$\rangle$ $\mathrm{Aut}(M_{40}) \simeq \mathrm{C}_2$

$M_{41} = \langle \texttt{[1,1,2],[2,1,3]} \rangle$ $\mathrm{Aut}(M_{41}) \simeq \mathrm{C}_2$	$M_{42} = \langle \texttt{[2,3,1],[1,3,2]} \rangle$, subgroup $\mathrm{Aut}(M_{42}) \simeq \mathrm{S}_3$
$M_{43} = \langle \texttt{[1,1,1],[2,3,1]} \rangle$ $\mathrm{Aut}(M_{43}) \simeq \mathrm{S}_3$	$M_{44} = \langle \texttt{[1,1,3],[2,3,1]} \rangle$ $\mathrm{Aut}(M_{44}) \simeq \mathrm{C}_6$
$M_{45} = \langle \texttt{[1,1,3],[1,3,1],[2,1,2]} \rangle$ $\mathrm{Aut}(M_{45}) \simeq 1$	$M_{46} = \langle \texttt{[1,1,3],[2,1,2],[1,2,2]} \rangle$ $\mathrm{Aut}(M_{46}) \simeq 1$
$M_{47} = \langle \texttt{[1,1,1],[2,2,1],[3,2,3]} \rangle$ $\mathrm{Aut}(M_{47}) \simeq 1$	$M_{48} = \langle \texttt{[1,1,3],[2,2,2],[1,2,2]} \rangle$ $\mathrm{Aut}(M_{48}) \simeq 1$
$M_{49} = \langle \texttt{[1,1,3],[2,2,1],[2,1,2]} \rangle$ $\mathrm{Aut}(M_{49}) \simeq 1$	$M_{50} = \langle \texttt{[1,1,1],[2,2,2],[1,3,3]} \rangle$ $\mathrm{Aut}(M_{50}) \simeq 1$
$M_{51} = \langle \texttt{[1,1,3],[1,3,1],[3,2,3]} \rangle$ $\mathrm{Aut}(M_{51}) \simeq 1$	$M_{52} = \langle \texttt{[1,1,3],[1,2,1],[2,2,2]} \rangle$ $\mathrm{Aut}(M_{52}) \simeq 1$
$M_{53} = \langle \texttt{[1,1,3],[1,1,2],[3,3,3]} \rangle$ $\mathrm{Aut}(M_{53}) \simeq 1$	$M_{54} = \langle \texttt{[1,1,3],[2,2,3],[1,2,1]} \rangle$ $\mathrm{Aut}(M_{54}) \simeq 1$
$M_{55} = \langle \texttt{[2,1,1],[2,3,3],[3,3,2]} \rangle$ $\mathrm{Aut}(M_{55}) \simeq 1$	$M_{56} = \langle \texttt{[2,1,1],[2,3,2],[2,2,3]} \rangle$ $\mathrm{Aut}(M_{56}) \simeq 1$
$M_{57} = \langle \texttt{[1,1,3],[2,2,1],[1,1,2]} \rangle$ $\mathrm{Aut}(M_{57}) \simeq 1$	$M_{58} = \langle \texttt{[1,1,3],[2,1,2],[2,3,2]} \rangle$ $\mathrm{Aut}(M_{58}) \simeq 1$
$M_{59} = \langle \texttt{[1,1,3],[2,2,2],[3,1,3]} \rangle$ $\mathrm{Aut}(M_{59}) \simeq 1$	$M_{60} = \langle \texttt{[1,1,3],[1,3,1],[1,2,1]} \rangle$ $\mathrm{Aut}(M_{60}) \simeq 1$
$M_{61} = \langle \texttt{[1,1,1],[2,2,1],[1,2,1]} \rangle$ $\mathrm{Aut}(M_{61}) \simeq 1$	$M_{62} = \langle \texttt{[1,1,3],[2,1,2],[1,3,3]} \rangle$ $\mathrm{Aut}(M_{62}) \simeq 1$
$M_{63} = \langle \texttt{[1,1,3],[2,2,1],[3,3,3]} \rangle$ $\mathrm{Aut}(M_{63}) \simeq 1$	$M_{64} = \langle \texttt{[1,1,3],[1,3,1],[2,2,2]} \rangle$ $\mathrm{Aut}(M_{64}) \simeq 1$
$M_{65} = \langle \texttt{[1,1,3],[1,3,3],[1,2,1]} \rangle$ $\mathrm{Aut}(M_{65}) \simeq 1$	$M_{66} = \langle \texttt{[2,1,1],[2,3,2],[1,3,3]} \rangle$ $\mathrm{Aut}(M_{66}) \simeq 1$
$M_{67} = \langle \texttt{[2,1,1],[1,1,2],[3,3,3]} \rangle$ $\mathrm{Aut}(M_{67}) \simeq 1$	$M_{68} = \langle \texttt{[1,1,3],[2,2,1],[2,2,3]} \rangle$ $\mathrm{Aut}(M_{68}) \simeq 1$
$M_{69} = \langle \texttt{[1,1,1],[2,2,1],[2,2,3]} \rangle$ $\mathrm{Aut}(M_{69}) \simeq 1$	$M_{70} = \langle \texttt{[1,1,3],[2,2,1],[1,2,1]} \rangle$ $\mathrm{Aut}(M_{70}) \simeq 1$
$M_{71} = \langle \texttt{[1,1,3],[2,2,3],[2,1,1]} \rangle$ $\mathrm{Aut}(M_{71}) \simeq 1$	$M_{72} = \langle \texttt{[1,1,3],[2,1,2],[3,3,3]} \rangle$ $\mathrm{Aut}(M_{72}) \simeq 1$
$M_{73} = \langle \texttt{[1,1,3],[2,2,2],[3,2,3]} \rangle$ $\mathrm{Aut}(M_{73}) \simeq 1$	$M_{74} = \langle \texttt{[1,1,3],[2,1,1],[3,3,3]} \rangle$ $\mathrm{Aut}(M_{74}) \simeq 1$
$M_{75} = \langle \texttt{[2,1,1],[2,3,3],[1,3,2]} \rangle$ $\mathrm{Aut}(M_{75}) \simeq \mathrm{C}_2$	$M_{76} = \langle \texttt{[1,1,1],[2,2,1],[3,2,2]} \rangle$ $\mathrm{Aut}(M_{76}) \simeq \mathrm{C}_2$
$M_{77} = \langle \texttt{[1,1,3],[2,2,3],[3,3,3]} \rangle$ $\mathrm{Aut}(M_{77}) \simeq \mathrm{C}_2$	$M_{78} = \langle \texttt{[1,1,3],[1,3,1],[1,2,2]} \rangle$ $\mathrm{Aut}(M_{78}) \simeq \mathrm{C}_2$
$M_{79} = \langle \texttt{[1,1,3],[2,2,2],[3,2,1]} \rangle$ $\mathrm{Aut}(M_{79}) \simeq \mathrm{C}_2$	$M_{80} = \langle \texttt{[1,1,1],[2,1,3],[3,3,1]} \rangle$ $\mathrm{Aut}(M_{80}) \simeq \mathrm{C}_2$

$M_{81} = \langle$ `[1,1,3],[1,3,2],[2,2,2]` $\rangle$ $\mathrm{Aut}(M_{81}) \simeq \mathrm{C}_2$	$M_{82} = \langle$ `[2,1,1],[2,3,2],[1,3,2]` $\rangle$ $\mathrm{Aut}(M_{82}) \simeq \mathrm{C}_2$
$M_{83} = \langle$ `[1,1,3],[2,2,1],[3,2,1]` $\rangle$ $\mathrm{Aut}(M_{83}) \simeq \mathrm{C}_2$	$M_{84} = \langle$ `[1,1,3],[2,2,1],[3,3,2]` $\rangle$ $\mathrm{Aut}(M_{84}) \simeq \mathrm{C}_2$
$M_{85} = \langle$ `[1,1,3],[2,2,3],[1,1,1]` $\rangle$ $\mathrm{Aut}(M_{85}) \simeq \mathrm{C}_2$	$M_{86} = \langle$ `[1,1,1],[2,2,2],[1,2,1]` $\rangle$ $\mathrm{Aut}(M_{86}) \simeq \mathrm{C}_2$
$M_{87} = \langle$ `[1,1,2],[2,3,3],[1,3,2]` $\rangle$ $\mathrm{Aut}(M_{87}) \simeq \mathrm{C}_2$	$M_{88} = \langle$ `[1,1,1],[1,3,2],[1,2,2]` $\rangle$ $\mathrm{Aut}(M_{88}) \simeq \mathrm{C}_2$
$M_{89} = \langle$ `[1,1,2],[2,1,3],[3,3,3]` $\rangle$ $\mathrm{Aut}(M_{89}) \simeq \mathrm{C}_2$	$M_{90} = \langle$ `[1,1,1],[2,3,3],[3,2,2]` $\rangle$ $\mathrm{Aut}(M_{90}) \simeq \mathrm{C}_2$
$M_{91} = \langle$ `[1,1,3],[1,3,1],[2,1,1]` $\rangle$ $\mathrm{Aut}(M_{91}) \simeq \mathrm{C}_2$	$M_{92} = \langle$ `[1,1,3],[1,3,3],[2,2,2]` $\rangle$ $\mathrm{Aut}(M_{92}) \simeq \mathrm{C}_2$
$M_{93} = \langle$ `[1,1,3],[1,3,2],[1,2,2]` $\rangle$ $\mathrm{Aut}(M_{93}) \simeq \mathrm{C}_2$	$M_{94} = \langle$ `[1,1,3],[1,3,1],[2,1,3]` $\rangle$ $\mathrm{Aut}(M_{94}) \simeq \mathrm{C}_2$
$M_{95} = \langle$ `[1,1,3],[2,2,1],[2,1,3]` $\rangle$ $\mathrm{Aut}(M_{95}) \simeq \mathrm{C}_2$	$M_{96} = \langle$ `[1,1,1],[2,2,2],[1,3,2]` $\rangle$ $\mathrm{Aut}(M_{96}) \simeq \mathrm{C}_2$
$M_{97} = \langle$ `[1,1,3],[1,3,1],[1,3,3]` $\rangle$ $\mathrm{Aut}(M_{97}) \simeq \mathrm{C}_2$	$M_{98} = \langle$ `[1,1,3],[2,2,1],[2,3,2]` $\rangle$ $\mathrm{Aut}(M_{98}) \simeq \mathrm{C}_2$
$M_{99} = \langle$ `[1,1,3],[1,3,3],[1,1,1]` $\rangle$ $\mathrm{Aut}(M_{99}) \simeq \mathrm{C}_2$	$M_{100} = \langle$ `[1,1,3],[1,3,1],[3,1,3]` $\rangle$ $\mathrm{Aut}(M_{100}) \simeq \mathrm{C}_2$
$M_{101} = \langle$ `[1,1,3],[2,2,1],[3,2,3]` $\rangle$ $\mathrm{Aut}(M_{101}) \simeq \mathrm{C}_2$	$M_{102} = \langle$ `[1,1,3],[2,2,2],[3,3,2]` $\rangle$ $\mathrm{Aut}(M_{102}) \simeq \mathrm{C}_2$
$M_{103} = \langle$ `[1,1,3],[3,1,1],[2,2,2]` $\rangle$ $\mathrm{Aut}(M_{103}) \simeq \mathrm{C}_2$	$M_{104} = \langle$ `[1,1,1],[2,1,3],[1,1,3]` $\rangle$ $\mathrm{Aut}(M_{104}) \simeq \mathrm{C}_2$
$M_{105} = \langle$ `[1,1,3],[2,1,2],[2,1,3]` $\rangle$ $\mathrm{Aut}(M_{105}) \simeq \mathrm{C}_2$	$M_{106} = \langle$ `[2,1,1],[2,3,2],[1,1,3]` $\rangle$ $\mathrm{Aut}(M_{106}) \simeq \mathrm{S}_3$
$M_{107} = \langle$ `[2,3,1],[1,3,2],[1,1,2]` $\rangle$ $\mathrm{Aut}(M_{107}) \simeq \mathrm{S}_3$	$M_{108} = \langle$ `[2,3,1],[1,3,2],[1,1,1]` $\rangle$ $\mathrm{Aut}(M_{108}) \simeq \mathrm{S}_3$
$M_{109} = \langle$ `[1,1,1],[2,2,2],[3,3,3]` $\rangle$ $\mathrm{Aut}(M_{109}) \simeq \mathrm{S}_3$	$M_{110} = \langle$ `[1,1,1],[2,1,3],[1,2,1]` $\rangle$ $\mathrm{Aut}(M_{110}) \simeq \mathrm{C}_2 \times \mathrm{C}_2$
$M_{111} = \langle$ `[1,1,3],[3,1,1],[1,1,1]` $\rangle$ $\mathrm{Aut}(M_{111}) \simeq \mathrm{C}_2 \times \mathrm{C}_2$	$M_{112} = \langle$ `[1,1,3],[1,3,1],[3,2,1]` $\rangle$ $\mathrm{Aut}(M_{112}) \simeq \mathrm{C}_2 \times \mathrm{C}_2$
$M_{113} = \langle$ `[1,1,3],[1,3,1],[3,1,1]` $\rangle$ $\mathrm{Aut}(M_{113}) \simeq \mathrm{C}_2 \times \mathrm{C}_2$	$M_{114} = \langle$ `[1,1,3],[2,2,2],[3,1,3],[1,3,3]` $\rangle$ $\mathrm{Aut}(M_{114}) \simeq 1$
$M_{115} = \langle$ `[1,1,3],[2,1,1],[3,3,3],[2,2,3]` $\rangle$ $\mathrm{Aut}(M_{115}) \simeq 1$	$M_{116} = \langle$ `[1,1,3],[1,1,2],[3,3,3],[2,1,2]` $\rangle$ $\mathrm{Aut}(M_{116}) \simeq 1$

$M_{117} = \langle$[1,1,3],[1,3,1],[2,2,2],[3,2,3]$\rangle$	$\mathrm{Aut}(M_{117}) \simeq 1$
$M_{118} = \langle$[1,1,3],[1,1,2],[3,3,3],[2,2,3]$\rangle$	$\mathrm{Aut}(M_{118}) \simeq 1$
$M_{119} = \langle$[1,1,1],[2,2,1],[2,2,3],[1,2,2]$\rangle$	$\mathrm{Aut}(M_{119}) \simeq 1$
$M_{120} = \langle$[1,1,3],[1,3,1],[1,2,1],[3,1,3]$\rangle$	$\mathrm{Aut}(M_{120}) \simeq 1$
$M_{121} = \langle$[1,1,3],[1,3,3],[1,2,1],[2,2,2]$\rangle$	$\mathrm{Aut}(M_{121}) \simeq 1$
$M_{122} = \langle$[1,1,3],[3,1,1],[2,2,2],[1,2,1]$\rangle$	$\mathrm{Aut}(M_{122}) \simeq 1$
$M_{123} = \langle$[1,1,3],[2,2,2],[3,1,3],[1,3,1]$\rangle$	$\mathrm{Aut}(M_{123}) \simeq 1$
$M_{124} = \langle$[1,1,3],[1,1,2],[3,3,3],[1,2,1]$\rangle$	$\mathrm{Aut}(M_{124}) \simeq 1$
$M_{125} = \langle$[1,1,3],[1,3,3],[1,2,1],[3,1,3]$\rangle$	$\mathrm{Aut}(M_{125}) \simeq 1$
$M_{126} = \langle$[1,1,3],[2,2,2],[3,1,3],[1,2,1]$\rangle$	$\mathrm{Aut}(M_{126}) \simeq 1$
$M_{127} = \langle$[1,1,3],[1,1,2],[3,3,3],[2,2,1]$\rangle$	$\mathrm{Aut}(M_{127}) \simeq 1$
$M_{128} = \langle$[1,1,3],[2,2,3],[1,2,1],[3,3,3]$\rangle$	$\mathrm{Aut}(M_{128}) \simeq 1$
$M_{129} = \langle$[1,1,3],[2,2,3],[1,2,1],[1,1,2]$\rangle$	$\mathrm{Aut}(M_{129}) \simeq 1$
$M_{130} = \langle$[1,1,3],[1,3,3],[1,2,1],[3,3,3]$\rangle$	$\mathrm{Aut}(M_{130}) \simeq 1$
$M_{131} = \langle$[1,1,3],[1,1,2],[3,3,3],[2,1,3]$\rangle$	$\mathrm{Aut}(M_{131}) \simeq \mathrm{C}_2$
$M_{132} = \langle$[1,1,3],[2,2,1],[2,2,3],[1,1,2]$\rangle$	$\mathrm{Aut}(M_{132}) \simeq \mathrm{C}_2$
$M_{133} = \langle$[1,1,3],[1,3,2],[2,2,2],[1,2,2]$\rangle$	$\mathrm{Aut}(M_{133}) \simeq \mathrm{C}_2$
$M_{134} = \langle$[1,1,3],[2,1,2],[1,2,2],[3,3,2]$\rangle$	$\mathrm{Aut}(M_{134}) \simeq \mathrm{C}_2$
$M_{135} = \langle$[1,1,3],[2,2,2],[3,1,3],[3,1,1]$\rangle$	$\mathrm{Aut}(M_{135}) \simeq \mathrm{C}_2$
$M_{136} = \langle$[1,1,3],[2,2,2],[3,1,3],[3,2,1]$\rangle$	$\mathrm{Aut}(M_{136}) \simeq \mathrm{C}_2$
$M_{137} = \langle$[1,1,3],[2,2,2],[3,1,3],[2,3,3]$\rangle$	$\mathrm{Aut}(M_{137}) \simeq \mathrm{C}_2$
$M_{138} = \langle$[1,1,3],[2,1,2],[2,1,3],[3,3,3]$\rangle$	$\mathrm{Aut}(M_{138}) \simeq \mathrm{C}_2$
$M_{139} = \langle$[1,1,1],[2,2,2],[1,3,3],[3,2,3]$\rangle$	$\mathrm{Aut}(M_{139}) \simeq \mathrm{C}_2$
$M_{140} = \langle$[1,1,3],[1,3,3],[1,2,1],[2,3,2]$\rangle$	$\mathrm{Aut}(M_{140}) \simeq \mathrm{C}_2$
$M_{141} = \langle$[1,1,3],[2,2,3],[1,2,1],[2,1,1]$\rangle$	$\mathrm{Aut}(M_{141}) \simeq \mathrm{C}_2$
$M_{142} = \langle$[1,1,1],[2,1,3],[1,1,3],[3,3,3]$\rangle$	$\mathrm{Aut}(M_{142}) \simeq \mathrm{C}_2$
$M_{143} = \langle$[1,1,3],[2,2,3],[1,2,1],[1,2,2]$\rangle$	$\mathrm{Aut}(M_{143}) \simeq \mathrm{C}_2$
$M_{144} = \langle$[1,1,3],[1,3,3],[1,1,1],[3,1,3]$\rangle$	$\mathrm{Aut}(M_{144}) \simeq \mathrm{C}_2$
$M_{145} = \langle$[1,1,3],[2,2,3],[1,1,1],[3,3,3]$\rangle$	$\mathrm{Aut}(M_{145}) \simeq \mathrm{C}_2$
$M_{146} = \langle$[1,1,3],[1,3,1],[1,3,3],[3,1,3]$\rangle$	$\mathrm{Aut}(M_{146}) \simeq \mathrm{C}_2 \times \mathrm{C}_2$
$M_{147} = \langle$[1,1,1],[2,2,2],[1,2,1],[1,2,2]$\rangle$	$\mathrm{Aut}(M_{147}) \simeq \mathrm{C}_2 \times \mathrm{C}_2$
$M_{148} = \langle$[1,1,3],[1,1,2],[3,3,3],[1,2,1],[2,2,1]$\rangle$	$\mathrm{Aut}(M_{148}) \simeq 1$
$M_{149} = \langle$[1,1,3],[2,2,3],[1,2,1],[3,3,3],[1,1,2]$\rangle$	$\mathrm{Aut}(M_{149}) \simeq 1$
$M_{150} = \langle$[1,1,3],[1,3,3],[1,2,1],[3,1,3],[2,2,2]$\rangle$	$\mathrm{Aut}(M_{150}) \simeq 1$
$M_{151} = \langle$[1,1,3],[1,1,2],[3,3,3],[2,2,3],[2,2,1]$\rangle$	$\mathrm{Aut}(M_{151}) \simeq \mathrm{C}_2$
$M_{152} = \langle$[1,1,3],[1,3,1],[1,3,3],[3,1,3],[2,2,2]$\rangle$	$\mathrm{Aut}(M_{152}) \simeq \mathrm{C}_2$
$M_{153} = \langle$[1,1,3],[2,2,3],[1,2,1],[3,3,3],[1,2,2]$\rangle$	$\mathrm{Aut}(M_{153}) \simeq \mathrm{C}_2$
$M_{154} = \langle$[1,1,3],[2,2,3],[1,2,1],[2,1,1],[3,3,3]$\rangle$	$\mathrm{Aut}(M_{154}) \simeq \mathrm{C}_2$

In particular, we have $M_{113} = \mathrm{S}_3^{\mathrm{mon}}$.

The list of occurring orders of representatives of isoclasses of submonoids of $\mathrm{S}_3^{\mathrm{mon}}$, is

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

1.5.3 Further calculations

1.5.3.1 Calculations concerning $\mathrm{S}_4^{\mathrm{mon}}$

Submonoids of $\mathrm{S}_4^{\mathrm{mon}}$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	19	10
2	955	663
3	23,912	20,979

The list of occurring orders of representatives of conjugacy classes of submonoids of $\mathrm{S}_4^{\mathrm{mon}}$ with $\leqslant 2$ generators, is

```
[ <1, 1>, <2, 6>, <3, 27>, <4, 70>, <5, 73>, <6, 96>, <7, 73>, <8, 77>,
  <9, 56>, <10, 48>, <11, 43>, <12, 44>, <13, 37>, <14, 38>, <15, 16>,
  <16, 22>, <17, 14>, <18, 26>, <19, 12>, <20, 12>, <21, 6>, <22, 6>, <23, 2>,
  <24, 28>, <25, 11>, <26, 7>, <27, 3>, <28, 3>, <29, 3>, <30, 2>, <31, 4>,
  <32, 3>, <33, 2>, <34, 6>, <38, 3>, <39, 1>, <40, 15>, <41, 6>, <42, 4>,
  <43, 4>, <44, 1>, <45, 4>, <46, 1>, <48, 4>, <52, 3>, <56, 4>, <57, 1>,
  <58, 4>, <59, 1>, <61, 2>, <62, 3>, <63, 2>, <64, 1>, <67, 5>, <68, 2>,
  <79, 1>, <97, 1>, <106, 1>, <116, 1>, <128, 1>, <145, 1>, <176, 1> ] .
```

The list of occurring orders of representatives of isoclasses of submonoids of $\mathrm{S}_4^{\mathrm{mon}}$ with $\leqslant 2$ generators, is

```
[ <1, 1>, <2, 2>, <3, 7>, <4, 25>, <5, 31>, <6, 48>, <7, 49>, <8, 46>, <9, 37>,
  <10, 37>, <11, 33>, <12, 34>, <13, 30>, <14, 35>, <15, 15>, <16, 22>,
  <17, 8>, <18, 23>, <19, 12>, <20, 11>, <21, 6>, <22, 6>, <23, 2>, <24, 25>,
  <25, 11>, <26, 6>, <27, 3>, <28, 3>, <29, 3>, <30, 2>, <31, 3>, <32, 3>,
  <33, 1>, <34, 6>, <38, 3>, <39, 1>, <40, 14>, <41, 6>, <42, 4>, <43, 4>,
  <44, 1>, <45, 4>, <46, 1>, <48, 4>, <52, 3>, <56, 4>, <57, 1>, <58, 4>,
  <59, 1>, <61, 2>, <62, 3>, <63, 2>, <64, 1>, <67, 5>, <68, 2>, <79, 1>,
  <97, 1>, <106, 1>, <116, 1>, <128, 1>, <145, 1>, <176, 1> ] .
```

The list of occurring orders of representatives of conjugacy classes of submonoids of $\mathrm{S}_4^{\mathrm{mon}}$ with $\leqslant 3$ generators, is

```
[ <1, 1>, <2, 6>, <3, 27>, <4, 105>, <5, 271>, <6, 546>, <7, 686>, <8, 889>,
  <9, 963>, <10, 1020>, <11, 887>, <12, 983>, <13, 912>, <14, 895>, <15, 872>,
  <16, 806>, <17, 656>, <18, 808>, <19, 698>, <20, 520>, <21, 369>, <22, 568>,
  <23, 459>, <24, 470>, <25, 391>, <26, 310>, <27, 276>, <28, 271>, <29, 188>,
  <30, 352>, <31, 364>, <32, 283>, <33, 236>, <34, 186>, <35, 128>, <36, 186>,
  <37, 142>, <38, 251>, <39, 333>, <40, 199>, <41, 203>, <42, 157>, <43, 179>,
  <44, 202>, <45, 143>, <46, 170>, <47, 139>, <48, 169>, <49, 211>, <50, 203>,
  <51, 104>, <52, 103>, <53, 120>, <54, 61>, <55, 138>, <56, 144>, <57, 102>,
  <58, 167>, <59, 119>, <60, 187>, <61, 49>, <62, 83>, <63, 131>, <64, 49>,
  <65, 28>, <66, 70>, <67, 107>, <68, 187>, <69, 53>, <70, 118>, <71, 36>,
  <72, 94>, <73, 50>, <74, 43>, <75, 45>, <76, 40>, <77, 65>, <78, 69>,
  <79, 36>, <80, 153>, <81, 24>, <82, 49>, <83, 70>, <84, 94>, <85, 43>,
  <86, 35>, <87, 25>, <88, 36>, <89, 20>, <90, 39>, <91, 34>, <92, 6>,
  <93, 6>, <94, 10>, <95, 43>, <96, 15>, <97, 9>, <98, 31>, <99, 2>, <100, 51>,
  <101, 13>, <102, 23>, <103, 23>, <104, 32>, <105, 7>, <106, 21>, <108, 12>,
  <109, 18>, <110, 14>, <111, 1>, <112, 1>, <114, 11>, <115, 7>, <116, 9>,
  <118, 1>, <120, 1>, <126, 7>, <128, 1>, <131, 3>, <132, 2>, <133, 1>,
  <136, 1>, <140, 2>, <143, 1>, <144, 1>, <145, 1>, <148, 1>, <150, 2>,
  <151, 1>, <163, 1>, <172, 1>, <174, 1>, <176, 1>, <180, 1>, <181, 1>,
  <188, 1>, <199, 1>, <235, 1>, <236, 1>, <244, 1>, <256, 1> ] .
```

The list of occurring orders of representatives of isoclasses of submonoids of $\mathrm{S}_4^{\mathrm{mon}}$ with $\leqslant 3$ generators, is

```
[ <1, 1>, <2, 2>, <3, 7>, <4, 35>, <5, 103>, <6, 260>, <7, 437>, <8, 602>,
  <9, 708>, <10, 749>, <11, 716>, <12, 823>, <13, 784>, <14, 764>, <15, 781>,
  <16, 725>, <17, 567>, <18, 738>, <19, 643>, <20, 503>, <21, 341>, <22, 516>,
  <23, 438>, <24, 448>, <25, 367>, <26, 289>, <27, 265>, <28, 262>, <29, 180>,
  <30, 318>, <31, 356>, <32, 264>, <33, 232>, <34, 180>, <35, 119>, <36, 177>,
  <37, 138>, <38, 244>, <39, 331>, <40, 197>, <41, 201>, <42, 143>, <43, 175>,
  <44, 199>, <45, 140>, <46, 168>, <47, 139>, <48, 167>, <49, 211>, <50, 203>,
  <51, 104>, <52, 103>, <53, 120>, <54, 61>, <55, 138>, <56, 144>, <57, 102>,
  <58, 167>, <59, 119>, <60, 187>, <61, 49>, <62, 83>, <63, 131>, <64, 49>,
  <65, 28>, <66, 70>, <67, 107>, <68, 187>, <69, 53>, <70, 118>, <71, 36>,
  <72, 94>, <73, 50>, <74, 43>, <75, 45>, <76, 40>, <77, 65>, <78, 69>,
  <79, 36>, <80, 153>, <81, 24>, <82, 49>, <83, 70>, <84, 94>, <85, 43>,
  <86, 35>, <87, 25>, <88, 36>, <89, 20>, <90, 39>, <91, 34>, <92, 6>,
  <93, 6>, <94, 10>, <95, 43>, <96, 15>, <97, 9>, <98, 31>, <99, 2>,
  <100, 51>, <101, 13>, <102, 23>, <103, 23>, <104, 32>, <105, 7>, <106, 21>,
  <108, 12>, <109, 18>, <110, 14>, <111, 1>, <112, 1>, <114, 11>, <115, 7>,
  <116, 9>, <118, 1>, <120, 1>, <126, 7>, <128, 1>, <131, 3>, <132, 2>,
  <133, 1>, <136, 1>, <140, 2>, <143, 1>, <144, 1>, <145, 1>, <148, 1>,
  <150, 2>, <151, 1>, <163, 1>, <172, 1>, <174, 1>, <176, 1>, <180, 1>,
  <181, 1>, <188, 1>, <199, 1>, <235, 1>, <236, 1>, <244, 1>, <256, 1> ] .
```

The following table contains some submonoids of S_4^{mon} together with the isoclass of the automorphism group of these monoids.

