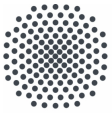
The Galois variety

Katrin Leitner

Bachelor Thesis

March 2020



University of Stuttgart
Germany

Contents

Chapter 0

Introduction

0.1 Galois extensions with a given Galois group

Suppose given a finite group G of order $n := |G|$.

Suppose given a field Q of characteristic 0, playing the role of a ground field.

In cases where G is of small order, we are interested in Galois extensions of Q with Galois group isomorphic to G.

0.1.1 Starting with a Galois extension

Suppose given a finite Galois extension $K|Q$ with Galois group isomorphic to G.

We may form the twisted group algebra $K \wr G$, defined as a K-vector space with basis G and multiplication determined by $\sigma a \cdot \rho b = \sigma\rho\, a^\rho b$ for σ, $\rho \in G$ and a, $b \in K$.

Then $K \wr G$ is, as a Q-algebra, isomorphic to $Q^{n\times n}$.

We choose an element $z \in K$ such that $(z^\sigma : \sigma \in G)$ is a normal basis of K over Q. In particular, we have $K = Q(z) = Q[z]$.

Our isomorphism from $K \wr G$ to $Q^{n\times n}$ sends z to a matrix $A \in Q^{n\times n}$. Hence $K = Q[z]$ is mapped isomorphically to the subalgebra $Q[A]$ of $Q^{n\times n}$.

$$\begin{array}{ccc} K \wr G & \xrightarrow{\sim} & Q^{n\times n} \\ \uparrow & & \uparrow \\ K \;=\; Q[z] & \xrightarrow{\sim} & Q[A] \end{array}$$

$$z \longmapsto A$$

First, consider $\rho \in G$. The action of ρ on K can be extended to the conjugation action of ρ on $K \wr G$. Since $(z^\sigma : \sigma \in G)$ is a normal basis of K over Q, a transport of this action along our

isomorphism yields a conjugation action with a permutation matrix $S_\rho \in \mathrm{GL}_n(Q)$ on $Q^{n\times n}$. Since conjugation with ρ on $K \wr G$ restricts to the action of ρ on $K \subseteq K \wr G$, the conjugation action with S_ρ restricts to $Q[A] \subseteq Q^{n\times n}$. I.e. we have $A^{S_\rho} \in Q[A]$.

Since $Q[A]$ is commutative, we obtain

$$A^{S_\rho} \cdot A \;=\; A \cdot A^{S_\rho}$$

for $\rho \in G$.

Choose generators $\rho_1, \ldots, \rho_m$ of G, so that $G = \langle \rho_1, \ldots, \rho_m \rangle$. Abbreviate $S_i := S_{\rho_i} \in \mathrm{GL}_n(Q)$ for $i \in [1, m]$. So we obtain in particular that

$$A^{S_i} \cdot A \;=\; A \cdot A^{S_i}$$

for $i \in [1, m]$.

Second, we remark that the minimal polynomial of z is irreducible and of degree n. By isomorphic transport, it equals the minimal polynomial of A. So, by Cayley-Hamilton, A has an irreducible characteristic polynomial $\chi_A(X) \in Q[X]$.

So K is isomorphic to $Q[A]$, as field extensions of Q, where A satisfies these two properties. Cf. Theorem 19.(i).

0.1.2 Starting with a matrix

We produce a converse to the procedure outlined in §0.1.1.

We keep the permutation matrices $S_1, \ldots, S_m \in \mathrm{GL}_n(Q)$ used there. We observe that $S_1, \ldots, S_m$ depend only on the group G, not on the Galois extension under consideration.

The subset

$$\{\, A \in \mathrm{GL}_n(Q) :\; A^{S_i} \cdot A = A \cdot A^{S_i} \text{ for } i \in [1, m] \,\} \;\subseteq\; \mathrm{GL}_n(Q) \;\subseteq\; Q^{n\times n}\,.$$

is called the Galois variety of G, with respect to the chosen generators. It is the zero set of a system of homogeneous polynomial equations of degree 2 in the matrix entries.

We show that a matrix A in the Galois variety that has an irreducible characteristic polynomial $\chi_A(X) \in Q[X]$ gives rise to a Galois extension

$$Q[A] \,|\, Q$$

with Galois group isomorphic to G. Cf. Theorem 19.(ii).

0.1.3 Conclusion

Given a Galois extension $K|Q$ with Galois group isomorphic to G, this extension $K|Q$ is isomorphic to $Q[A]|Q$, where A is a matrix in the Galois variety of G with irreducible characteristic polynomial $\chi_A(X) \in Q[X]$; cf. §0.1.1.

Conversely, each matrix A in the Galois variety of G that has an irreducible characteristic polynomial $\chi_A(X) \in Q[X]$ produces a Galois extension $Q[A]|Q$ with Galois group isomorphic to G; cf. §0.1.2.

So the subset of the Galois variety of G of those matrices with irreducible characteristic polynomial yields Galois extensions with Galois group isomorphic to G, and all of them.

Still, different element of the Galois variety of G may give isomorphic extensions; cf. Example 25.

0.2 Particular cases

We consider the ground field $Q := \mathbb{Q}$.

0.2.1 Galois group C_3

We consider the case of the Galois group being isomorphic to the cyclic group $G := \mathrm{C}_3$.

Note that each Galois extension $K|\mathbb{Q}$ of degree 3 has Galois group isomorphic to C_3.

We have an isomorphism from $\mathbb{Q} \wr \mathrm{C}_3$ to $\mathbb{Q}^{3\times 3}$ that maps a chosen generator of C_3 to

$$S \;:=\; S_1 \;=\; \left(\begin{smallmatrix} 0&1&0\\ 0&0&1\\ 1&0&0 \end{smallmatrix}\right) \in \mathbb{Q}^{3\times 3} \,.$$

So the Galois variety of C_3 is given by

$$\{\, A \in \mathrm{GL}_3(\mathbb{Q}) :\; A^S \cdot A = A \cdot A^S \,\} \;\subseteq\; \mathrm{GL}_3(\mathbb{Q}) \;\subseteq\; \mathbb{Q}^{3\times 3} \,.$$

Writing $A =: \left(\begin{smallmatrix} a&b&c\\ d&e&f\\ g&h&i \end{smallmatrix}\right)$, this Galois variety is the subset of $\mathrm{GL}_3(\mathbb{Q})$ defined by the following system of equations.

$$\begin{aligned}
0 &= -bc - cf + dg + gh \\
0 &= -ab - ag + bi - cd + eg + h^2 \\
0 &= -ah - b^2 - ce + ci + fg + hi \\
0 &= ac + ad + bg - ce - di - f^2 \\
0 &= bc + bh - df - dg \\
0 &= af - be + bi + c^2 - dh - ef \\
0 &= af - ch + d^2 + eg - fi - gi \\
0 &= -ah + bf + de - di + eh - g^2 \\
0 &= -bh + cf + df - gh
\end{aligned}$$

In order to reduce the number of variables, we observe that for each matrix A in the Galois variety having irreducible characteristic polynomial $\chi_A(X) \in \mathbb{Q}[X]$, the field $\mathbb{Q}[A]$ contains exactly one element of the form $\left(\begin{smallmatrix} 0&1&0\\ *&*&*\\ *&*&* \end{smallmatrix}\right)$, which, moreover, is an alternative generator of $\mathbb{Q}[A]$.

So we do not lose field extensions when intersecting the Galois variety with the affine subspace of the matrices of the form $\left(\begin{smallmatrix} 0&1&0\\ *&*&*\\ *&*&* \end{smallmatrix}\right)$. We are led to consider the subset

$$\mathcal{L} \;:=\; \{A = \left(\begin{smallmatrix} 0&1&0\\ d&e&f\\ g&h&i \end{smallmatrix}\right) \in \mathrm{GL}_3(\mathbb{Q}) : A^S \cdot A = A \cdot A^S\} \;\subseteq\; \mathrm{GL}_3(\mathbb{Q}) \;\subseteq\; \mathbb{Q}^{3\times 3} \,.$$

This subset $\mathcal{L}$ is defined by the following system of equations.

$$\begin{aligned} 0 &= dg + gh \\ 0 &= i + eg + h^2 \\ 0 &= -1 + fg + hi \\ 0 &= g - di - f^2 \\ 0 &= h - df - dg \\ 0 &= -e + i - dh - ef \\ 0 &= d^2 + eg - fi - gi \\ 0 &= f + de - di + eh - g^2 \\ 0 &= -h + df - gh \end{aligned}$$

A calculation by hand yields the following result.

$$\begin{aligned} \mathcal{L} &= \{A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \\ g & h & i \end{smallmatrix}\right) \in \mathrm{GL}_3(\mathbb{Q}) : A^S \cdot A = A \cdot A^S\} \\ &= \{\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & e & -1 \\ 0 & -1 & -1 \end{smallmatrix}\right) : e \in \mathbb{Q}\} \cup \{\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)\} \cup \{ \begin{pmatrix} 0 & 1 & 0 \\ -\frac{g^2+g+1}{i} & -\frac{(g^2+g+1)^2+i^3}{gi^2} & -g-1 \\ g & \frac{g^2+g+1}{i} & i \end{pmatrix} : g, i \in \mathbb{Q} \setminus \{0\}\}. \end{aligned}$$

So each Galois extension $K|\mathbb{Q}$ of degree 3 is isomorphic to $\mathbb{Q}[A]|\mathbb{Q}$ for some matrix $A \in \mathcal{L}$ that has an irreducible characteristic polynomial $\chi_A(X)$ in $\mathbb{Q}[X]$. Cf. Theorem 19.(i).

Conversely, for each matrix $A \in \mathcal{L}$ that has an irreducible characteristic polynomial $\chi_A(X)$ in $\mathbb{Q}[X]$, the field extension $\mathbb{Q}[A]|\mathbb{Q}$ is galois of degree 3. Cf. Theorem 19.(ii).

0.2.2 Galois group C_4

We consider the case of the Galois group being isomorphic to the cyclic group $G := \mathrm{C}_4$.

We have an isomorphism from $\mathbb{Q} \wr \mathrm{C}_4$ to $\mathbb{Q}^{4\times 4}$ that maps a chosen generator of C_4 to

$$S := S_1 = \left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right) \in \mathbb{Q}^{4\times 4}.$$

So the Galois variety of C_4 is given by

$$\{ A \in \mathrm{GL}_4(\mathbb{Q}) : \ A^S \cdot A = A \cdot A^S \} \subseteq \mathrm{GL}_4(\mathbb{Q}) \subseteq \mathbb{Q}^{4\times 4}.$$

In order to reduce the number of variables, we observe that for each matrix A in the Galois variety having irreducible characteristic polynomial $\chi_A(X) \in \mathbb{Q}[X]$, the field $\mathbb{Q}[A]$ contains exactly one element B of the form $\left(\begin{smallmatrix} 0 & 1 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{smallmatrix}\right)$.

A priori, $\mathbb{Q}[B]$ is either equal to $\mathbb{Q}[A]$ or a subfield $\mathbb{Q} \subset \mathbb{Q}[B] \subset \mathbb{Q}[A]$ with $[\mathbb{Q}[B] : \mathbb{Q}] = 2$.

We want to show that $\mathbb{Q}[B]$ is equal to $\mathbb{Q}[A]$. To this end, we *assume* that $[\mathbb{Q}[B] : \mathbb{Q}] = 2$. We have the surjective trace map $\mathrm{Tr}_{\mathbb{Q}[A]|\mathbb{Q}[B]} : \mathbb{Q}[A] \to \mathbb{Q}[B] : C \mapsto C + C^{S^2}$. In particular,

the inverse image of B under this $\mathbb{Q}$-linear map is an affine subspace of $\mathbb{Q}[A]$ of dimension 2. Hence there exists $\tilde{A} \in \mathbb{Q}[A] \setminus \mathbb{Q}[B]$ in this inverse image, so that $\mathbb{Q}[\tilde{A}] = \mathbb{Q}[A]$. However, a calculation reveals that such a matrix $\tilde{A}$ necessarily has a reducible characteristic polynomial and thus not an irreducible minimal polynomial of degree 4. We have arrived at a *contradiction*. So $\mathbb{Q}[B] = \mathbb{Q}[A]$.

In other words, we may right away suppose A to be of the form $\begin{pmatrix} 0&1&0&0 \\ *&*&*&* \\ *&*&*&* \\ *&*&*&* \end{pmatrix}$.

We are led to consider the subset

$$\mathcal{L} \;:=\; \{A = \begin{pmatrix} 0&1&0&0 \\ e&f&g&h \\ i&j&k&l \\ m&n&p&q \end{pmatrix} \in \mathrm{GL}_4(\mathbb{Q}) :\; A^S \cdot A = A \cdot A^S\} \;\subseteq\; \mathrm{GL}_4(\mathbb{Q}) \;\subseteq\; \mathbb{Q}^{4\times 4}.$$

This subset $\mathcal{L}$ seems too big to be calculated by hand.

With Magma [**2**], we can find a large subset of $\mathcal{L}$ in the following may. We have a system of equations that defines $\mathcal{L}$ as a subset of $\mathbb{Q}^{4\times 4}$. In other words, we have a system of ideal generators in the polynomial ring $\mathbb{Q}[e, i, m, k, l, n, p, q, f, g, h, j]$. Now we change the ground field from $\mathbb{Q}$ to $\mathbb{Q}(e, i, m)$, with formal variables e, i, m. Then we map our system of ideal generators to the polynomial ring $\mathbb{Q}(e, i, m)[k, l, n, p, q, f, g, h, j]$ and consider the ideal generated by its image.

This ideal then has a factor algebra of Krull dimension zero and can thus be treated with the Magma command `TriangularDecomposition`. We obtain solutions parametrized by e, i, m. It happens that such a solution contains polynomials in e, i, m as denominators. The values $e, i, m \in \mathbb{Q}$ for which such a denominator is zero yield a list of separate additional cases.

In treating the various cases, we make use of the Maple package Epsilon by Dongming Wang [**5**], in particular, of the command `ICS`.

However, it is possible that this change of ground fields from $\mathbb{Q}$ to $\mathbb{Q}(e, i, m)$ makes certain parts of $\mathcal{L}$ invisible, even with the separate cases taken into consideration. In other words, we can only assert that our procedure gives a subset $\mathcal{L}' \subseteq \mathcal{L}$. Collecting the results from all cases, $\mathcal{L}'$ is written as a union of 25 subsets, involving up to 3 parameters, as can be seen in Proposition 31.

Independently of our change-of-ground-field-approach, we have verified again that in fact $\mathcal{L}'$ is a subset of $\mathcal{L}$ and thus of the Galois variety of C_4.

Note that for each matrix $A \in \mathcal{L}$ that has an irreducible characteristic polynomial $\chi_A(X)$ in $\mathbb{Q}[X]$, the field extension $\mathbb{Q}[A]|\mathbb{Q}$ is galois with Galois group isomorphic to C_4; cf. Theorem 19.(ii). We give several examples, in which $A \in \mathcal{L}'$.

0.2.3 Galois group S_3

We consider the case of the Galois group being isomorphic to the symmetric group $G := \mathrm{S}_3$.

We have an isomorphism from $\mathbb{Q} \wr \mathrm{S}_3$ to $\mathbb{Q}^{6\times 6}$ that maps two chosen generators of S_3 to

$$S_1 \;=\; \begin{pmatrix} 0&1&0&0&0&0 \\ 1&0&0&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&0&0&1&0 \\ 0&0&0&1&0&0 \\ 0&0&1&0&0&0 \end{pmatrix} \qquad \text{resp. to} \qquad S_2 \;=\; \begin{pmatrix} 0&0&0&0&0&1 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&1&0&0&0&0 \\ 0&0&0&0&0&1 \\ 1&0&0&0&0&0 \end{pmatrix} \qquad \text{in} \quad \mathbb{Q}^{6\times 6}.$$

So the Galois variety of S_3 is given by

$$\{\, A \in \mathrm{GL}_6(\mathbb{Q}) :\ A^{S_1} \cdot A = A \cdot A^{S_1} \text{ and } A^{S_2} \cdot A = A \cdot A^{S_2} \,\} \ \subseteq\ \mathrm{GL}_6(\mathbb{Q}) \ \subseteq\ \mathbb{Q}^{6\times 6}\ .$$

This variety seems to be too big to be calculated as a whole with our means.

In order to be able to see at least a part of the Galois variety, we have a priori confined ourselves to the consideration of solutions of the form

$$A \ = \ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} \\ a_{3,1} & a_{3,1} & a_{3,1} & a_{3,1} & a_{3,1} & a_{3,1} \\ a_{4,1} & a_{4,2} & a_{4,1} & a_{4,4} & a_{4,5} & a_{4,6} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} \end{pmatrix} \in \mathrm{GL}_6(\mathbb{Q})\ .$$

The choice of this particular form of A is motivated only by the resulting subset of the Galois variety, parametrized by two parameters, which is the largest subset we could find.

For $(r,t) \in \mathbb{Q}\times\mathbb{Q}$ such that $r+2t+1 \neq 0$ and $t \neq 0$, we let

$$B_{r,t} := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ r & \frac{(r+1)(t+1)}{t} & r{+}1 & r & r{+}1 & \frac{(r+1)(t+1)}{t} \\ t & t & t & t & t & t \\ -\frac{t(t+2r+1)}{r+2t+1} & -\frac{2rt+r+t^2+3t+1}{r+2t+1} & -\frac{t(t+2r+1)}{r+2t+1} & -\frac{(2r+t+1)(t+1)}{r+2t+1} & -\frac{2rt+r+t^2+3t+1}{r+2t+1} & -\frac{(2r+t+1)(t+1)}{r+2t+1} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -\frac{r^2+rt+r+t^2}{r+2t+1} & -\frac{r^2t+r^2+rt^2+4rt+2r+t^3+2t^2+3t+1}{(r+2t+1)\,t} & -\frac{r^2+rt+2r+(t+1)^2}{r+2t+1} & -\frac{r^2+rt+t^2+t}{r+2t+1} & -\frac{r^2+rt+r+t^2}{r+2t+1} & -\frac{(t+1)(r^2+rt+t^2+r)}{(r+2t+1)t} \end{pmatrix}.$$

Then $B_{r,t}$ is an element of the Galois variety. So provided (r,t) is chosen such that $B_{r,t}$ has an irreducible characteristic polynomial $\chi_{B_{r,t}}(X) \in \mathbb{Q}[X]$, the field extension $\mathbb{Q}[B_{r,t}]|\mathbb{Q}$ is galois with Galois group isomorphic to S_3.

Conventions

Suppose given sets X, Y and Z. Suppose given $n \in \mathbb{Z}_{\geqslant 1}$. Suppose given a field Q.

(1) Given a map $f : X \to Y$, we write xf for the image of x under f.

(2) Suppose given maps $f : X \to Y$ and $g : Y \to Z$. The composite of the maps $X \xrightarrow{f} Y \xrightarrow{g} Z$ is written $X \xrightarrow{f \cdot g} Z$ or $X \xrightarrow{fg} Z$.

(3) Suppose given a matrix $A \in Q^{n \times n}$ and an invertible matrix $S \in Q^{n \times n}$.
We write $A^S := S^{-1} \cdot A \cdot S$.

(4) Suppose given $i, j \in [1, n]$. The matrix $\mathrm{e}_{i,j} \in Q^{n \times n}$ is supposed to have entry 1 at position (i, j) and entry 0 elsewhere.

(5) Suppose given $i \in [1, n]$. The matrix $\mathrm{e}_i \in Q^{1 \times n}$ is supposed to have entry 1 at position $(1, i)$ and entry 0 elsewhere.

(6) Suppose given vector spaces V and W and a linear map $f : V \to W$. Suppose given a basis B of V and a basis C of W. We write ${}_Bf_C$ for the representing matrix of f with respect to B and C.

(7) We write $\mathrm{I}_n \in Q^{n \times n}$ for the unit matrix.

(8) Suppose given a matrix $A \in Q^{n \times n}$.

(i) We write $\chi_A(X) := \det(X \cdot \mathrm{I}_n - A)$ for the characteristic polynomial of A.

(ii) We write $\mu_A(X)$ for the minimal polynomial of A.

(iii) We write $\mathrm{E}_\lambda(A) := \{x \in Q^{1 \times n} : x \cdot A = \lambda \cdot x\}$ for $\lambda \in Q$.

(9) Suppose given $x \in Q$. We identify x with $x \cdot \mathrm{I}_n$. So we obtain $Q \subseteq Q^{n \times n}$.

(10) Suppose given $\sigma \in \mathrm{S}_n$. We write $\mathrm{supp}(\sigma) := \{i \in [1, n] : i\sigma \neq i\}$, called support of σ.

(11) Suppose given a field K. We write $\mathrm{Aut}(K)$ for the group of field automorphisms of K.

(12) Suppose given a field extension $K|Q$. We write

$$\mathrm{Aut}(K|Q) \ := \ \{\, \sigma \in \mathrm{Aut}(K) : \ \sigma(Q) \subseteq Q \text{ and } \sigma|_Q^Q = \mathrm{id}_Q \,\}$$

for the group of automorphisms of $K|Q$.

(13) Whenever Maple is used, the package `linalg` and the package `epsilon` have to be loaded:

```
with(linalg):
with(epsilon):
```

If necessary, Maple can be led to produce output in an ordinary style by:

```
interface(prettyprint = 0);
```

Chapter 1

Galois extensions with a given Galois group

Let G be a finite group.

Let Q be a field with $\mathrm{char}(Q) = 0$.

Let $K|Q$ be a finite field extension, of degree $n := [K : Q]$.

Let $G \xrightarrow{\gamma} \mathrm{Aut}(K|Q)$ be an injective group morphism.

We often write $x^\sigma := x(\sigma\gamma)$ for $x \in K$ and $\sigma \in G$.

Note that $x^{1_G} = x(1_G\,\gamma) = x\ \mathrm{id}_K = x$ for $x \in K$.

Suppose that $Q = \{x \in K : x = x^\sigma \text{ for } \sigma \in G\}$.

So $K|Q$ is galois with Galois group $\mathrm{Gal}(K|Q) = G\gamma$ isomorphic to G; cf. Lemma 2 below.

We enumerate the elements of G such that $G = \{\sigma_1, \ldots, \sigma_n\}$ and $\sigma_1 := 1_G$.

Let $\bar{Q}$ be an algebraic closure of Q.

1.1 Preliminaries on field extensions

Proposition 1 (Fundamental theorem of Galois theory) Let $\mathcal{U}$ be the set of subgroups of G. Let $\mathcal{I}$ be the set of subfields of K that contain Q, i.e. the set of intermediate fields of $K|Q$.

For $H \in \mathcal{U}$, we write $\mathrm{Fix}_H(K) := \{x \in K : x^\sigma = x \text{ for } \sigma \in H\} \in \mathcal{I}$.

Then the map $\mathcal{U} \to \mathcal{I}$, $H \mapsto \mathrm{Fix}_H(K)$ is a bijection.

Moreover, H is a normal subgroup in G if and only if $\mathrm{Fix}_H(K)$ is galois over Q. In this case, the map $G/H \to \mathrm{Aut}(\mathrm{Fix}_H(K))$, $\sigma H \mapsto (\sigma\gamma)|^{\mathrm{Fix}_H(K)}_{\mathrm{Fix}_H(K)}$ is an injective group morphism with image $\mathrm{Gal}(\mathrm{Fix}_H(K)|Q)$.

Proof. See [**3,** Ch. VI, Th. 1.1]. □

Lemma 2 (Artin) Let L be a field and let H be a finite group.

Suppose given an injective group morphism $\psi : H \to \mathrm{Aut}(L)$.

Let $\mathrm{Fix}_H(L) := \{x \in L : x(\sigma\psi) = x \text{ for } \sigma \in H\}$ be the fixed field.

Then L is a finite Galois extension of $\mathrm{Fix}_H(L)$, and its Galois group is $H\psi$.

We have $[L : \mathrm{Fix}_H(L)] = |H|$.

Proof. See **[3,** Ch. VI, Th. 1.8], applied to $H\psi$. □

Proposition 3 (Normal basis) There exists an element $z \in K$ such that $(z^{\sigma_1}, \ldots, z^{\sigma_n})$ is a Q-linear basis of K.

Such a Q-linear basis of K is called a *normal basis* of $K|Q$.

Proof. See **[3,** Ch. VI, Th. 13.1]. □

The following fact I have learned from **[1,** p. 141, item (a)].

Remark 4 Suppose given $z \in K$ such that $(z^{\sigma_1}, \ldots, z^{\sigma_n})$ a normal basis of $K|Q$.

Then we have $K = Q(z)$.

Proof. Assume not. Then $M := Q(z) \subset K$. We write $M = \mathrm{Fix}_H(K)$ for a suitable subgroup $1 < H \leqslant G$; cf. Proposition 1.

Choose $k \in [1, n]$ such that $\sigma_k \in H \setminus \{\sigma_1\}$. Then $z^{\sigma_1} = z = z^{\sigma_k}$.

This is a *contradiction* to linear independence. □

Lemma 5 (Dedekind) Suppose given $a_\sigma \in K$ for $\sigma \in G$.

If $\sum_{\sigma \in G} y^\sigma a_\sigma = 0$ for $y \in K$, then we have $a_\sigma = 0$ for $\sigma \in G$.

Proof. See **[3,** Ch. VI, Th. 4.1] and the remark thereafter, on **[3,** p. 284, l. 3-10]. □

Definition 6 Suppose given a polynomial $f(X) \in Q[X]$.