$M_1 = \langle\ \rangle$	$\mathrm{Aut}(M_1) \simeq 1$
$M_2 = \langle$[1, 1, 2, 4],[1, 4, 2, 4],[1, 3, 3, 4]$\rangle$	$\mathrm{Aut}(M_2) \simeq C_2$
$M_3 = \langle$[1, 1, 2, 4],[2, 4, 3, 1]$\rangle$	$\mathrm{Aut}(M_3) \simeq C_3$
$M_4 = \langle$[1, 1, 3, 3],[3, 2, 1, 1],[1, 1, 1, 1]$\rangle$	$\mathrm{Aut}(M_4) \simeq C_2 \times C_2$
$M_5 = \langle$[1, 1, 2, 4],[3, 3, 3, 3],[2, 3, 1, 4]$\rangle$	$\mathrm{Aut}(M_5) \simeq S_3$
$M_6 = \langle$[1, 1, 3, 3],[3, 2, 2, 2],[3, 4, 2, 1]$\rangle$	$\mathrm{Aut}(M_6) \simeq D_4$
$M_7 = \langle$[1, 1, 1, 2],[1, 1, 1, 3],[2, 3, 1, 1]$\rangle$	$\mathrm{Aut}(M_7) \simeq D_6$
$M_8 = \langle$[2, 3, 1, 1],[2, 3, 1, 4],[1, 1, 1, 1]$\rangle$	$\mathrm{Aut}(M_8) \simeq C_3 \rtimes S_3$
$M_9 = \langle$[1, 3, 2, 2],[2, 2, 2, 1],[2, 1, 3, 1]$\rangle$	$\mathrm{Aut}(M_9) \simeq S_3 \times C_2 \times C_2$
$M_{10} = \langle$[1, 3, 4, 2],[2, 1, 3, 4]$\rangle$	$\mathrm{Aut}(M_{10}) \simeq S_4$
$M_{11} = \langle$[1, 3, 2, 2],[2, 2, 2, 1],[2, 3, 1, 4]$\rangle$	$\mathrm{Aut}(M_{11}) \simeq C_2 \times (C_3 \rtimes S_3)$
$M_{12} = \langle$[1, 1, 4, 3],[1, 3, 3, 4],[3, 1, 4, 1]$\rangle$	$\mathrm{Aut}(M_{12}) \simeq S_3 \times S_3$
$M_{13} = \langle$[1, 1, 2, 2],[2, 2, 1, 2],[1, 1, 2, 1] [1, 2, 1, 2],[1, 2, 2, 1],[2, 2, 1, 1] [1, 2, 1, 1]$\rangle$	$\mathrm{Aut}(M_{13}) \simeq S_3 \times D_4$
$M_{14} = \langle$[1, 1, 3, 3],[1, 1, 3, 1],[1, 3, 1, 3], [3, 1, 3, 1],[1, 1, 1, 3],[1, 3, 3, 3], [3, 1, 3, 3]$\rangle$	$\mathrm{Aut}(M_{14}) \simeq C_2 \times S_3 \times D_4$
$M_{15} = \langle$[1, 1, 3, 3],[1, 1, 3, 1],[1, 3, 1, 3], [1, 3, 3, 3],[1, 3, 3, 1],[3, 1, 3, 3]$\rangle$	$\mathrm{Aut}(M_{15}) \simeq S_4 \times C_2$

Note that as automorphism groups of subgroups of S_4 only 1, C_2, S_3, D_4 and S_4 occur, up to isomorphism.

1.5.3.2 Calculations in S_n^{mon} with variable n

The following table contains the number of submonoids in given degree n, the number of conjugacy classes and the number of isoclasses of submonoids in given degree n.

Submonoids of S_n^{mon}

n	number of submonoids	number of conjugacy classes	number of isoclasses
1	1	1	1
2	6	5	5
3	699	160	154

The following tables contain the number of conjugacy classes and the number of isoclasses of submonoids of the symmetric monoid $\mathrm{S}_n^{\mathrm{mon}}$ in given degree n, with $\leqslant g$ generators for a certain g.

Submonoids of $\mathrm{S}_n^{\mathrm{mon}}$ with $\leqslant 1$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	3	3
3	7	6
4	19	10
5	47	16
6	129	22
7	339	31

Submonoids of $\mathrm{S}_n^{\mathrm{mon}}$ with $\leqslant 2$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	5	5
3	49	44
4	955	663

Submonoids of $\mathrm{S}_n^{\mathrm{mon}}$ with $\leqslant 3$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	5	5
3	119	113
4	23,912	20,979

The following tables contain the number of conjugacy classes and of isoclasses of submonoids of order $\leqslant k$ for a certain k with $\leqslant g$ generators for a certain g.

Submonoids of S_n^{mon} of order $\leqslant 2$ with $\leqslant 2$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	3	3
3	4	3
4	7	3
5	9	3
6	14	3
7	18	3

Submonoids of S_n^{mon} of order $\leqslant 5$ with $\leqslant 2$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	5	5
3	28	23
4	177	66
5	930	113
6	4,522	113

Submonoids of S_n^{mon} of order $\leqslant 5$ with $\leqslant 3$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	5	5
3	42	36
4	410	148
5	3,010	249

Submonoids of S_n^{mon} of order $\leqslant 10$ with $\leqslant 2$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	5	5
3	45	40
4	527	283
5	5,934	1,410

Submonoids of S_n^{mon} of order $\leqslant 10$ with $\leqslant 3$ generators

n	number of conjugacy classes	number of isoclasses
1	1	1
2	5	5
3	102	96
4	4,514	2,904

1.5.3.3 Calculations in S_n^{mon} with variable cap on the number of generators

The following tables contain the number of conjugacy classes and the number of isoclasses of submonoids of the symmetric monoid S_n^{mon} in degree n, for a certain n, of order $\leqslant k$ for a certain k with $\leqslant g$ generators for a given g.

Submonoids of S_3^{mon} of order $\leqslant 5$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	7	6
2	28	23
3	42	36
4	43	37
5	43	37

Submonoids of S_3^{mon} of order $\leqslant 10$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	7	6
2	45	40
3	102	96
4	129	123
5	135	129
6	135	129

Submonoids of S_4^{mon} of order $\leqslant 5$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	19	10
2	177	66
3	410	148
4	441	163
5	441	163

Submonoids of S_4^{mon} of order $\leqslant 10$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	19	10
2	527	283
3	4,514	2,904
4	16,216	11,313
5	30,302	?
6	36,677	?
7	37,637	?
8	37,642	?
9	37,642	?

The entries marked "?" could not be calculated because of hardware limitations.

Submonoids of S_5^{mon} of order $\leqslant 5$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	46	15
2	930	113
3	3,010	249
4	3,328	273
5	3,328	273

Submonoids of S_5^{mon} of order $\leqslant 10$ with $\leqslant g$ generators

g	number of conjugacy classes	number of isoclasses
1	47	16
2	5,934	1,410

Chapter 2

From monoids to field extensions

Let K be a field.

2.1 Aim and methods

Let M be a finite monoid.

2.1.1 From monoid algebras to field extensions

Definition 20 Let $\mathbb{Q}M$ be the $\mathbb{Q}$-vector space with basis M. On $\mathbb{Q}M$, we have the multiplication

$$\begin{array}{ccccl} \mathbb{Q}M & \times & \mathbb{Q}M & \stackrel{(\cdot)}{\longrightarrow} & \mathbb{Q}M \\ (\sum_{m\in M} q_m \cdot m & , & \sum_{n\in M} r_n \cdot n) & \mapsto & (\sum_{m\in M} q_m \cdot m) \cdot (\sum_{n\in N} r_n \cdot n) := \sum_{m,n\in M} q_m \cdot r_n \cdot m \cdot n \\ & & & & = \sum_{x\in M} \left(\sum_{m,n\in M, m\cdot n = x} q_m \cdot r_n\right) \cdot x, \end{array}$$

Then $\mathbb{Q}M$ is a $\mathbb{Q}$-algebra, called *monoid algebra* of M with coefficients in $\mathbb{Q}$.

Remark 21 There is an isomorphism

$$w : \mathbb{Q}M/\operatorname{Jac}(\mathbb{Q}M) \stackrel{\sim}{\to} \Pi_{i=1}^{s} D_i^{n_i \times n_i},$$

where $s \geqslant 1$ and where D_i is a finite dimensional division algebra over $\mathbb{Q}$ for $i \in [1, s]$.

Then $\mathrm{Z}(D_i)$ is a finite field extension over $\mathbb{Q}$, i.e. a number field.

The center is preserved by isomorphisms so that w restricts to an isomorphism

$$w_{\mathrm{Z}} : \mathrm{Z}(\mathbb{Q}M/\operatorname{Jac}(\mathbb{Q}M)) \stackrel{\sim}{\to} \Pi_{i=1}^{s} \mathrm{Z}(D_i),$$

where we have identified z and $z \cdot \mathrm{E}_{n_i}$ for $z \in \mathrm{Z}(D_i)$.

We write $\overline{\mathbb{Q}M} := \mathbb{Q}M/\operatorname{Jac}(\mathbb{Q}M)$. So

$$w_{\mathrm{Z}} : \mathrm{Z}\big(\overline{\mathbb{Q}M}\big) \stackrel{\sim}{\to} \Pi_{i=1}^{s} \mathrm{Z}(D_i).$$

Let $1_{\mathrm{Z}(\overline{\mathbb{Q}M})} = \overline{e_1} + \cdots + \overline{e_s}$ be an orthogonal decomposition into primitive idempotents $\overline{e_i} \in \mathrm{Z}\big(\overline{\mathbb{Q}M}\big)$, numbered such that $w_{\mathrm{Z}}(\overline{e_i}\,\mathrm{Z}(\overline{\mathbb{Q}M})) = \mathrm{Z}(D_i)$ for $i \in [1, s]$.

Now let $Z_i := \overline{e_i} \cdot \mathrm{Z}\big(\overline{\mathbb{Q}M}\big)$ for $i \in [1, s]$.

Then $w_{\mathrm{Z}}(Z_i) = \mathrm{Z}(D_i)$.

Given $\sigma \in \mathrm{Aut}(M)$, we have a $\mathbb{Q}$-algebra automorphism

$$\begin{array}{rcl} \mathbb{Q}M & \stackrel{\sigma_{\mathbb{Q}}}{\longrightarrow} & \mathbb{Q}M \\ \Sigma_{m \in M}\; q_m \cdot m & \mapsto & \Sigma_{m \in M}\; q_m \cdot m\sigma \; . \end{array}$$

The Jacobson radical is preserved by isomorphism so that we obtain an induced $\mathbb{Q}$-algebra automorphism

$$\begin{array}{rcl} \overline{\mathbb{Q}M} & \stackrel{\overline{\sigma_{\mathbb{Q}}}}{\longrightarrow} & \overline{\mathbb{Q}M} \\ \Sigma_{m \in M}\; q_m \cdot m + \mathrm{Jac}(\overline{\mathbb{Q}M}) & \mapsto & \Sigma_{m \in M}\; q_m \cdot m\sigma + \mathrm{Jac}(\overline{\mathbb{Q}M}) \; . \end{array}$$

Then $\overline{\sigma_{\mathbb{Q}}}$ restricts to an automorphism of $\mathrm{Z}(\overline{\mathbb{Q}M})$.

For $i \in [1, s]$, we denote

$$\mathrm{Aut}_{\overline{e_i}}(M) := \{\sigma \in \mathrm{Aut}(M) : \overline{e_i}\; \overline{\sigma_{\mathbb{Q}}} = \overline{e_i}\} \leqslant \mathrm{Aut}(M) \; .$$

This yields a group morphism

$$\begin{array}{rcl} \mathrm{Aut}_{\overline{e_i}}(M) & \stackrel{\varphi_i}{\longrightarrow} & \mathrm{Aut}(Z_i) \\ \sigma & \mapsto & \overline{\sigma_{\mathbb{Q}}}|_{Z_i}^{Z_i} \; . \end{array}$$

We obtain the fixed field under this action, $F_i := \{x \in Z_i : x = x(\sigma\varphi_i) \text{ for } \sigma \in \mathrm{Aut}_{\overline{e_i}}(M)\}$.

Then $Z_i|F_i$ is a Galois extension with Galois group $\mathrm{Im}\,\varphi_i$.

$$\begin{array}{c} Z_i \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_i} \\ F_i \\ \Big| \\ \mathbb{Q} \end{array}$$

We search for examples for such number fields Z_i , together with $\mathrm{Gal}(Z_i \,|\, F_i)$.

2.1.2 From twisted monoid algebras to field extensions

Definition 22 A *two-cocycle* α of M is a map $\alpha : M \times M \longrightarrow \mathbb{Q}^{\times}$ such that (2C 1–3) hold.

(2C 1) We have $(1_M, m)\alpha = 1$ for $m \in M$.

(2C 2) We have $(m, 1_M)\alpha = 1$ for $m \in M$.

(2C 3) We have $1 = (n,l)\alpha \cdot ((m\cdot n, l)\alpha)^{-1} \cdot (m, n\cdot l)\alpha \cdot ((m,n)\alpha)^{-1}$ for $m,\ n,\ l \in M$.

Definition 23 Suppose given a finite monoid M. Suppose given a two-cocycle α.

Let $\mathbb{Q}_\alpha M$ be the $\mathbb{Q}$-vector space with basis M together with the multiplication

$$\begin{array}{cccccl} \mathbb{Q}_\alpha M & \times & \mathbb{Q}_\alpha M & \xrightarrow{(\cdot_\alpha)} & \mathbb{Q}_\alpha M \\ ((\Sigma_{m\in M} q_m \cdot m) & , & (\Sigma_{n\in M} r_n \cdot n)) & \mapsto & (\Sigma_{m\in M} q_m \cdot m) \cdot_\alpha (\Sigma_{n\in M} r_n \cdot n) \\ & & & & := \Sigma_{m,n\in M} q_m \cdot r_n \cdot (m,n)\alpha \cdot m\cdot n\ , \end{array}$$

$\mathbb{Q}_\alpha M$ becomes a $\mathbb{Q}$-algebra, called the *twisted monoid algebra* of M with coefficients in $\mathbb{Q}$ with respect to α.

Proof. We have to show that $m \cdot_\alpha 1_M \overset{!}{=} m$, that $1_M \cdot_\alpha m \overset{!}{=} m$ for $m \in M$ and the associativity of $\mathbb{Q}_\alpha M$.

Suppose given $m \in M$. We have $m \cdot_\alpha 1_M = (m, 1_M)\alpha \cdot m \cdot 1_M \overset{\text{(2C 2)}}{=} 1 \cdot m \cdot 1_M = m$.

We have $1_M \cdot_\alpha m = (1_M, m)\alpha \cdot 1_M \cdot m \overset{\text{(2C 1)}}{=} 1 \cdot 1_M \cdot m = m$.

We have

$$\begin{array}{cl} & ((\Sigma_{m\in M} q_m \cdot m) \cdot_\alpha (\Sigma_{n\in M} r_n \cdot n)) \cdot_\alpha (\Sigma_{l\in M} s_l \cdot l) \\ = & (\Sigma_{m,n\in M} q_m \cdot r_n \cdot (m,n)\alpha \cdot m\cdot n) \cdot_\alpha (\Sigma_{l\in M} s_l \cdot l) \\ = & \Sigma_{m,n,l\in M} q_m \cdot r_n \cdot s_l \cdot (m,n)\alpha \cdot (m\cdot n, l)\alpha \cdot m\cdot n\cdot l \\ \overset{\text{(2C 3)}}{=} & \Sigma_{m,n\in M} q_m \cdot r_n \cdot s_l \cdot (n,l)\alpha \cdot (m, n\cdot l)\alpha \cdot m\cdot n\cdot l \\ = & (\Sigma_{m\in M} q_m \cdot m) \cdot_\alpha (\Sigma_{n,l\in M} r_n \cdot s_l \cdot (n,l)\alpha \cdot n\cdot l) \\ = & (\Sigma_{m\in M} q_m \cdot m) \cdot_\alpha ((\Sigma_{n\in M} r_n \cdot n) \cdot_\alpha (\Sigma_{l\in M} s_l \cdot l)) \end{array}$$

for $\sum_{m\in M} q_m \cdot m$, $\sum_{n\in M} r_n \cdot n$, $\sum_{l\in M} s_l \cdot l \in \mathbb{Q}_\alpha M$. □

Remark 24 There is an isomorphism

$$w_\alpha : \mathbb{Q}_\alpha M / \operatorname{Jac}(\mathbb{Q}_\alpha M) \ \xrightarrow{\sim}\ \Pi_{i=1}^{s} D_i^{n_i\times n_i},$$

where $s \geqslant 1$ and where D_i is a finite dimensional division algebra over $\mathbb{Q}$ for $i \in [1, s]$.

Then $\mathrm{Z}(D_i)$ is a finite field extension over $\mathbb{Q}$, i.e. a number field.

The center is preserved by isomorphisms so that w restricts to an isomorphism

$$w_{\alpha,\mathrm{Z}} : \mathrm{Z}(\mathbb{Q}_\alpha M / \operatorname{Jac}(\mathbb{Q}_\alpha M)) \ \xrightarrow{\sim}\ \Pi_{i=1}^{s} \mathrm{Z}(D_i),$$

where we have identified z and $z \cdot \mathrm{E}_{n_i}$ for $z \in \mathrm{Z}(D_i)$.

We write $\overline{\mathbb{Q}_\alpha M} := \mathbb{Q}_\alpha M / \operatorname{Jac}(\mathbb{Q}_\alpha M)$. So

$$w_{\alpha,\mathrm{Z}} : \mathrm{Z}\big(\overline{\mathbb{Q}_\alpha M}\big) \ \xrightarrow{\sim}\ \Pi_{i=1}^{s} \mathrm{Z}(D_i)$$

Let $1_{\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})} = \overline{e_1} + \cdots + \overline{e_s}$ be an orthogonal decomposition into primitive idempotents $\overline{e_i} \in \mathrm{Z}\big(\overline{\mathbb{Q}_\alpha M}\big)$, numbered such that $w_{\alpha,\mathrm{Z}}(\overline{e_i}\,\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})) = \mathrm{Z}(D_i)$ for $i \in [1, s]$.

Now let $Z_i := \overline{e_i} \cdot \mathrm{Z}\big(\overline{\mathbb{Q}_\alpha M}\big)$ for $i \in [1, s]$.

Then $w_{\alpha,\mathrm{Z}}(Z_i) = \mathrm{Z}(D_i)$.

Let $\mathrm{Aut}_\alpha(M) := \{\sigma \in \mathrm{Aut}(M) : (m\sigma, n\sigma)\alpha = (m, n)\alpha \text{ for } m, n \in M\} \leqslant \mathrm{Aut}(M)$.

Given $\sigma \in \mathrm{Aut}_\alpha(M)$, we have a $\mathbb{Q}$-algebra automorphism

$$\begin{array}{rcl} \mathbb{Q}_\alpha M & \xrightarrow{\sigma_\mathbb{Q}} & \mathbb{Q}_\alpha M \\ \Sigma_{m\in M}\ q_m \cdot m & \mapsto & \Sigma_{m\in M}\ q_m \cdot m\sigma\ . \end{array}$$

In fact, for $m, n \in M$, we obtain

$$\begin{array}{rcl} m\sigma_\mathbb{Q} \cdot_\alpha n\sigma_\mathbb{Q} & = & (m\sigma, n\sigma)\alpha \cdot m\sigma \cdot n\sigma \\ & = & (m, n)\alpha \cdot (m \cdot n)\sigma \\ & = & (m, n)\alpha \cdot (m \cdot n)\sigma_\mathbb{Q} \\ & = & ((m, n)\alpha \cdot m \cdot n)\,\sigma_\mathbb{Q} \\ & = & (m \cdot_\alpha n)\sigma_\mathbb{Q}\ . \end{array}$$

The Jacobson radical is preserved by isomorphism so that we obtain an induced $\mathbb{Q}$-algebra automorphism

$$\begin{array}{rcl} \overline{\mathbb{Q}_\alpha M} & \xrightarrow{\overline{\sigma_\mathbb{Q}}} & \overline{\mathbb{Q}_\alpha M} \\ \Sigma_{m\in M}\ q_m \cdot m + \mathrm{Jac}(\overline{\mathbb{Q}_\alpha M}) & \mapsto & \Sigma_{m\in M}\ q_m \cdot m\sigma + \mathrm{Jac}(\overline{\mathbb{Q}_\alpha M}) \end{array}$$

Then $\overline{\sigma_\mathbb{Q}}$ restricts to an automorphism of $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$.

For $i \in [1, s]$, we denote

$$\mathrm{Aut}_{\alpha,\overline{e_i}}(M) := \{\sigma \in \mathrm{Aut}_\alpha(M) : \overline{e_i}\ \overline{\sigma_\mathbb{Q}} = \overline{e_i}\} \leqslant \mathrm{Aut}_\alpha(M) \leqslant \mathrm{Aut}(M)\ .$$

This yields a group morphism

$$\begin{array}{rcl} \mathrm{Aut}_{\alpha,\overline{e_i}}(M) & \xrightarrow{\varphi_i} & \mathrm{Aut}(Z_i) \\ \sigma & \mapsto & \overline{\sigma_\mathbb{Q}}|_{Z_i}^{Z_i} \end{array}$$

We obtain the fixed field under this action, $F_i := \{x \in Z_i : x = x(\sigma\varphi_i) \text{ for } \sigma \in \mathrm{Aut}_{\alpha,\overline{e_i}}(M)\}$.

Then $Z_i|F_i$ is a Galois extension with Galois group $\mathrm{Im}\,\varphi_i$.

$$\begin{array}{c} Z_i \\ \big|\ {\scriptstyle \mathrm{Im}\,\varphi_i} \\ F_i \\ \big| \\ \mathbb{Q} \end{array}$$

We search for examples for such number fields Z_i, together with $\mathrm{Gal}(Z_i \,|\, F_i)$.

Lemma 25 *Suppose given $k \geqslant 2$ and a map*

$$\begin{array}{rcl} f : M & \longrightarrow & \mathbb{Z}/k\mathbb{Z} \\ m & \mapsto & mf \end{array}$$

such that $(m \cdot n)f = mf + nf$ for $m, n \in M$.

So f is a monoid morphism from M to the additive group of $\mathbb{Z}/k\mathbb{Z}$

Let i be the map

$$\begin{array}{rcl} \mathbb{Z}/k\mathbb{Z} & \xrightarrow{i} & \mathbb{Q}/\mathbb{Z} \\ z + k\mathbb{Z} & \mapsto & \frac{z}{k} + \mathbb{Z} \end{array}$$

and let ρ be the residue class map

$$\begin{array}{rcl} \mathbb{Q} & \xrightarrow{\rho} & \mathbb{Q}/\mathbb{Z} \\ q & \mapsto & q + \mathbb{Z}\ . \end{array}$$

Let κ be the map

$$\begin{array}{rcl} \mathbb{Q}/\mathbb{Z} & \xrightarrow{\kappa} & \mathbb{Q} \\ q + \mathbb{Z} & \mapsto & q, \text{ with } 0 \leqslant q < 1 \end{array}$$

Let $\hat{f}$ be the map

$$\begin{array}{rcl} M & \xrightarrow{\hat{f}} & \mathbb{Q} \\ m & \mapsto & m\hat{f} := mfi\kappa \end{array}$$

Note that $\kappa\rho = \mathrm{id}_{\mathbb{Q}/\mathbb{Z}}$, so that $\hat{f}\rho = fi\kappa\rho = fi$.

Let $(m, n)\check{f} := (m \cdot n)\hat{f} - m\hat{f} - n\hat{f}$ for $m, n \in M$.

Note that

$$\begin{array}{rcl} (m, n)\check{f}\rho & = & ((m \cdot n)\hat{f} - m\hat{f} - n\hat{f})\rho \\ & = & (m \cdot n)\hat{f}\rho - m\hat{f}\rho - n\hat{f}\rho \\ & = & (m \cdot n)fi - mfi - nfi \\ & = & ((m \cdot n)f - mf - nf)i \\ & = & (0 + k\mathbb{Z})i = 0 + \mathbb{Z} \end{array}$$

hence $(m, n)\check{f} \in \mathbb{Z}$ for $m, n \in M$.

Suppose given $p \in \mathbb{Z}_{\geqslant 1}$.

Let τ be the map

$$\begin{array}{rcl} M \times M & \xrightarrow{\tau} & \mathbb{Q} \\ (m, n) & \mapsto & m\tau := p^{(m,n)\check{f}} \end{array}$$

Then the map τ is a two-cocycle.

Proof. We have to show $1 \overset{!}{=} (n, l)\tau \cdot ((m \cdot n, l)\tau)^{-1} \cdot (m, n \cdot l)\tau \cdot ((m, n)\tau)^{-1}$ for $m, n, l \in M$.

I.e. we have to show $0 \overset{!}{=} (n,l)\check{f} - (m\cdot n,l)\check{f} + (m,n\cdot l)\check{f} - (m,n)\check{f}$ for $m,n,l \in M$.

We have

$$\begin{aligned}
& (n,l)\check{f} - (m\cdot n,l)\check{f} + (m,n\cdot l)\check{f} - (m,n)\check{f} \\
= & \Big((n\cdot l)\hat{f} - n\hat{f} - l\hat{f}\Big) - \Big((m\cdot n\cdot l)\hat{f} - (m\cdot n)\hat{f} - l\hat{f}\Big) + \Big((m\cdot n\cdot l)\hat{f} - m\hat{f} - (n\cdot l)\hat{f}\Big) \\
& - \Big((m\cdot n)\hat{f} - m\hat{f} - n\hat{f}\Big) \\
= & -(m\cdot n\cdot l)\hat{f} + (m\cdot n)\hat{f} + (m\cdot n\cdot l)\hat{f} - m\hat{f} - (m\cdot n)\hat{f} + m\hat{f} \\
= & \; 0 \,.
\end{aligned}$$

□

2.2 Algorithmic search for field extensions

2.2.1 From monoid algebras to field extensions

We use the functions from §1, as can be loaded via `functions_chapter_1.txt`.

In the following, we let `Q:=Rationals()` be the rational field. Let `M` be a submonoid of a symmetric monoid. We compute the representing matrix of the multiplication map of an element `x` on `QM` with the function `RegularMatrix`.

First, the function `ProduceMseq` gives us a monoid as a list with the same elements as `M` and with the identity at the first place.

```
ProduceMseq := function(M) // M: monoid as a set of elements of the
                           // symmetric monoid
 return &cat SortedSubmon(M);
end function;
```

The input `ord` is the order of the submonoid `M`.

```
RegularMatrix := function(x,ord,Mseq) // x: element of Mseq, ord: order of Mseq
 // Mseq: monoid as a list of elements, where the identity comes first
 RM := MatrixRing(Q,ord)!0; // a matrix with all entries 0
 for i in [1..ord] do
  j := Index(Mseq,Compose(Mseq[i],x));
  RM[i,j] := 1;
 end for;
 return RM;
end function;
```

For example with

```
> M:=Submon([[1,1,3],[2,2,3],[1,2,1],[1,2,2]]);
> Mseq := ProduceMseq(M);
> Mseq;
```

we obtain

```
[
    [ 1, 2, 3 ],
    [ 1, 1, 1 ],
    [ 2, 2, 3 ],
    [ 2, 2, 2 ],
    [ 1, 2, 1 ],
    [ 1, 2, 2 ],
    [ 1, 1, 3 ],
    [ 2, 2, 1 ],
    [ 1, 1, 2 ]
] .
```

Then the function `RegularMatrix` gives

```
> RM := RegularMatrix([2,2,3],#Mseq,Mseq);
> RM;

[0 0 1 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 1 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 1 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0] .
```

For example `RM[5,4]` is `1`, which means that `Compose(Mseq[5],[2,2,3])` equals `[2,2,2]`, which is `Mseq[4]`.

Another example:

```
> M:=Submon([[4,1,4,1],[4,2,1,1]]);
> Mseq := ProduceMseq(M);
> Mseq;
[
    [ 1, 2, 3, 4 ],
    [ 1, 4, 1, 4 ],
    [ 1, 1, 4, 4 ],
    [ 1, 2, 4, 4 ],
    [ 1, 4, 4, 4 ],
    [ 4, 1, 1, 1 ],
    [ 4, 2, 1, 1 ],
    [ 4, 1, 4, 1 ],
    [ 4, 4, 1, 1 ]
]
```

```
> RM:=RegularMatrix([4,2,1,1],#Mseq,Mseq);
> RM;
[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 1]
[0 0 0 0 0 0 1 0 0]
[0 0 0 0 0 1 0 0 0]
[0 0 0 0 1 0 0 0 0]
[0 0 0 1 0 0 0 0 0]
[0 1 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 0 0]
```

For example `RM[8,2]` is `1`, which means that `Compose(Mseq[8],[4,2,1,1])` equals `[1,4,1,4]`, which is `Mseq[2]`.

The following functions `random_monoid_element` and `random_monoid_element_bijective` give a random element of the symmetric monoid S_d^{mon}, where the degree `d` has to be given as input. The second function yields only bijective elements.

```
random_monoid_element := function(d) // d: degree
 return [Random([1..d]) : i in [1..d]];
end function;


random_monoid_element_bijective := function(d) // d: degree
 remaining := {1..d};
 element := [];
 for k in [1..d] do
  i := Random(remaining);
  element cat:= [i];
  remaining := remaining diff {i};
 end for;
 return element;
end function;
```

The following function `Submon_capped` calculates the set of elements of the submonoid `M` of S_d^{mon} generated by a list of elements `s`. Additionally the output contains the information whether the order of the submonoid is less than or equal to the upper bound `ub`. Only in this case the output is correct. Otherwise we ignore the output.

```
Submon_capped := function(s,ub) // s: list of generators, i.e. list of elements
                                // of the symmetric monoid
 // ub : upper bound for order of the generated submonoid
 d := #s[1];
 id := [i : i in [1..d]];
 Todo := s;
 X := {id};
 bound_ok := true;
```

```
 while #Todo ge 1 and bound_ok do
  Todo := {x : x in Todo | not x in X}; // ejecting known elements
  X join:= Todo;
  if #X gt ub then
   bound_ok := false;
  end if;
  Todo := {Compose(x,y) : x in Todo, y in s};
 end while;
 return X, bound_ok;
end function;
```

Suppose given an automorphism `a` of the monoid `M`. The function `AutomOp` gives the image `ya` of an element `y` of `QM` under `a`, where both `y` and `ya` are given as regular matrices.

```
AutomOp := function(y,a,Mseq)
 // y: element of QM, given as regular matrix with respect to Mseq
 // a: element of Autom(<SortedSubmon(M[1]),M[2]>)
 // Mseq: monoid as a list of elements, where the identity comes first
 n := #Mseq;
 coeff_y := [y[1,i] : i in [1..n]]; // list of coefficients of y with respect
 // to the basis of the monoid ordered as in Mseq
 coeff_ya := [coeff_y[Index(a,i)] : i in [1..n]]; // action of a
 return &+[coeff_ya[i] * RegularMatrix(Mseq[i],n,Mseq) : i in [1..n]];
  // %% RegularMatrix is used here
end function;
```

We continue the example above, where

```
s := [[1,1,3],[2,2,3],[1,2,1],[1,2,2]];
M := <Submon(s),s>;
// M: monoid with generators
Mseq := ProduceMseq(M[1]);
RM := RegularMatrix([2,2,3],#Mseq,Mseq);
```

Then `Autom(<SortedSubmon(M[1]),M[2]>)` yields

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

We consider `a := [ 1, 4, 7, 2, 6, 5, 3, 9, 8 ]` as automorphism.

Then AutomOp(RM,a,Mseq) yields

```
[0 0 0 0 0 0 1 0 0]
[0 1 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 1 0 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 1 0 0 0 0 0 0 0]
[0 1 0 0 0 0 0 0 0].
```

This is exactly RegularMatrix(Mseq[7],#Mseq,Mseq). In fact, the matrix RM was obtained as RegularMatrix(Mseq[3],#Mseq,Mseq) and the automorphism a sends the element Mseq[3] to the element Mseq[7], since a[3] equals 7.

The following function ex_vers gives us examples of submonoids, where for each submonoid, we calculate its automorphism group and the resulting field extensions; cf. Remark 21.

Depending on the input variable v, there are different possibilities to generate the submonoids.

```
ex_vers := function(loops,d,ub,lb,deg,v)
 // loops: number of loops
 // d: degree of the symmetric monoid
 // ub: upper bound of the order of the submonoid
 // lb: lower bound of the order of the submonoid
 // deg: minimum degree of field extension is deg
 /*
 v: switch, possibilities to generate a submonoid
 v=1: 2 random generators
 v=2: 2 random generators, one of them bijective
 v=3: 3 random generators
 v=4: 3 generators: m random, m^sigma, m^(sigma^2) with sigma = (1,2,3)
 v=5: 4 generators: m random, m^sigma, m^(sigma^2), m^(sigma^3)
                    with sigma = (1,2,3,4)
 v=6: 4 generators: m random, m^sigma, m^rho, m^(sigma*rho)
                    with sigma = (1,2), rho = (3,4)
 */
 Q := Rationals();
 P<X> := PolynomialRing(Q);
 ex_list := [* *];
 id := [i : i in [1..d]];
 for i in [1..loops] do
  if i mod 10 eq 0 then
   print "counter i:= ", i;
  end if;
  if v eq 1 then
   gen1 := random_monoid_element(d);
```

```
 gen2 := random_monoid_element(d);
 gen_list := [gen1, gen2];
elif v eq 2 then
 gen1 := random_monoid_element(d);
 gen2 := random_monoid_element_bijective(d);
 gen_list := [gen1, gen2];
elif v eq 3 then
 gen1 := random_monoid_element(d);
 gen2 := random_monoid_element(d);
 gen3 := random_monoid_element(d);
 gen_list := [gen1, gen2, gen3];
elif v eq 4 then
 gen1 := random_monoid_element(d);
 sa4 := [2,3,1] cat [4..d];
 sa5 := Inverse(sa4);
 gen4 := Compose_list(d,[sa5,gen1,sa4]);
 gen5 := Compose_list(d,[sa4,gen1,sa5]);
 gen_list := [gen1,gen4,gen5];
elif v eq 5 then
 gen1 := random_monoid_element(d);
 sa5 := [2,3,4,1] cat [5..d]; // sa5 = sa5^-3
 sa6 := Compose(sa5,sa5); // sa5^2 = sa5^-2
 sa7 := Inverse(sa5); // sa5^3 = sa5^-1
 gen5 := Compose_list(d,[sa7,gen1,sa5]);
 gen6 := Compose_list(d,[sa6,gen1,sa6]);
 gen7 := Compose_list(d,[sa5,gen1,sa7]);
 gen_list := [gen1,gen5,gen6, gen7];
elif v eq 6 then
 gen1 := random_monoid_element(d);
 sigma := [2,1] cat [3..d];
 rho := [1,2] cat [4,3] cat [5..d];
 sr := [2,1,4,3] cat [5..d];
 gen2 := Compose_list(d,[sigma,gen1,sigma]);
 gen3 := Compose_list(d,[rho,gen1,rho]);
 gen4 := Compose_list(d,[sr,gen1,sr]);
 gen_list := [gen1, gen2, gen3, gen4];
end if;
M1, bound_ok := Submon_capped(gen_list,ub);
if bound_ok then // check upper bound
 M := <M1, gen_list>;
 print "Info_1: #M[1] = ", #M[1];
 if #M[1] le ub and #M[1] ge lb then
  M_sort_sub := <SortedSubmon(M[1]), gen_list>;
  Mseq := &cat M_sort_sub[1]; // Mseq: monoid as a list of elements, where
                              // the identity comes first
  ord := #Mseq; // order of the submonoid
  QM := MatrixAlgebra<Q, ord | [MatrixRing(Q,ord)!1] cat
```

```
  [RegularMatrix(x,ord,Mseq) : x in M[2]] >; // M[2]: list of generators
                                             // of submonoid M
J := JacobsonRadical(QM);
QMmodJ,res := quo<QM | J>;
ZQMmodJ := Center(QMmodJ);
e := CentralIdempotents(ZQMmodJ);
BZQMmodJ := Basis(ZQMmodJ);
Ktup := [ideal<ZQMmodJ | x > : x in e];
if not &and[Dimension(K) lt deg : K in Ktup] then // avoiding examples in
                              // which only fields of degree < deg appear
 print "Info_2: Tuple of dimensions of fields = ",
       [Dimension(K) : K in Ktup];
 A := Autom(M_sort_sub); // %%
 if #A ge 2 then // avoiding a trivial automorphism group
  print "Info_3: #Autom = ", #A;
  BB := [* Basis(K) : K in Ktup *];
  print "Info_4: BB = ", BB;
  MP := [*[<MinimalPolynomial(A),A,#B> : A in B] : B in BB*];
  MP_of_generators := [[tup : tup in sublist | Degree(tup[1]) eq tup[3]] :
                      sublist in MP];
  if &and[#sublist gt 0 : sublist in MP_of_generators] then
   MP_chosen := [sublist[1] : sublist in MP_of_generators];
  else
   print "Did not find generators everywhere!";
  end if;
  A_e := [];
  for i in [1..#e] do
   ee := QMmodJ!e[i];
   A_e cat:= [[a : a in A | AutomOp(ee@@res,a,Mseq)@res eq ee]];
   // %% AutomOp is used here
  end for;
  kernels_of_action := [[ a : a in A_e[i] |
    &and[AutomOp(bb@@res,a,Mseq)@res eq bb: bb in BB[i]] ] : i in [1..#e]];
  gen_fixed_field := [[&+[AutomOp(bb@@res,a,Mseq)@res : a in
    A_e[i]]/#kernels_of_action[i] : bb in BB[i]] : i in [1..#e]];
  print "Info_5: Generators of fixed fields = ", gen_fixed_field;
  // we form the trace of bb with respect to the subgroup given by the
  // image of A_e in the automorphism group of the field
  bases := [Basis(sub<ZQMmodJ | gen>) : gen in gen_fixed_field];
  bases_trans := [[QMmodJ!b : b in B] : B in bases];
  print "Info_6: Action of A_e: ", [[[AutomOp(bb@@res,a,Mseq)@res :
    bb in BB[i]] : a in A_e[i]] : i in [1..#e]];
  ex_list cat:= [*<A,<Mseq,M[2]>,MP_chosen,A_e,kernels_of_action,
                bases,bases_trans>*];
  print "Result, i := ", i, "<M[2],MP_chosen,A_e,kernels_of_action,bases,
    bases_trans> =", <M[2],MP_chosen,A_e,kernels_of_action,
    bases,bases_trans>;
```

```
      // resulting Galois group: A_e[i]/kernels_of_action[i]
     end if;
    end if;
   end if;
  end if;
 end for;
 return ex_list;
end function;
```

2.2.1.1 An example to illustrate the algorithm

We shall illustrate the function `ex_vers` with an example.

Suppose that `ex_vers`, using `v=3`, has randomly chosen the following list of generators in degree 8, internally called `M[2]`.

```
[
    [ 4, 4, 4, 6, 3, 8, 5, 5 ],
    [ 4, 4, 4, 6, 1, 8, 5, 5 ],
    [ 4, 4, 4, 6, 2, 8, 5, 5 ]
]
```

This list of generators generate the monoid M of order 16, internally called `M[1]`.

The following list, internally called `Mseq`, contains the elements of the monoid M.

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

We use the notation introduced in Remark 21.

The algorithm returns a tuple consisting of

- the automorphism group $\mathrm{Aut}(M)$ of the monoid M, called `A`,
- a tuple consisting of a list of elements of M and a list of chosen generators, called `<Mseq,M[2]>`,
- a list of minimal polynomials of generators of the fields Z_i, together with the respective generators and the degree of the minimal polynomials, called `MP_chosen`,
- the list of subgroups $\mathrm{Aut}_{\overline{e_i}}(M)$, called `A_e`,
- the list of kernels of the group morphisms $\varphi_i : \mathrm{Aut}_{\overline{e_i}}(M) \longrightarrow \mathrm{Aut}(Z_i)$, called `kernels_of_action`,
- a list of bases for the fixed fields F_i, expressed in terms of a standard basis of $\mathrm{Z}(\overline{\mathbb{Q}M})$, called `bases`,
- a list of bases for the fixed fields F_i, expressed in terms of a standard basis of $\overline{\mathbb{Q}M}$, called `bases_trans`.

In our example, the mentioned tuple has the following entries.

The automorphism group `A` of the monoid `M`, has order 24:

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

The automorphisms are given as maps from M to M with respect to the ordering in the list Mseq.

`MP_chosen` contains three tuples. Each tuple consists of a minimal polynomial, a corresponding generator and the degree of the minimal polynomial. One of them has degree 4.

```
[
    <X - 5, (0 1 1 1 1 1), 1>,
    <X - 1, ( 1 -1  0  0  0  0), 1>,
    <X^4 - 5*X^3 + 10*X^2 - 10*X + 5, ( 0  1  0  0  0 -1), 4>
]
```

With

```
> P<X> := PolynomialRing(Rationals());
> f := X^4 - 5*X^3 + 10*X^2 - 10*X + 5;
> K<a> := NumberField(f);
> [<i,IsIsomorphic(K,CyclotomicField(i))> : i in [1..30] |
   (IsIsomorphic(K,CyclotomicField(i)))];
```

we get

```
[ <5, true>, <10, true> ].
```

So this field extension is isomorphic to $\mathbb{Q}(\zeta_5)$.

The list of subgroups `A_e` of the automorphism group `A`, is `[A,A,A]`.

Then, `kernels_of_action`, contains the kernels of the actions of the entries of `A_e` on the occurring number fields.

For instance, we get `kernels_of_action[3]` as follows.

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

Additionally, we obtain the `bases` of the fixed fields:

```
[
    [ (0 1 1 1 1 1) ],
    [ ( 1 -1  0  0  0  0) ],
    [ (   0    1 -1/4 -1/4 -1/4 -1/4) ]
] .
```

We find that $\overline{\mathbb{Q}M}$ is commutative, so in this case, we get bases_trans = bases.

To consider a single specific example such as the one just found, we should be able to generate these data without a random search, but with a manual input. To do this, we use

```
> res := doc([[ 4, 4, 4, 6, 3, 8, 5, 5 ],
              [ 4, 4, 4, 6, 1, 8, 5, 5 ],[ 4, 4, 4, 6, 2, 8, 5, 5 ]]);
```

where the function doc can be found in the file doc.txt .

Using doc instead of ex_vers, we obtain A as res[1][2][1], Mseq as res[1][1][1][1], M[2] as res[1][1][1][2], MP_chosen as res[1][3], A_e[i] as res[i][4][1], kernels_of_action[i] as res[i][5][1] for $i \in [1, s]$, where s is given by #res, bases as res[1][9] and bases_trans as res[1][10].

The function doc also returns the image $\operatorname{Im}\varphi_i$ of the group morphisms φ_i as a group, which is given by res[i][8] for $i \in [1, s]$.

The function doc also returns A as a group, which is given by res[1][6] and the subgroup A_e[i] as a group, which is given by res[i][7] for $i \in [1, s]$.

2.2.1.2 Resulting examples

The following examples have been calculated using ex_vers; cf. §2.2.1.

We use the notation introduced in Remark 21 to describe the results.

Example 26 Consider the monoid M generated by

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

Then $|M| = 122$ and $\operatorname{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_8 \times Z_9 \times Z_{10}$.

The number field Z_8 has a generator with minimal polynomial

$$X^2 + X + \frac{1}{3} \in \mathbb{Q}[X].$$

In particular, $Z_8 \simeq \mathbb{Q}(\zeta_3)$.

We have $\operatorname{Aut}_{\overline{e_8}}(M) \simeq \mathrm{C}_2$. In particular, $|\operatorname{Aut}_{\overline{e_8}}(M)| = 2$.

The kernel of the action of φ_8 of $\operatorname{Aut}_{\overline{e_8}}(M)$ on Z_8 has order 1.

We get $\operatorname{Im}\varphi_8 \simeq \mathrm{C}_2$.

We have $F_8 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_8 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \scriptstyle \mathrm{Im}\,\varphi_8 \simeq \mathrm{C}_2 \\ F_8 \simeq \mathbb{Q} \end{array}$$

The number fields Z_9 and Z_{10} are isomorphic to the number field Z_8.

Example 27 Consider, as in §2.2.1.1, the monoid M generated by

```
[
    [ 4, 4, 4, 6, 3, 8, 5, 5 ],
    [ 4, 4, 4, 6, 1, 8, 5, 5 ],
    [ 4, 4, 4, 6, 2, 8, 5, 5 ]
] .
```

Then $|M| = 16$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_4$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3$.

The number field Z_3 has a generator with minimal polynomial

$$X^4 - 5X^3 + 10X^2 - 10X + 5 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_3}}(M)| = 24$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_4$.

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_4 \\ F_3 \simeq \mathbb{Q} \end{array}$$

Example 28 Consider the monoid M generated by

```
[
    [ 3, 3, 5, 9, 3, 8, 10, 9, 7, 6 ],
    [ 5, 1, 1, 9, 1, 8, 10, 9, 7, 6 ],
    [ 2, 5, 2, 9, 2, 8, 10, 9, 7, 6 ]
] .
```

Then $|M| = 51$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_4$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_9 \times Z_{10} \times Z_{11} \times Z_{12} \times Z_{13} \times Z_{14} \times Z_{15}$.

The number field Z_9 has a generator with minimal polynomial

$$X^4 - 10X^3 + 40X^2 - 80X + 80 \in \mathbb{Q}[X].$$

In particular, $Z_9 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_9}}(M) \simeq \mathrm{C}_4 \times \mathrm{C}_2$. In particular, $|\,\mathrm{Aut}_{\overline{e_9}}(M)| = 8$.

The kernel of the action of φ_9 of $\mathrm{Aut}_{\overline{e_9}}(M)$ on Z_9 has order 2.

We get $\mathrm{Im}\,\varphi_9 \simeq \mathrm{C}_4$.

We have $F_9 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_9 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \ \scriptstyle \mathrm{Im}\,\varphi_9 \simeq \mathrm{C}_4 \\ F_9 \simeq \mathbb{Q} \end{array}$$

The number fields Z_{10}, Z_{11}, Z_{12}, Z_{13} and Z_{14} are isomorphic to the number field Z_9 .

The number field Z_{15} has a generator with minimal polynomial

$$X^4 - 5X^3 + 10X^2 - 10X + 5 \in \mathbb{Q}[X].$$

In particular, $Z_{15} \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_{15}}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_{15}}}(M)| = 24$.

The kernel of the action of φ_{15} of $\mathrm{Aut}_{\overline{e_{15}}}(M)$ on Z_{15} has order 6.

We get $\mathrm{Im}\,\varphi_{15} \simeq \mathrm{C}_4$.

We have $F_{15} \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_{15} \simeq \mathbb{Q}(\zeta_5) \\ \Big| \ \scriptstyle \mathrm{Im}\,\varphi_{15} \simeq \mathrm{C}_4 \\ F_{15} \simeq \mathbb{Q} \end{array}$$

Example 29 Consider the monoid M generated by

```
[
    [ 1, 4, 8, 6, 2, 3, 5, 7 ],
    [ 1, 7, 1, 6, 6, 7, 1, 1 ]
] .
```

Then $|M| = 106$ and $\mathrm{Aut}(M) \simeq \mathrm{D}_7$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_5$.

The number field Z_5 has a generator with minimal polynomial

$$X^6 - 7X^5 + 21X^4 - 35X^3 + 35X^2 - 21X + 7 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_7)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_5}}(M)| = 14$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 7.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_7) \\ \Big| \scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2 \\ F_5 \simeq \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 30 Consider the monoid M generated by

```
[
    [ 10, 2, 5, 2, 6, 9, 11, 11, 7, 1, 14, 5, 12, 13 ],
    [ 1, 10, 5, 1, 6, 9, 11, 11, 7, 2, 14, 5, 12, 13 ],
    [ 10, 2, 2, 5, 6, 9, 11, 11, 7, 1, 14, 5, 12, 13 ],
    [ 1, 10, 1, 5, 6, 9, 11, 11, 7, 2, 14, 5, 12, 13 ]
] .
```

Then $|M| = 97$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_4 \times \mathrm{S}_3 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_6 \times Z_7 \times Z_8$.

The number field Z_6 has a generator with minimal polynomial

$$X^2 + 36 \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_6}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_6}}(M)| = 576$.

The kernel of the action of φ_6 of $\mathrm{Aut}_{\overline{e_6}}(M)$ on Z_6 has order 288.

We get $\mathrm{Im}\,\varphi_6 \simeq \mathrm{C}_2$.

We have $F_6 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_6 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \scriptstyle \mathrm{Im}\,\varphi_6 \simeq \mathrm{C}_2 \\ F_6 \simeq \mathbb{Q} \end{array}$$

The number field Z_7 is isomorphic to the number field Z_6.

The number field Z_8 has a generator with minimal polynomial

$$X^4 + 1296 \in \mathbb{Q}[X].$$

In particular, $Z_8 \simeq \mathbb{Q}(\zeta_8)$.

We have $\mathrm{Aut}_{\overline{e_8}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_8}}(M)| = 576$.

The kernel of the action of φ_8 of $\mathrm{Aut}_{\overline{e_8}}(M)$ on Z_8 has order 144.

We get $\mathrm{Im}\,\varphi_8 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_8 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_8 \simeq \mathbb{Q}(\zeta_8) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_8 \simeq \mathrm{C}_2 \times \mathrm{C}_2} \\ F_8 \simeq \mathbb{Q} \end{array}$$

Example 31 Consider the monoid M generated by

```
[
    [ 9, 7, 6, 6, 13, 10, 11, 6, 8, 5, 9, 11, 7, 10 ],
    [ 7, 9, 6, 6, 13, 10, 11, 6, 8, 5, 9, 11, 7, 10 ],
    [ 9, 7, 6, 6, 13, 10, 11, 6, 8, 5, 9, 11, 7, 10 ],
    [ 7, 9, 6, 6, 13, 10, 11, 6, 8, 5, 9, 11, 7, 10 ]
] .
```

Then $|M| = 17$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 + 16 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_4}}(M)| = 32$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 16.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2} \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^4 + 16 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_8)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_5}}(M)| = 32$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 8.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_8) \\ \Big| \; {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2 \times \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q} \end{array}$$

Example 32 Consider the monoid M generated by

```
[
    [ 7, 13, 14, 10, 13, 14, 9, 14, 12, 7, 13, 11, 6, 4 ],
    [ 14, 7, 13, 10, 13, 14, 9, 14, 12, 7, 13, 11, 6, 4 ],
    [ 13, 14, 7, 10, 13, 14, 9, 14, 12, 7, 13, 11, 6, 4 ]
] .
```

Then $|M| = 28$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_2 \times \mathrm{C}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3 \times Z_4$.

The number field Z_3 has a generator with minimal polynomial

$$X^2 - 9X + 27 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_3}}(M)| = 36$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 18.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2$.