Write $f(X) =: \sum_{k=0}^{m} a_k \cdot X^k$ where $a_k \in Q$.

Then we let $f'(X) := \sum_{k=1}^{m} a_k \cdot k \cdot X^{k-1}$ be the *formal derivative* of $f(X)$.

Remark 7 Suppose given a polynomials $f(X), g(X) \in Q[X]$.

Then $(f(X) \cdot g(X))' = f'(X) \cdot g(X) + f(X) \cdot g'(X)$.

Proof. See **[3,** p. 178, l. −9]. □

Remark 8 Suppose given $u(X), v(X) \in Q[X] \setminus \{0\}$.

Let $g(X) \in Q[X]$ be the monic polynomial with $(u(X), v(X)) = (g(X))$ as ideals in $Q[X]$.

Then $(u(X), v(X)) = (g(X))$ as ideals in $\bar{Q}[X]$, too, as follows from the Euclidean algorithm.

We write $g(X) := \gcd(u(X), v(X))$.

Lemma 9 Let $f(X) \in Q[X]$ a monic irreducible polynomial.

Then there is no $a \in \bar{Q}$ such that $(X-a)^2$ divides $f(X)$ in $\bar{Q}[X]$.

Proof. Assume that there exists $a \in \bar{Q}$ such that $(X-a)^2$ divides $f(X)$.

So there exists $h(X) \in \bar{Q}[X]$ with $f(X) = (X-a)^2 \cdot h(X)$.

Thus

$$f'(X) \overset{\text{D 6}}{=} 2 \cdot (X-a) \cdot h(X) + (X-a)^2 \cdot h'(X) = (X-a) \cdot (2 \cdot h(X) + (X-a) \cdot h'(X))$$

Thus $(X-a)$ divides $f(X)$ and $f'(X)$ in $\bar{Q}[X]$.

Let $g(X) := \gcd(f(X), f'(X))$. Then we obtain

$$(f(X), f'(X)) = (g(X)) \text{ in } Q[X]$$
$$(f(X), f'(X)) = (g(X)) \text{ in } \bar{Q}[X]$$

by Remark 8.

So $g(X)$ divides $f(X)$ in $Q[X]$. Since $f(X)$ is irreducible in $Q[X]$, we have $g(X) = 1$ or $g(X) = f(X)$. But $g(X)$ divides $f'(X)$, too. So

$$\deg(g(X)) \leqslant \deg(f'(X)) \overset{\text{char}(Q)=0}{=} \deg(f(X)) - 1 < \deg(f(X))$$

Thus $g(X) = 1$, so $\deg(g(X)) = 0$.

We can write $g(X) = u(X) \cdot f(X) + v(X) \cdot f'(X)$ where $u(X), v(X) \in Q[X]$.

Now $(X-a)$ divides $f(X)$ and $f'(X)$, so $(X-a)$ divides $g(X)$ in $\bar{Q}[X]$. Hence $\deg(g(X)) \geqslant 1$.

We have a *contradiction*. □

1.2 The twisted group algebra

Definition 10 The *twisted group algebra* is the K-vector space with basis G, i.e.

$$K \wr G := \left\{ \sum_{\sigma \in G} \sigma a_\sigma : a_\sigma \in K \text{ for } \sigma \in G \right\},$$

carrying the multiplication

$$(\sum_{\sigma \in G} \sigma a_\sigma) \cdot (\sum_{\rho \in G} \rho b_\rho) := \sum_{\sigma, \rho \in G} \sigma\rho \, a_\sigma^\rho b_\rho$$

for $\sum_{\sigma\in G}\sigma a_\sigma\,,\ \sum_{\rho\in G}\rho b_\rho\ \in\ K\wr G$.

We also identify

$$\begin{array}{rcccl} K & = & \{a : a\in K\} & = & \{1_G\cdot a : a\in K\} \ \subseteq\ K\wr G \\ G & = & \{\sigma : \sigma\in G\} & = & \{\sigma\cdot 1_K : \sigma\in G\} \ \subseteq\ K\wr G\,. \end{array}$$

Remark 11 The K-vector space $K\wr G$ is in fact a ring.

We have a ring morphism

$$\varepsilon\ :\ Q\ \to\ \mathrm{Z}(K\wr G),\ q\ \mapsto\ q\,.$$

Thus $K\wr G$, together with ε, is in fact a Q-algebra.

Proof. We show that $1_G = 1_G\cdot 1_K$ is neutral with respect to $(\cdot)$, i.e. that $1_G \stackrel{!}{=} 1_{K\wr G}$.

We have

$$\sum_{\sigma\in G}\sigma a_\sigma\cdot(1_G\cdot 1_K)\ =\ \sum_{\sigma\in G}\sigma\cdot 1_G\cdot a_\sigma^{1_G}1_K\ =\ \sum_{\sigma\in G}\sigma a_\sigma$$

and, moreover,

$$(1_G\cdot 1_K)\cdot\sum_{\sigma\in G}\sigma a_\sigma\ =\ \sum_{\sigma\in G}1_G\cdot\sigma\cdot 1_K^\sigma a_\sigma\ =\ \sum_{\sigma\in G}\sigma a_\sigma\quad .$$

We show that $(K\wr G,\cdot)$ is associative.

Suppose given $\sum_{\sigma\in G}\sigma a_\sigma\ ,\ \sum_{\rho\in G}\rho b_\rho\ ,\ \sum_{\tau\in G}\tau c_\tau\ \in\ K\wr G$. Then

$$\begin{array}{rcl} ((\sum_{\sigma\in G}\sigma a_\sigma)\cdot(\sum_{\rho\in G}\rho b_\rho))\cdot(\sum_{\tau\in G}\tau c_\tau) & = & (\sum_{\sigma,\,\rho\,\in G}\sigma\rho\, a_\sigma^\rho b_\rho)\cdot(\sum_{\tau\in G}\tau c_\tau) \\ & = & \sum_{\sigma,\rho,\tau\in G}\sigma\rho\tau(a_\sigma^\rho b_\rho)^\tau c_\tau \\ & = & \sum_{\sigma,\rho,\tau\in G}\sigma\rho\tau\, a_\sigma^{\rho\tau} b_\rho^\tau c_\tau \\ & = & (\sum_{\sigma\in G}\sigma a_\sigma)\cdot(\sum_{\rho,\tau\in G}\rho\tau\, b_\rho^\tau c_\tau) \\ & = & (\sum_{\sigma\in G}\sigma a_\sigma)\cdot((\sum_{\rho\in G}\rho b_\rho)\cdot(\sum_{\tau\in G}\tau c_\tau))\,. \end{array}$$

We show that ε actually maps to $\mathrm{Z}(Q\wr G)$.

Suppose given $q\in Q$. We show that $q = 1_G\cdot q \stackrel{!}{\in} \mathrm{Z}(Q\wr G)$.

Suppose given $\sum_{\sigma\in G}\sigma a_\sigma\in K\wr G$. Then

$$(1_G\cdot q)\cdot(\sum_{\sigma\in G}\sigma a_\sigma)\ =\ \sum_{\sigma\in G}1_G\sigma q^\sigma a_\sigma\ =\ \sum_{\sigma\in G}\sigma q a_\sigma\ =\ \sum_{\sigma\in G}\sigma a_\sigma^{1_G}q\ =\ (\sum_{\sigma\in G}\sigma a_\sigma)\cdot(1_G\cdot q)\,.$$

We show that ε is a ring morphism.

We have $(1_Q)\varepsilon = 1_Q = 1_K = 1_G \cdot 1_K = 1_{K \wr G}$. Moreover, ε is additive. Finally, for $q, r \in Q$, we have

$$(q)\varepsilon \cdot (r)\varepsilon \;=\; (1_G \cdot q) \cdot (1_G \cdot r) \;=\; 1_G \cdot 1_G \cdot q^{1_G} \cdot r \;=\; 1_G \cdot q \cdot r \;=\; (q \cdot r)\varepsilon.$$

□

Remark 12 Let $(y_1, \ldots, y_n)$ be a Q-linear basis of K.

Then $(\sigma_i y_j : i, j \in [1, n])$ is a Q-linear basis of $K \wr G$. In particular, $\dim_Q(K \wr G) = n^2$.

Definition 13 Suppose given $y \in K$. Suppose given $\xi = \sum_{\sigma \in G} \sigma a_\sigma \in K \wr G$. Let

$$y \cdot \xi \;:=\; \sum_{\sigma \in G} y^\sigma a_\sigma \;.$$

Lemma 14 Consider the map $\delta : K \wr G \to \mathrm{End}_Q(K)$, $\xi \mapsto \xi\delta$ with

$$\xi\delta \;:\; K \;\to\; K \;,\;\; y \;\mapsto\; y(\xi\delta) \;=\; y \cdot \xi \;.$$

Then δ is a Q-algebra isomorphism.

Proof. Suppose given $\xi = \sum_{\sigma \in G} \sigma a_\sigma$, $\xi' = \sum_{\rho \in G} \rho b_\rho \in K \wr G$. Suppose given $\lambda, \lambda' \in Q$.

We have to show that $1_{K \wr G} \;\delta \stackrel{!}{=} \mathrm{id}_K$, that $(\xi\lambda + \xi'\lambda')\delta \stackrel{!}{=} (\xi\delta)\lambda + (\xi'\delta)\lambda'$ and that $(\xi \cdot \xi')\delta \stackrel{!}{=} \xi\delta \cdot \xi'\delta$.

Suppose given $y \in K$.

We obtain

$$y(1_{K \wr G}\, \delta) \;=\; y \cdot 1_{K \wr G} \;=\; y \cdot (1_G \cdot 1_K) \;\stackrel{\mathrm{D}\,13}{=}\; y^{1_G} \cdot 1_K \;=\; y \;.$$

Moreover,

$$\begin{array}{rcll}
y((\xi \cdot \lambda + \xi' \cdot \lambda')\delta) & = & y \cdot (\xi \cdot \lambda + \xi' \cdot \lambda') & = \; y \cdot (\sum_{\sigma \in G} \sigma a_\sigma \cdot \lambda + \sum_{\sigma \in G} \sigma b_\sigma \cdot \lambda') \\
& = & y \cdot \sum_{\sigma \in G} \sigma(a_\sigma\lambda + b_\sigma\lambda') & \stackrel{\mathrm{D}\,13}{=} \; \sum_{\sigma \in G} y^\sigma (a_\sigma\lambda + b_\sigma\lambda') \\
& = & \sum_{\sigma \in G} y^\sigma \cdot a_\sigma \cdot \lambda + \sum_{\sigma \in G} y^\sigma \cdot b_\sigma \cdot \lambda' & \stackrel{\mathrm{D}\,13}{=} \; (y \cdot \sum_{\sigma \in G} \sigma a_\sigma) \cdot \lambda + (y \cdot \sum_{\sigma \in G} \sigma b_\sigma) \cdot \lambda' \\
& = & (y \cdot \xi) \cdot \lambda + (y \cdot \xi') \cdot \lambda' & = \; (y(\xi\,\delta)) \cdot \lambda + (y(\xi'\,\delta)) \cdot \lambda' \\
& = & y((\xi\delta)\lambda + (\xi'\delta)\lambda') \;. &
\end{array}$$

Finally,

$$\begin{array}{rclcl} y((\xi\cdot\xi')\delta) & = & y\cdot(\xi\cdot\xi') & = & y\cdot((\sum_{\sigma\in G}\sigma a_\sigma)(\sum_{\rho\in G}\rho b_\rho)) \\ & = & y\cdot(\sum_{\sigma,\rho\in G}\sigma\cdot\rho\cdot a_\sigma^\rho\cdot b_\rho) & \overset{\text{D 13}}{=} & \sum_{\sigma,\rho\in G} y^{\sigma\cdot\rho}\cdot a_\sigma^\rho\cdot b_\rho \\ \overset{\text{D 13}}{=} & (\sum_{\sigma\in G} y^\sigma a_\sigma)\cdot(\sum_{\rho\in G}\rho b_\rho) & \overset{\text{D 13}}{=} & (y\cdot(\sum_{\sigma\in G}\sigma a_\sigma))\cdot(\sum_{\rho\in G}\rho b_\rho) \\ & = & (y\cdot\xi)\cdot\xi' & = & (y(\xi\delta))(\xi'\delta) \\ & = & y((\xi\delta)\cdot(\xi'\delta))\ . & & \end{array}$$

We know that $\dim_Q(K\wr G)\overset{\text{R 12}}{=} n^2 = \dim_Q(\mathrm{End}_Q(K))$.

So it remains to show that δ is injective, i.e. that $\mathrm{Kern}(\delta)\overset{!}{=}0$.

Suppose given $\xi=\sum_{\sigma\in G}\sigma a_\sigma\in K\wr G$ such that $\xi\delta=0$. We have to show that $\xi\overset{!}{=}0$.

For $y\in K$, we get

$$0 \;=\; y(\xi\delta) \;=\; y\cdot\xi \;=\; y(\sum_{\sigma\in G}\sigma a_\sigma) \;\overset{\text{D 13}}{=}\; \sum_{\sigma\in G} y^\sigma a_\sigma,$$

so that $a_\sigma=0$ for $\sigma\in G$ by Lemma 5. Therefore, $\xi=0$.

So δ is a Q-algebra isomorphism. □

1.3 Matrices and Galois extensions

Definition 15 Suppose given $\rho\in G$. Recall that $G=\{\,\sigma_i:\ i\in[1,n]\,\}$.

Let $\alpha:\ [1,n]\to\ [1,n]$ be defined by $\sigma_j\cdot\rho=:\sigma_{j\alpha}$ for $j\in[1,n]$.

We *claim* that α is bijective. We have the diagram:

$$\begin{array}{ccccc} & & \sigma\longmapsto\sigma\cdot\rho & & \\ \sigma_j & & G\xrightarrow[\text{bij.}]{\psi} G & & \sigma_j \\ \uparrow & & \varphi\uparrow\text{bij.} \quad \varphi\uparrow\text{bij.} & & \uparrow \\ j & & [1,n] \qquad [1,n] & & j \end{array}$$

It suffices to show that $\alpha\overset{!}{=}\varphi\psi\varphi^{-1}$.

Suppose given $j\in[1,n]$. To show that

$$j\varphi\psi\varphi^{-1} \;\overset{!}{=}\; j\alpha\ ,$$

we show that

$$j\varphi\psi \stackrel{!}{=} (j\alpha)\varphi\,.$$

In fact,

$$j\varphi\psi = \sigma_j\psi = \sigma_j\cdot\rho = \sigma_{j\alpha} = (j\alpha)\varphi\,.$$

This proves the *claim*.

Consider the permutation matrix $S_\rho := \sum_{j\in[1,n]} \mathrm{e}_{j,j\alpha} \in Q^{n\times n}$.

Let $G_{\mathrm{mat}} := \{S_\rho : \rho \in G\} \leqslant \mathrm{GL}_n(Q)$.

Then we have the isomorphism $\gamma' : G \to G_{\mathrm{mat}},\ \rho \mapsto S_\rho\,.$

Definition 16 Choose $m \geqslant 1$ and $\rho_1, \ldots, \rho_m \in G$ such that $G = \langle \rho_1, \ldots, \rho_m\rangle$.

We write $S_i := S_{\rho_i}$ for $i \in [1, m]$.

Let $\mathbb{S} := \{S_i : i \in [1, m]\}$.

Then we have $G_{\mathrm{mat}} = \langle S_1, S_2, \ldots, S_m\rangle$.

Lemma 17 Suppose given a diagonal matrix $D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \in \bar{Q}^{n\times n}$, where $\lambda_i \neq \lambda_j$ for $i, j \in [1, n]$ with $i \neq j$.

Let $C := \{B \in \bar{Q}^{n\times n} : D\cdot B = B\cdot D\}$.

Then, for $B \in \bar{Q}^{n\times n}$, we have $B \in C$ if and only if B is a diagonal matrix.

Proof. First we show that if B is a diagonal matrix, then $B \in C$.

Suppose given $B = \begin{pmatrix} \kappa_1 & & \\ & \ddots & \\ & & \kappa_n \end{pmatrix} \in \bar{Q}^{n\times n}$. Then

$$D\cdot B = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}\cdot\begin{pmatrix} \kappa_1 & & \\ & \ddots & \\ & & \kappa_n \end{pmatrix} = \begin{pmatrix} \lambda_1\cdot\kappa_1 & & \\ & \ddots & \\ & & \lambda_n\cdot\kappa_n \end{pmatrix} = \begin{pmatrix} \kappa_1\cdot\lambda_1 & & \\ & \ddots & \\ & & \kappa_n\cdot\lambda_n \end{pmatrix} = B\cdot D$$

Thus $B \in C$.

Now we show that if $B \in C$, then B is a diagonal matrix.

Suppose given $B \in C$. Write $B =: (b_{i,j})_{i,j}$ for $i, j \in [1, n]$.

We show that $b_{k,l} \stackrel{!}{=} 0$ for $k, l \in [1, n]$ with $k \neq l$.

We have

$$D\cdot B = (\lambda_i\cdot b_{i,j})_{i,j} = (b_{i,j}\cdot\lambda_j)_{i,j} = B\cdot D.$$

Thus

$$\lambda_k\cdot b_{k,l} = \lambda_l\cdot b_{k,l}\,,$$

hence

$$(\lambda_l - \lambda_k)\cdot b_{k,l} = 0\,.$$

Since $k \neq l$, we conclude that $\lambda_k \neq \lambda_l$ and thus $b_{k,l} = 0$. □

Lemma 18 Suppose given $A \in Q^{n\times n}$ with $\chi_A(X)$ irreducible in $Q[X]$.

Let $U \subseteq Q^{1\times n}$ be a Q-linear subspace with $U \cdot A \subseteq U$.

Consider the map $\varphi : U \to U$, $x \mapsto x \cdot A$.

Write $d := \dim_Q U$. Let $F = (u_1, \ldots, u_d)$ be a Q-linear basis of U.

Let $M := {}_F\varphi_F \in Q^{d\times d}$ be the representing matrix of φ with respect to F.

Then M is diagonalizable in $\bar{Q}^{d\times d}$. Each eigenvalue of $M \in \bar{Q}^{d\times d}$ is also an eigenvalue of $A \in \bar{Q}^{n\times n}$.

Proof. Since $\chi_A(X)$ irreducible, there is no $a \in \bar{Q}$ such that $(X-a)^2$ divides $\chi_A(X)$ in $\bar{Q}[X]$; cf. Lemma 9.

Therefore, we may choose $T \in \bar{Q}^{n\times n}$ invertible such that

$$T^{-1} \cdot A \cdot T \;=\; D \;=\; \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \;\in\; \bar{Q}^{n\times n},$$

where $\lambda_i \neq \lambda_j$ for $i, j \in [1, n]$ with $i \neq j$.

Let $\bar{U} := {}_{\bar{Q}}\langle u_1, \ldots, u_d\rangle \subseteq \bar{Q}^{1\times n}$.

Since the rank of the matrix in $Q^{d\times n}$ containing the rows $u_1, \ldots, u_d$ equals d, this matrix, considered as element of $\bar{Q}^{d\times n}$, still has rank d, and therefore $F = (u_1, \ldots, u_d)$ is a $\bar{Q}$-linear basis of $\bar{U}$.

We know that $U \cdot A \subseteq U \subseteq \bar{U}$. So we have $u_i \cdot A \in \bar{U}$, for $i \in [1, d]$. And so we obtain

$$\bar{U} \cdot A \;\subseteq\; \bar{U}\,.$$

Let $\bar{V} := \bar{U} \cdot T = {}_{\bar{Q}}\langle u_1 \cdot T, \ldots, u_d \cdot T\rangle$.

Then we have

$$\begin{array}{rcccccl} \bar{V} \cdot D & = & \bar{V} \cdot T^{-1} \cdot A \cdot T & = & \bar{U} \cdot T \cdot T^{-1} \cdot A \cdot T & = & \bar{U} \cdot A \cdot T \\ & \subseteq & \bar{U} \cdot T & & = & & \bar{V}. \end{array}$$

Let $I := \{i \in [1, n] : \exists (\alpha_1, \ldots, \alpha_n) \in \bar{V} \text{ with } \alpha_i \neq 0\} \subseteq [1, n]$.

Now we show that $\bar{V} \stackrel{!}{=} {}_{\bar{Q}}\langle \mathrm{e}_i : i \in I\rangle$.

We have $\bar{V} \subseteq {}_{\bar{Q}}\langle \mathrm{e}_i : i \in I\rangle$ since given $(\alpha_1, \ldots, \alpha_n) \in \bar{V}$, we have $\alpha_j = 0$ for $j \in [1, n] \setminus I$, whence

$$(\alpha_1, \ldots, \alpha_n) \;=\; \sum_{k\in[1,n]} \alpha_k \cdot \mathrm{e}_k \;=\; \sum_{k\in I} \alpha_k \cdot \mathrm{e}_k \;\in\; {}_{\bar{Q}}\langle \mathrm{e}_i : i \in I\rangle.$$

We need to show that $\bar{V} \stackrel{!}{\supseteq} {}_{\bar{Q}}\langle \mathrm{e}_i : i \in I\rangle$.

Suppose given $i \in I$. We have to show that $\mathrm{e}_i \stackrel{!}{\in} \bar{V}$.

Since $i \in I$, we may choose $(\beta_1, \ldots, \beta_n) \in \bar{V}$ with $\beta_i \neq 0$.

Let $I' := \{i' \in [1,d] : \beta_{i'} \neq 0\}$. Then $i \in I' \subseteq I$.

We write $I' = \{i'_1, \dots, i'_\ell\}$ with $\ell := |I'|$ and $i'_1 < i'_2 < \cdots < i'_\ell$.

Then $\beta = \sum_{i' \in I'} \beta_{i'} \cdot \mathrm{e}_{i'}$.

Since $\beta \in \bar{V}$ and $\bar{V} \cdot D \subseteq \bar{V}$, we have $\beta \cdot D^t \in \bar{V}$ for $t \geqslant 0$.

For $t \geqslant 0$, we obtain

$$\beta \cdot D^t \;=\; \sum_{i' \in I'} \beta_{i'} \cdot \mathrm{e}_{i'} \cdot \begin{pmatrix} \lambda_1^t & & \\ & \ddots & \\ & & \lambda_n^t \end{pmatrix} \;=\; \sum_{i' \in I'} \beta_{i'} \cdot \mathrm{e}_{i'} \cdot \lambda_{i'}^t \;\in\; \bar{Q}\langle\, \mathrm{e}_{i'} : i' \in I' \rangle.$$

We *claim* $(\beta \cdot D^0, \dots, \beta \cdot D^{\ell-1})$ is $\bar{Q}$-linearly independent.

Suppose given $\kappa_0, \kappa_1, \dots, \kappa_{\ell-1} \in \bar{Q}$ such that

$$\sum_{t \in [0,l-1]} \kappa_t \cdot \beta \cdot D^t \;=\; \kappa_0 \cdot \beta \cdot D^0 + \kappa_1 \cdot \beta \cdot D^1 + \cdots + \kappa_{\ell-1} \cdot \beta \cdot D^{\ell-1} \;=\; 0\,.$$

We have to show that $\kappa_t \stackrel{!}{=} 0$ for $t \in [0, \ell-1]$.

We have

$$0 \;=\; \sum_{t \in [0,\ell-1]} \kappa_t \cdot \beta \cdot D^t \;=\; \sum_{t \in [0,\ell-1]} \kappa_t \cdot \sum_{i' \in I'} (\beta_{i'} \cdot \mathrm{e}_{i'} \cdot \lambda_{i'}^t) \;=\; \sum_{i' \in I'} \mathrm{e}_{i'} \cdot \beta_{i'} \cdot \sum_{t \in [0,\ell-1]} (\kappa_t \cdot \lambda_{i'}^t)\,.$$

Since $(\mathrm{e}_1, \dots, \mathrm{e}_n)$ is linearly independent, we conclude that $\beta_{i'} \cdot (\sum_{t \in [0,\ell-1]} \kappa_t \cdot \lambda_{i'}^t) = 0$ for $i' \in I'$.

Since $\beta_{i'} \neq 0$, we conclude that

$$\sum_{t \in [0,\ell-1]} \kappa_t \cdot \lambda_{i'}^t \;=\; 0$$

for $i' \in I'$.

We now consider the Vandermonde matrix $\mathrm{Vand} := (\lambda_{i'_s}^t)_{t \in [0,\ell-1],\, s \in [1,\ell]}$.

Let $\kappa := (\kappa_0, \dots, \kappa_{\ell-1})$.

Then we have $\kappa \cdot \mathrm{Vand} = 0$.

But $\det \mathrm{Vand} = \prod_{1 \leqslant r < s \leqslant \ell} (\lambda_{i'_s} - \lambda_{i'_r}) \neq 0$ since $\lambda_{i'_s} \neq \lambda_{i'_r}$ for $1 \leqslant r < s \leqslant \ell$.

Hence $\kappa = 0$.

This proves the *claim*.

For this claim, we could alternatively also have used **[3,** Ch. VI, Cor. 4.2].

We have $\bar{Q}\langle \beta \cdot D^0, \beta \cdot D^1, \dots, \beta \cdot D^{\ell-1} \rangle \subseteq \bar{Q}\langle\, \mathrm{e}_{i'} : i' \in I' \rangle$.

Both sides have dimension ℓ, since $(\beta \cdot D^0, \beta \cdot D^1, \dots, \beta \cdot D^{\ell-1})$ is $\bar{Q}$-linearly independent and since $|I'| = \ell$.