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \; {\scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2} \\ F_3 \simeq \mathbb{Q} \end{array}$$

The number field Z_4 has a generator with minimal polynomial

$$X^6 - 9X^3 + 27 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_9)$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_4}}(M)| = 36$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_6$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_9) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_6} \\ F_4 \simeq \mathbb{Q} \end{array}$$

Example 33 Consider the monoid M generated by

```
[
    [ 14, 14, 1, 5, 5, 9, 6, 15, 10, 11, 12, 1, 7, 8, 13, 11 ],
    [ 14, 14, 2, 5, 5, 9, 6, 15, 10, 11, 12, 2, 7, 8, 13, 11 ],
    [ 14, 14, 5, 1, 5, 9, 6, 15, 10, 11, 12, 1, 7, 8, 13, 11 ],
    [ 14, 14, 5, 2, 5, 9, 6, 15, 10, 11, 12, 2, 7, 8, 13, 11 ]
] .
```

Then $|M| = 45$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_{10}$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3$.

The number field Z_3 has a generator with minimal polynomial

$$X^{10} - 11X^9 + 55X^8 - 165X^7 + 330X^6 - 462X^5 + 462X^4 - 330X^3 + 165X^2 - 55X + 11 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_{11})$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_3}}(M)| = 40$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 4.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_{10}$.

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_{11}) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_{10}} \\ F_3 \simeq \mathbb{Q} \end{array}$$

Example 34 Consider the monoid M generated by

```
[
    [ 6, 2, 1, 8, 7, 3, 4, 5 ],
    [ 2, 6, 3, 8, 7, 1, 4, 5 ],
    [ 1, 3, 6, 8, 7, 2, 4, 5 ]
] .
```

Then $|M| = 48$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_4 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_9$.

The number field Z_5 has a generator with minimal polynomial

$$X^2 - 48X + 768 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_5}}(M)| = 48$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 2.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_5 .

The number field Z_7 has a generator with minimal polynomial

$$X^2 - 48X + 768 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_4)$.

We have $\mathrm{Aut}_{\overline{e_7}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_7}}(M)| = 48$.

The kernel of the action of φ_7 of $\mathrm{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 24.

We get $\mathrm{Im}\,\varphi_7 \simeq \mathrm{C}_2$.

We have $F_7 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_4) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_7 \simeq \mathrm{C}_2} \\ F_7 \simeq \mathbb{Q} \end{array}$$

The number field Z_8 is isomorphic to the number field Z_7 .

The number field Z_9 has a generator with minimal polynomial

$$X^4 + 192X^2 + 36864 \in \mathbb{Q}[X].$$

In particular, $Z_9 \simeq \mathbb{Q}(\zeta_{12})$.

We have $\mathrm{Aut}_{\overline{e_9}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_9}}(M)| = 48$.

The kernel of the action of φ_9 of $\mathrm{Aut}_{\overline{e_9}}(M)$ on Z_9 has order 12.

We get $\operatorname{Im}\varphi_9 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_9 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_9 \simeq \mathbb{Q}(\zeta_{12}) \\ \Big| \scriptstyle \operatorname{Im}\varphi_9 \simeq \mathrm{C}_2 \times \mathrm{C}_2 \\ F_9 \simeq \mathbb{Q} \end{array}$$

Example 35 Consider the monoid M generated by

```
[
    [ 24, 10, 24, 15, 29, 19, 5, 29, 28, 12, 17, 11, 16, 17, 6, 24, 25, 10, 13,
      21, 7, 11, 19, 12, 5, 19, 4, 20, 4 ],
    [ 24, 24, 10, 15, 29, 19, 5, 29, 28, 12, 17, 11, 16, 17, 6, 24, 25, 10, 13,
      21, 7, 11, 19, 12, 5, 19, 4, 20, 4 ],
    [ 10, 24, 24, 15, 29, 19, 5, 29, 28, 12, 17, 11, 16, 17, 6, 24, 25, 10, 13,
      21, 7, 11, 19, 12, 5, 19, 4, 20, 4 ]
] .
```

Then $|M| = 20$ and $\operatorname{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3$.

The number field Z_3 has a generator with minimal polynomial

$$X^{12} - 13X^{11} + 78X^{10} - 286X^9 + 715X^8 - 1287X^7 + 1716X^6$$

$$-1716X^5 + 1287X^4 - 715X^3 + 286X^2 - 78X + 13 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_{13})$.

We have $\operatorname{Aut}_{\overline{e_3}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_3}}(M)| = 6$.

The kernel of the action of φ_3 of $\operatorname{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\operatorname{Im}\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\zeta_{13})$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_{13}) \\ \Big\| \scriptstyle \operatorname{Im}\varphi_3 = 1 \\ F_3 = Z_3 \simeq \mathbb{Q}(\zeta_{13}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 36 Consider the monoid M generated by

```
[
    [ 8, 6, 11, 10, 6, 11, 9, 4, 5, 8, 7 ],
    [ 11, 8, 6, 10, 6, 11, 9, 4, 5, 8, 7 ],
    [ 6, 11, 8, 10, 6, 11, 9, 4, 5, 8, 7 ]
] .
```

Then $|M| = 46$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_4 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3 \times Z_4 \times Z_5$.

The number field Z_3 has a generator with minimal polynomial

$$X^2 - 15X + 75 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_3}}(M)| = 48$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 24.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2$.

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2} \\ F_3 \simeq \mathbb{Q} \end{array}$$

The number field Z_4 has a generator with minimal polynomial

$$X^4 - 15X^3 + 90X^2 - 270X + 405 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_4}}(M)| = 48$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 12.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_4$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_4} \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^8 - 15X^7 + 105X^6 - 450X^5 + 1305X^4 - 2700X^3 + 4050X^2 - 4050X + 2025 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_{15})$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6. In particular, $|\,\mathrm{Aut}_{\overline{e_5}}(M)| = 48$.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_4 \times \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_{15}) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_4 \times \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q} \end{array}$$

Example 37 Consider the monoid M generated by

```
[
    [ 6, 12, 13, 15, 10, 12, 11, 10, 9, 6, 10, 7, 4, 3, 3 ],
    [ 12, 6, 13, 15, 10, 12, 11, 10, 9, 6, 10, 7, 4, 3, 3 ],
    [ 6, 12, 15, 13, 10, 12, 11, 10, 9, 6, 10, 7, 3, 4, 4 ],
    [ 12, 6, 15, 13, 10, 12, 11, 10, 9, 6, 10, 7, 3, 4, 4 ]
] .
```

Then $|M| = 41$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6 \times Z_7$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 + 100 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_4}}(M)| = 16$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 8.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2} \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^4 - 20X^3 + 160X^2 - 640X + 1280 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_5}}(M)| = 16$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 4.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_4$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \, {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_4} \\ F_5 \simeq \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_5.

The number field Z_7 has a generator with minimal polynomial

$$X^8 + 160X^4 + 1600X^2 + 6400 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_{20})$.

We have $\mathrm{Aut}_{\overline{e_7}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_7}}(M)| = 16$.

The kernel of the action of φ_7 of $\mathrm{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 2.

We get $\mathrm{Im}\,\varphi_7 \simeq \mathrm{C}_4 \times \mathrm{C}_2$.

We have $F_7 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_{20}) \\ \Big| \, {\scriptstyle \mathrm{Im}\,\varphi_7 \simeq \mathrm{C}_4 \times \mathrm{C}_2} \\ F_7 \simeq \mathbb{Q} \end{array}$$

Example 38 Consider the monoid M generated by

```
[
    [ 13, 14, 5, 11, 6, 14, 12, 10, 13, 11, 13, 16, 7, 5, 11, 8 ],
    [ 5, 13, 14, 11, 6, 14, 12, 10, 13, 11, 13, 16, 7, 5, 11, 8 ],
    [ 14, 5, 13, 11, 6, 14, 12, 10, 13, 11, 13, 16, 7, 5, 11, 8 ]
] .
```

Then $|M| = 64$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_6 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3 \times Z_4 \times Z_5$.

The number field Z_3 has a generator with minimal polynomial

$$X^2 - 21X + 147 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_3}}(M)| = 72$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 36.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2$.

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \ \scriptstyle{\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2} \\ F_3 \simeq \mathbb{Q} \end{array}$$

The number field Z_4 has a generator with minimal polynomial

$$X^6 - 21X^5 + 189X^4 - 945X^3 + 2835X^2 - 5103X + 5103 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_7)$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_4}}(M)| = 72$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 12.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_6$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_7) \\ \Big| \ \scriptstyle{\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_6} \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^{12} - 21X^{11} + 210X^{10} - 1323X^9 + 5859X^8 - 19278X^7 + 48573X^6 - 95256X^5$$

$$+146853X^4 - 178605X^3 + 166698X^2 - 107163X + 35721 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_{21})$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_5}}(M)| = 72$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_6 \times \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_{21}) \\ \Big| \ \scriptstyle{\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_6 \times \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q} \end{array}$$

Example 39 Consider the monoid M generated by

```
[
    [ 11, 1, 10, 10, 9, 3, 12, 10, 9, 14, 2, 6, 7, 16, 2, 13, 11 ],
    [ 2, 11, 10, 10, 9, 3, 12, 10, 9, 14, 1, 6, 7, 16, 1, 13, 11 ],
    [ 11, 1, 10, 10, 9, 4, 12, 10, 9, 14, 2, 6, 7, 16, 2, 13, 11 ],
    [ 2, 11, 10, 10, 9, 4, 12, 10, 9, 14, 1, 6, 7, 16, 1, 13, 11 ]
] .
```

Then $|M| = 97$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_9$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 + 144 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_4}}(M)| = 32$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 16.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| {\scriptstyle \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2} \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^2 - 24X + 192 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_5}}(M)| = 32$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 16.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_3) \\ \Big| {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_5 .

The number field Z_7 has a generator with minimal polynomial
$$X^4 + 1296 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_8)$.

We have $\operatorname{Aut}_{\overline{e_7}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_7}}(M)| = 32$.

The kernel of the action of φ_7 of $\operatorname{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 8.

We get $\operatorname{Im}\varphi_7 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_7 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_8) \\ \Big| \; {\scriptstyle \operatorname{Im}\varphi_7 \simeq \mathrm{C}_2 \times \mathrm{C}_2} \\ F_7 \simeq \mathbb{Q} \end{array}$$

The number field Z_8 has a generator with minimal polynomial
$$X^4 + 48X^2 + 2304 \in \mathbb{Q}[X].$$

In particular, $Z_8 \simeq \mathbb{Q}(\zeta_{12})$.

We have $\operatorname{Aut}_{\overline{e_8}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_8}}(M)| = 32$.

The kernel of the action of φ_8 of $\operatorname{Aut}_{\overline{e_8}}(M)$ on Z_8 has order 8.

We get $\operatorname{Im}\varphi_8 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_8 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_8 \simeq \mathbb{Q}(\zeta_{12}) \\ \Big| \; {\scriptstyle \operatorname{Im}\varphi_8 \simeq \mathrm{C}_2 \times \mathrm{C}_2} \\ F_8 \simeq \mathbb{Q} \end{array}$$

The number field Z_9 has a generator with minimal polynomial
$$X^8 - 144X^4 + 20736 \in \mathbb{Q}[X].$$

In particular, $Z_9 \simeq \mathbb{Q}(\zeta_{24})$.

We have $\operatorname{Aut}_{\overline{e_9}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_9}}(M)| = 32$.

The kernel of the action of φ_9 of $\operatorname{Aut}_{\overline{e_9}}(M)$ on Z_9 has order 4.

We get $\operatorname{Im}\varphi_9 \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_9 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_9 \simeq \mathbb{Q}(\zeta_{24}) \\ \Big| \; {\scriptstyle \operatorname{Im}\varphi_9 \simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2} \\ F_9 \simeq \mathbb{Q} \end{array}$$

Example 40 Consider the monoid M generated by

```
[
    [ 22, 11, 20, 16, 7, 10, 18, 14, 9, 12, 17, 8, 18, 5, 22, 22, 9, 10, 14, 4,
      12, 20 ],
    [ 20, 22, 11, 16, 7, 10, 18, 14, 9, 12, 17, 8, 18, 5, 22, 22, 9, 10, 14, 4,
      12, 20 ],
    [ 11, 20, 22, 16, 7, 10, 18, 14, 9, 12, 17, 8, 18, 5, 22, 22, 9, 10, 14, 4,
      12, 20 ]
] .
```

Then $|M| = 91$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6 \times Z_7$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 + 196 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_4}}(M)| = 6$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\mathrm{Im}\,\varphi_4 = 1$.

We have $F_4 = Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_4 = 1} \\ F_4 = Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^6 - 28X^5 + 336X^4 - 2240X^3 + 8960X^2 - 21504X + 28672 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_7)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_5}}(M)| = 6$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\mathrm{Im}\,\varphi_5 = 1$.

We have $F_5 = Z_5 \simeq \mathbb{Q}(\zeta_7)$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_7) \\ \Big\| \,{\scriptstyle \operatorname{Im}\varphi_5 \,=\, 1} \\ F_5 = Z_5 \simeq \mathbb{Q}(\zeta_7) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_5 .

The number field Z_7 has a generator with minimal polynomial

$$X^{12} + 224X^8 - 896X^6 + 12544X^4 + 100352X^2 + 200704 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_{28})$.

We have $\operatorname{Aut}_{\overline{e_7}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_7}}(M)| = 6$.

The kernel of the action of φ_7 of $\operatorname{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 6.

We get $\operatorname{Im}\varphi_7 = 1$.

We have $F_7 = Z_7 \simeq \mathbb{Q}(\zeta_{28})$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_{28}) \\ \Big\| \,{\scriptstyle \operatorname{Im}\varphi_7 = 1} \\ F_7 = Z_7 \simeq \mathbb{Q}(\zeta_{28}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 41 Consider the monoid M generated by

```
[
    [ 18, 10, 26, 19, 42, 12, 5, 9, 24, 39, 4, 10, 33, 36, 29, 41, 40, 39, 24,
    10, 12, 21, 40, 21, 28, 7, 9, 23, 12, 40, 5, 21, 39, 6, 16, 24, 6, 15, 28,
    31, 35, 32 ],
    [ 26, 18, 10, 19, 42, 12, 5, 9, 24, 39, 4, 10, 33, 36, 29, 41, 40, 39, 24,
    10, 12, 21, 40, 21, 28, 7, 9, 23, 12, 40, 5, 21, 39, 6, 16, 24, 6, 15, 28,
    31, 35, 32 ],
    [ 10, 26, 18, 19, 42, 12, 5, 9, 24, 39, 4, 10, 33, 36, 29, 41, 40, 39, 24,
    10, 12, 21, 40, 21, 28, 7, 9, 23, 12, 40, 5, 21, 39, 6, 16, 24, 6, 15, 28,
    31, 35, 32 ]
]
```

Then $|M| = 109$ and $\operatorname{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3 \times Z_4 \times Z_5$.

The number field Z_3 has a generator with minimal polynomial

$$X^2 - 33X + 363 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_3}}(M)| = 6$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\mathrm{Im}\,\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\zeta_3)$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big\| {\scriptstyle \mathrm{Im}\,\varphi_3 = 1} \\ F_3 = Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_4 has a generator with minimal polynomial

$$X^{10} - 33X^9 + 495X^8 - 4455X^7 + 26730X^6 - 112266X^5 + 336798X^4$$
$$-721710X^3 + 1082565X^2 - 1082565X + 649539 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_{11})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\mathrm{Aut}_{\overline{e_4}}(M)| = 6$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\mathrm{Im}\,\varphi_4 = 1$.

We have $F_4 = Z_4 \simeq \mathbb{Q}(\zeta_{11})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_{11}) \\ \Big\| {\scriptstyle \mathrm{Im}\,\varphi_4 = 1} \\ F_4 = Z_4 \simeq \mathbb{Q}(\zeta_{11}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^{20} - 33X^{19} + 528X^{18} - 5445X^{17} + 40590X^{16} - 232551X^{15} + 1062666X^{14}$$
$$-3962277X^{13} + 12235212X^{12} - 31747221X^{11} + 70593930X^{10} - 137429622X^9$$
$$+236576538X^8 - 354864807X^7 + 448542765X^6 - 461244861X^5 + 375505713X^4$$
$$-235782657X^3 + 109555578X^2 - 35724645X + 7144929 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_{33})$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_5}}(M)| = 6$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\mathrm{Im}\,\varphi_5 = 1$.

We have $F_5 = Z_5 \simeq \mathbb{Q}(\zeta_{33})$.

$$Z_5 \simeq \mathbb{Q}(\zeta_{33})$$

$$\Big\| \; \mathrm{Im}\,\varphi_5 = 1$$

$$F_5 = Z_5 \simeq \mathbb{Q}(\zeta_{33})$$

$$\Big|$$

$$\mathbb{Q}$$

Example 42 Consider the monoid M generated by

```
[
    [ 13, 8, 6, 6, 11, 9, 21, 22, 22, 24, 23, 11, 19, 12, 24, 21, 21, 11, 4,
      16, 19, 7, 15, 18, 15 ],
    [ 6, 13, 8, 6, 11, 9, 21, 22, 22, 24, 23, 11, 19, 12, 24, 21, 21, 11, 4,
      16, 19, 7, 15, 18, 15 ],
    [ 8, 6, 13, 6, 11, 9, 21, 22, 22, 24, 23, 11, 19, 12, 24, 21, 21, 11, 4,
      16, 19, 7, 15, 18, 15 ]
] .
```

Then $|M| = 109$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3 \times Z_4 \times Z_5$.

The number field Z_3 has a generator with minimal polynomial

$$X^4 - 35X^3 + 490X^2 - 3430X + 12005 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_3}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_3}}(M)| = 6$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\mathrm{Im}\,\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\zeta_5)$.

$$Z_3 \simeq \mathbb{Q}(\zeta_5)$$

$$\Big\| \; \mathrm{Im}\,\varphi_3 = 1$$

$$F_3 = Z_3 \simeq \mathbb{Q}(\zeta_5)$$

$$\Big|$$

$$\mathbb{Q}$$

The number field Z_4 has a generator with minimal polynomial

$$X^6 - 35X^5 + 525X^4 - 4375X^3 + 21875X^2 - 65625X + 109375 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_7)$.

We have $\operatorname{Aut}_{\overline{e_4}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_4}}(M)| = 6$.

The kernel of the action of φ_4 of $\operatorname{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\operatorname{Im}\varphi_4 = 1$.

We have $F_4 = Z_4 \simeq \mathbb{Q}(\zeta_7)$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_7) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_4 = 1} \\ F_4 = Z_4 \simeq \mathbb{Q}(\zeta_7) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$\begin{gathered} X^{24} - 35X^{23} + 595X^{22} - 6615X^{21} + 54285X^{20} - 349650X^{19} + 1828925X^{18} - 7926975X^{17} \\ +28800975X^{16} - 88175500X^{15} + 227360000X^{14} - 490361375X^{13} + 870840250X^{12} \\ -1236943750X^{11} + 1336199375X^{10} - 1024283750X^{9} + 672280000X^{8} - 1302328125X^{7} \\ +3898409375X^{6} - 8193412500X^{5} + 12297621875X^{4} - 13955812500X^{3} \\ +12267609375X^{2} - 7803250000X + 2663609375 \in \mathbb{Q}[X]. \end{gathered}$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_{35})$.

We have $\operatorname{Aut}_{\overline{e_5}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_5}}(M)| = 6$.

The kernel of the action of φ_5 of $\operatorname{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\operatorname{Im}\varphi_5 = 1$.

We have $F_5 = Z_5 \simeq \mathbb{Q}(\zeta_{35})$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_{35}) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_5 = 1} \\ F_5 = Z_5 \simeq \mathbb{Q}(\zeta_{35}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 43 Consider the monoid M generated by

```
[
   [ 9, 5, 16, 18, 15, 8, 26, 9, 17, 17, 14, 6, 4, 15, 7, 22, 16, 21, 15, 8,
     23, 18, 8, 19, 19, 24, 4 ],
   [ 16, 9, 5, 18, 15, 8, 26, 9, 17, 17, 14, 6, 4, 15, 7, 22, 16, 21, 15, 8,
     23, 18, 8, 19, 19, 24, 4 ],
   [ 5, 16, 9, 18, 15, 8, 26, 9, 17, 17, 14, 6, 4, 15, 7, 22, 16, 21, 15, 8,
     23, 18, 8, 19, 19, 24, 4 ]
] .
```

Then $|M| = 124$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_9$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 + 400 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_4}}(M)| = 6$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\mathrm{Im}\,\varphi_4 = 1$.

We have $F_4 = Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_4 = 1} \\ F_4 = Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^4 - 40X^3 + 640X^2 - 5120X + 20480 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_5}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_5}}(M)| = 6$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\mathrm{Im}\,\varphi_5 = 1$.

We have $F_5 = Z_5 \simeq \mathbb{Q}(\zeta_5)$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_5) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_5 = 1} \\ F_5 = Z_5 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_5.

The number field Z_7 has a generator with minimal polynomial

$$X^4 + 10000 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_8)$.

We have $\operatorname{Aut}_{\overline{e_7}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_7}}(M)| = 6$.

The kernel of the action of φ_7 of $\operatorname{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 6.

We get $\operatorname{Im}\varphi_7 = 1$.

We have $F_7 = Z_7 \simeq \mathbb{Q}(\zeta_8)$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_8) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_7 = 1} \\ F_7 = Z_7 \simeq \mathbb{Q}(\zeta_8) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_8 has a generator with minimal polynomial

$$X^8 + 80X^6 + 2560X^4 + 1638400 \in \mathbb{Q}[X].$$

In particular, $Z_8 \simeq \mathbb{Q}(\zeta_{20})$.

We have $\operatorname{Aut}_{\overline{e_8}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_8}}(M)| = 6$.

The kernel of the action of φ_8 of $\operatorname{Aut}_{\overline{e_8}}(M)$ on Z_8 has order 6.

We get $\operatorname{Im}\varphi_8 = 1$.

We have $F_8 = Z_8 \simeq \mathbb{Q}(\zeta_{20})$.

$$\begin{array}{c} Z_8 \simeq \mathbb{Q}(\zeta_{20}) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_8 = 1} \\ F_8 = Z_8 \simeq \mathbb{Q}(\zeta_{20}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_9 has a generator with minimal polynomial

$$X^{16} + 80X^{12} + 38400X^8 - 2048000X^4 + 40960000 \in \mathbb{Q}[X].$$

In particular, $Z_9 \simeq \mathbb{Q}(\zeta_{40})$.

We have $\mathrm{Aut}_{\overline{e_9}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_9}}(M)| = 6$.

The kernel of the action of φ_9 of $\mathrm{Aut}_{\overline{e_9}}(M)$ on Z_9 has order 6.

We get $\mathrm{Im}\,\varphi_9 = 1$.

We have $F_9 = Z_9 \simeq \mathbb{Q}(\zeta_{40})$.

$$Z_9 \simeq \mathbb{Q}(\zeta_{40})$$
$$\Big\| \ \mathrm{Im}\,\varphi_9 = 1$$
$$F_9 = Z_9 \simeq \mathbb{Q}(\zeta_{40})$$
$$\Big|$$
$$\mathbb{Q}$$

Example 44 Consider the monoid M generated by

```
[
    [ 24, 24, 24, 16, 8, 21, 23, 6, 23, 1, 14, 13, 10, 5, 19, 11, 20, 19, 17,
      16, 9, 11, 17, 13, 20, 11 ],
    [ 24, 24, 24, 16, 8, 21, 23, 6, 23, 2, 14, 13, 10, 5, 19, 11, 20, 19, 17,
      16, 9, 11, 17, 13, 20, 11 ],
    [ 24, 24, 24, 16, 8, 21, 23, 6, 23, 3, 14, 13, 10, 5, 19, 11, 20, 19, 17,
      16, 9, 11, 17, 13, 20, 11 ]
] .
```

Then $|M| = 136$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6 \times Z_7$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 + 484 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\overline{e_4}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_4}}(M)| = 6$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\mathrm{Im}\,\varphi_4 = 1$.

We have $F_4 = Z_4 \simeq \mathbb{Q}(\mathrm{i})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big\| \ {\scriptstyle \operatorname{Im}\varphi_4 = 1} \\ F_4 = Z_4 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^{10} - 44X^9 + 880X^8 - 10560X^7 + 84480X^6 - 473088X^5 + 1892352X^4$$

$$-5406720X^3 + 10813440X^2 - 14417920X + 11534336 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_{11})$.

We have $\operatorname{Aut}_{\overline{e_5}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_5}}(M)| = 6$.

The kernel of the action of φ_5 of $\operatorname{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\operatorname{Im}\varphi_5 = 1$.

We have $F_5 = Z_4 \simeq \mathbb{Q}(\zeta_{11})$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_{11}) \\ \Big\| \ {\scriptstyle \operatorname{Im}\varphi_5 = 1} \\ F_5 = Z_5 \simeq \mathbb{Q}(\zeta_{11}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_5 .

The number field Z_7 has a generator with minimal polynomial

$$X^{20} + 5632X^{12} + 473088X^{10} + 5947392X^8 + 25772032X^6$$

$$+55508992X^4 - 31719424X^2 + 126877696 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_{44})$.

We have $\operatorname{Aut}_{\overline{e_7}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_7}}(M)| = 6$.

The kernel of the action of φ_7 of $\operatorname{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 6.

We get $\operatorname{Im}\varphi_7 = 1$.

We have $F_7 = Z_7 \simeq \mathbb{Q}(\zeta_{44})$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_{44}) \\ \Big\| \ \scriptstyle \operatorname{Im}\varphi_7 = 1 \\ F_7 = Z_7 \simeq \mathbb{Q}(\zeta_{44}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 45 Consider the monoid M generated by

```
[
    [ 13, 12, 11, 12, 8, 5, 17, 15, 13, 19, 13, 7, 20, 5, 16, 14, 4, 13, 19, 11 ],
    [ 11, 13, 12, 12, 8, 5, 17, 15, 13, 19, 13, 7, 20, 5, 16, 14, 4, 13, 19, 11 ],
    [ 12, 11, 13, 12, 8, 5, 17, 15, 13, 19, 13, 7, 20, 5, 16, 14, 4, 13, 19, 11 ]
] .
```

Then $|M| = 181$ and $\operatorname{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6 \times Z_7 \times Z_8 \times Z_9 \times Z_{10} \times Z_{11} \times Z_{12} \times Z_{13}$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 - 60X + 1200 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_3)$.

We have $\operatorname{Aut}_{\overline{e_4}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_4}}(M)| = 96$.

The kernel of the action of φ_4 of $\operatorname{Aut}_{\overline{e_4}}(M)$ on Z_4 has order 48.

We get $\operatorname{Im}\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \ \scriptstyle \operatorname{Im}\varphi_4 \simeq \mathrm{C}_2 \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^2 + 900 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\operatorname{Aut}_{\overline{e_5}}(M) = \operatorname{Aut}(M)$. In particular, $|\operatorname{Aut}_{\overline{e_5}}(M)| = 96$.

The kernel of the action of φ_5 of $\operatorname{Aut}_{\overline{e_5}}(M)$ on Z_5 has order 48.