So we have $\bar{Q}\langle \beta \cdot D^0, \beta \cdot D^1, \dots, \beta \cdot D^{\ell-1} \rangle = \bar{Q}\langle\, \mathrm{e}_{i'} : i' \in I' \rangle$.

We conclude that $\mathrm{e}_i \in {}_{\bar{Q}}\langle\, \mathrm{e}_{i'} : i' \in I' \rangle = {}_{\bar{Q}}\langle \beta \cdot D^0, \beta \cdot D^1, \ldots, \beta \cdot D^{\ell-1} \rangle \subseteq \bar{V}$.

Altogether we have $\bar{V} = {}_{\bar{Q}}\langle\, \mathrm{e}_i : i \in I \rangle$.

Now we consider the diagonalizability and the eigenvalues of $M = {}_F\varphi_F$.

We write $M =: (m_{i,j})_{i,j} \in Q^{d \times d} \subseteq \bar{Q}^{d \times d}$ for $i, j \in [1, d]$. So for $i \in [1, d]$, we have

$$u_i \cdot A \;=\; u_i\varphi \;=\; \sum_{j \in [1,d]} m_{i,j} \cdot u_j \,.$$

We consider the $\bar{Q}$-linear map $\bar{\varphi} : \bar{U} \to \bar{U}$, $x \mapsto x \cdot A$.

Since $F = (u_1, \ldots, u_d)$ is also $\bar{Q}$-linear basis of $\bar{U}$ and since

$$u_i\bar{\varphi} \;=\; u_i \cdot A \;=\; \sum_{j \in [1,d]} m_{i,j} \cdot u_j$$

for $i \in [1, d]$, we have $M = {}_F\bar{\varphi}_F$.

Now $\bar{V} = {}_{\bar{Q}}\langle\, \mathrm{e}_i : i \in I \rangle$. Hence

$$\bar{U} \;=\; \bar{V} \cdot T^{-1} \;=\; {}_{\bar{Q}}\langle\, \mathrm{e}_i \cdot T^{-1} : i \in I \rangle.$$

So $(\mathrm{e}_i \cdot T^{-1} : i \in I)$ is a $\bar{Q}$-linear basis of $\bar{U}$. Moreover,

$$(\mathrm{e}_i \cdot T^{-1})\bar{\varphi} \;=\; \mathrm{e}_i \cdot T^{-1} \cdot A \;=\; \mathrm{e}_i \cdot D \cdot T^{-1} \;=\; \lambda_i \cdot \mathrm{e}_i \cdot T^{-1}$$

for $i \in I$.

Thus $\bar{U}$ has a basis consisting of eigenvectors of $\bar{\varphi}$, with eigenvalues λ_i for $i \in I$.

Hence $M = {}_F\bar{\varphi}_F$ is diagonalizable with eigenvalues λ_i for $i \in I$, which are also eigenvalues of A.

□

Theorem 19

(i) Recall that $K|Q$ is galois with Galois group $\mathrm{Gal}(K|Q)$ isomorphic to G.

There exists $A \in Q^{n \times n}$ such that K is isomorphic to $Q[A]$ as a field extension of Q, such that $A^S \cdot A = A \cdot A^S$ for $S \in \mathbb{S}$ and such that $\chi_A(X) \in Q[X]$ is irreducible.

(ii) Recall that $\mathbb{S} = \{\, S_i : \; i \in [1, m] \,\}$, where the permutation matrix S_i belongs to the generator $\rho_i \in G$; cf. Definitions 15, 16.

Suppose given $A \in Q^{n \times n}$ such that $A^S \cdot A = A \cdot A^S$ for $S \in \mathbb{S}$ and such that $\chi_A(X) \in Q[X]$ is irreducible.

Then we have $B^S \in Q[A]$ for $B \in Q[A]$ and $S \in G_{\mathrm{mat}}$; cf. Definition 15. In particular, we have the automorphism $\sigma_S : Q[A] \to Q[A] : B \mapsto B^S$ for $S \in G_{\mathrm{mat}}$.

The field extension $Q[A]|Q$ is galois with Galois group

$$\mathrm{Gal}(Q[A]|Q) \;=\; \{\, \sigma_S : \; S \in G_{\mathrm{mat}} \,\}$$

isomorphic to G.

Proof. Ad (i).

By Lemma 14 we know that the map $\delta : K \wr G \to \mathrm{End}_Q(K)$, $\xi \mapsto \xi\delta$ with $\xi\delta : K \to K$, $y \mapsto y \cdot \xi$ is a Q-algebra isomorphism.

Let B be a normal basis of $K|Q$. So B is a Q-linear basis of K of the form $B = (z^{\sigma_1}, z^{\sigma_2}, \ldots, z^{\sigma_n})$ for a suitable element $z \in K$. Cf. Proposition 3.

Then $\eta_B : \mathrm{End}_Q(K) \to Q^{n\times n}$, $f \mapsto {}_Bf_B$ is a Q-algebra isomorphism.

So $\delta \cdot \eta_B : K \wr G \longrightarrow Q^{n\times n}$ is a Q-algebra isomorphism.

We show now that $\rho_i(\delta \cdot \eta_B) \stackrel{!}{=} S_i$ for $i \in [1, m]$; cf. Definitions 15, 16.

Recall that using the bijection $\alpha_i : [1, n] \to [1, n]$ satisfying $\sigma_j \cdot \rho_i = \sigma_{j\alpha_i}$ for $j \in [1, n]$, we have $S_i = \sum_{j\in[1,n]} \mathrm{e}_{j,j\alpha_i}$; cf. Definition 15.

To calculate

$$\rho_i(\delta \cdot \eta_B) \;=\; {}_B(\rho_i\delta)_B\,,$$

we map the elements of B via $\rho_i\delta$. Given $j \in [1, n]$, we obtain

$$z^{\sigma_j}(\rho_i\delta) \;=\; z^{\sigma_j} \cdot \rho_i \;\stackrel{\text{D 13}}{=}\; (z^{\sigma_j})^{\rho_i} \;=\; z^{\sigma_j\cdot\rho_i} \;=\; z^{\sigma_{j\alpha_i}}$$

So in the j-th row, the matrix ${}_B(\rho_i\delta)_B$ has entry 1 at position $(j, j\alpha_i)$ and entry 0 elsewhere.

Thus

$${}_B(\rho_i\delta)_B \;=\; \sum_{j\in[1,n]} \mathrm{e}_{j,j\alpha_i} \;=\; S_i\,.$$

By Remark 4, we have $K = Q(z) = Q[z]$.

Let now $A := z(\delta\eta_B) \in Q^{n\times n}$.

So we have

$$K(\delta\eta_B) \;=\; Q[z](\delta\eta_B) \;=\; Q[z(\delta\eta_B)] \;=\; Q[A]\,.$$

So $\check{\delta} := (\delta \cdot \eta_B)|_K^{Q[A]}$ is a Q-algebra isomorphism.

$$\begin{array}{ccc} K \wr G & \xrightarrow[\sim]{\delta\cdot\eta_B} & Q^{n\times n} \\ \uparrow & & \uparrow \\ K & \xrightarrow[\sim]{\check{\delta}} & Q[A] \end{array}$$

Suppose given $i \in [1, m]$, we show that $A^{S_i} \cdot A \stackrel{!}{=} A \cdot A^{S_i}$.

We have

$$\begin{aligned} A^{S_i} \;&=\; S_i^{-1} \cdot A \cdot S_i \;=\; (\rho_i(\delta\eta_B))^{-1} \cdot (z(\delta\eta_B)) \cdot (\rho_i(\delta\eta_B)) \;=\; (\rho_i^{-1} \cdot z \cdot \rho_i)(\delta\eta_B) \\ &=\; (\rho_i^{-1} \cdot \rho_i \cdot z^{\rho_i})(\delta\eta_B) \;=\; z^{\rho_i}(\delta\eta_B). \end{aligned}$$

Moreover,

$$\begin{aligned} A^{S_i} \cdot A \;&=\; (z^{\rho_i}(\delta\eta_B)) \cdot (z(\delta\eta_B)) \;=\; (z^{\rho_i} \cdot z)(\delta\eta_B) \;=\; (z \cdot z^{\rho_i})(\delta\eta_B) \\ &=\; (z(\delta\eta_B)) \cdot (z^{\rho_i}(\delta\eta_B)) \;=\; A \cdot A^{S_i}. \end{aligned}$$

We show now that $\chi_A(X)$ is irreducible.

We have

$$\deg(\mu_{z,Q}(X)) \;=\; [Q(z):Q] \;=\; [K:Q] \;=\; n.$$

Since $\delta\eta_B$ is a Q-algebra isomorphism, we have

$$\mu_{z,Q}(X) \;=\; \mu_{z(\delta\eta_B)}(X) \;=\; \mu_A(X),$$

and thus the minimal polynomial $\mu_A(X)$ is irreducible and of degree n.

Now $\mu_A(X)$ divides $\chi_A(X)$. Since $A \in Q^{n\times n}$, we have $\deg(\chi_A(X)) = n$. So $\chi_A(X) = \mu_A(X)$. Thus $\chi_A(X)$ is irreducible.

Ad (ii).

First we show that $Q[A]$ is a field.

We consider the Q-algebra morphism $Q[X] \to Q^{n\times n} : X \mapsto A$. Its image is $Q[A]$. Its kernel is the ideal generated by $\mu_A(X)$.

So this morphism factors through the isomorphism

$$\begin{aligned} Q[X]/(\mu_A(X)) &\to Q[A] \\ X + (\mu_A(X)) &\mapsto A. \end{aligned}$$

Now $Q[X]/(\mu_A(X))$ is a field if $\mu_A(X)$ is irreducible.

We know that $\mu_A(X)$ divides $\chi_A(X)$ and that $\chi_A(X)$ is irreducible. Thus $\mu_A(X) = \chi_A(X)$ is irreducible.

So $Q[A]$ is a field.

Now we *claim* that $C := \{B \in Q^{n\times n} : A\cdot B = B\cdot A\} \stackrel{!}{=} Q[A]$.

We have $C \supseteq Q[A]$.

It remains to be shown that $\dim_Q C \stackrel{!}{=} \dim_Q Q[A]$.

We have

$$\dim_Q Q[A] \;=\; \deg \mu_A(X) \;=\; \deg \chi_A(X) \;=\; n.$$

So $Q[A]|Q$ is a field extension of degree $[Q[A]:Q] = n$.

Let $\bar{C} := \{B \in \bar{Q}^{n\times n} : A\cdot B = B\cdot A\}$.

We have

$$\dim_Q C \;=\; \dim_Q\{B \in Q^{n\times n} : A\cdot B = B\cdot A\} \;=\; \dim_{\bar{Q}}\{B \in \bar{Q}^{n\times n} : A\cdot B = B\cdot A\} \;=\; \dim_{\bar{Q}} \bar{C}$$

Since $\chi_A(X)$ is irreducible in $Q[X]$, we have $\chi_A(X) = (X-\lambda_1)\cdot(X-\lambda_2)\cdot\ldots\cdot(X-\lambda_n) \in \bar{Q}[X]$, where $\lambda_i \neq \lambda_j$ for $i,j \in [1,n]$ with $i \neq j$; cf. Lemma 9.

So $A \in \bar{Q}^{n\times n}$ is diagonalizable. We may choose $T \in \bar{Q}^{n\times n}$ invertible with

$$T^{-1} \cdot A \cdot T \;=\; \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \;=:\; D\,.$$

Thus

$$\begin{aligned} \bar{C} &= \{B \in \bar{Q}^{n\times n} : A \cdot B = B \cdot A\} \\ &= \{B \in \bar{Q}^{n\times n} : T \cdot D \cdot T^{-1} \cdot B = B \cdot T \cdot D \cdot T^{-1}\} \\ &= \{B \in \bar{Q}^{n\times n} : D \cdot T^{-1} \cdot B \cdot T = T^{-1} \cdot B \cdot T \cdot D\} \\ &= \{T \cdot B' \cdot T^{-1} : B' \in \bar{Q}^{n\times n}, D \cdot B' = B' \cdot D\} \end{aligned}$$

where we have substituted $B' = T^{-1} \cdot B \cdot T$.

Let $\bar{C}' := \{B' \in \bar{Q}^{n\times n} : D \cdot B' = B' \cdot D\}$.

Consider the bijective $\bar{Q}$-linear map $\theta : \bar{C}' \to \bar{C} : B' \mapsto T \cdot B' \cdot T^{-1}$.

We know that $\bar{C}'$ is the set of all diagonal matrices; cf. Lemma 17.

Thus $\dim_{\bar{Q}} \bar{C} = \dim_{\bar{Q}} \bar{C}' = n$.

So $\dim_Q C = n = \dim_Q Q[A]$.

This proves the *claim*.

In particular, since $A \cdot A^S = A^S \cdot A$, we have $A^S \in C = Q[A]$ and thus $Q[A]^S = Q[A^S] \subseteq Q[A]$ for $S \in \mathbb{S}$. Hence $Q[A]^S = Q[A]$ since $\dim_Q Q[A]$ is finite.

Since $G_{\mathrm{mat}} = \langle \mathbb{S} \rangle$, we conclude that $Q[A]^S = Q[A]$ for $S \in G_{\mathrm{mat}}$.

Now we show that $A \cdot S \neq S \cdot A$ for $S \in G_{\mathrm{mat}} \setminus \{\mathrm{I}_n\}$.

Assume that $A \cdot S = S \cdot A$.

Let $\mathrm{e}_i \cdot S = \mathrm{e}_{i\sigma}$ with $\sigma \in \mathrm{S}_n$. Write $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_z$ as a product of disjoint cycles $\sigma_1, \ldots, \sigma_z \in \mathrm{S}_n$, including cycles of length 1.

So the set $[1, n]$ is the disjoint union of the sets $\mathrm{supp}(\sigma_s)$, where $s \in [1, z]$.

Note that $1 \leqslant z \leqslant n-1$ since $\mathrm{S} \neq \mathrm{I}_n$.

We show that $U := \mathrm{E}_1(S) \stackrel{!}{=} {}_Q\langle \sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_i : s \in [1, z] \rangle$.

Suppose given $x \in \mathrm{E}_1(S)$. So $x = x \cdot S$. Write $x = \sum_{i\in[1,n]} \alpha_i \, \mathrm{e}_i$ with $\alpha_i \in Q$.

Thus

$$\sum_{i\in[1,n]} \alpha_i \, \mathrm{e}_i \;=\; (\sum_{i\in[1,n]} \alpha_i \, \mathrm{e}_i) \cdot S \;=\; \sum_{i\in[1,n]} \alpha_i \, \mathrm{e}_{i\sigma} \;=\; \sum_{j\in[1,n]} \alpha_{j\sigma^{-1}} \, \mathrm{e}_j \;=\; \sum_{i\in[1,n]} \alpha_{i\sigma^{-1}} \, \mathrm{e}_i\,.$$

So we have

$$\alpha_i \;=\; \alpha_{i\sigma^{-1}}$$

and thus

$$\alpha_{i\sigma} \;=\; \alpha_i$$

for $i \in [1, n]$.

So $\alpha_i = \alpha_j$ for $i, j \in [1, n]$ such that exists $k \geqslant 0$ with $j = i\sigma^k$, i.e. such that there exists $s \in [1, z]$ such that $i, j \in \mathrm{supp}(\sigma_s)$. Therefore $x \in {}_Q\langle \sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_i \,:\, s \in [1, z]\rangle$.

Conversely, given $s \in [1, z]$, we have

$$(\sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_i) \cdot S \;=\; \sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_{i\sigma} \;=\; \sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_{i\sigma_s} \;=\; \sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_i \,.$$

So $\sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_i \in \mathrm{E}_1(S)$.

Altogether, $U = \mathrm{E}_1(S) = {}_Q\langle \sum_{i \in \mathrm{supp}(\sigma_s)} \mathrm{e}_i : s \in [1, z]\rangle$.

In particular, we have $1 \leqslant \dim(U) = z \leqslant n - 1$. So $0 \subset U \subset Q^{1\times n}$.

Given $x \in U = \mathrm{E}_1(S)$, we have

$$(x \cdot A) \cdot S \;=\; x \cdot S \cdot A \;=\; x \cdot A.$$

Thus $U \cdot A \subseteq U$.

Consider the map $\varphi : U \to U$, $x \mapsto x \cdot A$. Let M be the representing matrix of φ with respect to some basis of U.

Then M is diagonalizable in $\bar{Q}^{z\times z}$ and each eigenvalue of $M \in \bar{Q}^{z\times z}$ is also an eigenvalue of $A \in \bar{Q}^{n\times n}$; cf. Lemma 18.

Suppose given an eigenvalue λ of $M \in \bar{Q}^{z\times z}$. Then $\chi_M(\lambda) = 0$ and $\chi_A(\lambda) = 0$. Since $\chi_A(X)$ is irreducible in $Q[X]$ and since $\mu_{\lambda,Q}(X)$ divides $\chi_A(X)$, we conclude that $\chi_A(X) = \mu_{\lambda,Q}(X)$.

Moreover, $\mu_{\lambda,Q}(X)$ divides $\chi_M(X)$. Therefore $\chi_A(X)$ divides $\chi_M(X)$.

So

$$n \;=\; \deg(\chi_A(x)) \;\leqslant\; \deg(\chi_M(X)) \;=\; \dim_Q(U) \;=\; z \;\leqslant\; n - 1.$$

We have a *contradiction*.

We consider the group morphism $\gamma'' : G_{\mathrm{mat}} \to \mathrm{Aut}(Q[A]|Q)$, $S \mapsto (B \mapsto S^{-1} \cdot B \cdot S = B^S)$.

The group morphism γ'' is injective, since if $S \in G_{\mathrm{mat}}$ is sent to the identity, we have $A = A^S$, i.e. $S \cdot A = A \cdot S$, hence $S = \mathrm{I}_n$ by the preceding claim.

We compose $G \xrightarrow[\sim]{\gamma'} G_{\mathrm{mat}}$ from Definition 15 and $G_{\mathrm{mat}} \xrightarrow{\gamma''} \mathrm{Aut}(Q[A]|Q)$ to the injective group morphism

$$\gamma \;:=\; \gamma' \cdot \gamma'' \;:\; G \;\to\; \mathrm{Aut}(Q[A]|Q) \,.$$

By Lemma 2, we obtain the Galois extension $Q[A]|\,\mathrm{Fix}_G(Q[A])$ with Galois group $G\gamma$ isomorphic to G and with

$$[Q[A] : \mathrm{Fix}_G(Q[A])] \;=\; |G| \;=\; n.$$

Since $Q \subseteq \mathrm{Fix}_G(Q[A])$ and since

$$[Q[A] : \mathrm{Fix}_G(Q[A])] \;=\; n \;=\; [Q[A] : Q],$$

we obtain $Q = \mathrm{Fix}_G(Q[A])$.

Writing $\sigma_S := S\gamma'' : Q[A] \to Q[A] : B \mapsto B^S$ for $S \in G_{\mathrm{mat}} = G\gamma'$, we obtain that the field extension $Q[A]|Q$ is galois with Galois group

$$\mathrm{Gal}(Q[A]|Q) \;=\; G\gamma \;=\; G(\gamma' \cdot \gamma'') \;=\; G_{\mathrm{mat}}\gamma'' \;=\; \{\, \sigma_S :\; S \in G_{\mathrm{mat}} \,\}$$

isomorphic to G. □

Definition 20 The subset

$$\{\, A \in \mathrm{GL}_n(Q) :\; A^S \cdot A = A \cdot A^S \text{ for } S \in \mathbb{S} \,\} \;\subseteq\; \mathrm{GL}_n(Q) \;\subseteq\; Q^{n\times n}$$

is called the *Galois variety* of G, with respect to the chosen generators $\rho_1, \ldots, \rho_m$.

So by Theorem 19, each Galois extension of Q with Galois group isomorphic to G can be found, up to isomorphism, as $Q[A]|Q$ for some A in the Galois variety of G, provided $\chi_A(X) \in Q[X]$ is irreducible.

We need the following assertion in order to deal with the Galois variety in particular cases.

Lemma 21 Suppose given $A \in Q^{n\times n}$ such that $\chi_A(X) \in Q[X]$ is irreducible.

Then the Q-linear map $\varphi : Q[A] \to Q^{1\times n}$, $B \mapsto e_1 \cdot B$ is bijective.

Proof. The minimal polynomial $\mu_A(X)$ divides $\chi_A(X)$. Hence $\mu_A(X) = \chi_A(X)$.

We conclude that $\mu_A(X)$ is irreducible and that thus $Q[A]$ is a field.

Moreover, we conclude that

$$\dim_Q Q[A] \;=\; \deg(\mu_A(X)) \;=\; \deg(\chi_A(X)) \;=\; n \;=\; \dim_Q Q^{1\times n}.$$

So it sufficient to show that φ is injective, i.e. that $\mathrm{Kern}(\varphi) \stackrel{!}{=} 0$.

Suppose given $B \in Q[A]$ such that $0 = B\varphi = \mathrm{e}_1 \cdot B$.

Then B is not invertible. Since B is an element of the field $Q[A]$, it follows that $B = 0$, as was to be shown. □

Chapter 2

Particular cases

Recall that whenever Maple is used, we have to call:

```
with(linalg):
with(epsilon):
```

The latter package is used whenever a system of polynomial equations is solved with Maple.

2.1 The cyclic group C_3

Suppose that $G = \mathrm{C}_3 = \langle \rho_1 \rangle$ and that $Q = \mathbb{Q}$.

We write $\sigma_1 := \rho_1^0 = 1_{\mathrm{C}_3}$, $\sigma_2 := \rho_1^1$ and $\sigma_3 := \rho_1^2$.

To calculate the permutation matrix $S_1 = S_{\rho_1}$, in the notation of Definition 15, we obtain the bijection $\alpha : [1,3] \to [1,3]$ with $1\alpha = 2$, $2\alpha = 3$ and $3\alpha = 1$.

So we obtain $S := S_1 = \left(\begin{smallmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{smallmatrix}\right)$. Moreover, we have $\mathbb{S} := \{S\} = \{\left(\begin{smallmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{smallmatrix}\right)\}$.

We obtain $G_{\mathrm{mat}} = \{\mathrm{I}_3, S, S^2\}$; cf. Definition 15.

We want to classify the Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to C_3.

By Theorem 19.(i), each such Galois extension is, up to isomorphism, of the form $\mathbb{Q}[A]|\mathbb{Q}$ for some $A \in \mathbb{Q}^{3\times 3}$ such that $A \cdot A^S = A^S \cdot A$, and such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible.

Conversely, by Theorem 19.(ii), each $A \in \mathbb{Q}^{3\times 3}$ such that $A \cdot A^S = A^S \cdot A$ and such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible gives rise to a Galois extension $\mathbb{Q}[A]|\mathbb{Q}$ with Galois group isomorphic to C_3.

In other words, for our classification we have to find those elements A in the Galois variety of C_3 with $\chi_A(X) \in \mathbb{Q}[X]$ irreducible.

In a first attempt, we let Maple calculate the matrix equation for $A = \left(\begin{smallmatrix} a&b&c \\ d&e&f \\ g&h&i \end{smallmatrix}\right)$.

```
A := matrix([[a,b,c],[d,e,f],[g,h,i]]);
S := matrix([[0,1,0],[0,0,1],[1,0,0]]);
IS := inverse(S);
Dif := evalm(IS&*A&*S&*A - A&*IS&*A&*S);
for k from 1 to 3 do for j from 1 to 3 do printf("%a = 0\n",Dif[k,j]); od; od;
```

Maple gives the system of equations:

```
-b*c-c*f+d*g+g*h = 0
-a*b-a*g+b*i-c*d+e*g+h^2 = 0
-a*h-b^2-c*e+c*i+f*g+h*i = 0
a*c+a*d+b*g-c*e-d*i-f^2 = 0
b*c+b*h-d*f-d*g = 0
a*f-b*e+b*i+c^2-d*h-e*f = 0
a*f-c*h+d^2+e*g-f*i-g*i = 0
-a*h+b*f+d*e-d*i+e*h-g^2 = 0
-b*h+c*f+d*f-g*h = 0
```

The task now would be to search for all solutions $A = \left(\begin{smallmatrix} a & b & c \\ d & e & f \\ g & h & i \end{smallmatrix}\right)$ of this system of equations having an irreducible characteristic polynomial.

In a second attempt, we intersect the Galois variety with the affine subspace consisting of those matrices of the form $A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \\ g & h & i \end{smallmatrix}\right)$.

We have to justify this reduction step. We have to show that this intersection is still sufficient to describe all the Galois extensions we search.

Lemma 22 Suppose given $A \in \mathbb{Q}^{3\times 3}$ such that $A \cdot A^S = A^S \cdot A$ and such that $\chi_A(X)$ is irreducible.

Then there exists $B \in \mathbb{Q}^{3\times 3}$ such that $B \cdot B^S = B^S \cdot B$, such that $\chi_B(X)$ is irreducible, such that $\mathrm{e}_1 \cdot B = \mathrm{e}_2$ and such that

$$\mathbb{Q}[A] \;=\; \mathbb{Q}[B].$$

Proof. Let B be the unique element of $\mathbb{Q}[A]$ such that $\mathrm{e}_1 \cdot B = \mathrm{e}_2$; cf. Lemma 21.

We *claim* that $\mathbb{Q}[B] \stackrel{!}{=} \mathbb{Q}[A]$.