We get $\operatorname{Im}\varphi_5 \simeq \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \, {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q} \end{array}$$

The number field Z_6 is isomorphic to the number field Z_4.

The number field Z_7 has a generator with minimal polynomial

$$X^4 + 300X^2 + 90000 \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_{12})$.

We have $\mathrm{Aut}_{\overline{e_7}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_7}}(M)| = 96$.

The kernel of the action of φ_7 of $\mathrm{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 24.

We get $\mathrm{Im}\,\varphi_7 \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_7 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_{12}) \\ \Big| \, {\scriptstyle \mathrm{Im}\,\varphi_7 \simeq \mathrm{C}_2 \times \mathrm{C}_2} \\ F_7 \simeq \mathbb{Q} \end{array}$$

The number field Z_8 has a generator with minimal polynomial

$$X^4 - 60X^3 + 1440X^2 - 17280X + 103680 \in \mathbb{Q}[X].$$

In particular, $Z_8 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\overline{e_8}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_8}}(M)| = 96$.

The kernel of the action of φ_8 of $\mathrm{Aut}_{\overline{e_8}}(M)$ on Z_8 has order 24.

We get $\mathrm{Im}\,\varphi_8 \simeq \mathrm{C}_4$.

We have $F_8 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_8 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \, {\scriptstyle \mathrm{Im}\,\varphi_8 \simeq \mathrm{C}_4} \\ F_8 \simeq \mathbb{Q} \end{array}$$

The number field Z_9 is isomorphic to the number field Z_8.

The number field Z_{10} has a generator with minimal polynomial

$$X^8 - 60X^7 + 1680X^6 - 28800X^5 + 334080X^4 - 2764800X^3$$

$$+16588800X^2 - 66355200X + 132710400 \in \mathbb{Q}[X].$$

In particular, $Z_{10} \simeq \mathbb{Q}(\zeta_{15})$.

We have $\mathrm{Aut}_{\overline{e_{10}}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_{10}}}(M)| = 96$.

The kernel of the action of φ_{10} of $\mathrm{Aut}_{\overline{e_{10}}}(M)$ on Z_{10} has order 12.

We get $\mathrm{Im}\,\varphi_{10} \simeq \mathrm{C}_4 \times \mathrm{C}_2$.

We have $F_{10} \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_{10} \simeq \mathbb{Q}(\zeta_{15}) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_{10} \simeq \mathrm{C}_4 \times \mathrm{C}_2} \\ F_{10} \simeq \mathbb{Q} \end{array}$$

The number field Z_{11} has a generator with minimal polynomial

$$X^8 + 180X^6 + 12960X^4 + 41990400 \in \mathbb{Q}[X].$$

In particular, $Z_{11} \simeq \mathbb{Q}(\zeta_{20})$.

We have $\mathrm{Aut}_{\overline{e_{11}}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_{11}}}(M)| = 96$.

The kernel of the action of φ_{11} of $\mathrm{Aut}_{\overline{e_{11}}}(M)$ on Z_{11} has order 12.

We get $\mathrm{Im}\,\varphi_{11} \simeq \mathrm{C}_4 \times \mathrm{C}_2$.

We have $F_{11} \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_{11} \simeq \mathbb{Q}(\zeta_{20}) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_{11} \simeq \mathrm{C}_4 \times \mathrm{C}_2} \\ F_{11} \simeq \mathbb{Q} \end{array}$$

The number field Z_{12} is isomorphic to the number field Z_{10} .

The number field Z_{13} has a generator with minimal polynomial

$$X^{16} - 120X^{14} + 12240X^{12} - 475200X^{10} + 40435200X^8 - 155520000X^6$$

$$-4852224000X^4 + 22394880000X^2 + 268738560000 \in \mathbb{Q}[X].$$

In particular, $Z_{13} \simeq \mathbb{Q}(\zeta_{60})$.

We have $\mathrm{Aut}_{\overline{e_{13}}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_{13}}}(M)| = 96$.

The kernel of the action of φ_{13} of $\mathrm{Aut}_{\overline{e_{13}}}(M)$ on Z_{13} has order 6.

We get $\mathrm{Im}\,\varphi_{13} \simeq \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$.

We have $F_{13} \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_{13} \simeq \mathbb{Q}(\zeta_{60}) \\ \Big| \ {\scriptstyle \mathrm{Im}\,\varphi_{13} \simeq \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2} \\ F_{13} \simeq \mathbb{Q} \end{array}$$

Example 46 Consider the monoid M generated by

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

Then $|M| = 373$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2$.

We get $\mathrm{Z}(\overline{\mathbb{Q}M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_6 \times Z_7$.

The number field Z_6 has a generator with minimal polynomial

$$X^2 - \frac{20}{3}X + \frac{80}{9} \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\sqrt{5})$.

We have $\mathrm{Aut}_{\overline{e_6}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_6}}(M)| = 2$.

The kernel of the action of φ_6 of $\mathrm{Aut}_{\overline{e_6}}(M)$ on Z_6 has order 2.

We get $\mathrm{Im}\,\varphi_6 = 1$.

We have $F_6 = Z_7 \simeq \mathbb{Q}(\sqrt{5})$.

$$\begin{array}{c} Z_6 \simeq \mathbb{Q}(\sqrt{5}) \\ \Big\| \ {\scriptstyle \mathrm{Im}\,\varphi_6 = 1} \\ F_6 = Z_6 \simeq \mathbb{Q}(\sqrt{5}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_7 has a generator with minimal polynomial

$$X^2 + \frac{3}{2}X + \frac{3}{4} \in \mathbb{Q}[X].$$

In particular, $Z_7 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\overline{e_7}}(M) = \mathrm{Aut}(M)$. In particular, $|\,\mathrm{Aut}_{\overline{e_7}}(M)| = 2$.

The kernel of the action of φ_7 of $\mathrm{Aut}_{\overline{e_7}}(M)$ on Z_7 has order 1.

We get $\operatorname{Im}\varphi_7 \simeq \mathrm{C}_2$.

We have $F_7 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_7 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \scriptstyle \operatorname{Im}\varphi_7 \simeq \mathrm{C}_2 \\ F_7 \simeq \mathbb{Q} \end{array}$$

2.2.2 From twisted monoid algebras to field extensions

Let `M` be a submonoid of the symmetric monoid.

2.2.2.1 Finding two-cocycles

With the function `find_alpha` we randomly search for two-cocycles with values in $\{-1, +1\}$ for `M`.

```
find_alpha := function(M,Mseq,attempts)
 // M: submonoid of the symmetric monoid with generators
 // Mseq: monoid as a list of elements, where the identity comes first
 // attempts: number of candidates for two-cocycles alpha to be tested
 d := #Random(M[1]);
 id := [i : i in [1..d]];
 gen_list := M[2];
 found_alpha := false;
 ord := #Mseq;
 ind_gen := [Index(Mseq,gen) : gen in gen_list];
 for l in [1..attempts] do
  A := MatrixRing(Integers(),ord)!0; // defining the two-cocycle
  for i in [1..ord] do
   A[1,i] := 1;
   A[i,1] := 1;
  end for;
  values := [1,-1];
  for i in ind_gen do
   for j in [2..ord] do
    A[i,j] := Random(values);
   end for;
  end for;
  tree := Tree(M); // %%
  tree_cut := [t : t in tree | #t[2] ge 2];
  // employ necessary condition for a 2-cocycle
  for t in tree_cut do
   m := gen_list[t[2][1]];
   y := Compose_list(d,[gen_list[t[2][k]] : k in [2..#t[2]]]);
```

```
   // %% Compose_list is used here
   for j in [1..ord] do
    x := Mseq[j]; // j stands for ix
    im := Index(Mseq,m);
    iy := Index(Mseq,y);
    iyx := Index(Mseq,Compose(y,x)); // %% Compose is used here
    imy := Index(Mseq,t[1]);
    A[imy,j] := A[im,iyx] * A[iy,j] / A[im,iy];
   end for;
  end for;
  // Is it actually a 2-cocycle? : It is sufficient to test elements
  //                               not equal to one.
  is_two_cocycle := true;
  for i in [2..ord] do // give m
   for j in [2..ord] do // give ms
    imms := Index(Mseq,Compose(Mseq[i],Mseq[j])); // %% Compose is used here
    for k in [2..ord] do // give mss
     imsmss := Index(Mseq,Compose(Mseq[j],Mseq[k]));
     // %% Compose is used here
     if not A[imms,k] * A[i,j] eq A[i,imsmss] * A[j,k] then
      is_two_cocycle := false;
      break i;
     end if;
    end for;
   end for;
  end for;
  if is_two_cocycle then
   found_alpha := true;
   return <found_alpha,A>; // true
  end if;
 end for;
 return <found_alpha,A>; // false
end function;
```

For example, with

```
> s := [[1,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> alpha := find_alpha(M,Mseq,10000);
```

we may get

```
<
    true,

    [ 1  1]
    [ 1 -1]
> .
```

For example, with

```
> s := [[4,1,4,1],[4,2,1,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> alpha := find_alpha(M,Mseq,10000);
```

we may get

```
<
    true,

    [ 1  1  1  1  1  1  1  1  1]
    [ 1  1  1  1 -1  1 -1  1  1]
    [ 1  1  1  1 -1  1 -1  1  1]
    [ 1 -1  1  1  1  1  1  1  1]
    [ 1  1  1  1 -1 -1  1 -1 -1]
    [ 1  1  1  1 -1 -1  1 -1 -1]
    [ 1 -1 -1  1  1 -1  1 -1  1]
    [ 1  1  1  1 -1  1 -1  1  1]
    [ 1  1  1  1 -1  1 -1  1  1]
>
```

With the function `find_alpha_2` we search for two-cocycles for a given submonoid `M` of the symmetric monoid in the way introduced in Lemma 25.

```
find_alpha_2 := function(k,p,M,Mseq) // k: modulus, p: basis in calculation of
                                     // powers
 // M: submonoid of the symmetric monoid with generators
 // Mseq: monoid as a list of elements, where the identity comes first

 ord := #Mseq;
 alpha := <false, MatrixRing(Rationals(),ord)!0>; // 0 = dummy
 gen_list := M[2];
 tree := Tree(M); // %%
 tree_cut := [t : t in tree | #t[2] ge 1];
 Cart := CartesianPower(Integers(k),#gen_list);
 for z in Cart do
```

```
  if not z eq <Integers(k)!0 : i in [1..#gen_list]> then
   f := [Integers(k)!0 : m in Mseq];
   f[1] := Integers(k)!0; // no dummy
   for t in tree_cut do
    f[Index(Mseq,t[1])] := &+[z[i] : i in t[2]];
   end for;
   if &and[f[i] + f[j] eq f[Index(Mseq,Compose(Mseq[i],Mseq[j]))]
          : i,j in [1..ord]] then // %% Compose is used here
    alpha[1] := true;
    break z;
   end if;
  end if;
 end for;
 if alpha[1] then
  f_hat := [(Integers()!f[i])/k : i in [1..ord]];
  alpha[2] := MatrixRing(Rationals(),ord)!0;
  for i in [1..ord] do
   for j in [1..ord] do
    alpha[2][i,j] := p^(Integers()!(f_hat[Index(Mseq,Compose(Mseq[i],Mseq[j]))]
                         - f_hat[i] - f_hat[j])); // building two-cocycle
                                                  // %% Compose is used here
   end for;
  end for;
 end if;
 return alpha;
end function;
```

For example with

```
> s := [[2,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> k := 2;
> p := 2;
> alpha := find_alpha_2(k,p,M,Mseq);
```

we get

```
<
    true,

    [  1    1]
    [  1 1/2]
> .
```

For example with

```
> s := [[1,1,3],[3,2,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> k := 4;
> p := 5;
> alpha := find_alpha_2(k,p,M,Mseq);
```

we get

```
<
    true,

    [  1   1   1   1   1   1]
    [  1 1/5   1   1 1/5 1/5]
    [  1   1   1   1   1   1]
    [  1   1   1   1   1   1]
    [  1 1/5   1   1 1/5 1/5]
    [  1 1/5   1   1 1/5 1/5]
> .
```

For example with

```
> s := [[4,1,4,1],[4,2,1,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> k := 2;
> p := 3;
> alpha := find_alpha_2(k,p,M,Mseq);
```

we get

```
<
    true,

    [  1   1   1   1   1   1   1   1   1]
    [  1   1   1   1   1   1   1   1   1]
    [  1   1   1   1   1   1   1   1   1]
    [  1   1   1   1   1   1   1   1   1]
    [  1   1   1   1   1   1   1   1   1]
    [  1   1   1   1   1 1/3 1/3 1/3 1/3]
    [  1   1   1   1   1 1/3 1/3 1/3 1/3]
    [  1   1   1   1   1 1/3 1/3 1/3 1/3]
    [  1   1   1   1   1 1/3 1/3 1/3 1/3]
> .
```

2.2.2.2 Producing field extensions

In the following, we let `Q := Rationals()` be the rational field.

Let `alpha` be a two-cocycle of `M` as can be produced in §2.2.2.1. We compute the representing matrix of the multiplication map of an element `x` on the twisted group algebra `Q_alpha_M` with the function `RegularMatrix_Twist`.

```
RegularMatrix_Twist := function(x,ord,Mseq,alpha) // x: element of Mseq
                                                  // ord: order of Mseq
 // Mseq: monoid as a list of elements, where the identity comes first
 // alpha: two-cocycle
 RM := MatrixRing(Q,ord)!0;
 for i in [1..ord] do
  j := Index(Mseq,Compose(Mseq[i],x)); // %% Compose is used here
  RM[i,j] := alpha[i,Index(Mseq,x)];
 end for;
 return RM;
end function;
```

For example, with

```
> s := [[1,1,3],[3,2,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> k := 4;
> p := 5;
> alpha := find_alpha_2(k,p,M,Mseq);
> RM := RegularMatrix_Twist([3,2,1],#Mseq,Mseq,alpha[2]);
```

we obtain `alpha[2]` to be

```
[  1   1   1   1   1   1]
[  1 1/5   1   1 1/5 1/5]
[  1   1   1   1   1   1]
[  1   1   1   1   1   1]
[  1 1/5   1   1 1/5 1/5]
[  1 1/5   1   1 1/5 1/5]
```

and `RM` to be

```
[  0   1   0   0   0   0]
[1/5   0   0   0   0   0]
[  0   0   0   0   1   0]
[  0   0   0   0   0   1]
[  0   0 1/5   0   0   0]
[  0   0   0 1/5   0   0] .
```

For example, RM[5,3] is 1/5, which means that Compose(Mseq[5],[3,2,1]) equals [1,3,3] which is Mseq[3] and that alpha[2][5][Index(Mseq,[3,2,1])] is equal to 1/5.

For example, with

```
> s := [[4,1,4,1],[4,2,1,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> k := 2;
> p := 3;
> alpha := find_alpha_2(k,p,M,Mseq);
> RM := RegularMatrix_Twist([4,2,1,1],#Mseq,Mseq,alpha[2]);
```

we obtain alpha[2] to be

```
[  1    1    1    1    1    1    1    1    1]
[  1    1    1    1    1    1    1    1    1]
[  1    1    1    1    1    1    1    1    1]
[  1    1    1    1    1    1    1    1    1]
[  1    1    1    1    1    1    1    1    1]
[  1    1    1    1    1  1/3  1/3  1/3  1/3]
[  1    1    1    1    1  1/3  1/3  1/3  1/3]
[  1    1    1    1    1  1/3  1/3  1/3  1/3]
[  1    1    1    1    1  1/3  1/3  1/3  1/3]
```

and RM to be

```
[  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    1]
[  0    0    0    0    0    0    1    0    0]
[  0    0    0    0    0    1    0    0    0]
[  0    0    0    0  1/3    0    0    0    0]
[  0    0    0  1/3    0    0    0    0    0]
[  0  1/3    0    0    0    0    0    0    0]
[  0    0  1/3    0    0    0    0    0    0]
```

For example, RM[6,5] is 1/3, which means that Compose(Mseq[6],[4,2,1,1]) equals [1, 4, 4, 4] which is Mseq[5] and that alpha[2][6][Index(Mseq,[4,2,1,1])] is equal to 1/3.

Suppose given an automorphism a of the submonoid M. The function AutomOp_Twist gives the image ya of an element y of $\mathbb{Q}_\alpha M$ under a, where both y and ya are given as regular matrices with respect to alpha.

```
AutomOp_Twist := function(y,a,Mseq,alpha)
 // y: element of Q_alpha_M given as regular matrix with respect to Mseq
 // a: element of Autom(<SortedSubmon(M[1]),M[2]>)
 // Mseq: monoid as a list of elements, where the identity comes first
 // alpha: two-cocycle
 n := #Mseq;
 coeff := [y[1,i] : i in [1..n]]; // list of coefficients of y with respect
 // to the basis of the monoid ordered as in Mseq
 coeff_a := [coeff[Index(a,i)] : i in [1..n]]; // action of a
 return &+[coeff_a[i] * RegularMatrix_Twist(Mseq[i],n,Mseq,alpha)
           : i in [1..n]]; // %% RegularMatrix_Twist is used here
end function;
```

We consider the example above, where

```
> s := [[1,1,3],[3,2,1]];
> M := <Submon(s),s>;
> Mseq := ProduceMseq(M[1]);
> k := 4;
> p := 5;
> alpha := find_alpha_2(k,p,M,Mseq);
> RM := RegularMatrix_Twist([3,2,1],#Mseq,Mseq,alpha[2]);
```

Then `Autom(<SortedSubmon(M[1]),M[2]>)` yields

```
[
    [ 1, 2, 4, 3, 6, 5 ],
    [ 1, 2, 3, 4, 5, 6 ]
] .
```

We consider `a := [ 1, 2, 4, 3, 6, 5 ]` as automorphism.

Then `AutomOp_Twist(RM,a,Mseq,alpha[2])` yields

```
[  0   1   0   0   0   0]
[1/5   0   0   0   0   0]
[  0   0   0   0   1   0]
[  0   0   0   0   0   1]
[  0   0 1/5   0   0   0]
[  0   0   0 1/5   0   0] .
```

This is exactly `RM` because the automorphism fixes the element `2` which is `Index(Mseq,[3,2,1])`.

The following function `ex_2cocycles_vers` gives us examples of submonoids, where for each submonoid, we calculate its automorphism group and the resulting field extensions in the twisted case; cf. Remark 24.

Depending on the input variable `w` there are different possibilities to generate the two-cocycle `alpha`.

If the input variable `w` is equal to 1, then we randomly search for a two-cocycle `alpha` with the function `find_alpha` as described in §2.2.2.1.

Otherwise, if the input variable `w` is equal to 2 we calculate the two-cocycle `alpha` by fixed input variables `k` and `p` with the function `find_alpha_2` as described in Lemma 25 and §2.2.2.1.

```
ex_2cocycles_vers := function(loops,d,ub,lb,deg,a,k,p,v,w)
 // loops: number of loops
 // d: degree of the symmetric monoid
 // ub: upper bound of the order of the submonoid
 // lb: lower bound of the order of the submonoid
 // deg: minimum degree of field extension is deg
 // a: number of candidates of two-cocycles alpha
 // k: modulus
 // p: basis in calculation of powers
 /*
 v: switch, possibilities to generate a submonoid
 v=1: 2 random generators
 v=2: 2 random generators, one of them bijective
 v=3: 3 random generators
 v=4: 3 generators: m random, m^sigma, m^(sigma^2) with sigma = (1,2,3)
 v=5: 4 generators: m random, m^sigma, m^(sigma^2), m^(sigma^3)
                    with sigma = (1,2,3,4)
 v=6: 4 generators: m random, m^sigma, m^rho, m^(sigma*rho)
                    with sigma = (1,2), rho = (3,4)
 */
 /*
 w: switch, possibilities to look for a two-cocycle alpha
 w=1: find_alpha(M,Mseq,a)
 w=2: find_alpha_2(k,p,M,Mseq)
 */
 Q := Rationals();
 P<X> := PolynomialRing(Q);
 ex_list := [* *];
 id := [i : i in [1..d]];
 for i in [1..loops] do
  if i mod 10 eq 0 then
   print "counter i:= ", i;
  end if;
  if v eq 1 then
   gen1 := random_monoid_element(d);
   gen2 := random_monoid_element(d);
   gen_list := [gen1, gen2];
  elif v eq 2 then
   gen1 := random_monoid_element(d);
```

```
 gen2 := random_monoid_element_bijective(d);
 gen_list := [gen1, gen2];
elif v eq 3 then
 gen1 := random_monoid_element(d);
 gen2 := random_monoid_element(d);
 gen3 := random_monoid_element(d);
 gen_list := [gen1, gen2, gen3];
elif v eq 4 then
 gen1 := random_monoid_element(d);
 sa4 := [2,3,1] cat [4..d];
 sa5 := Inverse(sa4);
 gen4 := Compose_list(d,[sa5,gen1,sa4]);
 gen5 := Compose_list(d,[sa4,gen1,sa5]);
 gen_list := [gen1,gen4,gen5];
elif v eq 5 then
 gen1 := random_monoid_element(d);
 sa5 := [2,3,4,1] cat [5..d]; // sa5 = sa5^-3
 sa6 := Compose(sa5,sa5); // sa5^2 = sa5^-2
 sa7 := Inverse(sa5); // sa5^3 = sa5^-1
 gen5 := Compose_list(d,[sa7,gen1,sa5]);
 gen6 := Compose_list(d,[sa6,gen1,sa6]);
 gen7 := Compose_list(d,[sa5,gen1,sa7]);
 gen_list := [gen1,gen5,gen6, gen7];
elif v eq 6 then
 gen1 := random_monoid_element(d);
 sigma := [2,1] cat [3..d];
 rho := [1,2] cat [4,3] cat [5..d];
 sr := [2,1,4,3] cat [5..d];
 gen2 := Compose_list(d,[sigma,gen1,sigma]);
 gen3 := Compose_list(d,[rho,gen1,rho]);
 gen4 := Compose_list(d,[sr,gen1,sr]);
 gen_list := [gen1, gen2, gen3, gen4];
end if;
M1, bound_ok := Submon_capped(gen_list,ub);
if bound_ok then // check upper bound
 M := <M1, gen_list>;
 print "Info_1: #M[1] = ", #M[1];
 if #M[1] le ub and #M[1] ge lb then
  M_sort_sub := <SortedSubmon(M[1]), gen_list>;
  // %% SortedSubmon is used here
  Mseq := &cat M_sort_sub[1]; // Mseq: monoid as a list of elements,
                              // where the identity comes first
  ord := #Mseq; // order of the submonoid
  if w eq 1 then
   alpha := find_alpha(M,Mseq,a); // %%
  elif w eq 2 then
   alpha := find_alpha_2(k,p,M,Mseq); // %%
```

```
end if;
if alpha[1] then
 alpha := alpha[2];
 Q_alpha_M := MatrixAlgebra<Q, ord | [MatrixRing(Q,ord)!1] cat
   [RegularMatrix_Twist(x,ord,Mseq,alpha) : x in M[2]] >;
   // %% RegularMatrix_Twist is used here,
   // M[2]: list of generators of submonoid M
 J := JacobsonRadical(Q_alpha_M);
 Q_alpha_MmodJ,res := quo<Q_alpha_M | J>;
 ZQ_alpha_MmodJ := Center(Q_alpha_MmodJ);
 e := CentralIdempotents(ZQ_alpha_MmodJ);
 BZQ_alpha_MmodJ := Basis(ZQ_alpha_MmodJ);
 Ktup := [ideal<ZQ_alpha_MmodJ | x > : x in e];
 if not &and[Dimension(K) lt deg : K in Ktup] then // avoiding examples
   // in which only fields of degree < deg appear
  print "Info_2: Tuple of dimensions of fields = ",
        [Dimension(K) : K in Ktup];
  BB := [* Basis(K) : K in Ktup *];
  print "Info_3: BB = ", BB;
  MP := [*[<MinimalPolynomial(b),b,#B> : b in B] : B in BB*];
  MP_of_generators := [[tup : tup in sublist | Degree(tup[1]) eq tup[3]] :
                      sublist in MP];
  if &and[#sublist gt 0 : sublist in MP_of_generators] then
   MP_chosen := [sublist[1] : sublist in MP_of_generators];
   print "Info_4: MP_chosen := ", MP_chosen;
  else
   print "Did not find generators everywhere!";
  end if;
  A := Autom(M_sort_sub); // %%
  print "Info_5: #Autom = ", #A;
  A_alpha := [u : u in A | &and[alpha[i,j] eq alpha[u[i],u[j]]
             : i,j in [1..ord]]]; // automorphisms respecting alpha
  print "Info_6: #Autom_alpha = ", #A_alpha;
  if #A_alpha ge 2 then // avoiding a trivial subgroup
                        // of automorphism group
   A_e := [];
   for i in [1..#e] do
    ee := Q_alpha_MmodJ!e[i];
    A_e cat:= [[a : a in A_alpha | AutomOp_Twist(ee@@res,a,Mseq,alpha)@res
               eq ee]]; // %% AutomOp_Twist is used here
   end for;
   kernels_of_action := [[ a : a in A_e[i] |
     &and[AutomOp_Twist(bb@@res,a,Mseq,alpha)@res eq bb: bb in BB[i]] ] :
                         i in [1..#e]];
   gen_fixed_field := [[&+[AutomOp_Twist(bb@@res,a,Mseq,alpha)@res :
                          a in A_e[i]]/#kernels_of_action[i] :
                        bb in BB[i]] : i in [1..#e]];
```

```
      print "Info_7: Generators of fixed fields = ", gen_fixed_field; // we
      // form the trace of bb with respect to the subgroup given by the image
      // of A_e in the automorphism group of the field
      bases := [Basis(sub<ZQ_alpha_MmodJ | gen>) : gen in gen_fixed_field];
      bases_trans := [[Q_alpha_MmodJ!b : b in B] : B in bases];
      print "Info_8: Action of A_e: ",
            [[[AutomOp_Twist(bb@@res,a,Mseq,alpha)@res :
                bb in BB[i]] : a in A_e[i]] : i in [1..#e]];
      ex_list cat:= [* <A,<Mseq,M[2]>,MP_chosen,A_e,kernels_of_action,
                                  bases,bases_trans,alpha> *];
      print "Result, i:= ", i, "<M[2],MP_chosen,A_e,kernels_of_action,
        bases,bases_trans> =", <M[2],MP_chosen,A_e,kernels_of_action,bases,
        bases_trans,alpha>;
      // resulting Galois group: A_e[i]/kernels_of_action[i]
     end if;
    end if;
   end if;
  end if;
 end if;
 end for;
 return ex_list;
end function;
```

2.2.2.3 An example to illustrate the algorithm

We shall illustrate the function `ex_2cocycles_vers` with an example.

Suppose that `ex_2cocycles_vers`, using `v=4`, has randomly chosen the following list of generators in degree 4, internally called `M[2]`.

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

This list of generators generate the monoid M of order 10, internally called `M[1]`.