We have $\mathbb{Q}[B] \subseteq \mathbb{Q}[A]$.

The subfields of $\mathbb{Q}[A]$ are $\mathbb{Q}[A]$ and $\mathbb{Q}$, since the subgroups of C_3 are 1 and C_3; cf. Proposition 1.

We have $B \notin \mathbb{Q} \cdot \mathrm{I}_3 = \mathbb{Q}$, since B is of the form $B = \left(\begin{smallmatrix} 0 & 1 & 0 \\ * & * & * \\ * & * & * \end{smallmatrix}\right)$.

So $\mathbb{Q}[A] = \mathbb{Q}[B]$. Thus the *claim* is shown.

Since $B \in \mathbb{Q}[A]$, we have $B^S \in \mathbb{Q}[A]$ by Theorem 19.(ii). Thus $B \cdot B^S = B^S \cdot B$ by commutativity of $\mathbb{Q}[A]$.

Finally, $\mathbb{Q}[A] = \mathbb{Q}[B]$ entails

$$\deg(\mu_B(X)) \;=\; \dim_{\mathbb{Q}} \mathbb{Q}[B] \;=\; \dim_{\mathbb{Q}} \mathbb{Q}[A] \;=\; \deg(\mu_A(X)) \;=\; \deg(\chi_A(X)) \;=\; 3$$

and thus $\chi_B(X) = \mu_B(X)$ is irreducible. □

Now we let Maple calculate the new matrix equation for $A = \begin{pmatrix} 0 & 1 & 0 \\ d & e & f \\ g & h & i \end{pmatrix}$.

```
A := matrix([[0,1,0],[d,e,f],[g,h,i]]);
S := matrix([[0,1,0],[0,0,1],[1,0,0]]);
IS := inverse(S);
Dif := evalm(IS&*A&*S&*A - A&*IS&*A&*S);
for k from 1 to 3 do for j from 1 to 3 do printf("%a = 0\n",Dif[k,j]); od; od;
```

Maple gives the system of equations:

```
d*g+g*h = 0
e*g+h^2+i = 0
f*g+h*i-1 = 0
-d*i-f^2+g = 0
-d*f-d*g+h = 0
-d*h-e*f-e+i = 0
d^2+e*g-f*i-g*i = 0
d*e-d*i+e*h-g^2+f = 0
d*f-g*h-h = 0
```

We solve this system by hand.

Now we see

$$d \cdot g + g \cdot h \;=\; g \cdot (d + h) \;=\; 0.$$

So we have two cases.

The first case is $g = 0$:

$$\begin{aligned} h^2 + i &= 0 \\ h \cdot i - 1 &= 0 \\ -d \cdot i - f^2 &= 0 \\ -d \cdot f + h &= 0 \\ -d \cdot h - e \cdot f - e + i &= 0 \\ d^2 - f \cdot i &= 0 \\ d \cdot e - d \cdot i + e \cdot h + f &= 0 \\ d \cdot f - h &= 0 \end{aligned}$$

We know that

$$-h^2 \;=\; i$$

and

$$-h^3 \;=\; 1 \;\Rightarrow\; h \;=\; -1.$$

Thus

$$i \;=\; -1.$$

We have now:

$$\begin{aligned} d - f^2 &= 0 \\ -d \cdot f - 1 &= 0 \\ d - e \cdot f - e - 1 &= 0 \\ d^2 + f &= 0 \\ d \cdot e + d - e + f &= 0. \end{aligned}$$

We see

$$-d^2 \;=\; f,$$

thus

$$d^3 \;=\; 1 \;\Rightarrow\; d \;=\; 1.$$

So we have

$$f \;=\; -1.$$

So we obtain the set of solutions $\{\begin{pmatrix} 0 & 1 & 0 \\ 1 & e & -1 \\ 0 & -1 & -1 \end{pmatrix} : e \in \mathbb{Q}\}$ in this case.

Note that this matrix has determinant 1.

The second case is $h = -d$ and $g \neq 0$:

$$\begin{aligned} e \cdot g + d^2 + i &= 0 \\ f \cdot g - d \cdot i - 1 &= 0 \\ -d \cdot i - f^2 + g &= 0 \\ -d \cdot f - d \cdot g - d &= 0 \\ d^2 - e \cdot f - e + i &= 0 \\ d^2 + e \cdot g - f \cdot i - g \cdot i &= 0 \\ -d \cdot i - g^2 + f &= 0. \end{aligned}$$

From the first and sixth equations it follows that

$$i(1 + f + g) \;=\; 0.$$

So we have two subcases.

The first subcase is $i = 0$:

$$\begin{aligned} e \cdot g + d^2 &= 0 \\ f \cdot g - 1 &= 0 \\ -f^2 + g &= 0 \\ -d \cdot f - d \cdot g - d &= 0 \\ d^2 - e \cdot f - e &= 0 \\ -g^2 + f &= 0. \end{aligned}$$

We see

$$f^2 = g.$$

So we have

$$f^3 = 1 \Rightarrow f = 1.$$

Thus

$$g = 1.$$

We have now:

$$\begin{aligned} e + d^2 &= 0 \\ -3 \cdot d &= 0 \\ d^2 - 2 \cdot e &= 0. \end{aligned}$$

So we have

$$d = 0 \Rightarrow h = 0$$

and

$$e = 0.$$

So we obtain the set of solutions $\{\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)\}$ in this subcase.

The second subcase is $1 + f + g = 0$ and $i \neq 0$:

$$\begin{aligned} e \cdot g + d^2 + i &= 0 \\ -g - g^2 - d \cdot i - 1 &= 0. \end{aligned}$$

So we have

$$d = -\frac{g^2 + g + 1}{i} \Rightarrow h = \frac{g^2 + g + 1}{i}.$$

Thus

$$e = -\frac{d^2 + i}{g} = -\frac{(g^2 + g + 1)^2 + i^3}{gi^2}.$$

So we obtain the set of solutions $\{\begin{pmatrix} 0 & 1 & 0 \\ -\frac{g^2+g+1}{i} & -\frac{(g^2+g+1)^2+i^3}{gi^2} & -g-1 \\ g & \frac{g^2+g+1}{i} & i \end{pmatrix} : g, i \in \mathbb{Q} \backslash \{0\}\}$ in this subcase.

Note that this matrix has determinant equal to 1.

So we obtain

$$\begin{aligned}\mathcal{L} &:= \{A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ d & e & f \\ g & h & i \end{smallmatrix}\right) \in \mathrm{GL}_3(\mathbb{Q}) : A^S \cdot A = A \cdot A^S\} \\ &= \{\left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & e & -1 \\ 0 & -1 & -1 \end{smallmatrix}\right) : e \in \mathbb{Q}\} \cup \{\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)\} \cup \{\begin{pmatrix} 0 & 1 & 0 \\ -\frac{g^2+g+1}{i} & -\frac{(g^2+g+1)^2+i^3}{gi^2} & -g-1 \\ g & \frac{g^2+g+1}{i} & i \end{pmatrix} : g, i \in \mathbb{Q} \setminus \{0\}\}.\end{aligned}$$

But not all matrices in this set have an irreducible characteristic polynomial. This has to be decided for each such matrix separately. In other words, for each finite extension $K|\mathbb{Q}$ with Galois group isomorphic to C_3, K is isomorphic to a field in the following set.

$$\{\mathbb{Q}[A] : A \in \mathcal{L},\, \chi_A(X) \in \mathbb{Q}[X] \text{ is irreducible}\}$$

Remark 23 For $A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{smallmatrix}\right)$, we have $\chi_A(X) = X^3 - 1$, which is reducible in $\mathbb{Q}[X]$.

Remark 24 Let $A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & e & -1 \\ 0 & -1 & -1 \end{smallmatrix}\right) \in \mathbb{Q}^{3\times 3}$, where $e \in \mathbb{Q}$. Its characteristic polynomial is

$$\chi_A(X) \;=\; X^3 - X^2(e-1) - X(e+2) - 1\,.$$

This polynomial is irreducible for $e \in \mathbb{Z}$.

Proof. If e is even, then $\chi_A(X) \equiv_2 X^3 + X^2 + 1$ is irreducible in $\mathbb{F}_2[X]$.

It e is odd, then $\chi_A(X) \equiv_2 X^3 + X + 1$ is irreducible in $\mathbb{F}_2[X]$.

So $\chi_A(X)$ is irreducible in $\mathbb{Z}[X]$, hence in $\mathbb{Q}[X]$. □

Example 25 Let $A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & -1 & -1 \end{smallmatrix}\right) \in \mathbb{Q}^{3\times 3}$. Its characteristic polynomial is

$$\chi_A(X) \;=\; X^3 + X^2 - 2X - 1\,.$$

By Remark 24, this polynomial is irreducible in $\mathbb{Q}[X]$.

Let $\tilde{A} = \left(\begin{smallmatrix} 0 & 1 & 0 \\ -3 & -10 & -2 \\ 1 & 3 & 1 \end{smallmatrix}\right) \in \mathbb{Q}^{3\times 3}$. Its characteristic polynomial is

$$\chi_{\tilde{A}}(X) \;=\; X^3 + 9X^2 - X - 1$$

We can ask Magma whether the characteristic polynomial is irreducible:

```
P<X> := PolynomialRing(Rationals());
f := X^3 + 9*X^2 - X - 1;
IsIrreducible(f);
```

Magma gives `true`. Thus the characteristic polynomial $\chi_{\tilde{A}}$ is irreducible in $\mathbb{Q}[X]$.

We can now use Magma to see if $\mathbb{Q}[A] \simeq \mathbb{Q}[\tilde{A}]$.

```
K<i> := NumberField(X^3 + 9*X^2 - X - 1);
L<j> := NumberField(X^3 + X^2 - 2*X - 1);
IsIsomorphic(K,L);
```

Magma gives:

```
true Mapping from: FldNum: K to FldNum: L
```

So $\mathbb{Q}[A] \simeq \mathbb{Q}[\tilde{A}]$.

Note that $\mathbb{Q}[A] \neq \mathbb{Q}[\tilde{A}]$ as subalgebras of $\mathbb{Q}^{3\times 3}$:

Assume that $\mathbb{Q}[A] = \mathbb{Q}[\tilde{A}]$. Then $A, \tilde{A} \in \mathbb{Q}[A]$ and

$$\mathrm{e}_1 A \;=\; (0\,1\,0) \;=\; \mathrm{e}_1 \tilde{A},$$

thus, by Lemma 21, $A = \tilde{A}$. But $A \neq \tilde{A}$. So we have a *contradiction*.

Finally, we verify with Magma that the Galois group of our extension is isomorphic to C_3.

```
K<i> := NumberField(X^3 + 9*X^2 - X - 1);
G,d,data := GaloisGroup(K);
GaloisProof(X^3 + 9*X^2 - X - 1,data);
G;
```

Magma gives `true` and

```
Permutation group acting on a set of cardinality 3
Order = 3
```

Example 26 Putting $e := -1/2$, we obtain $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1/2 & -1 \\ 0 & -1 & -1 \end{pmatrix} \in \mathcal{L}$, having the characteristic polynomial

$$\chi_A(X) \;=\; X^3 + \tfrac{3}{2}X^2 - \tfrac{3}{2}X - 1 \;=\; (X+2)(X+\tfrac{1}{2})(X-1).$$

So the characteristic polynomial of A is reducible.

This factorisation also shows that it coincides with the minimal polynomial of A. Thus $\mathbb{Q}[A]$ is not a field. In fact,

$$\mathbb{Q}[A] \;\simeq\; \mathbb{Q}[X]/((X+2)(X+\tfrac{1}{2})(X-1)) \;\simeq\; \mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}$$

by the Chinese Remainder Theorem.

So this example shows that the condition on the characteristic polynomial to be irreducible in $\mathbb{Q}[X]$ cannot be omitted.

Example 27 Let $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1/2 & -1 \\ 0 & -1 & -1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$. Its characteristic polynomial is

$$\chi_A(X) \;=\; X^3 + \tfrac{1}{2}X^2 - \tfrac{5}{2}X - 1\,.$$

Maple gives that this characteristic polynomial is irreducible in $\mathbb{Q}[X]$:

```
A := matrix([[0,1,0],[1,1/2,-1],[0,-1,-1]]);
factor(charpoly(A,X));
```

This gives the factorisation `X^3+1/2*X^2-5/2*X-1`.

As in Example 25, one can verify with Magma that $\mathbb{Q}[A]|\mathbb{Q}$ is galois with Galois group isomorphic to C_3.

Example 28 Let $A = \left(\begin{smallmatrix} 0 & 1 & 0 \\ -7 & -2 & -3 \\ 2 & 5 & 1 \end{smallmatrix}\right) \in \mathbb{Q}^{3\times 3}$. Its characteristic polynomial is

$$\chi_A(X) \;=\; X^3 + 24X^2 + 3X - 1\,.$$

In $\mathbb{F}_2[X]$ the characteristic polynomial $\chi_A(X) \equiv_2 X^3+X+1$ is irreducible. Thus $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible.

As in Example 25, one can verify with Magma that $\mathbb{Q}[A]|\mathbb{Q}$ is galois with Galois group isomorphic to C_3.

2.2 The cyclic group C_4

Suppose that $G = \mathrm{C}_4 = \langle \rho_1 \rangle$ and $Q = \mathbb{Q}$.

We write $\sigma_1 := \rho_1^0 = 1_{\mathrm{C}_4}$, $\sigma_2 := \rho_1^1$, $\sigma_3 := \rho_1^2$ and $\sigma_4 := \rho_1^3$.

To calculate the permutation matrix $S_1 = S_{\rho_1}$, in the notation of Definition 15, we obtain the bijection $\alpha : [1,4] \to [1,4]$ with $1\alpha = 2$, $2\alpha = 3$, $3\alpha = 4$ and $4\alpha = 1$.

So we obtain $S := S_1 = \left(\begin{smallmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{smallmatrix}\right)$. Moreover, we have $\mathbb{S} := \{S\} = \{\left(\begin{smallmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{smallmatrix}\right)\}$.

We obtain $G_{\mathrm{mat}} = \{\mathrm{I}_4, S, S^2, S^3\}$; cf. Definition 15.

We want to classify the Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to C_4.

By Theorem 19.(i), each such Galois extension is, up to isomorphism, of the form $\mathbb{Q}[A]|\mathbb{Q}$ for some $A \in \mathbb{Q}^{4\times 4}$ such that $A \cdot A^S = A^S \cdot A$, and such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible.

Conversely, by Theorem 19.(ii), each $A \in \mathbb{Q}^{4\times 4}$ such that $A \cdot A^S = A^S \cdot A$ and such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible gives rise to a Galois extension $\mathbb{Q}[A]|\mathbb{Q}$ with Galois group isomorphic to C_4.

In other words, for our classification we have to find those elements A in the Galois variety of C_4 with $\chi_A(X) \in \mathbb{Q}[X]$ irreducible.

2.2.1 A reduction step by intersection

We intersect the Galois variety of C_4 with the affine subspace consisting of those matrices of the form $\left(\begin{smallmatrix} 0&1&0&0 \\ *&*&*&* \\ *&*&*&* \\ *&*&*&* \end{smallmatrix}\right)$.

We have to show that this intersection is still sufficient to describe all the Galois extensions we search.

Lemma 29 Suppose given $A \in \mathbb{Q}^{4\times 4}$ such that $A \cdot A^S = A^S \cdot A$ and such that $\chi_A(X)$ is irreducible.

Then there exists $B \in \mathbb{Q}^{4\times 4}$ such that $B \cdot B^S = B^S \cdot B$, such that $\chi_B(X)$ is irreducible, such that $\mathrm{e}_1 \cdot B = \mathrm{e}_2$ and such that

$$\mathbb{Q}[A] \;=\; \mathbb{Q}[B].$$

Proof. Note that for A, we are in the situation of Theorem 19.(ii).

By Lemma 21, there exists a unique $B \in \mathbb{Q}[A]$ such that $\mathrm{e}_1 \cdot B = \mathrm{e}_2$.

We want to show that $\mathbb{Q}[A] \stackrel{!}{=} \mathbb{Q}[B]$.

We have $\mathbb{Q}[B] \subseteq \mathbb{Q}[A]$.

Assume that $\mathbb{Q}[B] \subset \mathbb{Q}[A]$.

The subfields of $\mathbb{Q}[A]$ are $\mathbb{Q}[A]$, $L := \{C \in \mathbb{Q}[A] : C^{S^2} = C\}$ and $\mathbb{Q}$, since the subgroups of C_4 are C_4, C_2 and 1, cf. Proposition 1.

We have $B \notin \mathbb{Q} \cdot \mathrm{I}_4 = \mathbb{Q}$, since B is of the form $B = \begin{pmatrix} 0&1&0&0 \\ *&*&*&* \\ *&*&*&* \\ *&*&*&* \end{pmatrix}$.

So $\mathbb{Q} \subset \mathbb{Q}[B] \subset \mathbb{Q}[A]$, and thus $\mathbb{Q}[B] = L$. Thus $B = B^{S^2}$ and $\dim_{\mathbb{Q}}(\mathbb{Q}[B]) = 2$ with irreducible minimal polynomial $\mu_B(X) \in \mathbb{Q}[X]$ of degree 2.

Writing $B = \begin{pmatrix} 0&1&0&0 \\ e&f&g&h \\ i&j&k&l \\ m&n&p&q \end{pmatrix} \in \mathbb{Q}^{4\times 4}$, we obtain $B^{S^2} = \begin{pmatrix} k&l&i&j \\ p&q&m&n \\ 0&0&0&1 \\ g&h&e&f \end{pmatrix}$

Comparing B and B^{S^2} gives $B = \begin{pmatrix} 0&1&0&0 \\ e&f&g&h \\ 0&0&0&1 \\ g&h&e&f \end{pmatrix}$.

We have the surjective trace map $\mathrm{Tr}_{\mathbb{Q}[A]|\mathbb{Q}[B]} : \mathbb{Q}[A] \to \mathbb{Q}[B] : C \mapsto C + C^{S^2}$.

In particular, the inverse image of B under this $\mathbb{Q}$-linear map is an affine subspace of $\mathbb{Q}[A]$ of dimension 2.

We calculate the intersection of this inverse image with $\mathbb{Q}[B]$.

Let $C \in \mathbb{Q}[B]$ be such that $\mathrm{Tr}_{\mathbb{Q}[A]|\mathbb{Q}[B]}(C) = B$.

Then

$$B \;=\; \mathrm{Tr}_{\mathbb{Q}[A]|\mathbb{Q}[B]}(C) \;=\; C + C^{S^2} \;=\; C + C,$$

and thus $C = \frac{1}{2}B$. So this intersection equals $\{\frac{1}{2}B\}$. Therefore, there exists $\tilde{A} \in \mathbb{Q}[A] \setminus \mathbb{Q}[B]$ with $\tilde{A} + \tilde{A}^{S^2} = B$.

Now we invoke the condition $B \cdot B^S = B^S \cdot B$ using Maple.

```
B := matrix([[0,1,0,0],[e,f,g,h],[0,0,0,1],[g,h,e,f]]);
S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
IS := inverse(S);
Dif := evalm(IS &* B &* S &* B - B &* IS &* B &* S);
for a from 1 to 4 do for c from 1 to 4 do printf("%a = 0\n",Dif[a,c]); od; od;
```

Maple gives the system of equations:

```
2*g*e = 0
e*h+f*g+f = 0
e^2+g^2-1 = 0
e*f+g*h+h = 0
```

We distinguish two cases.

Case 1: $g = 0$.

```
e*h+f = 0
e^2-1 = 0
e*f+h = 0
```

We distinguish two subcases.

Subcase 1.1: $e = 1$.

```
h+f = 0
```

Thus we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & f & 0 & -f \\ 0 & 0 & 0 & 1 \\ 0 & -f & 1 & f \end{pmatrix}$ for $f \in \mathbb{Q}$.

We know that I_4, B and B^2 are linearly dependent.

We get the matrices $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & f & 0 & -f \\ 0 & 0 & 0 & 1 \\ 0 & -f & 1 & f \end{pmatrix}$, $B^2 = \begin{pmatrix} 1 & f & 0 & -f \\ f & 2f^2+1 & -f & -2f^2 \\ 0 & -f & 1 & f \\ -f & -2f^2 & f & 2f^2+1 \end{pmatrix}$ and $\mathrm{I}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

We conclude that $f = 0$.

So we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Hence B has reducible minimal polynomial

$$\mu_B(X) \;=\; X^2 - 1 \;=\; (X-1)\cdot(X+1).$$

We have a *contradiction* in this Subcase.

Subcase 1.2: $e = -1$.

```
-h+f = 0
```

Thus we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & f & 0 & f \\ 0 & 0 & 0 & 1 \\ 0 & f & -1 & f \end{pmatrix}$ for $f \in \mathbb{Q}$.

We know that I_4, B and B^2 are linearly dependent.

We get the matrices $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & f & 0 & f \\ 0 & 0 & 0 & 1 \\ 0 & f & -1 & f \end{pmatrix}$, $B^2 = \begin{pmatrix} -1 & f & 0 & f \\ -f & 2f^2-1 & -f & 2f^2 \\ 0 & f & -1 & f \\ -f & 2f^2 & -f & 2f^2-1 \end{pmatrix}$ and $\mathrm{I}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

We conclude that $f = 0$.

So we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$. Hence B has irreducible minimal polynomial

$$\mu_B(X) \;=\; X^2 + 1 \;\in\; \mathbb{Q}[X]\,.$$

We shall continue to consider this Subcase below.

Case 2: $e = 0$.

```
f*g+f = 0
g^2-1 = 0
g*h+h = 0
```

We distinguish two subcases.

Subcase 2.1: $g = 1$.

```
2*f = 0
2*h = 0
```

Thus we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

We know that I_4, B and B^2 are linearly dependent.

We get the matrices $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$, $B^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ and $\mathrm{I}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

But I_4, B and B^2 are linearly independent. We have a *contradiction* in this Subcase.

Subcase 2.2: $g = -1$. Our system of equations reduces to `0 = 0`.

Thus we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix}$, where $f, h \in \mathbb{Q}$.

We know that I_4, B and B^2 are linearly dependent.

We get the matrices $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix}$, $B^2 = \begin{pmatrix} 0 & f & -1 & h \\ -h & f^2{+}h^2 & -f & 2fh{-}1 \\ -1 & h & 0 & f \\ -f & 2fh{-}1 & -h & f^2{+}h^2 \end{pmatrix}$ and $\mathrm{I}_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

But I_4, B and B^2 are linearly independent. We have a *contradiction* in this Subcase.

Thus we only have to derive a contradiction in Subcase 1.2, where we have $B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

Now we search all $\tilde{A} =: \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & p & q \end{pmatrix} \in \mathbb{Q}[A] \setminus \mathbb{Q}[B]$ such that $B = \tilde{A} + \tilde{A}^{S^2}$ with Maple. We know that such a matrix $\tilde{A}$ exists by the trace argument above. Since $\tilde{A} \notin \mathbb{Q}[B]$, we have $\mathbb{Q}[\tilde{A}] = \mathbb{Q}[A]$. In particular,

$$\deg(\mu_{\tilde{A}}(X)) \;=\; \dim_{\mathbb{Q}} \mathbb{Q}[\tilde{A}] \;=\; \dim_{\mathbb{Q}} \mathbb{Q}[A] \;=\; \deg(\mu_A(X)) \;=\; \deg(\chi_A(X)) \;=\; 4$$

and thus $\chi_{\tilde{A}}(X) = \mu_{\tilde{A}}(X)$ is irreducible.

```
AA := matrix([[a,b,c,d],[e,f,g,h],[i,j,k,l],[m,n,p,q]]);
B := matrix([[0,1,0,0],[-1,0,0,0],[0,0,0,1],[0,0,-1,0]]);
S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
IS := inverse(S);
Dif := evalm(AA + IS^2 &* AA &* S^2 - B);
for r from 1 to 4 do for w from 1 to 4 do printf("%a = 0\n",Dif[r,w]); od; od;
```

Maple gives the system of equations:

```
a+k = 0
b+l-1 = 0
c+i = 0
d+j = 0
e+p+1 = 0
f+q = 0
g+m = 0
h+n = 0
```

Thus we have $\tilde{A} = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ -c & -d & -a & 1-b \\ -g & -h & -1-e & -f \end{pmatrix}$.