The following list, internally called `Mseq` contains the elements of the monoid M.

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

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

We use the notation introduced in Remark 24.

The algorithm returns a tuple consisting of

- the automorphism group $\mathrm{Aut}(M)$ of the monoid M, called `A`,
- a tuple consisting of a list of elements of M and a list of chosen generators, called `<Mseq,M[2]>`,
- a list of minimal polynomials of generators of the fields Z_i, together with the respective generators, called `MP_chosen`,
- the list of subgroups $\mathrm{Aut}_{\alpha,\overline{e_i}}(M)$, called `A_e`,
- the list of kernels of the group morphisms $\varphi_i :\ \mathrm{Aut}_{\alpha,\overline{e_i}}(M) \longrightarrow \mathrm{Aut}(Z_i)$, called `kernels_of_action`,
- a list of bases for the fixed fields F_i, expressed in terms of a standard basis of $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$, called `bases`,
- a list of bases for the fixed fields F_i, expressed in terms of a standard basis of $\overline{\mathbb{Q}_\alpha M}$, called `bases_trans`
- the two-cocycle α, called `alpha`.

In our example, the mentioned tuple has the following entries.

The automorphism group `A` of the monoid `M` has order 12:

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

The automorphisms are given as maps from M to M with respect to the ordering in the list `Mseq`.

`MP_chosen` contains three tuples. Each tuple consists of a minimal polynomial, a corresponding generator and the degree of the minimal polynomial. One of them has degree 3.

```
[
    <X - 1, ( 1 -1  0  0), 1>,
    <X^3 - 1/2, (0 0 1 0), 3>
]
```

The corresponding field extension is isomorphic to $\mathbb{Q}(\sqrt[3]{2})$.

The list of subgroups `A_e` of the automorphism group `A` contains the following subgroup of order 6 twice.

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

Then, `kernels_of_action` contains the kernels of the actions of the entries of `A_e` on the occurring number fields.

For instance, we get `kernels_of_action[2]` as follows.

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

Additionally, we obtain the `bases` of the fixed fields:

```
[
    [ ( 1 -1  0  0) ],
    [ (0 1 0 0), (0 0 1 0), (0 0 0 1) ]
].
```

We find that $\overline{\mathbb{Q}_\alpha M}$ is commutative, so in this case, we get `bases_trans` = `bases`.

Finally, the two-cocycle `alpha` is returned, too. In this case, `alpha` is obtained using `k=3`, `p=2` and `w=2`.

```
[  1   1   1   1   1   1   1   1   1   1]
[  1   1   1   1   1   1   1   1   1   1]
[  1   1   1   1   1   1   1   1   1   1]
[  1   1   1   1   1   1   1   1   1   1]
[  1   1   1   1   1   1 1/2 1/2 1/2   1]
[  1   1   1   1   1   1 1/2 1/2 1/2   1]
[  1   1   1   1 1/2 1/2 1/2 1/2 1/2 1/2]
[  1   1   1   1 1/2 1/2 1/2 1/2 1/2 1/2]
[  1   1   1   1 1/2 1/2 1/2 1/2 1/2 1/2]
[  1   1   1   1   1   1 1/2 1/2 1/2   1]
```

The matrix entries are the values of `alpha` at pairs of monoid elements with respect to the ordering in the list `Mseq`.

To consider a single specific example such as the one just found, we should be able to generate these data without a random search, but with a manual input. To do this, we use

```
> res_2 := doc_2([[ 2, 3, 1, 3 ],[ 2, 3, 1, 1 ],
                  [ 2, 3, 1, 2 ]],1,3,2,2);
```

Using `doc_2` instead of `ex_2cocycles_vers`, we obtain `A` as `res_2[1][2][1]`, `Mseq` as `res_2[1][1][1][1]`, `M[2]` as `res_2[1][1][1][2]`, `MP_chosen` as `res_2[1][4]`, `A_e[i]` as `res_2[i][5][1]`, `kernels_of_action[i]` as `res_2[i][6][1]` for $i \in [1, s]$, where s is given by `#res_2`, `bases` as `res_2[1][11]`, `bases_trans` as `res_2[1][12]` and `alpha` as `res_2[1][3][1]`.

The function `doc_2` also returns `A` as a group, which is given by `res_2[1][7]`, the subgroup `A_e[i]` as a group, which is given by `res_2[i][9]` for $i \in [1, s]$, the subgroup $\mathrm{Aut}_\alpha(M)$ of the automorphism group $\mathrm{Aut}(M)$, called `A_alpha`, which is given as a list by `res_2[1][3][2]` and as a group by `res_2[1][8]`, and the image $\mathrm{Im}\,\varphi_i$ of the group morphisms φ_i as a group, which is given by `res_2[i][10]` for $i \in [1, s]$.

2.2.2.4 Resulting examples obtained using the first method to generate two-cocycles

The following examples have been calculated using `ex_2_cocycles_vers` and the switch `w=1`; cf. §2.2.2.2

We use the notation introduced in Remark 24 to describe the results.

Example 47 Consider the monoid M generated by

```
[
    [ 8, 11, 11, 9, 8, 12, 8, 12, 10, 5, 12, 9 ],
    [ 11, 8, 11, 9, 8, 12, 8, 12, 10, 5, 12, 9 ],
    [ 11, 11, 8, 9, 8, 12, 8, 12, 10, 5, 12, 9 ]
] .
```

Then $|M| = 9$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

We obtain the monoid `M` and the two-cocycle `alpha`, as follows.

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

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 6:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3$.

The number field Z_3 has a generator with minimal polynomial

$$X^4 - 5X^3 + 10X^2 - 10X + 5 \in \mathbb{Q}[X].$$

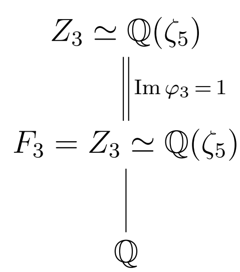
In particular, $Z_3 \simeq \mathbb{Q}(\zeta_5)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 6$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\mathrm{Im}\,\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\zeta_5)$.



Example 48 Consider the monoid M generated by

```
[
    [ 4, 6, 6, 9, 8, 9, 7, 6, 5 ],
    [ 6, 4, 6, 9, 8, 9, 7, 6, 5 ],
    [ 6, 6, 4, 9, 8, 9, 7, 6, 5 ]
] .
```

Then $|M| = 8$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

We obtain the monoid `M` and the two-cocycle `alpha`, as follows.

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

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 2:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2$.

The number field Z_2 has a generator with minimal polynomial

$$X^4 + 1 \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\zeta_8)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 2$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 2.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\zeta_8)$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\zeta_8) \\ \Big\| \;\mathrm{Im}\,\varphi_2 = 1 \\ F_2 = Z_2 \simeq \mathbb{Q}(\zeta_8) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 49 Consider the monoid M generated by

```
[
    [ 3, 1, 2, 5, 6, 5 ]
] .
```

Then $|M| = 7$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2$.

We obtain the monoid `M` and the two-cocycle `alpha`, as follows.

```
[ 1, 2, 3, 4, 5, 6 ]        [ 1  1  1  1  1  1  1]
[ 1, 2, 3, 6, 5, 6 ]        [ 1  1  1  1  1  1  1]
[ 1, 2, 3, 5, 6, 5 ]        [ 1  1 -1 -1 -1  1  1]
[ 3, 1, 2, 6, 5, 6 ]        [ 1  1 -1  1  1 -1  1]
[ 2, 3, 1, 6, 5, 6 ]        [ 1  1 -1  1  1  1 -1]
[ 2, 3, 1, 5, 6, 5 ]        [ 1  1  1 -1  1 -1 -1]
[ 3, 1, 2, 5, 6, 5 ]        [ 1  1  1  1 -1 -1 -1]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M)$ = `A_alpha` of order 2:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3$.

The number field Z_2 has a generator with minimal polynomial

$$X^2 + 9 \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 2$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 2.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\mathrm{i})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\mathrm{i}) \\ \big\| \; {\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\mathrm{i}) \\ \big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 has a generator with minimal polynomial

$$X^4 + 3X^2 + 9 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_{12})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 2$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 1.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2$.

We have $F_3 \simeq \mathbb{Q}(\mathrm{i})$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_{12}) \\ \big| \; {\scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2} \\ F_3 \simeq \mathbb{Q}(\mathrm{i}) \\ \big| \\ \mathbb{Q} \end{array}$$

2.2.2.5 Resulting examples obtained using the second method to generate two-cocycles

The following examples have been calculated using `ex_2_cocycles_vers` and the switch `w=2`; cf. §2.2.2.2.

We use the notation introduced in Remark 24 to describe the results.

Example 50 Consider the monoid M generated by

```
[
    [ 1, 3, 2, 5, 6, 4 ],
    [ 3, 2, 1, 5, 6, 4 ],
    [ 2, 1, 3, 5, 6, 4 ]
] .
```

Then $|M| = 18$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_2$.

Using `k=3` and `p=-1` we obtain the monoid `M` and the two-cocycle `alpha` as follows.

```
[ 1, 2, 3, 4, 5, 6 ]    [ 1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1]
[ 1, 3, 2, 4, 5, 6 ]    [ 1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1]
[ 2, 1, 3, 4, 5, 6 ]    [ 1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1]
[ 3, 2, 1, 4, 5, 6 ]    [ 1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1]
[ 3, 1, 2, 5, 6, 4 ]    [ 1  1  1  1  1  1  1 -1  1  1 -1 -1 -1 -1  1  1  1 -1]
[ 2, 3, 1, 4, 5, 6 ]    [ 1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1]
[ 1, 2, 3, 5, 6, 4 ]    [ 1  1  1  1  1  1  1 -1  1  1 -1 -1 -1 -1  1  1  1 -1]
[ 2, 3, 1, 6, 4, 5 ]    [ 1  1  1  1 -1  1 -1 -1  1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 3, 1, 2, 4, 5, 6 ]    [ 1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1  1]
[ 2, 3, 1, 5, 6, 4 ]    [ 1  1  1  1  1  1  1 -1  1  1 -1 -1 -1 -1  1  1  1 -1]
[ 1, 2, 3, 6, 4, 5 ]    [ 1  1  1  1 -1  1 -1 -1  1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 3, 1, 2, 6, 4, 5 ]    [ 1  1  1  1 -1  1 -1 -1  1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 1, 3, 2, 6, 4, 5 ]    [ 1  1  1  1 -1  1 -1 -1  1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 2, 1, 3, 6, 4, 5 ]    [ 1  1  1  1 -1  1 -1 -1  1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
[ 3, 2, 1, 5, 6, 4 ]    [ 1  1  1  1  1  1  1 -1  1  1 -1 -1 -1 -1  1  1  1 -1]
[ 1, 3, 2, 5, 6, 4 ]    [ 1  1  1  1  1  1  1 -1  1  1 -1 -1 -1 -1  1  1  1 -1]
[ 2, 1, 3, 5, 6, 4 ]    [ 1  1  1  1  1  1  1 -1  1  1 -1 -1 -1 -1  1  1  1 -1]
[ 3, 2, 1, 6, 4, 5 ]    [ 1  1  1  1 -1  1 -1 -1  1 -1 -1 -1 -1 -1 -1 -1 -1 -1]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 6:

```
[
    [ 1, 4, 3, 2, 10, 9, 7, 12, 6, 5, 11, 8, 18, 14, 16, 15, 17, 13 ],
    [ 1, 4, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 18, 13, 17, 15, 16, 14 ],
    [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 ],
    [ 1, 2, 4, 3, 10, 9, 7, 12, 6, 5, 11, 8, 13, 18, 17, 16, 15, 14 ],
    [ 1, 3, 2, 4, 10, 9, 7, 12, 6, 5, 11, 8, 14, 13, 15, 17, 16, 18 ],
    [ 1, 3, 4, 2, 5, 6, 7, 8, 9, 10, 11, 12, 14, 18, 16, 17, 15, 13 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 - 18X + 108 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_4}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_4}}(M)| = 6$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 6.

We get $\mathrm{Im}\,\varphi_4 = 1$.

We have $F_4 = Z_4 \simeq \mathbb{Q}(\zeta_3)$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_3) \\ \Big\| \, \scriptstyle \operatorname{Im}\varphi_4 = 1 \\ F_4 = Z_4 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_5 and Z_6 are isomorphic to the number field Z_4.

Example 51 Consider the monoid M generated by

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

Then $|M| = 12$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

Using `k=3` and `p=-1` we obtain the monoid `M` and the two-cocycle `alpha` as follows.

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

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 2:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3 \times Z_4 \times Z_5 \times Z_6$.

The number field Z_3 has a generator with minimal polynomial

$$X^2 - 12X + 48 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 2$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 2.

We get $\operatorname{Im}\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\zeta_3)$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_3 = 1} \\ F_3 = Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_4 is isomorphic to the number field Z_3 .

The number field Z_5 has a generator with minimal polynomial

$$X^2 + 36 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\mathrm{i})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_5}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_5}}(M)| = 2$.

The kernel of the action of φ_5 of $\operatorname{Aut}_{\alpha,\overline{e_5}}(M)$ on Z_5 has order 2.

We get $\operatorname{Im}\varphi_5 = 1$.

We have $F_5 = Z_5 \simeq \mathbb{Q}(\mathrm{i})$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big\| \, {\scriptstyle \operatorname{Im}\varphi_5 = 1} \\ F_5 = Z_5 \simeq \mathbb{Q}(\mathrm{i}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_6 has a generator with minimal polynomial

$$X^4 + 12X^2 + 144 \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\zeta_{12})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_6}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_6}}(M)| = 2$.

The kernel of the action of φ_6 of $\operatorname{Aut}_{\alpha,\overline{e_6}}(M)$ on Z_6 has order 1.

We get $\operatorname{Im}\varphi_6 \simeq \mathrm{C}_2$.

We have $F_6 \simeq \mathbb{Q}(\zeta_3)$.

$$\begin{array}{c} Z_6 \simeq \mathbb{Q}(\zeta_{12}) \\ \Big| \, {\scriptstyle \operatorname{Im}\varphi_6 \simeq \mathrm{C}_2} \\ F_6 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 52 Consider, as in §2.2.2.3, the monoid M generated by

```
[
    [ 2, 3, 1, 3 ],
    [ 2, 3, 1, 1 ],
    [ 2, 3, 1, 2 ]
] .
```

Then $|M| = 10$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as follows.

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

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 6:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2$.

The number field Z_2 has a generator with minimal polynomial

$$X^3 - \frac{1}{2} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 6$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 6.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 53 Consider the monoid M generated by

```
[
    [ 4, 2, 8, 1, 6, 5, 3, 7 ],
    [ 6, 3, 7, 5, 4, 1, 2, 8 ]
] .
```

Then $|M| = 48$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{S}_4$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as follows.

```
[ 1, 2, 3, 4, 5, 6, 7, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 2, 3, 5, 4, 1, 7, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 3, 2, 6, 1, 4, 8, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 8, 7, 1, 6, 5, 3, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 7, 8, 1, 6, 5, 2, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 3, 2, 1, 6, 5, 8, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 2, 3, 1, 6, 5, 7, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 3, 2, 5, 4, 1, 8, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 7, 8, 5, 4, 1, 2, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 8, 7, 4, 5, 6, 3, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 7, 8, 6, 1, 4, 2, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 8, 7, 6, 1, 4, 3, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 7, 8, 4, 5, 6, 2, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 8, 7, 5, 4, 1, 3, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 2, 3, 6, 1, 4, 7, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 3, 2, 4, 5, 6, 8, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 3, 7, 4, 5, 6, 2, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 1, 2, 7, 4, 5, 6, 8, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 2, 8, 4, 5, 6, 3, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 1, 8, 2, 4, 5, 6, 7, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 1, 7, 2, 4, 5, 6, 3, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 7, 3, 4, 5, 6, 8, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 1, 3, 8, 4, 5, 6, 7, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 8, 3, 4, 5, 6, 2, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 8, 3, 1, 6, 5, 2, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 6, 7, 3, 5, 4, 1, 8, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 6, 2, 8, 5, 4, 1, 3, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 4, 7, 3, 1, 6, 5, 8, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 5, 3, 8, 6, 1, 4, 7, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 2, 8, 1, 6, 5, 3, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 5, 3, 7, 6, 1, 4, 2, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 4, 8, 2, 1, 6, 5, 7, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 6, 3, 8, 5, 4, 1, 7, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 2, 7, 6, 1, 4, 8, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 6, 8, 3, 5, 4, 1, 2, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 8, 2, 6, 1, 4, 7, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 5, 8, 3, 6, 1, 4, 2, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 7, 2, 1, 6, 5, 3, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 6, 8, 2, 5, 4, 1, 7, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 5, 2, 8, 6, 1, 4, 3, 7 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 5, 7, 3, 6, 1, 4, 8, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 4, 2, 7, 1, 6, 5, 8, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 6, 3, 7, 5, 4, 1, 2, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 6, 7, 2, 5, 4, 1, 3, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 7, 2, 6, 1, 4, 3, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 6, 2, 7, 5, 4, 1, 8, 3 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 3, 7, 1, 6, 5, 2, 8 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a a 1 1 1 a 1 1 1 a a a 1 a a 1 1 1 a 1 a a a 1 a]
[ 4, 3, 8, 1, 6, 5, 7, 2 ]     [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 72 generated by the following elements.

```
[
    [ 1, 7, 11, 8, 14, 9, 2, 5, 4, 16, 12, 3, 10, 6, 15, 13, 19, 24, 22, 20, 18, 17, 23, 21, 44, 47, 28, 43, 29, 26, 40, 39, 48, 37, 38, 36, 45,
     46, 32, 41, 31, 35, 30, 42, 34, 25, 27, 33 ],
    [ 1, 15, 4, 9, 8, 14, 2, 12, 3, 13, 6, 5, 16, 11, 7, 10, 17, 24, 22, 19, 21, 20, 18, 23, 33, 36, 41, 39, 42, 26, 47, 27, 34, 25, 29, 30, 48,
     44, 40, 28, 32, 35, 31, 45, 38, 37, 43, 46 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_5 \times Z_6 \times Z_7 \times Z_8$.

The number field Z_5 has a generator with minimal polynomial

$$X^3 - 2048 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_5}}(M) = \mathrm{Aut}_{\alpha}(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_5}}(M)| = 72$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\alpha,\overline{e_5}}(M)$ on Z_5 has order 72.

We get $\mathrm{Im}\,\varphi_5 = 1$.

We have $F_5 = Z_5 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \ {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq 1} \\ F_5 = Z_5 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_6 has a generator with minimal polynomial

$$X^3 - 2048 \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_6}}(M) \simeq \mathrm{C}_2 \times \mathrm{A}_4$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_6}}(M)| = 24$.

The kernel of the action of φ_6 of $\mathrm{Aut}_{\alpha,\overline{e_6}}(M)$ on Z_6 has order 24.

We get $\mathrm{Im}\,\varphi_6 = 1$.

We have $F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \ {\scriptstyle \mathrm{Im}\,\varphi_6 = 1} \\ F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_7 and Z_8 are isomorphic to the number field Z_6 .

Example 54 Consider the monoid M generated by

```
[
    [ 1, 2, 6, 6, 7, 7, 4, 4 ],
    [ 7, 2, 8, 6, 3, 4, 1, 5 ]
] .
```

Then $|M| = 97$ and $\mathrm{Aut}(M) \simeq \mathrm{D}_4 \times \mathrm{S}_3 \times \mathrm{C}_2$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as can be found in the file `two_cocycles.txt` under number 1.

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 48 generated by the following elements.

```
[
    [ 1, 2, 4, 3, 6, 5, 10, 9, 8, 7, 12, 11, 19, 21, 18, 27, 20, 15, 13, 17, 14, 29, 25, 28, 23, 30, 16, 24, 22, 26, 74, 46, 55, 51, 67, 41, 73, 72,
      69, 59, 36, 44, 61, 42, 56, 32, 53, 68, 77, 64, 34, 76, 47, 62, 33, 45, 58, 57, 40, 71, 43, 54, 75, 50, 66, 65, 35, 48, 39, 78, 60, 38, 37, 31,
      63, 52, 49, 70 ],
    [ 1, 2, 4, 3, 6, 5, 8, 7, 10, 9, 11, 12, 13, 29, 20, 30, 18, 17, 19, 15, 22, 21, 23, 24, 25, 27, 26, 28, 14, 16, 48, 73, 78, 75, 59, 38, 46, 36,
      47, 67, 72, 76, 64, 52, 58, 37, 39, 31, 54, 61, 63, 44, 69, 49, 70, 57, 56, 45, 35, 65, 50, 77, 51, 43, 60, 71, 40, 74, 53, 55, 66, 41, 32, 68,
      34, 42, 62, 33 ],
    [ 1, 2, 3, 4, 5, 6, 11, 9, 12, 7, 8, 10, 21, 19, 18, 28, 20, 23, 29, 25, 14, 13, 17, 27, 15, 24, 16, 30, 22, 26, 54, 45, 35, 70, 61, 66, 57, 31,
      34, 64, 68, 43, 67, 53, 65, 49, 42, 36, 48, 59, 69, 50, 63, 37, 75, 46, 71, 73, 78, 58, 44, 74, 33, 76, 41, 56, 55, 77, 52, 40, 38, 60, 62, 72,
      47, 39, 32, 51 ],
    [ 1, 2, 4, 3, 6, 5, 10, 9, 8, 7, 12, 11, 19, 21, 18, 27, 20, 15, 13, 17, 14, 29, 25, 28, 23, 30, 16, 24, 22, 26, 54, 41, 35, 64, 33, 46, 38, 37,
      76, 70, 32, 47, 75, 53, 65, 36, 42, 49, 48, 51, 50, 69, 44, 31, 67, 66, 71, 60, 78, 58, 63, 74, 61, 34, 45, 56, 55, 77, 52, 40, 57, 73, 72, 62,
      43, 39, 68, 59 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \times Z_4 \times Z_5 \times Z_6$.

The number field Z_4 has a generator with minimal polynomial

$$X^2 - 6X + 12 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_4}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_4}}(M)| = 48$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 24.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \ \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2 \\ F_4 \simeq \mathbb{Q} \end{array}$$

The number field Z_5 is isomorphic to the number field Z_4 .

The number field Z_6 has a generator with minimal polynomial

$$X^3 - 16 \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_6}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_6}}(M)| = 48$.

The kernel of the action of φ_6 of $\mathrm{Aut}_{\alpha,\overline{e_6}}(M)$ on Z_6 has order 48.

We get $\mathrm{Im}\,\varphi_6 = 1$.

We have $F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$
\begin{array}{c}
Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}) \\
\Big\| \ {\scriptstyle \operatorname{Im}\varphi_6 \simeq 1} \\
F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}) \\
\Big| \\
\mathbb{Q}
\end{array}
$$

Example 55 Consider the monoid M generated by

```
[
    [ 2, 8, 2, 2, 8, 5, 8, 6 ],
    [ 7, 3, 4, 1, 5, 6, 2, 8 ]
] .
```

Then $|M| = 113$ and $\operatorname{Aut}(M) \simeq \mathrm{D}_5 \times \mathrm{C}_2$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as can be found in the file `two_cocycles.txt` under number 2.

Consequently we get the subgroup $\operatorname{Aut}_\alpha(M) =$ `A_alpha` of order 10 generated by the following elements.

```
[
    [ 1, 4, 5, 2, 3, 24, 7, 18, 15, 20, 27, 22, 29, 14, 9, 31, 26, 8, 25, 10, 28, 12, 23, 6, 19, 17, 11, 21, 13, 30, 16, 45, 67, 55, 72, 37, 36,
      58, 69, 59, 48, 46, 60, 83, 32, 42, 64, 41, 49, 54, 74, 57, 66, 50, 34, 56, 52, 38, 40, 43, 82, 77, 80, 47, 76, 53, 33, 68, 39, 70, 71, 35,
      79, 51, 75, 65, 62, 78, 73, 63, 81, 61, 44, 92, 88, 91, 89, 85, 87, 93, 86, 84, 90, 113, 102, 107, 105, 99, 98, 108, 104, 95, 106, 101, 97,
       103, 96, 100, 112, 111, 110, 109, 94 ],
    [ 1, 4, 5, 2, 3, 25, 17, 22, 18, 16, 26, 24, 21, 29, 19, 10, 7, 9, 15, 30, 13, 8, 23, 12, 6, 11, 27, 28, 14, 20, 31, 69, 64, 35, 34, 40, 70,
      71, 39, 36, 41, 53, 77, 44, 56, 60, 81, 79, 73, 66, 72, 63, 42, 62, 82, 45, 68, 83, 59, 46, 76, 54, 52, 33, 74, 50, 67, 57, 32, 37, 38, 51,
      49, 65, 75, 61, 43, 78, 48, 80, 47, 55, 58, 90, 86, 85, 91, 92, 93, 84, 87, 88, 89, 104, 100, 113, 102, 108, 112, 95, 110, 97, 111, 94, 109,
       107, 106, 98, 105, 101, 103, 99, 96 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3 \times Z_4$.

The number field Z_2 has a generator with minimal polynomial

$$X^3 + \frac{27}{4} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_2}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_2}}(M)| = 10$.

The kernel of the action of φ_2 of $\operatorname{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 10.

We get $\operatorname{Im}\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \ {\scriptstyle \operatorname{Im}\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 is isomorphic to the number field Z_2 .

The number field Z_4 has a generator with minimal polynomial

$$X^4 - 5X^3 + 10X^2 - 10X + 5 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_5)$.

We have $\operatorname{Aut}_{\alpha,\overline{e_4}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_4}}(M)| = 10$.

The kernel of the action of φ_4 of $\operatorname{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 5.

We get $\operatorname{Im}\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_5) \\ \Big| \ {\scriptstyle \operatorname{Im}\varphi_4 \simeq \mathrm{C}_2} \\ F_4 \simeq \mathbb{Q}(\zeta_5 + \zeta_5^{-1}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 56 Consider the monoid M generated by

```
[
        [ 2, 8, 5, 7, 7, 7, 4, 1 ],
        [ 8, 1, 5, 7, 7, 7, 4, 2 ],
        [ 2, 8, 7, 5, 7, 7, 3, 1 ],
        [ 8, 1, 7, 5, 7, 7, 3, 2 ]
] .
```

Then $|M| = 199$ and $\operatorname{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as can be found in the file `two_cocycles.txt` under number 3.

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 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, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38,
    39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74,
    75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107,
    108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136,
    137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165,
    166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194,
    195, 196, 197, 198, 199 ],
  [ 1, 12, 3, 15, 5, 16, 19, 8, 17, 14, 18, 2, 20, 10, 4, 6, 9, 11, 7, 13, 33, 22, 27, 31, 32, 29, 23, 30, 26, 28, 24, 25, 21, 83, 66, 45, 77, 73,
    74, 61, 41, 42, 43, 52, 36, 68, 63, 50, 65, 48, 51, 44, 56, 55, 54, 53, 81, 60, 67, 58, 40, 76, 47, 69, 49, 35, 59, 46, 64, 72, 71, 70, 38, 39,
    79, 62, 37, 82, 75, 80, 57, 78, 34, 108, 96, 87, 86, 100, 97, 93, 107, 92, 90, 106, 104, 85, 89, 98, 102, 88, 103, 99, 101, 95, 109, 94, 91,
    84, 105, 125, 113, 126, 111, 123, 117, 120, 115, 131, 122, 116, 134, 119, 114, 130, 110, 112, 133, 135, 132, 124, 118, 129, 127, 121, 128, 137,
    136, 150, 140, 139, 149, 181, 178, 154, 157, 177, 170, 179, 141, 138, 159, 175, 163, 144, 162, 160, 145, 182, 151, 156, 172, 155, 153, 166, 174,
    164, 176, 183, 185, 147, 184, 161, 186, 165, 152, 167, 146, 143, 148, 188, 142, 158, 168, 171, 169, 173, 189, 180, 187, 191, 190, 193, 192, 195,
    194, 198, 199, 196, 197 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3 \times Z_4 \times Z_5 \times Z_6$.

The number field Z_2 has a generator with minimal polynomial

$$X^3 - \frac{1}{4} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 2$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 2.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_3, Z_4 and Z_5 are isomorphic to the number field Z_2 .

The number field Z_6 has a generator with minimal polynomial

$$X^6 - \frac{15}{8}X^3 + \frac{29791}{6912} \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_6}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_6}}(M)| = 2$.

The kernel of the action of φ_6 of $\mathrm{Aut}_{\alpha,\overline{e_6}}(M)$ on Z_6 has order 2.

We get $\mathrm{Im}\,\varphi_6 = 1$.

We have $F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

$$Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

$$\Big\| \ \mathrm{Im}\,\varphi_6 = 1$$

$$F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

$$\Big|$$

$$\mathbb{Q}$$

Example 57 Consider the monoid M generated by

```
[
    [ 4, 4, 5, 5, 2, 4, 4, 5 ],
    [ 3, 4, 6, 5, 2, 7, 1, 8 ]
] .
```

Then $|M| = 48$ and $\mathrm{Aut}(M) \simeq D_4 \times \mathrm{S}_3$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as follows.