Since $\tilde{A}$, $\tilde{A}^S \in \mathbb{Q}[A]$, we have $\tilde{A}^S \cdot \tilde{A} - \tilde{A} \cdot \tilde{A}^S = 0$, which we want to use now:

```
AA := matrix([[a,b,c,d],[e,f,g,h],[-c,-d,-a,1-b],[-g,-h,-1-e,-f]]);
S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
IS := inverse(S);
Dif := simplify(evalm(IS &* AA &* S &* AA - AA &* IS &* AA &* S));
for r from 1 to 4 do for w from 1 to 4 do printf("%a = 0\n",Dif[r,w]); od; od;
```

Maple gives the system of equations:

```
-d+g = 0
(d+e+1)*h+(-b+g)*a-f*b+c*(d-e)-g*f = 0
2*a*h-b^2-2*c*f+d^2+e^2-g^2+2*e+1 = 0
(d+e+1)*a+(-d+e+1)*f+(b-g-1)*h-c*(b+g) = 0
(b-g-1)*h+(d+e)*a-b*c-c*g-f*(d-e) = 0
(d-e-1)*c+(-b+g)*a-f*b+h*d+e*h-g*f = 0
2*a*h-b^2-2*c*f+d^2+e^2-g^2+b+e = 0
2*a*h-b^2-2*c*f+d^2+e^2-g^2+2*b-1 = 0
(-b-g+1)*c+(d+e)*a+h*b-f*d+e*f-g*h = 0
(-b+g+1)*a+(d-e-1)*c+(-b-g+1)*f+h*(d+e) = 0
(-b+g+1)*a+(-b-g+1)*f+(d+e+1)*h+c*(d-e) = 0
2*a*h-b^2-2*c*f+d^2+e^2-g^2+b+e = 0
(d+e+1)*a+(-b-g+1)*c+(-d+e+1)*f+h*(b-g) = 0
```

We see $d = g$.

```
AA := matrix([[a,b,c,d],[e,f,d,h],[-c,-d,-a,1-b],[-d,-h,-1-e,-f]]);
S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
IS := inverse(S);
Dif := simplify(evalm(IS &* AA &* S &* AA - AA &* IS &* AA &* S));
for r from 1 to 4 do for w from 1 to 4 do printf("%a = 0\n",Dif[r,w]); od; od;
```

Maple gives the system of equations:

```
(a+c-f+h)*d+(e+1)*h-b*a-f*b-c*e = 0
2*a*h-b^2-2*c*f+e^2+2*e+1 = 0
(a-c-f-h)*d+(e+1)*a+(e+1)*f+(b-1)*h-b*c = 0
(a-c-f-h)*d+(b-1)*h+a*e-b*c+e*f = 0
(a+c-f+h)*d+c*(-1-e)-b*a-f*b+e*h = 0
2*a*h-b^2-2*c*f+e^2+b+e = 0
2*a*h-b^2-2*c*f+e^2+2*b-1 = 0
(a-c-f-h)*d+(1-b)*c+a*e+h*b+e*f = 0
(a+c-f+h)*d+(1-b)*a+c*(-1-e)+f*(1-b)+e*h = 0
(a+c-f+h)*d+(1-b)*a+f*(1-b)+(e+1)*h-c*e = 0
(a-c-f-h)*d+(e+1)*a+(1-b)*c+(e+1)*f+h*b = 0
```

Now we can equate the equations:

```
2*a*h-b^2-2*c*f+e^2+2*e+1    = 0
2*a*h-b^2-2*c*f+e^2+b+e      = 0
```

Then we get $2e + 1 = b + e$.

Thus $e = b - 1$.

```
AA := matrix([[a,b,c,d],[b-1,f,d,h],[-c,-d,-a,1-b],[-d,-h,-b,-f]]);
S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
IS := inverse(S);
Dif := simplify(evalm(IS &* AA &* S &* AA - AA &* IS &* AA &* S));
for r from 1 to 4 do for w from 1 to 4 do printf("%a = 0\n",Dif[r,w]); od; od;
```

Maple gives the system of equations:

```
(-a-c-f+h)*b+(a+c-f+h)*d+c = 0
2*a*h-2*c*f = 0
(a-c+f+h)*b+(a-c-f-h)*d-h = 0
(a-c+f+h)*b+(a-c-f-h)*d-a-f-h = 0
(-a-c-f+h)*b+(a+c-f+h)*d-h = 0
(a-c+f+h)*b+(a-c-f-h)*d-a+c-f = 0
(-a-c-f+h)*b+(a+c-f+h)*d+a+f-h = 0
(-a-c-f+h)*b+(a+c-f+h)*d+a+c+f = 0
(a-c+f+h)*b+(a-c-f-h)*d+c = 0
```

We can equate three equations:

```
(-a-c-f+h)*b+(a+c-f+h)*d+c     = 0
(-a-c-f+h)*b+(a+c-f+h)*d+a+f-h = 0
(-a-c-f+h)*b+(a+c-f+h)*d+a+c+f = 0
```

Then we get $c = a + f - h = a + c + f$.

So we have $-a = f$ and $-c = h$.

```
AA := matrix([[a,b,c,d],[b-1,-a,d,-c],[-c,-d,-a,1-b],[-d,c,-b,a]]);
S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
IS := inverse(S);
Dif := simplify(evalm(IS &* AA &* S &* AA - AA &* IS &* AA &* S));
for r from 1 to 4 do for w from 1 to 4 do printf("%a = 0\n",Dif[r,w]); od; od;
```

Maple gives the system of equations:

```
2*a*d-2*b*c+c = 0.
```

We distinguish two cases.

Case 1: $a \neq 0$.

We have $d = \frac{c(2b-1)}{2a}$ and the matrix

$$\tilde{A} = \begin{pmatrix} a & b & c & \frac{c(2b-1)}{2a} \\ b-1 & -a & \frac{c(2b-1)}{2a} & -c \\ -c & -\frac{c(2b-1)}{2a} & -a & 1-b \\ -\frac{c(2b-1)}{2a} & c & -b & a \end{pmatrix}$$

for $a \in \mathbb{Q} \setminus \{0\}$, $b, c \in \mathbb{Q}$.

Now we factor the characteristic polynomial of $\tilde{A}$ with Maple.

```
AA := matrix([[a,b,c,c*(2*b-1)/(2*a)],[b-1,-a,c*(2*b-1)/(2*a),-c],
[-c,-c*(2*b-1)/(2*a),-a,1-b],[-c*(2*b-1)/(2*a),c,-b,a]]);
factor(16*a^4*charpoly(AA,X));
```

```
(4*X^2*a^2-4*a^4-4*a^2*b^2+4*a^2*c^2+4*b^2*c^2+4*a^2*b-4*b*c^2+c^2)^2
```

We see that the characteristic polynomial is reducible. We have a *contradiction* in this Case.

Case 2: $a = 0$.

We have $c \cdot (1 - 2 \cdot b) = 0$. Thus we distinguish two subcases.

Subcase 2.1: $c = 0$.

We have $\tilde{A} = \begin{pmatrix} 0 & b & 0 & d \\ b-1 & 0 & d & 0 \\ 0 & -d & 0 & 1-b \\ -d & 0 & -b & 0 \end{pmatrix}$ for $b, d \in \mathbb{Q}$.

We factor the characteristic polynomial of $\tilde{A}$ with Maple.

```
AA := matrix([[0,b,0,d],[b-1,0,d,0],[0,-d,0,1-b],[-d,0,-b,0]]);
factor(charpoly(AA,X));

(X^2-b^2+d^2+b)^2
```

We see that the characteristic polynomial is reducible. We have a *contradiction* in this Subcase.

Subcase 2.2: $b = 1/2$.

we have $\tilde{A} = \begin{pmatrix} 0 & 1/2 & c & d \\ -1/2 & 0 & d & -c \\ -c & -d & 0 & 1/2 \\ -d & c & -1/2 & 0 \end{pmatrix}$ for $c, d \in \mathbb{Q}$.

We factor the characteristic polynomial of $\tilde{A}$ with Maple.

```
AA := matrix([[0,1/2,c,d],[-1/2,0,d,-c],[-c,-d,0,1/2],[-d,c,-1/2,0]]);
factor(charpoly(AA,X));

1/16*(4*X^2+4*c^2+4*d^2+1)^2
```

We see that the characteristic polynomial is reducible. We have a *contradiction* in this Subcase.

Thus we have obtained a contradiction in each Case or Subcase.

Thus $\mathbb{Q}[B] = \mathbb{Q}[A]$.

Since $B \in \mathbb{Q}[A]$, we have $B^S \in \mathbb{Q}[A]$ by Theorem 19.(ii). Thus $B \cdot B^S = B^S \cdot B$ by commutativity of $\mathbb{Q}[A]$.

Finally, $\mathbb{Q}[A] = \mathbb{Q}[B]$ entails

$$\deg(\mu_B(X)) \;=\; \dim_{\mathbb{Q}} \mathbb{Q}[B] \;=\; \dim_{\mathbb{Q}} \mathbb{Q}[A] \;=\; 4$$

and thus $\chi_B(X) = \mu_B(X)$ is irreducible. □

So Theorem 19 together with Lemma 29 gives the following.

Lemma 30

(i) Suppose that $K|\mathbb{Q}$ is galois with Galois group isomorphic to C_4.

There exists $A \in \mathbb{Q}^{4\times 4}$ such that K is isomorphic to $\mathbb{Q}[A]$ as a field extension of $\mathbb{Q}$, such that $A^S \cdot A = A \cdot A^S$, such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible and such that $\mathrm{e}_1 \cdot A = \mathrm{e}_2$.

(ii) Suppose given $A \in \mathbb{Q}^{4\times 4}$ such that $\mathrm{e}_1 \cdot A = \mathrm{e}_2$, such that $A^S \cdot A = A \cdot A^S$ and such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible.

Then the field extension $\mathbb{Q}[A]|\mathbb{Q}$ is galois with Galois group $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q})$ isomorphic to C_4.

2.2.2 Using function fields to search for a subset of solutions

Consider the set of solutions

$$\mathcal{L} \;:=\; \{A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ i & j & k & l \\ m & n & p & q \end{pmatrix} \in \mathrm{GL}_4(\mathbb{Q}) :\; A^S \cdot A = A \cdot A^S\}.$$

We let Maple calculate the matrix equation $A^S \cdot A = A \cdot A^S$ for $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ i & j & k & l \\ m & n & p & q \end{pmatrix} \in \mathrm{GL}_4(\mathbb{Q})$.

We use the following procedure.

```
mat_eq := proc(A)
 local S,IS,Dif,b,c;
 with(linalg):
 S := matrix([[0,1,0,0],[0,0,1,0],[0,0,0,1],[1,0,0,0]]);
 IS := inverse(S);
 Dif := evalm(IS&*A&*S&*A - A&*IS&*A&*S);
 for b from 1 to 4 do
  for c from 1 to 4 do
   if not Dif[b,c] = 0 then
    printf("%a = 0\n",Dif[b,c]);
   end if;
  od;
 od;
end proc;
```

We apply it as follows.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[i,j,k,l],[m,n,p,q]]));
```

Maple gives the system of equations:

```
e*m+i*n+m*p = 0
f*m+j*n+n*p+q = 0
g*m+k*n+p^2-1 = 0
h*m+l*n+p*q = 0
-e*q-g*h-h*l+i = 0
-e*g-e*m-h*i+j = 0
-e*n-f*g-h*j-f+k = 0
-e*p-g^2-h*k+l = 0
e^2+f*i+g*m-h*k-i*q-l^2 = 0
e*f-e*k+f*j+g*n-i*l-i*m+h = 0
e*g+g*p-i*n-j*l-j = 0
e*h+f*l-g*k+g*q-i*p-k*l = 0
e*i-h*p+i*j+k*m-l*q-m*q = 0
-e*p+f*i-i*q+j^2+k*n-m^2+l = 0
-f*p+g*i+j*k-j*q+k*p-m*n-n = 0
-g*p+h*i+j*l-m*p = 0
```

Using Magma, we find a subset of the set of solutions $\mathcal{L}$ in the following way. Since Magma produces a triangular decomposition of an ideal only in the case of Krull dimension zero of the factor algebra, we have to pass to a function field in some of our variables as ground field. This will produce a subset $\mathcal{L}'$ of our set of solutions $\mathcal{L}$, as we will verify independently at the end.

```
K<e,i,m> := FunctionField(Rationals(),3);
R< k, l, n, p, q, f, g, h, j > := PolynomialRing(K, 9);
I := ideal<R |
e*m+i*n+m*p,
f*m+j*n+n*p+q,
g*m+k*n+p^2-1,
h*m+l*n+p*q,
-e*q-g*h-h*l+i,
-e*g-e*m-h*i+j,
-e*n-f*g-h*j-f+k,
-e*p-g^2-h*k+l,
e^2+f*i+g*m-h*k-i*q-l^2,
e*f-e*k+f*j+g*n-i*l-i*m+h,
e*g+g*p-i*n-j*l-j,
e*h+f*l-g*k+g*q-i*p-k*l,
e*i-h*p+i*j+k*m-l*q-m*q,
-e*p+f*i-i*q+j^2+k*n-m^2+l,
-f*p+g*i+j*k-j*q+k*p-m*n-n,
-g*p+h*i+j*l-m*p
>;
TriangularDecomposition(I);
```

Magma gives the solution:

```
Ideal of Polynomial ring of rank 9 over Multivariate rational function
field of rank 3 over Rational Field
Order: Lexicographical
Variables: k, l, n, p, q, f, g, h, j
Inhomogeneous, Dimension 0
Groebner basis:
[
  k + (-e^2 - m^2 - 2*m - 1)/(e^2*i)*j^2 +
  (-e^3 + e*m^2 - e - 2*i^2*m - 2*i^2)/(e^2*i)*j +
  (e*i*m - e*i - i^3)/e^2,
  l + (m + 1)/e*j + (e + i^2)/e,
  n - m/i*j,
  p + j + e,
  q + (m^2 + m)/(e*i)*j + i*m/e,
  f + (-e^2 - m - 1)/(e*i)*j - i/e,
  g + (-m - 1)/e*j + (e*m - i^2)/e,
  h + m/i*j + i,
```

```
  j^3 + (e^3*m + e^2*i^2 - e*m^3 + e*m + 2*i^2*m^2 + 2*i^2*m)/
  (e^2*m + m^3 + 2*m^2 + m)*j^2 + (2*e^3*i^2 + 2*e*i^2*m + i^4*m)/
  (e^2*m + m^3 + 2*m^2 + m)*j +
  (e^4*i^2 - e^2*i^2*m^2 - e^2*i^2 + e*i^4*m)/(e^2*m + m^3 + 2*m^2 + m)
]
```

If $e \neq 0$ and $i \neq 0$ and $e^2m + m^3 + 2m^2 + m \neq 0$, this can be used to find solutions to our original system of equations over $\mathbb{Q}$.

Note that

$$e^2m + m^3 + 2m^2 + m \;\; = \;\; m(e^2 + (m+1)^2)$$

is zero if and only if $m = 0$.

So we should consider the case $e = 0$, the case $i = 0$ and the case $m = 0$ separately.

We have four cases, which may overlap.

Case 1: $e \neq 0$ and $i \neq 0$ and $m \neq 0$.

Let

$$N_{e,i,m} \;\; := \;\; \{t \in \mathbb{Q} : \; t^3 + \tfrac{e(e^2m+ei^2-m^3+m)+2i^2m(m+1)}{m(e^2+(m+1)^2)}t^2 + \tfrac{i^2(2e^3+2em+i^2m)}{m(e^2+(m+1)^2)}t + \tfrac{i^2e(e^3-em^2-e+i^2m)}{m(e^2+(m+1)^2)} = 0\}.$$

Our triangular system yields, for $j \in N_{e,i,m}$,

$$A \;\; = \;\; \tfrac{1}{e^2i}\begin{pmatrix} 0 & e^2i & 0 & 0 \\ e^3i & (e^2+m+1)ej+ei^2 & (m+1)eij+(i^2-em)ei & -e^2mj-e^2i^2 \\ e^2i^2 & je^2i & (e^2+(m+1)^2)j^2+(e^3+(1-m^2)e+2i^2(m+1))j+(i^2+(1-m)e)i^2 & -(m+1)eij-(e+i^2)ei \\ e^2im & e^2mj & (-j-e)e^2i & -(m(m+1))ej-ei^2m \end{pmatrix} .$$

For $j \in N_{e,i,m}$, we use Magma to calculate the determinant.

```
K<e,i,m> := FunctionField(Rationals(),3);
P<X> := PolynomialRing(K);
L<j> := quo< P |
X^3+(e^3*m+e^2*i^2-e*m^3+e*m+2*i^2*m^2+2*i^2*m)/(e^2*m+m^3+2*m^2+m)*X^2
                    +(2*e^3*i^2+2*e*i^2*m+i^4*m)/(e^2*m+m^3+2*m^2+m)*X
         +(e^4*i^2-e^2*i^2*m^2-e^2*i^2+e*i^4*m)/(e^2*m+m^3+2*m^2+m)>;
A := RMatrixSpace(L,4,4)!Matrix([
[0,1,0,0],
[e,(e^2+m+1)/(e*i)*j+i/e,(m+1)/e*j-(e*m-i^2)/e,-m/i*j-i],
[i,j,(e^2+m^2+2*m+1)/(e^2*i)*j^2+(e^3-e*m^2+e+2*i^2*m+2*i^2)/(e^2*i)*j
                                +(-e*i*m+e*i+i^3)/e^2,-(m+1)/e*j-(e+i^2)/e],
[m,m/i*j,-j-e,-(m^2+m)/(e*i)*j-i*m/e]]);
Determinant(A);
```

This yields $\det(A) = 1$.

Thus

$$\{\tfrac{1}{e^2i}\begin{pmatrix} 0 & e^2i & 0 & 0 \\ e^3i & (e^2+m+1)ej+ei^2 & (m+1)eij+(i^2-em)ei & -e^2mj-e^2i^2 \\ e^2i^2 & je^2i & (e^2+(m+1)^2)j^2+(e^3+(1-m^2)e+2i^2(m+1))j+(i^2+(1-m)e)i^2 & -(m+1)eij-(e+i^2)ei \\ e^2im & e^2mj & (-j-e)e^2i & -(m(m+1))ej-ei^2m \end{pmatrix} :$$

$$e, i, m \in \mathbb{Q} \setminus \{0\},\, j \in N_{e,i,m}\} \;\; \subseteq \;\; \mathcal{L} \, .$$

Case 2: $e = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ i & j & k & l \\ m & n & p & q \end{pmatrix}$.

We let Maple calculate the new matrix equation:

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[i,j,k,l],[m,n,p,q]]));
```

Maple gives the system of equations:

```
i*n+m*p = 0
f*m+j*n+n*p+q = 0
g*m+k*n+p^2-1 = 0
h*m+l*n+p*q = 0
-g*h-h*l+i = 0
-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
f*i+g*m-h*k-i*q-l^2 = 0
f*j+g*n-i*l-i*m+h = 0
g*p-i*n-j*l-j = 0
f*l-g*k+g*q-i*p-k*l = 0
-h*p+i*j+k*m-l*q-m*q = 0
f*i-i*q+j^2+k*n-m^2+l = 0
-f*p+g*i+j*k-j*q+k*p-m*n-n = 0
-g*p+h*i+j*l-m*p = 0
```

We use again Magma to find a subset of the set of solutions.

```
K<i,m> := FunctionField(Rationals(),2);
R< k, l, n, p, q, f, g, h, j > := PolynomialRing(K, 9);
I := ideal<R |
i*n+m*p,
f*m+j*n+n*p+q,
g*m+k*n+p^2-1,
h*m+l*n+p*q,
-g*h-h*l+i,
-h*i+j,
-f*g-h*j-f+k,
-g^2-h*k+l,
f*i+g*m-h*k-i*q-l^2,
f*j+g*n-i*l-i*m+h,
g*p-i*n-j*l-j,
f*l-g*k+g*q-i*p-k*l,
-h*p+i*j+k*m-l*q-m*q,
f*i-i*q+j^2+k*n-m^2+l,
```

```
-f*p+g*i+j*k-j*q+k*p-m*n-n,
-g*p+h*i+j*l-m*p
>;
TriangularDecomposition(I);
```

Magma gives the solution:

```
Ideal of Polynomial ring of rank 9 over Multivariate rational function
field of rank 2 over Rational Field
Order: Lexicographical
Variables: k, l, n, p, q, f, g, h, j
Inhomogeneous, Dimension 0
Groebner basis:
[
    k + (-m - 1)/i*g + (-i^4 + m^2 + 2*m + 1)/(i*m^2 + i*m),
    l + g + m + 1,
    n + i*m/(m + 1),
    p - i^2/(m + 1),
    q + m/i*g + m^2/i,
    f - 1/i*g - m/i,
    g^2 + (-i^4 + m^4 + 3*m^3 + 4*m^2 + 3*m + 1)/(m^3 + 2*m^2 + m),
    h + i/(m + 1),
    j + i^2/(m + 1)
]
```

If $i \neq 0$ and $m \notin \{0, -1\}$, this can be used to find solutions to our original system of equations over $\mathbb{Q}$.

So we should consider the case $m = 0$, the case $i = 0$ and the case $m = -1$ separately.

We have four subcases, which may overlap.

Case 2.1: $e = 0$ and $i \neq 0$ and $m \notin \{0, -1\}$.

Let

$$N'_{i,m} \;:=\; \{t \in \mathbb{Q} :\; t^2 + \tfrac{-i^4+m^4+3m^3+4m^2+3m+1}{m^3+2m^2+m} = 0\}.$$

Our triangular system yields, for $g \in N'_{i,m}$,

$$A \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & \frac{g+m}{i} & g & -\frac{i}{m+1} \\ i & -\frac{i^2}{m+1} & \frac{m+1}{i}g + \frac{i^4-(m+1)^2}{im(m+1)} & -g-m-1 \\ m & -\frac{im}{m+1} & \frac{i^2}{m+1} & -\frac{mg+m^2}{i} \end{pmatrix} .$$

For $g \in N'_{i,m}$, we use Magma to calculate the determinant.

```
K<i,m> := FunctionField(Rationals(),2);
P<X> := PolynomialRing(K);
L<g> := quo< P | X^2 + (-i^4 + m^4 + 3*m^3 + 4*m^2 + 3*m + 1)/(m^3 + 2*m^2 + m)>;
A := RMatrixSpace(L,4,4)!Matrix([
```

```
[0,1,0,0],
[0,1/i*g + m/i,g,-i/(m + 1)],
[i,-i^2/(m + 1),(m + 1)/i*g + (i^4 - m^2 - 2*m - 1)/(i*m^2 + i*m),-g - m - 1],
[m,-i*m/(m + 1),i^2/(m + 1),-m/i*g - m^2/i]]);
Determinant(A);
```

This yields $\det(A) = 1$.

Thus

$$\left\{ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & \frac{g+m}{i} & g & -\frac{i}{m+1} \\ i & -\frac{i^2}{m+1} & \frac{m+1}{i}g+\frac{i^4-(m+1)^2}{im(m+1)} & -g-m-1 \\ m & -\frac{im}{m+1} & \frac{i^2}{m+1} & -\frac{mg+m^2}{i} \end{pmatrix} : \; i \in \mathbb{Q} \setminus \{0\},\; m \in \mathbb{Q} \setminus \{0,-1\},\; g \in N'_{i,m} \right\} \subseteq \mathcal{L}\,.$$

Case 2.2: $e = 0$ and $m = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ i & j & k & l \\ 0 & n & p & q \end{pmatrix}$.

We let Maple calculate the new matrix equation:

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[i,j,k,l],[0,n,p,q]]));
```

Maple gives the system of equations:

```
n*i = 0
j*n+n*p+q = 0
k*n+p^2-1 = 0
l*n+p*q = 0
-g*h-h*l+i = 0
-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
f*i-h*k-i*q-l^2 = 0
f*j+g*n-i*l+h = 0
g*p-i*n-j*l-j = 0
f*l-g*k+g*q-i*p-k*l = 0
-h*p+i*j-l*q = 0
f*i-i*q+j^2+k*n+l = 0
-f*p+g*i+j*k-j*q+k*p-n = 0
-g*p+h*i+j*l = 0
```

Now $n \cdot i = 0$ leads to $n = 0$ or $i = 0$.

So we have two subcases.

Case 2.2.1: $e = 0$ and $m = 0$ and $i = 0$.

Then $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ 0 & j & k & l \\ 0 & n & p & q \end{pmatrix}$ is not invertible and thus is not contained in the Galois variety.

Case 2.2.2: $e = 0$ and $m = 0$ and $n = 0$.

We obtain $p^2 = 1$ and $q = 0$.

We have two subcases.

Case 2.2.2.1: $e = 0$ and $m = 0$ and $n = 0$ and $q = 0$ and $p = 1$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[i,j,k,l],[0,0,1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l+i = 0
-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
f*i-h*k-l^2 = 0
f*j-i*l+h = 0
-j*l+g-j = 0
f*l-g*k-k*l-i = 0
i*j-h = 0
f*i+j^2+l = 0
g*i+j*k-f+k = 0
h*i+j*l-g = 0
```

We know $j = h \cdot i$ and $i \cdot j - h = 0$.

Thus $h \cdot (i^2 - 1) = 0$.

We have three subcases.

Case 2.2.2.1.1: $e = 0$ and $m = 0$ and $n = 0$ and $q = 0$ and $p = 1$ and $h = 0$.

We obtain $i = 0$ and have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & 0 \\ 0 & j & k & l \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Then A is not invertible and thus is not contained in the Galois variety.

Case 2.2.2.1.2: $e = 0$ and $m = 0$ and $n = 0$ and $q = 0$ and $p = 1$ and $i = 1$.

We obtain $j = h$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[1,h,k,l],[0,0,1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l+1 = 0
-f*g-h^2-f+k = 0
-g^2-h*k+l = 0
-h*k-l^2+f = 0
f*h+h-l = 0
-h*l+g-h = 0
```

```
f*l-g*k-k*l-1 = 0
h^2+f+l = 0
h*k-f+g+k = 0
h*l-g+h = 0
```

Now we use the command `ICS` of the Maple with the package `epsilon`, which decomposes a polynomial system into irreducible triangular systems.