```
[ 1, 2, 3, 4, 5, 6, 7, 8 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 2, 7, 4, 5, 1, 3, 8 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 4, 3, 5, 2, 6, 7, 8 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 1, 5, 3, 2, 4, 6, 7, 8 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 7, 2, 1, 4, 5, 3, 6, 8 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 3, 2, 6, 4, 5, 7, 1, 8 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 5, 7, 2, 4, 1, 3, 8 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 6, 4, 7, 5, 2, 1, 3, 8 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 3, 5, 6, 2, 4, 7, 1, 8 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 7, 4, 1, 5, 2, 3, 6, 8 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 7, 5, 1, 2, 4, 3, 6, 8 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 3, 4, 6, 5, 2, 7, 1, 8 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 2, 2, 2, 4, 5, 2, 4, 4 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 2, 2, 4, 5, 5, 5, 2 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 2, 4, 4, 5, 5, 4, 5 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 2, 4, 5, 4, 2, 4 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 2, 5, 4, 5, 4, 4, 5 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 2, 5, 4, 5, 5, 2, 2 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 2, 2, 4, 5, 2, 2, 4 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 4, 4, 5, 2, 2, 4 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 2, 4, 4, 5, 4, 4, 5 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 5, 4, 5, 5, 5, 2 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 2, 4, 4, 5, 4, 5, 5 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 2, 5, 4, 5, 2, 5, 2 ]      [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 4, 5, 2, 2, 4, 2, 2, 4 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 5, 2, 2, 4, 5, 5, 2 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 5, 5, 2, 4, 2, 5, 2 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 4, 5, 5, 2, 2, 5, 2 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 4, 5, 4, 2, 4, 4, 5, 5 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 4, 2, 5, 2, 4, 2, 4 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 5, 5, 5, 2, 4, 5, 2, 2 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 5, 4, 2, 5, 2, 5, 5, 2 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 2, 4, 2, 5, 2, 2, 4, 4 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 5, 4, 4, 5, 2, 4, 4, 5 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 2, 4, 5, 5, 2, 5, 5, 2 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 5, 4, 5, 5, 2, 5, 2, 2 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 4, 4, 2, 5, 2, 2, 2, 4 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 2, 5, 2, 2, 4, 2, 4, 4 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 5, 2, 2, 4, 4, 2, 4 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 4, 4, 5, 2, 2, 2, 4 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 2, 5, 4, 2, 4, 2, 2, 4 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 5, 4, 2, 4, 5, 4, 5 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 4, 4, 5, 2, 5, 4, 5 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 5, 5, 4, 2, 4, 4, 4, 5 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 4, 5, 5, 2, 4, 4, 5 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 4, 4, 4, 5, 2, 4, 5, 5 ]      [1 1 1 a 1 1 a 1 a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a 1 a 1 a 1 1 1 1 1 1 a a 1 a a 1 a 1 1 a a]
[ 2, 5, 5, 2, 4, 5, 5, 2 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 4, 5, 5, 2, 4, 4, 4, 5 ]      [1 1 a a 1 1 a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
```

Consequently we get the cyclic subgroup $\mathrm{Aut}_\alpha(M)$ = `A_alpha` of order 24 generated by the following element.

```
[
    [ 1, 2, 3, 4, 6, 5, 7, 8, 11, 12, 9, 10, 21, 16, 14, 17, 24, 19, 23, 15, 18, 13, 22, 20, 29, 39, 41, 40, 47, 45, 25, 30, 34, 36, 33, 37, 46, 44,
      48, 43, 42, 26, 32, 31, 28, 35, 38, 27 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq Z_1 \times Z_2 \times Z_3 \times Z_4$.

The number field Z_1 has a generator with minimal polynomial

$$X^3 - \frac{1}{4} \in \mathbb{Q}[X].$$

In particular, $Z_1 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_1}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_1}}(M)| = 24$.

The kernel of the action of φ_1 of $\mathrm{Aut}_{\alpha,\overline{e_1}}(M)$ on Z_1 has order 24.

We get $\mathrm{Im}\,\varphi_1 = 1$.

We have $F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_1 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_1 = 1} \\ F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_2 and Z_3 are isomorphic to the number field Z_1 .

The number field Z_4 has a generator with minimal polynomial

$$X^6 + 4 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\sqrt[3]{2}, \mathrm{i})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_4}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_4}}(M)| = 24$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 12.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\sqrt[3]{2}, \mathrm{i}) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_2} \\ F_4 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 58 Consider the monoid M generated by

```
[
    [ 1, 2, 2, 1, 1, 8, 2, 8 ],
    [ 8, 1, 7, 3, 6, 4, 5, 2 ]
] .
```

Then $|M| = 60$ and $\mathrm{Aut}(M) \simeq (\mathrm{C}_5 \rtimes \mathrm{C}_4) \times \mathrm{S}_3$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as follows.

```
[ 1, 2, 3, 4, 5, 6, 7, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 8, 3, 4, 5, 6, 7, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 3, 4, 5, 6, 7, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 1, 2, 7, 3, 6, 4, 5, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 4, 6, 7, 5, 3, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 5, 7, 4, 3, 6, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 6, 5, 3, 7, 4, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 8, 1, 7, 3, 6, 4, 5, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 4, 6, 7, 5, 3, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 4, 6, 7, 5, 3, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 5, 7, 4, 3, 6, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 7, 3, 6, 4, 5, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 5, 7, 4, 3, 6, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 6, 5, 3, 7, 4, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 6, 5, 3, 7, 4, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 2, 2, 1, 8, 2, 8, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 8, 1, 2, 2, 1, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 1, 1, 2, 8, 8, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 8, 2, 1, 8, 1, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 1, 2, 8, 8, 2, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 1, 2, 1, 2, 8, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 2, 2, 8, 1, 1, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 2, 8, 1, 1, 8, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 1, 8, 2, 1, 2, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 8, 2, 2, 1, 8, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 8, 1, 8, 1, 2, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 2, 8, 2, 8, 1, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 8, 8, 1, 2, 2, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 2, 1, 1, 8, 2, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 1, 8, 8, 2, 1, 8 ]    [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 8, 8, 2, 1, 8, 1, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 2, 8, 2, 8, 1, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 2, 1, 8, 2, 8, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 1, 2, 8, 8, 2, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 1, 8, 8, 2, 1, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 2, 8, 2, 8, 1, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 8, 1, 8, 1, 2, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 8, 1, 2, 2, 1, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 2, 1, 1, 8, 2, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 2, 8, 1, 1, 8, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 2, 2, 8, 1, 1, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 8, 8, 1, 2, 2, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 1, 1, 2, 8, 8, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 2, 1, 1, 8, 2, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 1, 2, 8, 8, 2, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 8, 2, 1, 8, 1, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 1, 8, 8, 2, 1, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 8, 2, 2, 1, 8, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 8, 1, 1, 2, 1, 2, 8, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 2, 8, 1, 1, 8, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 8, 1, 2, 2, 1, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 1, 8, 2, 1, 2, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 2, 2, 8, 1, 1, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 8, 8, 1, 2, 2, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 1, 2, 1, 2, 8, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 2, 1, 8, 2, 8, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 8, 2, 2, 1, 8, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 2, 8, 1, 1, 2, 8, 8, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
[ 8, 1, 8, 1, 8, 1, 2, 2 ]    [ 1 a 1 1 1 1 1 1 a 1 1 a a 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a 1 1 a 1 a a 1 a 1 1 1 1 1 1 1 a 1 1 a a 1 a a a a a a 1 a]
[ 2, 8, 1, 8, 2, 1, 2, 1 ]    [ 1 a a 1 1 1 1 a a a a a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M)$ = `A_alpha` of order 60 generated by the following elements.

```
[
    [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 23, 27, 29, 17, 26, 28, 25, 21, 20, 19, 22, 18, 30, 16, 24, 51, 43, 40, 37, 52, 58, 53,
      32, 56, 49, 48, 35, 44, 33, 59, 38, 60, 46, 42, 55, 36, 45, 57, 47, 54, 50, 31, 39, 41, 34 ],
    [ 1, 2, 3, 6, 7, 5, 4, 11, 15, 14, 10, 13, 9, 8, 12, 26, 25, 22, 21, 30, 20, 28, 29, 27, 19, 17, 23, 18, 16, 24, 55, 40, 59, 47, 52, 50, 51,
      48, 56, 44, 42, 43, 41, 33, 35, 49, 60, 46, 45, 39, 57, 32, 54, 58, 34, 37, 31, 53, 38, 36 ],
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq Z_1 \times Z_2 \times Z_3$.

The number field Z_1 has a generator with minimal polynomial

$$X^3 - \frac{1}{4} \in \mathbb{Q}[X].$$

In particular, $Z_1 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_1}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_1}}(M)| = 60$.

The kernel of the action of φ_1 of $\mathrm{Aut}_{\alpha,\overline{e_1}}(M)$ on Z_1 has order 60.

We get $\mathrm{Im}\,\varphi_1 = 1$.

We have $F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_1 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_1 = 1} \\ F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_2 is isomorphic to the number field Z_1 .

The number field Z_3 has a generator with minimal polynomial

$$X^{12} - \frac{5}{4}X^9 + \frac{25}{16}X^6 + \frac{125}{64}X^3 + \frac{125}{256} \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_5)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 60$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 15.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_4$.

We have $F_3 = \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_5) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_4} \\ F_3 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 59 Consider the monoid M generated by

```
[
    [ 6, 7, 9, 10, 7, 11, 12, 16, 8, 6, 9, 5, 11, 9, 11, 4 ],
    [ 9, 6, 7, 10, 7, 11, 12, 16, 8, 6, 9, 5, 11, 9, 11, 4 ],
    [ 7, 9, 6, 10, 7, 11, 12, 16, 8, 6, 9, 5, 11, 9, 11, 4 ]
]
```

Then $|M| = 64$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_6 \times \mathrm{C}_2$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as can be found in the file `two_cocycles.txt` under number 4.

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 36 generated by the following elements.

```
[
    [ 1, 3, 2, 4, 8, 7, 6, 5, 9, 10, 18, 11, 12, 20, 28, 25, 23, 15, 21, 26, 27,
    16, 19, 17, 22, 14, 24, 13, 39, 33, 40, 56, 44, 63, 31, 51, 57, 36, 62, 48,
    64, 58, 61, 59, 60, 53, 52, 47, 34, 45, 38, 35, 42, 37, 49, 46, 54, 32, 41,
    50, 55, 29, 43, 30 ],
    [ 1, 4, 2, 3, 9, 10, 6, 5, 8, 7, 14, 17, 20, 28, 26, 23, 22, 19, 25, 18, 15,
    21, 11, 13, 24, 12, 16, 27, 58, 45, 54, 39, 48, 51, 41, 49, 40, 63, 53, 30,
    60, 62, 36, 50, 59, 29, 44, 57, 42, 64, 61, 37, 55, 47, 38, 43, 35, 34, 52,
    33, 46, 56, 32, 31 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq Z_1 \times Z_2 \times Z_3 \times Z_4 \times Z_5$. i The number field Z_2 has a generator with minimal polynomial

$$X^3 - \frac{343}{2} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 36$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 36.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \; {\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 has a generator with minimal polynomial

$$X^{18} + \frac{35}{2}X^{12} + \frac{833}{16}X^6 + \frac{343}{64} \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_7)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 36$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_6$.

We have $F_3 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\sqrt[3]{2}, \zeta_7) \\ \big|\ \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_6 \\ F_3 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \big| \\ \mathbb{Q} \end{array}$$

Example 60 Consider the monoid M generated by

```
[
    [ 5, 1, 2, 6, 7, 8, 3, 4 ],
    [ 3, 5, 2, 6, 7, 8, 1, 4 ],
    [ 3, 1, 5, 6, 7, 8, 2, 4 ]
] .
```

Then $|M| = 180$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_5 \times \mathrm{C}_2$.

Using `k=3` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as can be found in the file `two_cocycles.txt` under number 5.

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 120 generated by the following elements.

```
[
    [ 1, 5, 3, 7, 2, 9, 4, 10, 6, 8, 11, 13, 12, 15, 14, 16, 75, 35, 49, 30, 23, 28, 21, 76, 74, 45, 38, 22, 43, 20, 52, 62, 66, 53, 18, 73, 50, 27,
     59, 63, 42, 41, 29, 78, 26, 71, 72, 51, 19, 37, 48, 31, 34, 57, 60, 64, 54, 69, 39, 55, 70, 32, 40, 56, 67, 33, 65, 68, 58, 61, 46, 47, 36, 25,
     17, 24, 77, 44, 100, 90, 96, 102, 92, 87, 94, 101, 84, 99, 95, 80, 98, 83, 97, 85, 89, 81, 93, 91, 88, 79, 86, 82, 124, 119, 118, 111, 115, 116,
     122, 110, 106, 130, 121, 114, 107, 108, 123, 105, 104, 126, 113, 109, 117, 103, 125, 120, 128, 127, 129, 112, 131, 132, 139, 145, 147, 148, 158,
     154, 133, 159, 172, 168, 176, 169, 134, 170, 135, 136, 178, 177, 163, 160, 161, 138, 156, 155, 173, 137, 140, 152, 153, 165, 151, 167, 162, 179,
     164, 142, 144, 146, 175, 141, 157, 180, 171, 143, 150, 149, 166, 174 ],
    [ 1, 11, 4, 2, 15, 7, 8, 13, 16, 3, 14, 9, 5, 10, 6, 12, 74, 18, 49, 70, 45, 63, 73, 39, 54, 32, 43, 35, 52, 37, 31, 62, 66, 34, 30, 75, 53, 76,
     48, 20, 27, 38, 19, 47, 44, 24, 25, 29, 71, 33, 42, 46, 69, 21, 22, 51, 57, 61, 59, 50, 60, 72, 40, 56, 67, 58, 23, 68, 28, 55, 41, 36, 17, 65,
     26, 64, 77, 78, 85, 97, 91, 80, 88, 81, 96, 90, 83, 86, 101, 92, 102, 87, 99, 93, 79, 89, 94, 100, 82, 84, 95, 98, 114, 113, 104, 116, 128,
     131, 117, 127, 122, 125, 107, 111, 110, 126, 124, 115, 129, 103, 112, 132, 108, 106, 121, 109, 119, 130, 118, 105, 123, 120, 135, 179, 158, 133,
     136, 143, 168, 176, 170, 139, 142, 164, 144, 134, 165, 153, 152, 146, 155, 140, 147, 162, 163, 166, 151, 159, 137, 138, 149, 148, 167, 171, 154,
     172, 180, 160, 145, 156, 173, 175, 169, 150, 141, 178, 174, 161, 177, 157 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq Z_1 \times Z_2 \times Z_3 \times Z_4$.

The number field Z_1 has a generator with minimal polynomial

$$X^3 - 108000 \in \mathbb{Q}[X].$$

In particular, $Z_1 \simeq \mathbb{Q}(\sqrt[3]{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_1}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_1}}(M)| = 120$.

The kernel of the action of φ_1 of $\mathrm{Aut}_{\alpha,\overline{e_1}}(M)$ on Z_1 has order 120.

We get $\operatorname{Im}\varphi_1 = 1$.

We have $F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_1 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big\| \;{\scriptstyle \operatorname{Im}\varphi_1 = 1} \\ F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_2 and Z_3 are isomorphic to the number field Z_1 .

The number field Z_4 has a generator with minimal polynomial

$$X^6 - \frac{1600}{27}X^3 + \frac{128000}{729} \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_4}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_4}}(M)| = 120$.

The kernel of the action of φ_4 of $\operatorname{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 60.

We get $\operatorname{Im}\varphi_4 \simeq \mathrm{C}_2$.

We have $F_4 = \mathbb{Q}(\sqrt[3]{2})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) \\ \Big| \;{\scriptstyle \operatorname{Im}\varphi_4 \simeq \mathrm{C}_2} \\ F_4 \simeq \mathbb{Q}(\sqrt[3]{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 61 Consider the monoid M generated by

```
[
    [ 4, 6, 6, 5, 2, 5 ],
    [ 6, 4, 6, 5, 3, 5 ],
    [ 6, 6, 4, 5, 1, 5 ]
] .
```

Then $|M| = 22$ and $\operatorname{Aut}(M) \simeq \mathrm{C}_3$.

Using `k=3` and `p=3` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/3` as follows.

```
[ 1, 2, 3, 4, 5, 6 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 3, 3, 3, 4, 5, 4 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 2, 4, 5, 4 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 2, 6, 5, 6 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 1, 1, 6, 5, 6 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 3, 3, 3, 6, 5, 6 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 1, 1, 4, 5, 4 ]        [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 6, 6, 6, 5, 1, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 4, 4, 4, 5, 2, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 4, 4, 4, 5, 3, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 4, 4, 4, 5, 1, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 5, 5, 5, 2, 6, 2 ]        [1 1 1 1 1 1 1 a a a a a a a a a a a a a a a]
[ 6, 6, 6, 5, 3, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 5, 5, 5, 3, 6, 3 ]        [1 1 1 1 1 1 1 a a a a a a a a a a a a a a a]
[ 5, 5, 5, 2, 4, 2 ]        [1 1 1 1 1 1 1 a a a a a a a a a a a a a a a]
[ 6, 6, 6, 5, 2, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 5, 5, 5, 1, 4, 1 ]        [1 1 1 1 1 1 1 a a a a a a a a a a a a a a a]
[ 5, 5, 5, 1, 6, 1 ]        [1 1 1 1 1 1 1 a a a a a a a a a a a a a a a]
[ 5, 5, 5, 3, 4, 3 ]        [1 1 1 1 1 1 1 a a a a a a a a a a a a a a a]
[ 6, 4, 6, 5, 3, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 4, 6, 6, 5, 2, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
[ 6, 6, 4, 5, 1, 5 ]        [1 1 1 1 1 1 1 1 1 1 1 a 1 a a 1 a a a 1 1 1]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 3:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2$.

The number field Z_2 has a generator with minimal polynomial

$$X^3 - \frac{1}{3} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{3})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 3$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 3.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{3})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{3}) \\ \Big\| {\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{3}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 62 Consider the monoid M generated by

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

Then $|M| = 199$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

Using `k=3` and `p=3` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/3` as can be found in the file `two_cocycles.txt` under number 6.

Consequently we get the cyclic subgroup $\mathrm{Aut}_\alpha(M)$ = `A_alpha` of order 2 generated by the following element.

```
[ 1, 17, 5, 14, 3, 18, 12, 9, 8, 10, 11, 7, 19, 4, 15, 20, 2, 6, 13, 16, 23, 30, 21, 27, 32, 29, 24, 31, 26, 22, 28, 25, 33, 66, 69, 54, 47, 75, 71,
 56, 43, 42, 41, 58, 68, 53, 37, 76, 74, 73, 81, 52, 46, 36, 65, 40, 62, 44, 79, 60, 77, 57, 83, 67, 55, 34, 64, 45, 35, 70, 39, 72, 50, 49, 38, 48,
 61, 78, 59, 82, 51, 80, 63, 107, 94, 97, 102, 95, 103, 108, 91, 106, 98, 85, 88, 109, 86, 93, 101, 104, 99, 87, 89, 100, 105, 92, 84, 90, 96, 111,
 110, 124, 123, 131, 116, 115, 125, 127, 121, 133, 119, 128, 113, 112, 117, 132, 118, 122, 130, 129, 114, 126, 120, 135, 134, 137, 136, 169, 186, 181,
 143, 151, 141, 184, 166, 161, 158, 159, 155, 168, 142, 179, 175, 182, 149, 180, 170, 147, 148, 177, 146, 165, 178, 189, 162, 145, 171, 150, 138, 157,
 167, 173, 172, 176, 153, 174, 160, 163, 152, 156, 140, 154, 188, 144, 187, 139, 185, 183, 164, 191, 190, 193, 192, 195, 194, 199, 198, 197, 196 ]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3 \times Z_4 \times Z_5$.

The number field Z_2 has a generator with minimal polynomial

$$X^3 - \frac{8}{81} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{3})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 2$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 2.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{3})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{3}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{3}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_3, Z_4 and Z_5 are isomorphic to the number field Z_2 .

The number field Z_6 has a generator with minimal polynomial

$$X^6 + 90X^3 + \frac{29791}{3} \in \mathbb{Q}[X].$$

In particular, $Z_6 \simeq \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_6}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_6}}(M)| = 2$.

The kernel of the action of φ_6 of $\mathrm{Aut}_{\alpha,\overline{e_6}}(M)$ on Z_6 has order 2.

We get $\mathrm{Im}\,\varphi_6 = 1$.

We have $F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{3}, \zeta_3)$.

$$\begin{array}{c} Z_6 \simeq \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \\ \Big\| \ \mathrm{Im}\,\varphi_6 = 1 \\ F_6 = Z_6 \simeq \mathbb{Q}(\sqrt[3]{3}, \zeta_3) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 63 Consider the monoid M generated by

```
[
    [ 3, 3, 6, 6, 4, 2 ],
    [ 5, 2, 4, 3, 1, 6 ]
] .
```

Then $|M| = 12$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_2 \times \mathrm{C}_2$.

Using `k=3` and `p=5` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/5` as follows.

```
[ 1, 2, 3, 4, 5, 6 ]        [  1 1 1 1 1 1 1 1 1 1 1 1]
[ 5, 2, 4, 3, 1, 6 ]        [  1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 4, 4, 2, 6 ]        [  1 1 1 1 1 1 1 1 1 1 1 1]
[ 2, 2, 3, 3, 2, 6 ]        [  1 1 1 1 1 1 1 1 1 1 1 1]
[ 3, 3, 6, 6, 3, 2 ]        [  1 1 1 1 1 a 1 a 1 1 1 1]
[ 6, 6, 2, 2, 6, 3 ]        [  1 1 1 1 a a a a a a a a]
[ 4, 4, 6, 6, 4, 2 ]        [  1 1 1 1 1 a 1 a 1 1 1 1]
[ 6, 6, 2, 2, 6, 4 ]        [  1 1 1 1 a a a a a a a a]
[ 3, 4, 6, 6, 4, 2 ]        [  1 1 1 1 1 a 1 a 1 1 1 1]
[ 4, 3, 6, 6, 3, 2 ]        [  1 1 1 1 1 a 1 a 1 1 1 1]
[ 3, 3, 6, 6, 4, 2 ]        [  1 1 1 1 1 a 1 a 1 1 1 1]
[ 4, 4, 6, 6, 3, 2 ]        [  1 1 1 1 1 a 1 a 1 1 1 1]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 4:

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

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times \mathbb{Q} \times Z_3$.

The number field Z_5 has a generator with minimal polynomial

$$X^3 - \frac{1}{5} \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\sqrt[3]{5})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 4$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_3 has order 4.

We get $\mathrm{Im}\,\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\sqrt[3]{5})$.

```
    Z₃ ≃ ℚ(∛5)
         ‖  Im φ₃ = 1
F₃ = Z₃ ≃ ℚ(∛5)
         |
         ℚ
```

Example 64 Consider the monoid M generated by

```
[
    [ 1, 4, 3, 5, 2, 2 ],
    [ 1, 2, 4, 5, 3, 6 ]
] .
```

Then $|M| = 39$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_3 \rtimes \mathrm{S}_3$.

Using `k=3` and `p=6` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/6` as follows.

```
[ 1, 2, 3, 4, 5, 6 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 4, 5, 3, 6 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 2, 5, 3, 4, 6 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 2, 3, 4, 5, 3 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 3, 4, 5, 5 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 2, 3, 4, 5, 4 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 3, 2, 5, 4, 2 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 3, 2, 5, 4, 5 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 3, 2, 5, 4, 4 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 4, 5, 2, 3, 5 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 4, 5, 2, 3, 3 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 4, 5, 2, 3, 2 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 5, 4, 3, 2, 3 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 5, 4, 3, 2, 2 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 5, 4, 3, 2, 4 ]   [ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[ 1, 4, 2, 3, 5, 2 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 4, 2, 3, 5, 5 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 3, 5, 4, 2, 2 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 3, 5, 4, 2, 5 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 3, 5, 4, 2, 4 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 3, 4, 2, 5, 2 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 3, 4, 2, 5, 5 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 3, 4, 2, 5, 4 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 5, 2, 4, 3, 4 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 5, 2, 4, 3, 3 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 5, 2, 4, 3, 2 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 4, 3, 5, 2, 5 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 2, 4, 5, 3, 5 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 2, 4, 5, 3, 4 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 2, 5, 3, 4, 3 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 4, 3, 5, 2, 3 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 4, 3, 5, 2, 2 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 2, 4, 5, 3, 3 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 2, 5, 3, 4, 5 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 2, 5, 3, 4, 4 ]   [ 1 a 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a 1 1 1 1 1 1 1 a a 1 1 1 a 1 1 a a a a]
[ 1, 5, 3, 2, 4, 4 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 5, 3, 2, 4, 3 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 5, 3, 2, 4, 2 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
[ 1, 4, 2, 3, 5, 3 ]   [ 1 a a 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a a a a a a a a a]
```

Consequently we get the subgroup $\mathrm{Aut}_{\alpha}(M) =$ `A_alpha` of order 9 generated by the following elements.

```
[
    [ 1, 2, 3, 5, 6, 4, 14, 15, 13, 9, 8, 7, 10, 12, 11, 18, 20, 38, 36, 37, 26, 24, 25, 31, 27, 32, 23, 29, 33, 34, 22, 21, 28, 35, 30, 39, 17,
      16, 19 ],
    [ 1, 2, 3, 4, 5, 6, 15, 13, 14, 7, 9, 8, 12, 11, 10, 19, 18, 36, 37, 38, 24, 25, 26, 27, 32, 31, 21, 28, 29, 30, 23, 22, 33, 34, 35, 17, 16,
      39, 20 ],
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3$.

The number field Z_2 has a generator with minimal polynomial

$$X^3 - \frac{16}{9} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[3]{6})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 9$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 9.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{6})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[3]{6}) \\ \Big\| \; {\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[3]{6}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 is isomorphic to the number field Z_2 .

Example 65 Consider the monoid M generated by

```
[
    [ 2, 6, 7, 3, 7, 2, 4, 6 ],
    [ 8, 1, 4, 7, 5, 2, 3, 6 ]
] .
```

Then $|M| = 84$ and $\mathrm{Aut}(M) \simeq D_4 \times \mathrm{S}_3$.

Using `k=3` and `p=5` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/5` as can be found in the file `two_cocycles.txt` under number 7.

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 24 generated by the following elements.

```
[
    [ 1, 2, 3, 4, 6, 5, 7, 8, 10, 9, 12, 11, 13, 20, 15, 21, 23, 18, 19, 14, 16, 22, 17, 24, 25, 26, 30, 28, 35, 27, 31, 36, 33, 34, 29, 32, 56,
      51, 45, 40, 43, 42, 41, 44, 39, 46, 52, 48, 49, 50,38, 47, 53, 54, 60, 37, 57, 58, 59, 55, 61, 71, 80, 65, 64, 66, 67, 68, 76, 70, 62, 72,
      73, 74, 75, 69, 81, 82, 79, 63, 77, 78, 83, 84 ],
    [ 1, 2, 3, 4, 6, 5, 7, 8, 10, 9, 12, 11, 17, 15, 16, 19, 18, 20, 23, 24, 13, 14, 22, 21, 29, 32, 28, 35, 34, 25, 30, 33, 27, 36, 26, 31, 49,
      50, 44, 52, 53, 43, 46, 55, 57, 39, 58, 37, 51, 47, 40, 48, 45, 41, 42, 59, 60, 56, 38, 54, 63, 83, 75, 68, 61, 78, 81, 80, 84, 82, 67, 62,
      65, 71, 76, 73, 70, 74, 69, 79, 66, 72, 77, 64 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq Z_1 \times Z_2 \times Z_3 \times Z_4 \times Z_5$.

The number field Z_1 has a generator with minimal polynomial

$$X^3 - \frac{8}{5} \in \mathbb{Q}[X].$$

In particular, $Z_1 \simeq \mathbb{Q}(\sqrt[3]{5})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_1}}(M) = \mathrm{Aut}_{\alpha}(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_1}}(M)| = 24$.

The kernel of the action of φ_1 of $\mathrm{Aut}_{\alpha,\overline{e_1}}(M)$ on Z_1 has order 24.

We get $\mathrm{Im}\,\varphi_1 = 1$.

We have $F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{5})$.

$$\begin{array}{c} Z_1 \simeq \mathbb{Q}(\sqrt[3]{5}) \\ \Big\| \; {\scriptstyle \mathrm{Im}\,\varphi_1 = 1} \\ F_1 = Z_1 \simeq \mathbb{Q}(\sqrt[3]{5}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number fields Z_2, Z_3 and Z_4 are isomorphic to the number field Z_1 .

The number field Z_5 has a generator with minimal polynomial

$$X^6 + \frac{64}{625} \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\sqrt[3]{5}, \mathrm{i})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_5}}(M) = \mathrm{Aut}_{\alpha}(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_5}}(M)| = 24$.

The kernel of the action of φ_5 of $\mathrm{Aut}_{\alpha,\overline{e_5}}(M)$ on Z_5 has order 12.

We get $\mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}(\sqrt[3]{5})$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\sqrt[3]{5}, \mathrm{i}) \\ \Big| \; {\scriptstyle \mathrm{Im}\,\varphi_5 \simeq \mathrm{C}_2} \\ F_5 \simeq \mathbb{Q}(\sqrt[3]{5}) \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 66 Consider the monoid M generated by

```
[
    [ 9, 9, 6, 14, 11, 16, 9, 9, 15, 6, 6, 5, 14, 8, 4, 5 ],
    [ 6, 9, 9, 14, 11, 16, 9, 9, 15, 6, 6, 5, 14, 8, 4, 5 ],
    [ 9, 6, 9, 14, 11, 16, 9, 9, 15, 6, 6, 5, 14, 8, 4, 5 ]
]
```

Then $|M| = 61$ and $\mathrm{Aut}(M) \simeq \mathrm{S}_3 \times \mathrm{C}_4 \times \mathrm{C}_2$.

Using `k=2` and `p=2` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/2` as can be found in the file `two_cocycles.txt` under number 8.

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 48 generated by the following elements.

```
[
    [ 1, 3, 2, 4, 5, 7, 6, 10, 11, 8, 9, 13, 12, 19, 22, 16, 25, 18, 14, 20, 21, 15, 24, 23, 17, 36, 27, 34, 29, 35, 37, 32, 33, 28, 30, 26, 31, 51,
      53, 46, 55, 56, 48, 54, 60, 40, 57, 43, 58, 52, 38, 50, 39, 44, 41, 42, 47, 49, 61, 45, 59 ],
    [ 1, 4, 2, 3, 7, 5, 6, 11, 10, 8, 13, 9, 12, 19, 20, 25, 16, 14, 18, 22, 23, 15, 24, 21, 17, 27, 36, 34, 35, 29, 37, 31, 28, 33, 30, 26, 32, 60,
      53, 46, 57, 40, 52, 54, 51, 56, 55, 49, 58, 48, 38, 50, 42, 41, 44, 39, 47, 43, 61, 59, 45 ],
    [ 1, 2, 3, 4, 5, 6, 7, 12, 11, 13, 9, 8, 10, 23, 19, 20, 15, 21, 24, 18, 16, 14, 25, 17, 22, 34, 33, 35, 32, 37, 36, 27, 29, 30, 31, 28, 26, 53,
      52, 49, 60, 48, 55, 51, 56, 58, 61, 41, 57, 54, 39, 44, 50, 38, 45, 43, 59, 47, 40, 42, 46 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3 \times Z_4 \times Z_5\,.$

The number field Z_2 has a generator with minimal polynomial

$$X^2 - 50 \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt{2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 48$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 48.

We get $\mathrm{Im}\,\varphi_2 = 1\,.$

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt{2})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt{2}) \\ \Big\| \scriptstyle \mathrm{Im}\,\varphi_2 = 1 \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 has a generator with minimal polynomial

$$X^2 + 50 \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\sqrt{-2})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 48$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 24.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2\,.$

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\sqrt{-2}) \\ \Big| \ \scriptstyle \operatorname{Im}\varphi_3 \simeq \mathrm{C}_2 \\ F_3 \simeq \mathbb{Q} \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_4 has a generator with minimal polynomial

$$X^8 + 40X^4 - 200X^2 + 400 \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_5, \sqrt{2})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_4}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_4}}(M)| = 48$.

The kernel of the action of φ_4 of $\operatorname{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 12.

We get $\operatorname{Im}\varphi_4 \simeq \mathrm{C}_4$.

We have $F_4 = \mathbb{Q}(\sqrt{2})$.

$$\begin{array}{c} Z_4 \simeq \mathbb{Q}(\zeta_5, \sqrt{2}) \\ \Big| \ \scriptstyle \operatorname{Im}\varphi_4 \simeq \mathrm{C}_4 \\ F_4 \simeq \mathbb{Q}(\sqrt{2}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_5 has a generator with minimal polynomial

$$X^8 + 40X^4 + 200X^2 + 400 \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_5, \sqrt{-2})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_5}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_5}}(M)| = 48$.

The kernel of the action of φ_5 of $\operatorname{Aut}_{\alpha,\overline{e_5}}(M)$ on Z_5 has order 6.

We get $\operatorname{Im}\varphi_5 \simeq \mathrm{C}_4 \times \mathrm{C}_2$.

We have $F_5 = \mathbb{Q}$.

$$\begin{array}{c} Z_5 \simeq \mathbb{Q}(\zeta_5, \sqrt{-2}) \\ \Big| \ \scriptstyle \operatorname{Im}\varphi_5 \simeq \mathrm{C}_4 \times \mathrm{C}_2 \\ F_5 \simeq \mathbb{Q} \\ \Big| \\ \mathbb{Q} \end{array}$$

Example 67 Consider the monoid M generated by

```
[
    [ 16, 10, 7, 6, 6, 11, 7, 1, 12, 1, 9, 5, 2, 11, 6, 2 ],
    [ 10, 16, 7, 6, 6, 11, 7, 2, 12, 2, 9, 5, 1, 11, 6, 1 ],
    [ 16, 10, 6, 7, 6, 11, 7, 1, 12, 1, 9, 5, 2, 11, 6, 2 ],
    [ 10, 16, 6, 7, 6, 11, 7, 2, 12, 2, 9, 5, 1, 11, 6, 1 ]
]
```

Then $|M| = 41$ and $\mathrm{Aut}(M) \simeq \mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2$.

Using `k=2` and `p=3` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/3` as follows.

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

```
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
[1 1 1 1 1 a a a a 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 a a a a a a a a a a a a a a a a]
```

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 16 generated by the following elements.

```
[
   [ 1, 2, 3, 4, 5, 7, 6, 9, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 35, 30, 39, 38, 27, 41, 40, 37, 36, 26, 34,
     33, 29, 28, 32, 31 ],
   [ 1, 3, 2, 5, 4, 8, 9, 6, 7, 15, 17, 11, 12, 16, 14, 10, 13, 20, 21, 22, 25, 23, 18, 19, 24, 30, 31, 38, 37, 41, 40, 26, 34, 28, 27, 39,
     36, 33, 29, 35, 32 ],
   [ 1, 2, 3, 4, 5, 7, 6, 9, 8, 13, 10, 16, 14, 11, 12, 17, 15, 21, 20, 25, 22, 24, 19, 18, 23, 39, 38, 31, 32, 29, 33, 36, 35, 27, 28, 30,
     26, 40, 41, 34, 37 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq \mathbb{Q} \times Z_2 \times Z_3 \times Z_4 \times Z_5$.

The number field Z_2 has a generator with minimal polynomial

$$X^2 - \frac{100}{3} \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt{3})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 16$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 16.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt{3})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt{3}) \\ \Big\| \;{\scriptstyle \mathrm{Im}\,\varphi_2 = 1} \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt{3}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 has a generator with minimal polynomial

$$X^2 + \frac{100}{3} \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 16$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 8.

We get $\mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2$.

We have $F_3 \simeq \mathbb{Q}$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\zeta_3) \\ \Big| \;{\scriptstyle \mathrm{Im}\,\varphi_3 \simeq \mathrm{C}_2} \\ F_3 \simeq \mathbb{Q} \end{array}$$

The number field Z_4 has a generator with minimal polynomial

$$X^8 + \frac{160}{9}X^4 - \frac{1600}{27}X^2 + \frac{6400}{81} \in \mathbb{Q}[X].$$

In particular, $Z_4 \simeq \mathbb{Q}(\zeta_5, \sqrt{3})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_4}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\,\mathrm{Aut}_{\alpha,\overline{e_4}}(M)| = 16$.

The kernel of the action of φ_4 of $\mathrm{Aut}_{\alpha,\overline{e_4}}(M)$ on Z_4 has order 4.

We get $\mathrm{Im}\,\varphi_4 \simeq \mathrm{C}_4$.

We have $F_4 \simeq \mathbb{Q}(\sqrt{3})$.

$$Z_4 \simeq \mathbb{Q}(\zeta_5, \sqrt{3})$$

$\Big|\ \operatorname{Im}\varphi_4 \simeq \mathrm{C}_4$

$$F_4 \simeq \mathbb{Q}(\sqrt{3})$$

$\Big|$

$$\mathbb{Q}$$

The number field Z_5 has a generator with minimal polynomial

$$X^8 + \frac{160}{9}X^4 + \frac{1600}{27}X^2 + \frac{6400}{81} \in \mathbb{Q}[X].$$

In particular, $Z_5 \simeq \mathbb{Q}(\zeta_{15})$.

We have $\operatorname{Aut}_{\alpha,\overline{e_5}}(M) = \operatorname{Aut}_\alpha(M)$. In particular, $|\operatorname{Aut}_{\alpha,\overline{e_5}}(M)| = 16$.

The kernel of the action of φ_5 of $\operatorname{Aut}_{\alpha,\overline{e_5}}(M)$ on Z_5 has order 2.

We get $\operatorname{Im}\varphi_5 \simeq \mathrm{C}_4 \times \mathrm{C}_2$.

We have $F_5 \simeq \mathbb{Q}$.

$$Z_5 \simeq \mathbb{Q}(\zeta_{15})$$

$\Big|\ \operatorname{Im}\varphi_5 \simeq \mathrm{C}_4 \times \mathrm{C}_2$

$$F_5 \simeq \mathbb{Q}$$

Example 68 Consider the monoid M generated by

```
[
    [ 9, 9, 14, 8, 12, 4, 14, 7, 6, 6, 5, 11, 12, 6 ],
    [ 14, 9, 9, 8, 12, 4, 14, 7, 6, 6, 5, 11, 12, 6 ],
    [ 9, 14, 9, 8, 12, 4, 14, 7, 6, 6, 5, 11, 12, 6 ]
]
```

Then $|M| = 19$ and $\operatorname{Aut}(M) \simeq \mathrm{S}_3$.

Using `k=5` and `p=3` we obtain the monoid `M` and the two-cocycle `alpha` with entries `a = 1/3` as follows.

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

Consequently we get the subgroup $\mathrm{Aut}_\alpha(M) =$ `A_alpha` of order 6 generated by the following elements.

```
[
    [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 18, 17 ],
    [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 17 ]
]
```

We get $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M}) \simeq Z_1 \times Z_2 \times Z_3 \times Z_4 \times Z_5$.

The number field Z_2 has a generator with minimal polynomial

$$X^5 - 9 \in \mathbb{Q}[X].$$

In particular, $Z_2 \simeq \mathbb{Q}(\sqrt[5]{3})$.

We have $\mathrm{Aut}_{\alpha,\overline{e_2}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_2}}(M)| = 6$.

The kernel of the action of φ_2 of $\mathrm{Aut}_{\alpha,\overline{e_2}}(M)$ on Z_2 has order 6.

We get $\mathrm{Im}\,\varphi_2 = 1$.

We have $F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[5]{3})$.

$$\begin{array}{c} Z_2 \simeq \mathbb{Q}(\sqrt[5]{3}) \\ \Big\| \ \scriptstyle \mathrm{Im}\,\varphi_2 = 1 \\ F_2 = Z_2 \simeq \mathbb{Q}(\sqrt[5]{3}) \\ \Big| \\ \mathbb{Q} \end{array}$$

The number field Z_3 has a generator with minimal polynomial

$$X^{10} + X^5 + \frac{1}{3} \in \mathbb{Q}[X].$$

In particular, $Z_3 \simeq \mathbb{Q}(\sqrt[5]{3}, \zeta_3)$.

We have $\mathrm{Aut}_{\alpha,\overline{e_3}}(M) = \mathrm{Aut}_\alpha(M)$. In particular, $|\mathrm{Aut}_{\alpha,\overline{e_3}}(M)| = 6$.

The kernel of the action of φ_3 of $\mathrm{Aut}_{\alpha,\overline{e_3}}(M)$ on Z_3 has order 6.

We get $\mathrm{Im}\,\varphi_3 = 1$.

We have $F_3 = Z_3 \simeq \mathbb{Q}(\sqrt[5]{3}, \zeta_3)$.

$$\begin{array}{c} Z_3 \simeq \mathbb{Q}(\sqrt[5]{3}, \zeta_3) \\ \Big\| \ \scriptstyle \mathrm{Im}\,\varphi_3 = 1 \\ F_3 = Z_3 \simeq \mathbb{Q}(\sqrt[5]{3}, \zeta_3) \\ \Big| \\ \mathbb{Q} \end{array}$$

Appendix A

Explanation for electronic appendix

On the memory stick attached there is a directory called `electronic_appendix`. It contains lists of representatives of conjugation classes and lists of representatives of isoclasses of submonoids of the symmetric monoid S_n^{mon}. They are named e.g. `conj_5_3_5` or `iso_5_3_5`. The first number gives the degree n of the symmetric monoid, the second number gives the upper bound g for the number of generators of the submonoids and the third number gives the upper bound m for the order of the submonoids.

It can be loaded into Magma with `load iso_5_3_5`. This file contains a list, also called `iso_5_3_5`, of representatives of all isoclasses of submonoids of S_5^{mon}, that have $\leqslant 3$ generators and $\leqslant 5$ elements. For example `#iso_5_3_5` yields `249` and `iso_5_3_5[1]` yields

```
<{
    [ 1, 2, 3, 4, 5 ],
    [ 2, 1, 1, 1, 1 ],
    [ 1, 2, 2, 2, 2 ],
    [ 1, 2, 2, 4, 4 ],
    [ 1, 2, 4, 2, 4 ]
}, [
    [ 2, 1, 1, 1, 1 ],
    [ 1, 2, 2, 4, 4 ],
    [ 1, 2, 4, 2, 4 ]
]>.
```

The first entry of this tuple is the monoid, the second entry consists of generators of the monod.

The electronic appendix also contains the file `aut_4`. It gives a list of submonoids of S_4^{mon} with their generators and their automorphism groups. For example `aut_4[11422]` yields

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

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

after `aut_4` is loaded into Magma with `load aut_4`. So `aut_4[11422]` consists of the monoid, a list of generators of this monoid and its automorphism group.

The files `aut_4_k`, where `k` is contained in `[2, 3, 4, 6, 8, 12, 18, 24, 36]` are the sublists of the lists saved in `aut_4` containing the monoids whose automorphism groups have order `k`.

For example, with `load aut_4_6` the input `aut_4_6[132]` yields

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

The file `two-cocycles.txt` contains six monoids with its generators and one two-cocycle for each monoid, referring to the examples where this file is mentioned. The file `two-cocycles` is not meant to be loaded into Magma directly.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput., 24, 235-265, 1997

[2] Benjamin Steinberg, Representation theory of finite monoids, Springer, 2016

[3] Ariane M. Masuda, Luciane Quoos and Benjamin Steinberg, Character theory of monoids over an arbitary field, arxiv1410.7107v1, 2014

Zusammenfassung

Monoide

Ein Monoid ist eine Menge zusammen mit einer assoziativen Multiplikation und einem neutralen Element, vgl. Definition 1. Z. B. besteht das symmetrische Monoid $\mathrm{S}_n^{\mathrm{mon}}$ von Grad n aus allen Abbildungen von $[1, n]$ nach $[1, n]$, mit der Komposition als Multiplikation. Nach Cayleys Lemma ist jedes endliche Monoid isomorph zu einem Teilmonoid von $\mathrm{S}_n^{\mathrm{mon}}$ für ein geeignetes n, vgl. Lemma 12. Z. B. gibt es in Grad $n = 3$ insgesamt 699 Teilmonoide von $\mathrm{S}_3^{\mathrm{mon}}$, die 160 Konjugationsklassen und 154 Isoklassen bilden.

Monoidalgebren und Körpererweiterungen

Zu einem endlichen Monoid M ist die Monoidalgebra $\mathbb{Q}M$ der $\mathbb{Q}$-Vektorraum mit Basis M, wobei die Multiplikation durch die Multiplikation auf M induziert ist, vgl. Definition 20. Da $\overline{\mathbb{Q}M} := \mathbb{Q}M/\operatorname{Jac}(\mathbb{Q}M)$ halbeinfach ist, ist es isomorph zu einem direkten Produkt von Matrixalgebren über Schiefkörpern. Sein Zentrum ist somit ein direktes Produkt von Zahlkörpern. Ein Automorphismus σ des Monoids M induziert einen $\mathbb{Q}$-Algebrenautomorphismus $\sigma_{\mathbb{Q}}$ der Monoidalgebra $\mathbb{Q}M$, wodurch wir einen Automorphismus $\overline{\sigma_{\mathbb{Q}}}$ von $\overline{\mathbb{Q}M}$ erhalten. Nun schränkt $\overline{\sigma_{\mathbb{Q}}}$ auf einen Automorphismus von $\mathrm{Z}(\overline{\mathbb{Q}M})$ ein. Sei $1_{\mathrm{Z}(\overline{\mathbb{Q}M})} = \overline{e_1} + \cdots + \overline{e_s}$ eine orthogonale Zerlegung in primitive zentrale Idempotente. Die Automorphismen, welche ein gegebenes Idempotent $\overline{e_i}$ von $\mathrm{Z}(\overline{\mathbb{Q}M})$ festhalten, bilden eine Untergruppe $\operatorname{Aut}_{\overline{e_i}}(M)$ der Automorphismengruppe $\operatorname{Aut}(M)$ von M. Diese Untergruppe operiert auf dem Zahlkörper $Z_i := \overline{e_i} \cdot \mathrm{Z}(\overline{\mathbb{Q}M})$. Daraus erhalten wir den Fixkörper F_i unter dieser Operation und die Galoiserweiterung $Z_i \,|\, F_i$, vgl. Remark 21. Ihre Galoisgruppe ist isomorph zur Faktorgruppe von $\operatorname{Aut}_{\overline{e_i}}(M)$ modulo dem Kern dieser Operation.

Das Clifford-Munn-Ponizovsky-Theorem stellt eine enge Verbindung zwischen einer Darstellung eines Monoids und einer Darstellung einer geeigneten Gruppe her [**2,** Th. 5.5][**3,** Th. 2.7]. Unklar für mich ist, ob auch die Endomorphismenringe dieser Darstellungen isomorph sind.

In unseren Beispielen sind die Körper Z_i immer abelsche Erweiterungen über $\mathbb{Q}$.

Getwistete Monoidalgebren und Körpererweiterungen

Ein Zweikozykel ist eine Abbildung $\alpha : M \times M \longrightarrow \mathbb{Q}^{\times}$, welche

$$1 = (n, l)\alpha \cdot ((m \cdot n, l)\alpha)^{-1} \cdot (m, n \cdot l)\alpha \cdot ((m, n)\alpha)^{-1}$$

für m, n, $l \in M$ und

$$1 = (1_M, m)\alpha = (m, 1_M)\alpha$$

für $m \in M$ erfüllt; vgl. Definition 22.

Zu einem endlichen Monoid M ist die getwistete Monoidalgebra $\mathbb{Q}_\alpha M$ der $\mathbb{Q}$-Vektorraum mit Basis M, wobei die Multiplikation durch die Multiplikation auf M induziert ist und zusätzlich ein von α abhängiger Faktor eingebracht wird, vgl. Definition 20. Da $\overline{\mathbb{Q}_\alpha M} := \mathbb{Q}_\alpha M / \operatorname{Jac}(\mathbb{Q}_\alpha M)$ halbeinfach ist, ist es isomorph zu einem direkten Produkt von Matrixalgebren über Schiefkörpern. Sein Zentrum ist somit ein direktes Produkt von Zahlkörpern. Ein Automorphismus σ des Monoids M, welcher den Zweikozykel α respektiert, induziert einen $\mathbb{Q}$-Algebrenautomorphismus $\sigma_\mathbb{Q}$ der getwisteten Monoidalgebra $\mathbb{Q}_\alpha M$, wodurch wir einen Automorphismus $\overline{\sigma_\mathbb{Q}}$ von $\overline{\mathbb{Q}_\alpha M}$ erhalten. Nun schränkt $\overline{\sigma_\mathbb{Q}}$ auf einen Automorphismus von $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$ ein. Sei $1_{\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})} = \overline{e_1} + \cdots + \overline{e_s}$ eine orthogonale Zerlegung in primitive zentrale Idempotente. Die Automorphismen, welche ein gegebenes Idempotent $\overline{e_i}$ von $\mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$ festhalten, bilden eine Untergruppe $\operatorname{Aut}_{\alpha,\overline{e_i}}(M)$ der Automorphismengruppe $\operatorname{Aut}_\alpha(M)$ von M. Diese Untergruppe operiert auf dem Zahlkörper $Z_i := \overline{e_i} \cdot \mathrm{Z}(\overline{\mathbb{Q}_\alpha M})$. Daraus erhalten wir den Fixkörper F_i unter dieser Operation und die Galoiserweiterung $Z_i \,|\, F_i$, vgl. Remark 24. Seine Galoisgruppe ist isomorph zur Faktorgruppe von $\operatorname{Aut}_{\alpha,\overline{e_i}}(M)$ modulo dem Kern dieser Operation.

Mit dieser Methode erhalten wir z. B. die Zahlkörper $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$, $\mathbb{Q}(\sqrt[3]{2},\mathrm{i})$, $\mathbb{Q}(\sqrt[3]{2},\zeta_5)$, $\mathbb{Q}(\sqrt[3]{2},\zeta_7)$, $\mathbb{Q}(\sqrt[3]{2},\sqrt{5})$, $\mathbb{Q}(\sqrt[3]{3},\zeta_3)$ und $\mathbb{Q}(\sqrt[5]{3},\zeta_3)$, von welchen keiner in einem Kreisteilungskörper enthalten ist.

In jedem gefundenen Beispiel ist $Z_i \,|\, F_i$ eine abelsche Erweiterung; also operiert nur ein abelscher Teil von $\operatorname{Aut}(M)$ auf Z_i .

Es stellt sich die Frage, welche endlichen Gruppen als Bild der Operation von $\operatorname{Aut}_{\alpha,\overline{e_i}}(M)$ auf dem Zahlkörper Z_i und somit als $\operatorname{Gal}(Z_i \,|\, F_i)$ auftreten.

Versicherung

Hiermit versichere ich,

1. dass ich meine Arbeit selbstständig verfasst habe,
2. dass ich keine anderen als die angegeben Quellen benutzt habe und alle wörtlich oder sinngemäß aus anderen Werken übernommenen Aussagen als solche gekennzeichnet habe,
3. dass die eingereichte Arbeit weder vollständig noch in wesentlichen Teilen Gegenstand eines anderen Prüfungsverfahrens gewesen ist und
4. dass das elektronische Exemplar mit den anderen Exemplaren übereinstimmt.

Stuttgart, 18.10.2019

Jannik Hess