```
ICS({
-g*h-h*l+1,
-f*g-h^2-f+k,
-g^2-h*k+l,
-h*k-l^2+f,
f*h+h-l,
-h*l+g-h,
f*l-g*k-k*l-1,
h^2+f+l,
h*k-f+g+k,
h*l-g+h},
[f,h,g,k,l]);
```

This gives:

```
[h+1, f-g, f^2+f-k+1, f^2-k-l],
[f+1, h-1, g-1, 1+k, l]
```

So in the first case we have $h = -1$, $g = f$, $k = f^2 + f + 1$ and $l = -f - 1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & f & -1 \\ 1 & -1 & f^2+f+1 & -f-1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1$.

In the second case, we have $f = -1$, $h = 1$, $g = 1$, $k = -1$ and $l = 0$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = -1$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & f & -1 \\ 1 & -1 & f^2+f+1 & -f-1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : f \in \mathbb{Q}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \subseteq \mathcal{L}$.

Case 2.2.2.1.3: $e = 0$ and $m = 0$ and $n = 0$ and $q = 0$ and $p = 1$ and $i = -1$.

We obtain $j = -h$ and $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ -1 & -h & k & l \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[-1,-h,k,l],[0,0,1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l-1 = 0
-f*g+h^2-f+k = 0
-g^2-h*k+l = 0
-h*k-l^2-f = 0
-f*h+h+l = 0
h*l+g+h = 0
f*l-g*k-k*l+1 = 0
h^2-f+l = 0
-h*k-f-g+k = 0
```

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
-g*h-h*l-1,
-f*g+h^2-f+k,
-g^2-h*k+l,
-h*k-l^2-f,
-f*h+h+l,
h*l+g+h,
f*l-g*k-k*l+1,
h^2-f+l,
-h*k-f-g+k},
[f,h,g,k,l]);
```

This gives:

```
[h-1, f+g, f^2-f+k+1, f^2+k-l],
[f-1, h+1, g-1, -1+k, l]
```

We have $\det\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -f & 1 \\ -1 & -1 & -f^2+f-1 & f-1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1$. We have $\det\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = -1$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -f & 1 \\ -1 & -1 & -f^2+f-1 & f-1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : f \in \mathbb{Q}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \subseteq \mathcal{L}$.

Case 2.2.2.2: $e = 0$ and $m = 0$ and $n = 0$ and $q = 0$ and $p = -1$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ i & j & k & l \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[i,j,k,l],[0,0,-1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l+i = 0
```

```
-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
f*i-h*k-l^2 = 0
f*j-i*l+h = 0
-j*l-g-j = 0
f*l-g*k-k*l+i = 0
i*j+h = 0
f*i+j^2+l = 0
g*i+j*k+f-k = 0
h*i+j*l+g = 0
```

We know $j = h \cdot i$ and $i \cdot j + h = 0$. Thus $h \cdot (i^2 + 1) = 0$.

So $h = 0$ and $j = 0$. Then $g = 0$ and $l = 0$. Moreover, $i = 0$. We obtain $k = f$. So we have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & f & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$. But A is not invertible and thus is not contained in the Galois variety.

Case 2.3: $e = 0$ and $i = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ 0 & j & k & l \\ m & n & p & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[0,j,k,l],[m,n,p,q]]));
```

Maple gives the system of equations:

```
p*m = 0
f*m+j*n+n*p+q = 0
g*m+k*n+p^2-1 = 0
h*m+l*n+p*q = 0
-g*h-h*l = 0
j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
g*m-h*k-l^2 = 0
f*j+g*n+h = 0
g*p-j*l-j = 0
f*l-g*k+g*q-k*l = 0
-h*p+k*m-l*q-m*q = 0
j^2+k*n-m^2+l = 0
-f*p+j*k-j*q+k*p-m*n-n = 0
-g*p+j*l-m*p = 0
```

We obtain $j = 0$.

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
p*m,
f*m+n*p+q,
g*m+k*n+p^2-1,
h*m+l*n+p*q,
-g*h-h*l,
-f*g-f+k,
-g^2-h*k+l,
g*m-h*k-l^2,
g*n+h,
g*p,
f*l-g*k+g*q-k*l,
-h*p+k*m-l*q-m*q,
k*n-m^2+l,
-f*p+k*p-m*n-n,
-g*p-m*p},
[g,n,h,f,k,l,q,m,p]);
```

This gives:

```
[g+1, h-n, k, l-1, f-q, m+1, p],
[g*n+h, f*n-1, f*g+f-k, g+l, f-q, m+1, p],
[g, n, h, f-k, l, q, m, p-1],
[g, n, h, f-k, l, q, m, p+1],
[g^2+1, n, h, f*g+f-k, l+1, g*k-g*q+f-k, g*m-1, p],
[g-1, n, h, f, k, l-1, q, m-1, p]
```

Note that $g^2+1 \neq 0$ for $g \in \mathbb{Q}$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix} = -1$.

We have $\det(\frac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & fg & -g \\ 0 & 0 & f^2g+f^2 & -fg \\ -f & 1 & 0 & f^2 \end{pmatrix}) = g$, which is nonzero if $g \in \mathbb{Q} \setminus \{0\}$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & f & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 0$. Thus A is not invertible and thus not in the Galois variety.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & f & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix} = 0$. Thus A is not invertible and thus not in the Galois variety.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = -1$.

Thus

$$\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix} : \ f,h \in \mathbb{Q}\} \cup \{\frac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & fg & -g \\ 0 & 0 & f^2g+f^2 & -fg \\ -f & 1 & 0 & f^2 \end{pmatrix} : \ f \in \mathbb{Q}\setminus\{0\}, \ g \in \mathbb{Q}\setminus\{0\}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}\} \subseteq \mathcal{L}.$$

Case 2.4: $e = 0$ and $m = -1$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ i & j & k & l \\ -1 & n & p & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[i,j,k,l],[-1,n,p,q]]));
```

Maple gives the system of equations:

```
i*n-p = 0
j*n+n*p-f+q = 0
k*n+p^2-g-1 = 0
l*n+p*q-h = 0
-g*h-h*l+i = 0
-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
f*i-h*k-i*q-l^2-g = 0
f*j+g*n-i*l+h+i = 0
g*p-i*n-j*l-j = 0
f*l-g*k+g*q-i*p-k*l = 0
-h*p+i*j-l*q-k+q = 0
f*i-i*q+j^2+k*n+l-1 = 0
-f*p+g*i+j*k-j*q+k*p = 0
-g*p+h*i+j*l+p = 0
```

We obtain $p = in$ and $j = hi$.

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
h*i*n+i*n^2-f+q,
i^2*n^2+k*n-g-1,
i*n*q+l*n-h,
-g*h-h*l+i,
-h^2*i-f*g-f+k,
-g^2-h*k+l,
f*i-h*k-i*q-l^2-g,
f*h*i+g*n-i*l+h+i,
g*i*n-h*i*l-h*i-i*n,
-i^2*n+f*l-g*k+g*q-k*l,
h*i^2-h*i*n-l*q-k+q,
h^2*i^2+f*i-i*q+k*n+l-1,
-f*i*n+h*i*k-h*i*q+i*k*n+g*i,
-g*i*n+h*i*l+h*i+i*n},
[i,n,f,h,g,k,l,q]);
```

This gives:

```
[i, h-n, g+1, k, l-1, f-q],
[i, f*n-1, f*h+g, f^2*h-f+k, f^2*h^2+h*k-l, f-q]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix} = -1$.

We have $\det(\frac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & -f^2h & fh \\ 0 & 0 & -f^3h+f^2 & f^2h \\ -f & 1 & 0 & f^2 \end{pmatrix}) = -fh$, which is nonzero if $f, h \in \mathbb{Q} \setminus \{0\}$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix} : \ f, h \in \mathbb{Q}\} \cup \{\frac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & -f^2h & fh \\ 0 & 0 & -f^3h+f^2 & f^2h \\ -f & 1 & 0 & f^2 \end{pmatrix} : \ f, h \in \mathbb{Q} \setminus \{0\}\} \subseteq \mathcal{L}$.

Case 3: $i = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ 0 & j & k & l \\ m & n & p & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[0,j,k,l],[m,n,p,q]]));
```

Maple gives the system of equations:

```
e*m+m*p = 0
f*m+j*n+n*p+q = 0
g*m+k*n+p^2-1 = 0
h*m+l*n+p*q = 0
-e*q-g*h-h*l = 0
-e*g-e*m+j = 0
-e*n-f*g-h*j-f+k = 0
-e*p-g^2-h*k+l = 0
e^2+g*m-h*k-l^2 = 0
e*f-e*k+f*j+g*n+h = 0
e*g+g*p-j*l-j = 0
e*h+f*l-g*k+g*q-k*l = 0
-h*p+k*m-l*q-m*q = 0
-e*p+j^2+k*n-m^2+l = 0
-f*p+j*k-j*q+k*p-m*n-n = 0
-g*p+j*l-m*p = 0
```

We use again Magma to find a subset of the set of solutions.

```
K<h,j> := FunctionField(Rationals(),2);
R< k, l, n, p, q, f, g, e, m > := PolynomialRing(K, 9);
I := ideal<R |
e*m+m*p,
f*m+j*n+n*p+q,
```

```
g*m+k*n+p^2-1,
h*m+l*n+p*q,
-e*q-g*h-h*l,
-e*g-e*m+j,
-e*n-f*g-h*j-f+k,
-e*p-g^2-h*k+l,
e^2+g*m-h*k-l^2,
e*f-e*k+f*j+g*n+h,
e*g+g*p-j*l-j,
e*h+f*l-g*k+g*q-k*l,
-h*p+k*m-l*q-m*q,
-e*p+j^2+k*n-m^2+l,
-f*p+j*k-j*q+k*p-m*n-n,
-g*p+j*l-m*p
>;
TriangularDecomposition(I);
```

Magma gives the solution:

```
Ideal of Polynomial ring of rank 9 over Multivariate rational function
field of rank 2 over Rational Field
Order: Lexicographical
Variables: k, l, n, p, q, f, g, e, m
Inhomogeneous, Dimension 0
Groebner basis:
[
    k - 2*j/h*e + (-j^2 + 2)/h,
    l - j*e + 1,
    n + h,
    p + e + j,
    q + h*e,
    f + (h^2*j^2 - h^2 - j^3)/(h*j^2 + h)*e +
    (2*h^2*j + j^2 + 2)/(h*j^2 + h),
    g + j*e,
    e^2 + 1,
    m
]
```

If $h \neq 0$, this can be used to find solutions to our original system of equations over $\mathbb{Q}$.

So we should consider the case $h = 0$ separately.

We have two subcases, which may overlap.

Case 3.1: $i = 0$ and $h \neq 0$.

But $e^2 = -1$ is impossible for $e \in \mathbb{Q}$.

Case 3.2: $i = 0$ and $h = 0$.
We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & 0 \\ 0 & j & k & l \\ m & n & p & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,0],[0,j,k,l],[m,n,p,q]]));
```

Maple gives the system of equations:

```
e*m+m*p = 0
f*m+j*n+n*p+q = 0
g*m+k*n+p^2-1 = 0
l*n+p*q = 0
-e*q = 0
-e*g-e*m+j = 0
-e*n-f*g-f+k = 0
-e*p-g^2+l = 0
e^2+g*m-l^2 = 0
e*f-e*k+f*j+g*n = 0
e*g+g*p-j*l-j = 0
f*l-g*k+g*q-k*l = 0
k*m-l*q-m*q = 0
-e*p+j^2+k*n-m^2+l = 0
-f*p+j*k-j*q+k*p-m*n-n = 0
-g*p+j*l-m*p = 0
```

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
e*m+m*p,
f*m+j*n+n*p+q,
g*m+k*n+p^2-1,
l*n+p*q,
-e*q,
-e*g-e*m+j,
-e*n-f*g-f+k,
-e*p-g^2+l,
e^2+g*m-l^2,
e*f-e*k+f*j+g*n,
e*g+g*p-j*l-j,
f*l-g*k+g*q-k*l,
k*m-l*q-m*q,
-e*p+j^2+k*n-m^2+l,
-f*p+j*k-j*q+k*p-m*n-n,
-g*p+j*l-m*p},
[e,k,l,n,p,q,f,g,j,m]);
```

This gives:

```
[e+l, n, p+1, q, f-k, g, j, m],
[-l+e, n, p-1, q, f-k, g, j, m],
[e, k, l-1, n, p, -q+f, g+1, j, m+1],
[e, l, k*n-1, p, k-q, f-k, g, j, m+1],
[e, l+1, n, p, k^2-2*k*q+2*q^2, f-k+q, g*k-g*q+f-k, j, k*m-m*q+q],
[k, l+1, n, e+p, q, f, e^2-g^2-1, j, g+m],
[e-1, k, l+1, n, p+1, q, f, g, j-m],
[e+1, k, l+1, n, p-1, q, f, g, j+m],
[e^2+1, e+l, n, p-1, q, e*f-k, e-g-1, e*g-j, m],
[e^2+1, -l+e, n, p+1, q, e*f+k, e+g+1, e*g-j, m],
[e, k, l-1, n, p, q, f, g-1, j, m-1],
[e^2+1, k, e*l-1, n, p-1, q, f, e+g-1, e*g-j, m],
[e^2+1, k, e*l+1, n, p+1, q, f, e-g+1, e*g-j, m]
```

Note that $e^2 + 1 \neq 0$ for $e \in \mathbb{Q}$.

In the fifth case, note that $k^2 - 2kq + 2q^2 = (k-q)^2 + q^2 = 0$ only if $k = 0$ and $q = 0$. However, isolating variables needs denominators. We obtain them via iniset:

```
with(charsets);
iniset([e, l+1, n, p, k^2-2*k*q+2*q^2, f-k+q, g*k-g*q+f-k, j, k*m-m*q+q],
[e,k,l,n,p,q,f,g,j,m]);
```

This gives `{k-q}`, so $k \neq q$. So the fifth case does not yield a solution. Cf. the handbook of [**5**], p. 19: l. 8, p. 4: E.2, p. 17: 10.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix} = e^2$, which is nonzero if $e \in \mathbb{Q} \setminus \{0\}$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & e \\ 0 & 0 & 1 & 0 \end{pmatrix} = e^2$, which is nonzero if $e \in \mathbb{Q} \setminus \{0\}$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & f \end{pmatrix} = -1$.

We have $\det(\frac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & 0 & 0 \\ 0 & 0 & f^2 & 0 \\ -f & 1 & 0 & f^2 \end{pmatrix}) = 0$. Thus A is not invertible and thus not in the Galois variety.

We have $e^2 - g^2 = 1$ and $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 0 & g & 0 \\ 0 & 0 & 0 & -1 \\ -g & 0 & -e & 0 \end{pmatrix} = e^2 - g^2 = 1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ j & 0 & -1 & 0 \end{pmatrix} = 1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ -j & 0 & 1 & 0 \end{pmatrix} = 1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} = -1$.

Thus we obtain the following subset.

$$\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix} : f \in \mathbb{Q},\ e \in \mathbb{Q} \setminus \{0\}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : f \in \mathbb{Q},\ e \in \mathbb{Q} \setminus \{0\}\}$$
$$\cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & f \end{pmatrix} : f \in \mathbb{Q}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 0 & g & 0 \\ 0 & 0 & 0 & -1 \\ -g & 0 & -e & 0 \end{pmatrix} : e, g \in \mathbb{Q},\ e^2 - g^2 = 1\}$$
$$\cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ j & 0 & -1 & 0 \end{pmatrix} : j \in \mathbb{Q}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ -j & 0 & 1 & 0 \end{pmatrix} : j \in \mathbb{Q}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}\} \subseteq \mathcal{L}\,.$$

Case 4: $m = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ i & j & k & l \\ 0 & n & p & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[i,j,k,l],[0,n,p,q]]));
```

Maple gives the system of equations:

```
n*i = 0
j*n+n*p+q = 0
k*n+p^2-1 = 0
l*n+p*q = 0
-e*q-g*h-h*l+i = 0
-e*g-h*i+j = 0
-e*n-f*g-h*j-f+k = 0
-e*p-g^2-h*k+l = 0
e^2+f*i-h*k-i*q-l^2 = 0
e*f-e*k+f*j+g*n-i*l+h = 0
e*g+g*p-i*n-j*l-j = 0
e*h+f*l-g*k+g*q-i*p-k*l = 0
e*i-h*p+i*j-l*q = 0
-e*p+f*i-i*q+j^2+k*n+l = 0
-f*p+g*i+j*k-j*q+k*p-n = 0
-g*p+h*i+j*l = 0
```

We obtain $n = 0$ or $i = 0$.

Thus we have two subcases.

Case 4.1: $m = 0$ and $n = 0$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[i,j,k,l],[0,0,p,q]]));
```

Maple gives the system of equations:

```
q = 0
p^2-1 = 0
```

```
p*q = 0
-e*q-g*h-h*l+i = 0
-e*g-h*i+j = 0
-f*g-h*j-f+k = 0
-e*p-g^2-h*k+l = 0
e^2+f*i-h*k-i*q-l^2 = 0
e*f-e*k+f*j-i*l+h = 0
e*g+g*p-j*l-j = 0
e*h+f*l-g*k+g*q-i*p-k*l = 0
e*i-h*p+i*j-l*q = 0
-e*p+f*i-i*q+j^2+l = 0
-f*p+g*i+j*k-j*q+k*p = 0
-g*p+h*i+j*l = 0
```

We have $q = 0$ and $p^2 = 1$. So we have two subcases.

Case 4.1.1: $m = 0$ and $n = 0$ and $q = 0$ and $p = 1$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[i,j,k,l],[0,0,1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l+i = 0
-e*g-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k-e+l = 0
e^2+f*i-h*k-l^2 = 0
e*f-e*k+f*j-i*l+h = 0
e*g-j*l+g-j = 0
e*h+f*l-g*k-k*l-i = 0
e*i+i*j-h = 0
f*i+j^2-e+l = 0
g*i+j*k-f+k = 0
h*i+j*l-g = 0
```

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
-g*h-h*l+i,
-e*g-h*i+j,
-f*g-h*j-f+k,
-g^2-h*k-e+l,
e^2+f*i-h*k-l^2,
e*f-e*k+f*j-i*l+h,
e*g-j*l+g-j,
e*h+f*l-g*k-k*l-i,
```

```
e*i+i*j-h,
f*i+j^2-e+l,
g*i+j*k-f+k,
h*i+j*l-g},
[e,i,k,l,j,f,g,h]);
```

This gives:

```
[i, e-l, j, f-k, g, h],
[-e^2*i*k+i^4+e^3-e*i^2+e^2-2*i^2+e+1, e*l+i^2-1,
e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],
[e, i-1, -l^2+k-l-1, j*l-l^2+j+k, j^2+f+l, f*j-j*l+g-l, f*j+h-l],
[e, i+1, l^2+k+l+1, j*l-l^2+j-k, -j^2+f-l, f*j+j*l-g+l, f*j+h+l],
[-i+e-1, e^2*i*k+e*i^3+e^2*i+e^2-e*i-i^2-2*i-1, e*i-e*l+i+1,
e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],
[i+e-1, e^2*i*k-e*i^3-e^2*i+e^2+e*i-i^2+2*i-1, e*i+e*l+i-1,
e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],
[e^2+1, i, e+l, e+j+1, -j*k+f-k, e*j+g, e*f-e*k+f*j+h],
[e, i-1, k-1, l+1, j+1, f, g, 1+h],
[e, i-1, k+1, l, j-1, f+1, -1+g, -1+h],
[e, i+1, k-1, l, j-1, f-1, -1+g, 1+h],
[e, i+1, k+1, l+1, j+1, f, g, -1+h],
[e+1, i-2, 2+k, l+1, j-2, f+2, -2+g, -2+h],
[e+1, i+2, -2+k, l+1, j-2, f-2, -2+g, 2+h],
[e^2+1, i, k, e*l-1, e-j+1, f, -j*l+g, h]
```

Note that $e^2 + 1 \neq 0$ for $e \in \mathbb{Q}$.

In the first case we have $\det \begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&e \\ 0&0&1&0 \end{pmatrix} = e^2$, which is nonzero if $e \in \mathbb{Q} \setminus \{0\}$.

Thus $\{ \begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&e \\ 0&0&1&0 \end{pmatrix} : f \in \mathbb{Q},\ e \in \mathbb{Q} \setminus \{0\} \} \ \subseteq\ \mathcal{L}$.

In the second case, isolating variables needs denominators. We obtain them via `iniset`:

```
with(charsets);
iniset([-e^2*i*k+i^4+e^3-e*i^2+e^2-2*i^2+e+1, e*l+i^2-1,
e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],[e,i,k,l,j,f,g,h]);
```

Maple gives:

```
{e, i, e*i^2 + e*l + i^2 - 1}
```

Thus the inequalities $e \neq 0$, $i \neq 0$ and $ei^2+el+i^2-1 \neq 0$ are presupposed in the parametrization of the set of solutions in this case. Cf. the handbook of [**5**], p. 19: l. 8, p. 4: E.2, p. 17: 10.

We use `simplify` as follows.

```
k := -(i^4+e^3-e*i^2+e^2-2*i^2+e+1)/(-e^2*i);
l := -(i^2-1)/e;
j := simplify(-(e^2*i^2+e*i^2)/(e*i^2+e*l+i^2-1));
f := simplify(-(-j^2+e-l)/(-i));
g := simplify(-(e*f*i-e*i*k+f*i*j-i^2*l-j*l));
h := simplify(-(e*f-e*k+f*j-i*l));
```

This gives:

```
k = (i^4+e^3-e*i^2+e^2-2*i^2+e+1)/(e^2*i)
l = -(i^2-1)/e
j = -e-1
f = (-e^3-e^2+i^2-e-1)/e/i
g = (i^2-e-1)/e
h = -i
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & \frac{-e^3-e^2+i^2-e-1}{ei} & \frac{i^2-e-1}{e} & -i \\ i & -e-1 & \frac{i^4+e^3-ei^2+e^2-2i^2+e+1}{e^2i} & \frac{-i^2+1}{e} \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1.$

Thus $\{ \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & \frac{-e^3-e^2+i^2-e-1}{ei} & \frac{i^2-e-1}{e} & -i \\ i & -e-1 & \frac{i^4+e^3-ei^2+e^2-2i^2+e+1}{e^2i} & \frac{-i^2+1}{e} \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e, i \in \mathbb{Q} \setminus \{0\} \} \subseteq \mathcal{L}.$

In the third case, we get:

```
[e, i-1, -l^2+k-l-1, j*l-l^2+j+k, j^2+f+l, f*j-j*l+g-l, f*j+h-l]
```

So we have $k = l^2 + l + 1$. Then

$$0 \ = \ jl - l^2 + j + k \ = \ jl + j + l + 1 \ = \ (j+1)(l+1) \, .$$

Now we use `iniset` of the Maple package `charsets`:

```
iniset([e, i-1, -l^2+k-l-1, j*l-l^2+j+k, j^2+f+l, f*j-j*l+g-l, f*j+h-l],
[e,i,k,l,j,f,g,h]);
```

This gives:

```
{l + 1}
```

Thus $l+1 \neq 0$ and therefore $j = -1$.

So we have $f = -1-l$, $g = -1-l$ and $h = -1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1-l & -1-l & -1 \\ 1 & -1 & l^2+l+1 & l \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1-l & -1-l & -1 \\ 1 & -1 & l^2+l+1 & l \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ l \in \mathbb{Q} \setminus \{-1\}\} \subseteq \mathcal{L}$.

In the fourth case, we get:

```
[e, i+1, l^2+k+l+1, j*l-l^2+j-k, -j^2+f-l, f*j+j*l-g+l, f*j+h+l]
```

So we have $k = -l^2 - l - 1$. Then

$$0 \ = \ jl - l^2 + j - k \ = \ jl + j + l + 1 \ = \ (j+1)(l+1) \, .$$

Now we use `iniset` of the Maple package `charsets`:

```
iniset([e, i+1, l^2+k+l+1, j*l-l^2+j-k, -j^2+f-l, f*j+j*l-g+l, f*j+h+l],
[e,i,k,l,j,f,g,h]);
```

This gives:

```
{l + 1}
```

Thus $l+1 \neq 0$ and therefore $j = -1$.

So we have $f = 1+l$, $g = -1-l$ and $h = 1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1+l & -1-l & 1 \\ -1 & -1 & -l^2-l-1 & l \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1+l & -1-l & 1 \\ -1 & -1 & -l^2-l-1 & l \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ l \in \mathbb{Q} \setminus \{-1\}\} \subseteq \mathcal{L}$.

In the fifth case, we get:

```
[-i+e-1, e^2*i*k+e*i^3+e^2*i+e^2-e*i-i^2-2*i-1, e*i-e*l+i+1,
e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h]
```

Now we use `iniset` of the Maple package `charsets`:

```
iniset([-i+e-1, e^2*i*k+e*i^3+e^2*i+e^2-e*i-i^2-2*i-1, e*i-e*l+i+1,
     e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
     e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],[e,i,k,l,j,f,g,h]);
```

This gives:

```
{e, i, e*i^2 + e*l + i^2 - 1}
```

Thus $e \neq 0$, $i \neq 0$ and $ei^2 + el + i^2 - 1 \neq 0$.

Since $e = i + 1$, we have $e \notin \{0, 1\}$.

We use Maple to put $i = e - 1$:

```
expand(simplify(eval([-i+e-1, e^2*i*k+e*i^3+e^2*i+e^2-e*i-i^2-2*i-1,
e*i-e*l+i+1, e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],i=e-1)));
```

This gives:

```
[0, e^4 + e^3*k - 2*e^3 - e^2*k + e^2, e^2 - e*l, e^4 + e^3*j - e^3 -
e^2*j + e*j*l - e^2 - e*j + e, -e*f - j^2 + e + f - l,
e^2*f - e^2*k - e^2*l + e*f*j - e*f + e*k + 2*e*l - f*j - j*l + g - l,
e*f - e*k - e*l + f*j + h + l]
```

So we have $(e^3 - e^2)k = -e^4 + 2e^3 - e^2$.

We obtain $k = -e + 1$. We use Maple to put $k = -e + 1$:

```
expand(simplify(eval([e^4 + e^3*k - 2*e^3 - e^2*k + e^2, e^2 - e*l,
e^4 + e^3*j - e^3 - e^2*j + e*j*l - e^2 - e*j + e,
-e*f - j^2 + e + f - l,
e^2*f - e^2*k - e^2*l + e*f*j - e*f + e*k +2*e*l - f*j - j*l + g - l,
e*f - e*k - e*l + f*j + h + l], k=1-e)));
```

This gives:

```
[0, e^2 - e*l, e^4 + e^3*j - e^3 - e^2*j + e*j*l - e^2 - e*j + e,
-e*f - j^2 + e + f - l, e^3 + e^2*f - e^2*l + e*f*j - 2*e^2 - e*f +
2*e*l - f*j - j*l + e + g - l, e^2 + e*f - e*l + f*j - e + h + l]
```

We obtain $l = e$.

In particular, $0 \neq ei^2 + el + i^2 - 1 = ei^2 + e^2 + i^2 - 1 = e(e-1)^2 + e^2 + (e-1)^2 - 1 = e(e^2 - 1)$. So we have $e \notin \{-1, 0, 1\}$.

We use Maple to put $l = e$:

```
expand(simplify(eval([e^4 + e^3*k - 2*e^3 - e^2*k + e^2, e^2 - e*l,
e^4 + e^3*j - e^3 - e^2*j + e*j*l - e^2 - e*j + e,
-e*f - j^2 + e + f - l, e^2*f - e^2*k - e^2*l + e*f*j - e*f + e*k +
2*e*l - f*j - j*l + g - l, e*f - e*k - e*l + f*j + h + l],
[k=1-e,l=e])));
```

This gives:

```
[0, 0, e^4 + e^3*j - e^3 - e^2 - e*j + e, -e*f - j^2 + f,
e^2*f + e*f*j - e*f - e*j - f*j + g, e*f + f*j + h]
```

So we have $(e^3-e)j = -e^4+e^3+e^2-e = (e^3-e)(1-e)$. Thus $j = 1-e$.

We use Maple to put $j = 1-e$:

```
expand(simplify(eval([e^4 + e^3*k - 2*e^3 - e^2*k + e^2, e^2 - e*l,
e^4 + e^3*j - e^3 - e^2*j + e*j*l - e^2 - e*j + e,
-e*f - j^2 + e + f - l, e^2*f - e^2*k - e^2*l + e*f*j - e*f + e*k +
2*e*l - f*j - j*l + g - l, e*f - e*k - e*l + f*j + h + l],
[k=1-e,l=e,j=1-e])));
```

This gives:

```
[0, 0, 0, -e^2 - e*f + 2*e + f - 1, e^2 + e*f - e - f + g, f + h]
```

We obtain $f = 1-e$. Then $g = 1-e$ and $h = e-1$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 1-e & 1-e & e-1 \\ e-1 & 1-e & 1-e & e \\ 0 & 0 & 1 & 0 \end{pmatrix} = 2e-1$, which is nonzero if $e \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1\}$.

Thus $\{ \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 1-e & 1-e & e-1 \\ e-1 & 1-e & 1-e & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1\}\} \subseteq \mathcal{L}$.

In the sixth case, we have

```
[ i+e-1, e^2*i*k-e*i^3-e^2*i+e^2+e*i-i^2+2*i-1, e*i+e*l+i-1,
e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h]
```

Now we use `iniset` of the Maple package `charsets`:

```
iniset( [i+e-1, e^2*i*k-e*i^3-e^2*i+e^2+e*i-i^2+2*i-1, e*i+e*l+i-1,
     e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
     e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],[e,i,k,l,j,f,g,h]);
```

This gives:

```
{e, i, e*i^2 + e*l + i^2 - 1}
```

Thus $e \neq 0$, $i \neq 0$ and $ei^2 + el + i^2 - 1 \neq 0$.

Since $e = 1-i$, we have $e \notin \{0, 1\}$.

We use Maple to put $i = 1 - e$:

```
expand(simplify(eval([ i+e-1, e^2*i*k-e*i^3-e^2*i+e^2+e*i-i^2+2*i-1,
e*i+e*l+i-1, e^2*i^2+e*i^2*j+e*i^2+e*j*l+i^2*j-j, -f*i-j^2+e-l,
e*f*i-e*i*k+f*i*j-i^2*l-j*l+g, e*f-e*k+f*j-i*l+h],i=1-e)));
```

This gives:

```
[0, e^4-e^3*k-2*e^3+e^2*k+e^2, -e^2+e*l,
e^4+e^3*j-e^3-e^2*j+e*j*l-e^2-e*j+e, e*f-j^2+e-f-l,
-e^2*f+e^2*k-e^2*l-e*f*j+e*f-e*k+2*e*l+f*j-j*l+g-l,
e*f-e*k+e*l+f*j+h-l]
```

So we have $(e^3 - e^2)k = e^4 - 2e^3 + e^2$.

We have $k = e - 1$. We use Maple to put $k = e - 1$:

```
expand(simplify(eval([0, e^4-e^3*k-2*e^3+e^2*k+e^2, -e^2+e*l,
e^4+e^3*j-e^3-e^2*j+e*j*l-e^2-e*j+e, e*f-j^2+e-f-l, -e^2*f+e^2*k-e^2*l-
e*f*j+e*f-e*k+2*e*l+f*j-j*l+g-l, e*f-e*k+e*l+f*j+h-l],k=e-1)));
```

This gives:

```
[0, 0, -e^2+e*l, e^4+e^3*j-e^3-e^2*j+e*j*l-e^2-e*j+e, e*f-j^2+e-f-l,
e^3-e^2*f-e^2*l-e*f*j-2*e^2+e*f+2*e*l+f*j-j*l+e+g-l,
-e^2+e*f+e*l+f*j+e+h-l]
```

We obtain $l = e$.

In particular, $0 \neq ei^2 + el + i^2 - 1 = ei^2 + e^2 + i^2 - 1 = e(1-e)^2 + e^2 + (1-e)^2 - 1 = e(e^2 - 1)$. So we have $e \notin \{-1, 0, 1\}$.

We use Maple to put $l = e$:

```
expand(simplify(eval([0, 0, -e^2+e*l,
e^4+e^3*j-e^3-e^2*j+e*j*l-e^2-e*j+e, e*f-j^2+e-f-l, e^3-e^2*f-e^2*l-
e*f*j-2*e^2+e*f+2*e*l+f*j-j*l+e+g-l, -e^2+e*f+e*l+f*j+e+h-l],l=e)));
```

This gives:

```
[0, 0, 0, e^4+e^3*j-e^3-e^2-e*j+e, e*f-j^2-f,
-e^2*f-e*f*j+e*f-e*j+f*j+g, e*f+f*j+h]
```

We obtain $(e^3 - e)j = -e^4 + e^3 + e^2 - e = (e^3 - e)(1 - e)$. So $j = 1 - e$.

We use Maple to put $j = 1 - e$:

```
expand(simplify(eval([0, 0, 0, e^4+e^3*j-e^3-e^2-e*j+e, e*f-j^2-f,
-e^2*f-e*f*j+e*f-e*j+f*j+g, e*f+f*j+h],j=1-e)));
```

This gives:

```
[0, 0, 0, 0, -e^2+e*f+2*e-f-1, e^2-e*f-e+f+g, f+h]
```

We obtain $f = e - 1$ then $g = 1 - e$ and $h = 1 - e$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & e-1 & 1-e & 1-e \\ 1-e & 1-e & e-1 & e \\ 0 & 0 & 1 & 0 \end{pmatrix} = 2e - 1$, which is nonzero if $e \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1\}$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & e-1 & 1-e & 1-e \\ 1-e & 1-e & e-1 & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1\}\} \subseteq \mathcal{L}$.

In the eighth case, we get:

```
[e, i-1, k-1, l+1, j+1, f, g, 1+h]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1$.

In the ninth case, we get:

```
[e, i-1, k+1, l, j-1, f+1, -1+g, -1+h]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = -1$.

In the tenth case, we get:

```
[e, i+1, k-1, l, j-1, f-1, -1+g, 1+h]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = -1$.

In the eleventh case, we get:

```
[e, i+1, k+1, l+1, j+1, f, g, -1+h]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = 1$.

In the twelfth case, we get:

```
[e+1, i-2, 2+k, l+1, j-2, f+2, -2+g, -2+h]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -2 & 2 & 2 \\ 2 & 2 & -2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = -3$.

In the thirteenth case, we get:

```
[e+1, i+2, -2+k, l+1, j-2, f-2, -2+g, 2+h]
```

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 2 & -2 \\ -2 & 2 & 2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = -3$.

Thus

$$\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\}$$
$$\cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -2 & 2 & 2 \\ 2 & 2 & -2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \cup \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 2 & -2 \\ -2 & 2 & 2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \subseteq \mathcal{L}.$$

Case 4.1.2: $m = 0$ and $n = 0$ and $q = 0$ and $p = -1$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[i,j,k,l],[0,0,-1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l+i = 0
-e*g-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+e+l = 0
e^2+f*i-h*k-l^2 = 0
e*f-e*k+f*j-i*l+h = 0
e*g-j*l-g-j = 0
e*h+f*l-g*k-k*l+i = 0
e*i+i*j+h = 0
f*i+j^2+e+l = 0
g*i+j*k+f-k = 0
h*i+j*l+g = 0
```

We use again Magma to find a subset of the set of solutions.

```
K<e,i> := FunctionField(Rationals(),2);
R< k, l, j, f, g, h > := PolynomialRing(K, 6);
I := ideal<R |
-g*h-h*l+i,
-e*g-h*i+j,
-f*g-h*j-f+k,
-g^2-h*k+e+l,
e^2+f*i-h*k-l^2,
e*f-e*k+f*j-i*l+h,
e*g-g-j*l-j,
e*h+f*l-g*k-k*l+i,
e*i+i*j+h,
f*i+e+j^2+l,
g*i+f+j*k-k,
h*i+g+j*l
>;
TriangularDecomposition(I);
```

Magma gives the solutions:

```
Ideal of Polynomial ring of rank 6 over Multivariate rational function
field of rank 2 over Rational Field
Order: Lexicographical
Variables: k, l, j, f, g, h
Inhomogeneous, Dimension 0
Groebner basis:
[
    k + (e^3 - e^2 + e*i^2 + e - i^4 - 2*i^2 - 1)/(e^2*i),
    l + (i^2 + 1)/e,
    j + e - 1,
    f + (e^3 - e^2 + e - i^2 - 1)/(e*i),
    g + (e - i^2 - 1)/e,
    h + i
]
```

If $e \neq 0$ and $i \neq 0$, this can be used to find solutions to our original system of equations over $\mathbb{Q}$.

So we should consider the case $e = 0$ and the case $i = 0$ separately.

We have three subcases, which may overlap.

Case 4.1.2.1: $m = 0$ and $n = 0$ and $q = 0$ and $p = -1$ and $e \neq 0$ and $i \neq 0$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & \frac{-e^3+e^2-e+i^2+1}{ei} & \frac{-e+i^2+1}{e} & -i \\ i & 1-e & \frac{-e^3+e^2-ei^2-e+i^4+2i^2+1}{e^2i} & \frac{-i^2-1}{e} \\ 0 & 0 & -1 & 0 \end{pmatrix} = 1.$

Thus $\{ \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & \frac{-e^3+e^2-e+i^2+1}{ei} & \frac{-e+i^2+1}{e} & -i \\ i & 1-e & \frac{-e^3+e^2-ei^2-e+i^4+2i^2+1}{e^2i} & \frac{-i^2-1}{e} \\ 0 & 0 & -1 & 0 \end{pmatrix} : \ i, e \in \mathbb{Q} \setminus \{0\} \} \subseteq \mathcal{L}.$

Case 4.1.2.2: $m = 0$ and $n = 0$ and $q = 0$ and $p = -1$ and $e = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & g & h \\ i & j & k & l \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[0,f,g,h],[i,j,k,l],[0,0,-1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l+i = 0
-h*i+j = 0
-f*g-h*j-f+k = 0
-g^2-h*k+l = 0
f*i-h*k-l^2 = 0
f*j-i*l+h = 0
-j*l-g-j = 0
```

```
f*l-g*k-k*l+i = 0
i*j+h = 0
f*i+j^2+l = 0
g*i+j*k+f-k = 0
h*i+j*l+g = 0
```

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
-g*h-h*l+i,
-h*i+j,
-f*g-h*j-f+k,
-g^2-h*k+l,
f*i-h*k-l^2,
f*j-i*l+h,
-j*l-g-j,
f*l-g*k-k*l+i,
i*j+h,
f*i+j^2+l,
g*i+j*k+f-k,
h*i+j*l+g},
[i,f,l,k,j,h,g]);
```

This gives:

```
[i, l, f-k, j, h, g],
[i^2+1, -i*l+f-i, -i^3*k+l^3+f^2-2*f*i-f*k+2*l^2+l-1, f*j-i*j-i*l,
                                                    f*j-i*l+h, j*l+g+j],
[i^2+1, f-i, l, i-k, j+1, h-i, g-1],
[i^2+1, f-i, l, i+k, j-1, h+i, g+1]
```

Note that $i^2 + 1 \neq 0$ for $i \in \mathbb{Q}$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & f & 0 \\ 0 & 0 & -1 & 0 \end{pmatrix}$. But A is not invertible and thus not in the Galois variety.

Case 4.1.2.3: $m = 0$ and $n = 0$ and $q = 0$ and $p = -1$ and $i = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ 0 & j & k & l \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[0,j,k,l],[0,0,-1,0]]));
```

Maple gives the system of equations:

```
-g*h-h*l = 0
-e*g+j = 0
-f*g-h*j-f+k = 0
```

```
-g^2-h*k+e+l = 0
e^2-h*k-l^2 = 0
e*f-e*k+f*j+h = 0
e*g-j*l-g-j = 0
e*h+f*l-g*k-k*l = 0
h = 0
j^2+e+l = 0
j*k+f-k = 0
j*l+g = 0
```

Putting $h = 0$, we obtain:

```
-e*g+j = 0
-f*g-f+k = 0
-g^2+e+l = 0
e^2-l^2 = 0
e*f-e*k+f*j = 0
e*g-j*l-g-j = 0
f*l-g*k-k*l = 0
j^2+e+l = 0
j*k+f-k = 0
j*l+g = 0
```

Now we use the command ICS of the Maple package epsilon:

```
ICS({
-e*g+j,
-f*g-f+k,
-g^2+e+l,
e^2-l^2,
e*f-e*k+f*j,
e*g-j*l-g-j,
f*l-g*k-k*l,
j^2+e+l,
j*k+f-k,
j*l+g},
[e,i,f,l,k,j,g]);
```

This yields

```
[e+l, f-k, j, g],
[e^2+1, -l+e, e*k-f, e+j-1, e*j+g],
[e^2+1, f, -l+e, k, e-j-1, e*j+g]
```

Note that $e^2 + 1 \neq 0$ for $e \in \mathbb{Q}$.

We have $\det \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix} = e^2$, which is nonzero if $e \in \mathbb{Q} \setminus \{0\}$.

Thus $\{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix} : f \in \mathbb{Q},\ e \in \mathbb{Q} \setminus \{0\}\} \subseteq \mathcal{L}$.

Case 4.2: $m = 0$ and $i = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ 0 & j & k & l \\ 0 & n & p & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[0,j,k,l],[0,n,p,q]]));
```

Maple gives the system of equations:

```
j*n+n*p+q = 0
k*n+p^2-1 = 0
l*n+p*q = 0
-e*q-g*h-h*l = 0
-e*g+j = 0
-e*n-f*g-h*j-f+k = 0
-e*p-g^2-h*k+l = 0
e^2-h*k-l^2 = 0
e*f-e*k+f*j+g*n+h = 0
e*g+g*p-j*l-j = 0
e*h+f*l-g*k+g*q-k*l = 0
-h*p-l*q = 0
-e*p+j^2+k*n+l = 0
-f*p+j*k-j*q+k*p-n = 0
-g*p+j*l = 0
```

We use again Magma to find a subset of the set of solutions.

```
K<p,q> := FunctionField(Rationals(),2);
R< e, k, l, n, j, f, g, h > := PolynomialRing(K, 8);
I := ideal<R |
j*n+n*p+q,
k*n+p^2-1,
l*n+p*q,
-e*q-g*h-h*l,
-e*g+j,
-e*n-f*g-h*j-f+k,
-e*p-g^2-h*k+l,
e^2-h*k-l^2,
e*f-e*k+f*j+g*n+h,
e*g+g*p-j*l-j,
e*h+f*l-g*k+g*q-k*l,
-h*p-l*q,
-e*p+j^2+k*n+l,
-f*p+j*k-j*q+k*p-n,
```

```
-g*p+j*l
>;
TriangularDecomposition(I);
```

Magma gives the solutions:

```
Ideal of Polynomial ring of rank 8 over Multivariate rational function
field of rank 2 over Rational Field
Order: Lexicographical
Variables: e, k, l, n, j, f, g, h
Inhomogeneous, Dimension 0
Groebner basis:
[
    e - 1/q*h,
    k + (p^2 - 1)/q^2*h,
    l + p/q*h,
    n + h,
    j + 1/q*h + p,
    f - 2/p*h + (p^2 - p*q^2 - 1)/(p*q),
    g - p/q*h + 1,
    h^2 + q^2
]
```

If $q \neq 0$ and $p \neq 0$, this can be used to find solutions to our original system of equations over $\mathbb{Q}$.

So we should consider the case $p = 0$ and the case $q = 0$ separately.

We have three subcases, which may overlap.

Case 4.2.1: $m = 0$ and $i = 0$ and $q \neq 0$ and $p \neq 0$.

Note that $h^2 + q^2 \neq 0$ since $q \neq 0$.

Thus we do not have a solution in $\mathbb{Q}$ in this case.

Case 4.2.2: $m = 0$ and $i = 0$ and $p = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ 0 & j & k & l \\ 0 & n & 0 & q \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[0,j,k,l],[0,n,0,q]]));
```

Maple gives the system of equations:

```
j*n+q = 0
k*n-1 = 0
n*l = 0
-e*q-g*h-h*l = 0
-e*g+j = 0
-e*n-f*g-h*j-f+k = 0
```

```
-g^2-h*k+l = 0
e^2-h*k-l^2 = 0
e*f-e*k+f*j+g*n+h = 0
e*g-j*l-j = 0
e*h+f*l-g*k+g*q-k*l = 0
-q*l = 0
j^2+k*n+l = 0
j*k-j*q-n = 0
j*l = 0
```

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({
j*n+q,
k*n-1,
n*l,
-e*q-g*h-h*l,
-e*g+j,
-e*n-f*g-h*j-f+k,
-g^2-h*k+l,
e^2-h*k-l^2,
e*f-e*k+f*j+g*n+h,
e*g-j*l-j,
e*h+f*l-g*k+g*q-k*l,
-q*l,
j^2+k*n+l,
j*k-j*q-n,
j*l},
[g,e,q,k,l,n,j,f,h]);
```

This gives:

```
[g+1, e^2+1, e-2*q+1, k-2*q, l, e*q+n, e+j, e*q-h],
[g+1, e^2+1, e+2*q+1, k-2*q, l, e*q+n, e+j, e*q-h],
[g-1, e^2+1, e-2*q-1, k-2*q, l, e*q-n, e-j, f-q, e*q+h],
[g-1, e^2+1, e+2*q-1, k-2*q, l, e*q-n, e-j, f-q, e*q+h],
[g^2+1, e-1, g-2*q-1, k-2*q, l, g*q-n, g-j, f*g-3*g*q-f-q, f*g+f+h-3*q],
[g^2+1, e-1, g+2*q-1, k-2*q, l, g*q-n, g-j, f*g-3*g*q-f-q, f*g+f+h-3*q],
[g^2+1, e+1, g-2*q+1, k-2*q, l, g*q+n, g+j, f*g-3*g*q-f-q, f*g+f-h-3*q],
[g^2+1, e+1, g+2*q+1, k-2*q, l, g*q+n, g+j, f*g-3*g*q-f-q, f*g+f-h-3*q]
```

But $e^2+1 \neq 0$ for $e \in \mathbb{Q}$ and $g^2+1 \neq 0$ for $g \in \mathbb{Q}$. Thus we obtain no solution in this case.

Case 4.2.3: $m = 0$ and $i = 0$ and $q = 0$.

We have $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ 0 & j & k & l \\ 0 & n & p & 0 \end{pmatrix}$.

```
mat_eq(matrix([[0,1,0,0],[e,f,g,h],[0,j,k,l],[0,n,p,0]]));
```

Maple gives the system of equations:

```
j*n+n*p = 0
k*n+p^2-1 = 0
n*l = 0
-g*h-h*l = 0
-e*g+j = 0
-e*n-f*g-h*j-f+k = 0
-e*p-g^2-h*k+l = 0
e^2-h*k-l^2 = 0
e*f-e*k+f*j+g*n+h = 0
e*g+g*p-j*l-j = 0
e*h+f*l-g*k-k*l = 0
-p*h = 0
-e*p+j^2+k*n+l = 0
-f*p+j*k+k*p-n = 0
-g*p+j*l = 0
```

Now we use the command `ICS` of the Maple package `epsilon`:

```
ICS({j*n+n*p, k*n+p^2-1, n*l, -g*h-h*l, -e*g+j, -e*n-f*g-h*j-f+k, -e*p-g^2-h*k+l,
e^2-h*k-l^2, e*f-e*k+f*j+g*n+h, e*g+g*p-j*l-j, e*h+f*l-g*k-k*l, -p*h,
-e*p+j^2+k*n+l, -f*p+j*k+k*p-n, -g*p+j*l}, [e,g,k,l,n,j,f,h,p]);
```

This gives:

```
[g, e-l, n, j, f-k, h, p-1],
[g, e+l, n, j, f-k, h, p+1],
[e^2+1, e*g+e-1, e-l, n, e*g-j, e*g*k+f-k, h, p+1],
[e^2+1, e*g+e+1, e+l, n, e*g-j, e*g*k-f+k, h, p-1],
[e^2+1, e-g+1, k, e-l, n, e*g-j, f, h, p+1],
[e^2+1, e+g-1, k, e+l, n, e*g-j, f, h, p-1]
```

Note that $e^2+1 \neq 0$ for $e \in \mathbb{Q}$.

So in the first case, we have $\det \begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&e \\ 0&0&1&0 \end{pmatrix} = e^2$, which is nonzero if $e \in \mathbb{Q} \setminus \{0\}$.

In the second case, we have $\det \begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&-e \\ 0&0&-1&0 \end{pmatrix} = e^2$, which is nonzero if $e \in \mathbb{Q} \setminus \{0\}$.

Thus $\{\begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&e \\ 0&0&1&0 \end{pmatrix} : \ f \in \mathbb{Q}, \ e \in \mathbb{Q} \setminus \{0\}\} \cup \{\begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&-e \\ 0&0&-1&0 \end{pmatrix} : \ f \in \mathbb{Q}, \ e \in \mathbb{Q} \setminus \{0\}\} \subseteq \mathcal{L}$.

Proposition 31 Recall that

$$\begin{aligned} N_{e,i,m} &= \{t \in \mathbb{Q} : \ t^3 + \tfrac{e(e^2m+ei^2-m^3+m)+2i^2m(m+1)}{m(e^2+(m+1)^2)}t^2 + \tfrac{i^2(2e^3+2em+i^2m)}{m(e^2+(m+1)^2)}t + \tfrac{i^2e(e^3-em^2-e+i^2m)}{m(e^2+(m+1)^2)} = 0\} \\ N'_{i,m} &= \{t \in \mathbb{Q} : \ t^2 + \tfrac{-i^4+m^4+3m^3+4m^2+3m+1}{m^3+2m^2+m} = 0\} \ . \end{aligned}$$

We have the following subset of the Galois variety.

$$\mathcal{L} = \{A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & g & h \\ i & j & k & l \\ m & n & p & q \end{pmatrix} \in \mathrm{GL}_4(\mathbb{Q}) : \ A^S \cdot A = A \cdot A^S\}$$

$$\supseteq \mathcal{L}' := \{\tfrac{1}{e^2 i} \begin{pmatrix} 0 & e^2 i & 0 & 0 \\ e^3 i & (e^2+m+1)ej+ei^2 & (m+1)eij+(i^2-em)ei & -e^2mj-e^2i^2 \\ e^2 i^2 & je^2 i & (e^2+(m+1)^2)j^2+(e^3+(1-m^2)e+2i^2(m+1))j+(i^2+(1-m)e)i^2 & -(m+1)eij-(e+i^2)ei \\ e^2 im & e^2 mj & (-j-e)e^2 i & -(m(m+1))ej-ei^2 m \end{pmatrix}$$
$$: \ e, i, m \in \mathbb{Q} \setminus \{0\} \ , \ j \in N_{e,i,m}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & \frac{g+m}{i} & g & -\frac{i}{m+1} \\ i & -\frac{i^2}{m+1} & \frac{m+1}{i}g+\frac{i^4-(m+1)^2}{im(m+1)} & -g-m-1 \\ m & -\frac{im}{m+1} & \frac{i^2}{m+1} & -\frac{mg+m^2}{i} \end{pmatrix} : \ i \in \mathbb{Q} \setminus \{0\}, \ m \in \mathbb{Q} \setminus \{0, -1\}, \ g \in N'_{i,m}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & \frac{-e^3-e^2+i^2-e-1}{ei} & \frac{i^2-e-1}{e} & -i \\ i & -e-1 & \frac{i^4+e^3-ei^2+e^2-2i^2+e+1}{e^2 i} & \frac{-i^2+1}{e} \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e, i \in \mathbb{Q} \setminus \{0\}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & \frac{-e^3+e^2-e+i^2+1}{ei} & \frac{-e+i^2+1}{e} & -i \\ i & 1-e & \frac{-e^3+e^2-ei^2-e+i^4+2i^2+1}{e^2 i} & \frac{-i^2-1}{e} \\ 0 & 0 & -1 & 0 \end{pmatrix} : \ i, e \in \mathbb{Q} \setminus \{0\}\}$$

$$\cup \ \{\tfrac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & fg & -g \\ 0 & 0 & f^2 g+f^2 & -fg \\ -f & 1 & 0 & f^2 \end{pmatrix} : \ f \in \mathbb{Q} \setminus \{0\}, \ g \in \mathbb{Q} \setminus \{0\}\}$$

$$\cup \ \{\tfrac{1}{f} \begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & -f^2 h & fh \\ 0 & 0 & -f^3 h+f^2 & f^2 h \\ -f & 1 & 0 & f^2 \end{pmatrix} : \ f, h \in \mathbb{Q} \setminus \{0\}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & f & -1 \\ 1 & -1 & f^2+f+1 & -f-1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ f \in \mathbb{Q}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -f & 1 \\ -1 & -1 & -f^2+f-1 & f-1 \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ f \in \mathbb{Q}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & f & -1 & h \\ 0 & 0 & 0 & 1 \\ -1 & h & 0 & f \end{pmatrix} : \ f, h \in \mathbb{Q}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix} : \ f \in \mathbb{Q}, \ e \in \mathbb{Q} \setminus \{0\}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ f \in \mathbb{Q}, \ e \in \mathbb{Q} \setminus \{0\}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1-l & -1-l & -1 \\ 1 & -1 & l^2+l+1 & l \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ l \in \mathbb{Q} \setminus \{-1\}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1+l & -1-l & 1 \\ -1 & -1 & -l^2-l-1 & l \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ l \in \mathbb{Q} \setminus \{-1\}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 0 & g & 0 \\ 0 & 0 & 0 & -1 \\ -g & 0 & -e & 0 \end{pmatrix} : \ e, g \in \mathbb{Q}, \ e^2 - g^2 = 1\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 1-e & 1-e & e-1 \\ e-1 & 1-e & 1-e & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e \in \mathbb{Q} \setminus \{-1, 0, \tfrac{1}{2}, 1\}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & e-1 & 1-e & 1-e \\ 1-e & 1-e & e-1 & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e \in \mathbb{Q} \setminus \{-1, 0, \tfrac{1}{2}, 1\}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ j & 0 & -1 & 0 \end{pmatrix} : \ j \in \mathbb{Q}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ -j & 0 & 1 & 0 \end{pmatrix} : \ j \in \mathbb{Q}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}\}$$

$$\cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -2 & 2 & 2 \\ 2 & 2 & -2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 2 & -2 \\ -2 & 2 & 2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}\}$$

So for each element A of this subset $\mathcal{L}'$ of $\mathcal{L}$ that has an irreducible characteristic polynomial $\chi_A(X) \in \mathbb{Q}[X]$, the field extension $\mathbb{Q}[A]|\mathbb{Q}$ is galois with Galois group isomorphic to C_4. Cf. also Lemma 30.

Remark 32 Each matrix in the subset

$$\begin{array}{rl}
& \{\frac{1}{f}\begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & fg & -g \\ 0 & 0 & f^2g+f^2 & -fg \\ -f & 1 & 0 & f^2 \end{pmatrix} : \ f \in \mathbb{Q}\setminus\{0\},\ g \in \mathbb{Q}\setminus\{0,\tfrac{1}{2}\}\} \\
\cup & \{\frac{1}{f}\begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & -f^2h & fh \\ 0 & 0 & -f^3h+f^2 & f^2h \\ -f & 1 & 0 & f^2 \end{pmatrix} : \ f,h \in \mathbb{Q}\setminus\{0\}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix} : \ f \in \mathbb{Q},\ e \in \mathbb{Q}\setminus\{0\}\} \\
\cup & \{\begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&e \\ 0&0&1&0 \end{pmatrix} : \ f \in \mathbb{Q},\ e \in \mathbb{Q}\setminus\{0\}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 0 & g & 0 \\ 0 & 0 & 0 & -1 \\ -g & 0 & -e & 0 \end{pmatrix} : \ e^2-g^2=1,\ e,g \in \mathbb{Q}\} \\
\cup & \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 1-e & 1-e & e-1 \\ e-1 & 1-e & 1-e & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e \in \mathbb{Q}\setminus\{-1,0,\tfrac{1}{2},1\}\} \ \cup \ \{\begin{pmatrix} 0 & 1 & 0 & 0 \\ e & e-1 & 1-e & 1-e \\ 1-e & 1-e & e-1 & e \\ 0 & 0 & 1 & 0 \end{pmatrix} : \ e \in \mathbb{Q}\setminus\{-1,0,\tfrac{1}{2},1\}\} \\
\cup & \{\begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&j&0&-1 \\ j&0&-1&0 \end{pmatrix} : \ j \in \mathbb{Q}\} \ \cup \ \{\begin{pmatrix} 0&1&0&0 \\ -1&0&0&0 \\ 0&j&0&-1 \\ -j&0&1&0 \end{pmatrix} : \ j \in \mathbb{Q}\} \\
\cup & \{\begin{pmatrix} 0&1&0&0 \\ 0&-1&1&1 \\ 1&1&-1&0 \\ 0&0&1&0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0&1&0&0 \\ 0&1&1&-1 \\ -1&1&1&0 \\ 0&0&1&0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0&1&0&0 \\ -1&-2&2&2 \\ 2&2&-2&-1 \\ 0&0&1&0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0&1&0&0 \\ -1&2&2&-2 \\ -2&2&2&-1 \\ 0&0&1&0 \end{pmatrix}\} \ \cup \ \{\begin{pmatrix} 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \end{pmatrix}\} \\
\subseteq & \mathcal{L},
\end{array}$$

has a reducible characteristic polynomial in $\mathbb{Q}[X]$.

Proof. The matrix $A := \frac{1}{f}\begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & fg & -g \\ 0 & 0 & f^2g+f^2 & -fg \\ -f & 1 & 0 & f^2 \end{pmatrix}$, where $f \in \mathbb{Q}\setminus\{0\},\ g \in \mathbb{Q}\setminus\{0,\frac{1}{2}\}$, has

$$\begin{aligned}
\chi_A(X) &= \det(X\,\mathrm{I}_4 - A) = \det(\begin{pmatrix} X&0&0&0 \\ 0&X&0&0 \\ 0&0&X&0 \\ 0&0&0&X \end{pmatrix} - \tfrac{1}{f}\begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & fg & -g \\ 0 & 0 & f^2g+f^2 & -fg \\ -f & 1 & 0 & f^2 \end{pmatrix}) \\
&= \tfrac{1}{f^2}\,(X-f)^2(X^2f^2 + X(-f^3g-f^3)+g).
\end{aligned}$$

The matrix $A := \frac{1}{f}\begin{pmatrix} 0 & f & 0 & 0 \\ 0 & f^2 & -f^2h & fh \\ 0 & 0 & -f^3h+f^2 & f^2h \\ -f & 1 & 0 & f^2 \end{pmatrix}$, where $f,h \in \mathbb{Q}\setminus\{0\}$, has

$$\chi_A(X) = \det(X\,\mathrm{I}_4 - A) = \tfrac{1}{f}\,(X-f)^2(X^2f + X(f^3h-f^2)-h).$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & f & 0 & 0 \\ 0 & 0 & f & -e \\ 0 & 0 & -1 & 0 \end{pmatrix}$, where $f \in \mathbb{Q},\ e \in \mathbb{Q}\setminus\{0\}$, has

$$\chi_A(X) = \det(X\,\mathrm{I}_4 - A) = (X^2 - Xf - e)^2.$$

The matrix $A := \begin{pmatrix} 0&1&0&0 \\ e&f&0&0 \\ 0&0&f&e \\ 0&0&1&0 \end{pmatrix}$, where $f \in \mathbb{Q},\ e \in \mathbb{Q}\setminus\{0\}$, has

$$\chi_A(X) = \det(X\,\mathrm{I}_4 - A) = (X^2 - Xf - e)^2.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 0 & g & 0 \\ 0 & 0 & 0 & -1 \\ -g & 0 & -e & 0 \end{pmatrix}$ with $e^2 - g^2 = 1$, where $e, g \in \mathbb{Q}\}$, has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X^2 - e + g)(X^2 - e - g).$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & 1-e & 1-e & e-1 \\ e-1 & 1-e & 1-e & e \\ 0 & 0 & 1 & 0 \end{pmatrix}$, where $e \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1\}$, has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X+1)(X-1)^2(X+2e-1).$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ e & e-1 & 1-e & 1-e \\ 1-e & 1-e & e-1 & e \\ 0 & 0 & 1 & 0 \end{pmatrix}$, where $e \in \mathbb{Q} \setminus \{-1, 0, \frac{1}{2}, 1\}$, has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X-1)(X+1)^2(X-2e+1).$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ j & 0 & -1 & 0 \end{pmatrix}$, where $j \in \mathbb{Q}$, has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X-1)^2(X+1)^2.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & j & 0 & -1 \\ -j & 0 & 1 & 0 \end{pmatrix}$, where $j \in \mathbb{Q}$, has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X^2+1)^2.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X-1)(X+1)^3.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X+1)(X-1)^3.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & -2 & 2 & 2 \\ 2 & 2 & -2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X+3)(X-1)(X+1)^2.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 2 & -2 \\ -2 & 2 & 2 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X+1)(X-3)(X-1)^2.$$

The matrix $A := \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ has

$$\chi_A(X) \;=\; \det(X\,\mathrm{I}_4 - A) \;=\; (X-1)(X+1)(X^2+1).$$

□

Example 33 In the 7th subset in the union occurring in Proposition 31, for $f = 2$ we have the matrix $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 2 & 2 & -1 \\ 1 & -1 & 7 & -3 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

It has the characteristic polynomial $\chi_A(X) = X^4 - 9X^3 + 19X^2 - 9X + 1$.

We can see with Maple that this characteristic polynomial is irreducible:

```
A := matrix([[0, 1, 0, 0], [0, 2, 2, -1], [1, -1, 7, -3], [0, 0, 1, 0]]);
factor(charpoly(A,X));
```

This has a single factor. Thus $\chi_A(X)$ is irreducible in $\mathbb{Q}[X]$.

We test with Magma whether $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q}) \simeq \mathrm{C}_4$:

```
P<X> := PolynomialRing(Rationals());
f := X^4 - 9*X^3 + 19*X^2 - 9*X + 1;
G := GaloisGroup(f);
print "Order(G) =", Order(G);
print "G.2 :", G.2;
```

Magma gives:

```
Order(G) = 4
G.2 : (1, 2, 3, 4)
```

Thus $\mathbb{Q}[A] \simeq \mathrm{C}_4$.

Example 34 In the 22nd subset in the union occurring in Proposition 31, we have the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} .$$

It has the characteristic polynomial $\chi_A(X) = X^4 + X^3 + X^2 + X + 1$.

This polynomial is the 5th cyclotomic polynomial. I.e. it is the minimal polynomial of ζ_5 over $\mathbb{Q}$. In particular, it is irreducible in $\mathbb{Q}[X]$.

In the 21st subset in the union occurring in Proposition 31, we have the matrix

$$\tilde{A} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} .$$

It has the characteristic polynomial $\chi_{\tilde{A}}(X) = X^4 - X^3 + X^2 - X + 1$, which is the minimal polynomial of $-\zeta_5$ over $\mathbb{Q}$. In particular, it is irreducible in $\mathbb{Q}[X]$.

So $\mathbb{Q}[A] \simeq \mathbb{Q}(\zeta_5) = \mathbb{Q}(-\zeta_5) \simeq \mathbb{Q}[\tilde{A}]$. In particular, $\mathbb{Q}[A] \simeq \mathbb{Q}[\tilde{A}]$.

Note that $\mathbb{Q}[A] \neq \mathbb{Q}[\tilde{A}]$ as subalgebra of $\mathbb{Q}^{4\times 4}$, as follows by Lemma 21:

Assume that $\mathbb{Q}[A] = \mathbb{Q}[\tilde{A}]$. Then $A, \tilde{A} \in \mathbb{Q}[A]$ and

$$\mathrm{e}_1 A \;=\; (0\,1\,0\,0) \;=\; \mathrm{e}_1 \tilde{A}.$$

Thus, by Lemma 21, $A = \tilde{A}$. But $A \neq \tilde{A}$. So we have a *contradiction*.

Finally, $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q}) \simeq \mathrm{C}_4$.

Example 35 In the 4th subset in the union occurring in Proposition 31, for $e = 1$ and $i = -1$ we have the matrix $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 1 \\ -1 & 0 & -2 & -2 \\ 0 & 0 & -1 & 0 \end{pmatrix}$.

It has the characteristic polynomial $\chi_A(X) = X^4 + 3X^3 - X^2 - 3X + 1$.

We can see with Maple that this characteristic polynomial is irreducible:

```
A := matrix([[0, 1, 0, 0], [1, -1, 1, 1], [-1, 0, -2, -2], [0, 0, -1, 0]]);
factor(charpoly(A,X));
```

This has a single factor. Thus $\chi_A(X)$ is irreducible in $\mathbb{Q}[X]$.

We test with Magma whether $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q}) \simeq \mathrm{C}_4$:

```
P<X> := PolynomialRing(Rationals());
f := X^4 + 3*X^3 - X^2 - 3*X + 1;
G := GaloisGroup(f);
print "Order(G) =", Order(G);
print "G.2 :", G.2;
```

Magma gives:

```
Order(G) = 4
G.2 : (1, 4, 3, 2)
```

Thus $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q}) \simeq \mathrm{C}_4$.

Example 36 In the 5th subset in the union occurring in Proposition 31, for $e = 1$ and $i = -1$ we have the matrix $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 3 & -1 & 1 \\ -1 & -2 & -2 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

It has the characteristic polynomial $\chi_A(X) = X^4 - X^3 - 9X^2 - X + 1$.

We can see with Maple that this characteristic polynomial is irreducible:

```
A := matrix([[0, 1, 0, 0], [1, 3, -1, 1], [-1, -2, -2, 0], [0, 0, 1, 0]]);
factor(charpoly(A,X));
```

This has a single factor. Thus $\chi_A(X)$ is irreducible in $\mathbb{Q}[X]$.

We test with Magma whether $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q}) \simeq \mathrm{C}_4$:

```
P<X> := PolynomialRing(Rationals());
f := X^4 - X^3 - 9*X^2 - X + 1;
G := GaloisGroup(f);
print "Order(G) =", Order(G);
print "G.2 :", G.2;
```

Magma gives:

```
Order(G) = 4
G.2 : (1, 3, 4, 2)
```

Thus $\mathrm{Gal}(\mathbb{Q}[A]|\mathbb{Q}) \simeq \mathrm{C}_4$.

2.3 The symmetric group S_3

Suppose that $G = \mathrm{S}_3 = \langle \rho_1, \rho_2 \rangle := \langle (1,2),\ (1,2,3) \rangle$ and $Q = \mathbb{Q}$.

We write

$$\begin{array}{rcccl} \sigma_1 & := & \rho_1^0 \cdot \rho_2^0 & = & 1_{\mathrm{S}_3}, \\ \sigma_2 & := & \rho_1^1 \cdot \rho_2^0 & = & (1,2), \\ \sigma_3 & := & \rho_1^1 \cdot \rho_2^1 & = & (1,3), \\ \sigma_4 & := & \rho_1^1 \cdot \rho_2^2 & = & (2,3), \\ \sigma_5 & := & \rho_1^0 \cdot \rho_2^1 & = & (1,2,3), \\ \sigma_6 & := & \rho_1^0 \cdot \rho_2^2 & = & (1,3,2)\,. \end{array}$$

To calculate the permutation matrix $S_1 = S_{\rho_1}$, in the notation of Definition 15, we obtain the bijection $\alpha : [1,6] \to [1,6]$ with $1\alpha = 2$, $2\alpha = 1$, $3\alpha = 6$, $4\alpha = 5$, $5\alpha = 4$ and $6\alpha = 3$.

So we obtain $S_1 := \begin{pmatrix} 0&1&0&0&0&0 \\ 1&0&0&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&0&0&1&0 \\ 0&0&0&1&0&0 \\ 0&0&1&0&0&0 \end{pmatrix}$.

To calculate the permutation matrix $S_2 = S_{\rho_2}$, in the notation of Definition 15, we obtain the bijection $\alpha : [1,6] \to [1,6]$ with $1\alpha = 5$, $2\alpha = 3$, $3\alpha = 4$, $4\alpha = 2$, $5\alpha = 6$ and $6\alpha = 1$.

So we obtain $S_2 := \begin{pmatrix} 0&0&0&0&1&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&1&0&0&0&0 \\ 0&0&0&0&0&1 \\ 1&0&0&0&0&0 \end{pmatrix}$.

Moreover, we have $\mathbb{S} := \{S_1, S_2\}$.

We want to find Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to S_3. By Theorem 19, each such Galois extension is, up to isomorphism, of the form $\mathbb{Q}[A]|\mathbb{Q}$ for some $A \in \mathbb{Q}^{6\times 6}$ such that $A \cdot A^{S_1} = A^{S_1} \cdot A$ and such that $A \cdot A^{S_2} = A^{S_2} \cdot A$ and such that $\chi_A(X) \in \mathbb{Q}[X]$ is irreducible.

So we search elements of the Galois variety of S_3 that have an irreducible characteristic polynomial.

The Galois variety of S_3 is given by

$$\{A \in \mathrm{GL}_6(\mathbb{Q}) \ : \ A \cdot A^{S_1} = A^{S_1} \cdot A \ \text{ and } \ A \cdot A^{S_2} = A^{S_2} \cdot A\}\,.$$

This system of equations turned out to be too big for a treatment with our computer algebra means.

So we restrict our consideration to matrices of the form $A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} \\ a_{3,1} & a_{3,1} & a_{3,1} & a_{3,1} & a_{3,1} & a_{3,1} \\ a_{4,1} & a_{4,2} & a_{4,1} & a_{4,4} & a_{4,5} & a_{4,6} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} \end{pmatrix} \in \mathrm{GL}_6(\mathbb{Q})$.

This restriction is artificial and only justified by the result: a two-parameter-family of solutions.

We let Maple calculate the matrices equations $A^{S_1} \cdot A = A \cdot A^{S_1}$ and $A^{S_2} \cdot A = A \cdot A^{S_2}$.

```
A := matrix([[0,1,0,0,0,0],[a21,a22,a23,a24,a25,a26],[a31,a31,a31,a31,a31,a31],
[a41,a42,a41,a44,a45,a46],[0,0,0,1,0,0],[a61,a62,a63,a64,a65,a66]]);
S1 := matrix([[0,1,0,0,0,0],[1,0,0,0,0,0],[0,0,0,0,0,1],[0,0,0,0,1,0],
[0,0,0,1,0,0],[0,0,1,0,0,0]]);
S2 := matrix([[0,0,0,0,1,0],[0,0,1,0,0,0],[0,0,0,1,0,0],[0,1,0,0,0,0],
[0,0,0,0,0,1],[1,0,0,0,0,0]]);
IS1 := inverse(S1);
IS2 := inverse(S2);
Dif1  := evalm(IS1&*A&*S1 &* A - A &* IS1&*A&*S1);
Dif2 := evalm(IS2&*A&*S2 &* A - A &* IS2&*A&*S2);
for i from 1 to 6 do for j from 1 to 6 do printf("%a = 0\n",Dif1[i,j]); od; od;
for i from 1 to 6 do for j from 1 to 6 do printf("%a = 0\n",Dif2[i,j]); od; od;
```

Maple gives a system of equations, which we use to continue with Magma as follows.

```
K<a21,a31> := FunctionField(Rationals(),2);
R<a22,a23,a24,a25,a26,a41,a42,a44,a45,a46,a63,a66,a61,a62,a64,a65>
  := PolynomialRing(K, 16);
I := ideal<R |
a21^2+a23*a61+a25*a41+a26*a31-1,
a21*a22+a23*a62+a25*a42+a26*a31+a22,
a21*a23+a23*a63+a25*a41+a26*a31,
a21*a24+a23*a64+a25*a44+a26*a31+a24,
a21*a25+a23*a65+a25*a45+a26*a31,
a21*a26+a23*a66+a25*a46+a26*a31,
-a21*a22-a23*a62-a25*a42-a26*a31-a22,
-a21^2-a23*a61-a25*a41-a26*a31+1,
-a21*a26-a23*a66-a25*a46-a26*a31,
-a21*a25-a23*a65-a25*a45-a26*a31,
-a21*a24-a23*a64-a25*a44-a26*a31-a24,
-a21*a23-a23*a63-a25*a41-a26*a31,
a21*a61-a22*a31-a31^2-a31*a42-a31*a62+a31*a66+a41*a65+a61*a63-a31,
-a21*a31+a22*a61-a31^2-a31*a41-a31*a61+a31*a66+a42*a65+a62*a63+a62,
a23*a61-a26*a31-a31^2-a31*a46+a41*a65+a63^2,
a24*a61-a25*a31-a31^2-a31*a45-a31*a65+a31*a66+a44*a65+a63*a64+a64,
-a24*a31+a25*a61-a31^2-a31*a44-a31*a64+a31*a66+a45*a65+a63*a65-a31,
-a23*a31+a26*a61-a31^2-a31*a41-a31*a63+a31*a66+a46*a65+a63*a66,
-a22*a41-a31*a46-a41*a62-a42*a45-a42,
-a21*a41-a31*a46-a41*a45-a41*a61,
-a26*a41-a31*a46-a41*a66-a45*a46,
```

```
-a25*a41-a31*a46-a41*a65-a45^2+1,
-a24*a41-a31*a46-a41*a64-a44*a45-a44,
-a23*a41-a31*a46-a41*a45-a41*a63,
a21*a41+a31*a46+a41*a45+a41*a61,
a22*a41+a31*a46+a41*a62+a42*a45+a42,
a23*a41+a31*a46+a41*a45+a41*a63,
a24*a41+a31*a46+a41*a64+a44*a45+a44,
a25*a41+a31*a46+a41*a65+a45^2-1,
a26*a41+a31*a46+a41*a66+a45*a46,
a21*a31-a22*a61+a31^2+a31*a41+a31*a61-a31*a66-a42*a65-a62*a63-a62,
-a21*a61+a22*a31+a31^2+a31*a42+a31*a62-a31*a66-a41*a65-a61*a63+a31,
a23*a31-a26*a61+a31^2+a31*a41+a31*a63-a31*a66-a46*a65-a63*a66,
a24*a31-a25*a61+a31^2+a31*a44+a31*a64-a31*a66-a45*a65-a63*a65+a31,
-a24*a61+a25*a31+a31^2+a31*a45+a31*a65-a31*a66-a44*a65-a63*a64-a64,
-a23*a61+a26*a31+a31^2+a31*a46-a41*a65-a63^2,
a21*a64+a31*a62+a41*a63+a61*a65-a46,
a22*a64+a31*a62+a42*a63+a62*a65-a44+a66,
a23*a64+a31*a62+a41*a63+a63*a65-a42,
a24*a64+a31*a62+a44*a63+a64*a65-a41+a61,
a25*a64+a31*a62+a45*a63+a65^2-a41,
a26*a64+a31*a62+a46*a63+a65*a66-a45,
a21*a44-a21*a66-a22*a46-a23*a26-a24*a31+a31*a42+a41^2+a45*a61,
-a21*a64-a23*a24-a24*a31+a31*a42+a41*a42+a45*a62-a26+a46,
-a21*a62-a22*a23-a22*a42+a23*a44-a24*a31+a31*a42+a41^2+a45*a63-a25,
-a21*a63-a22*a41-a23^2-a24*a31+a24*a44+a31*a42+a41*a44+a45*a64+a41,
-a21*a23-a21*a61-a22*a41-a24*a31+a25*a44+a31*a42+a41*a45+a45*a65,
-a21*a65-a22*a45-a23*a25-a24*a31+a26*a44+a31*a42+a41*a46+a45*a66,
a21*a24+a22*a31+a23*a41+a25*a61-a26*a31-a31^2-a31*a46-a31*a66,
a22*a24+a22*a31+a23*a42-a24*a31+a25*a62-a31^2-a31*a44-a31*a64+a26-a31,
a23*a24+a23*a41+a25*a63-a31^2-a31*a42-a31*a62-a31,
a22*a31-a23*a31+a23*a44+a24^2+a25*a64-a31^2-a31*a41-a31*a63+a21,
-a21*a31+a22*a31+a23*a45+a24*a25+a25*a65-a31^2-a31*a41-a31*a61,
a22*a31+a23*a46+a24*a26-a25*a31+a25*a66-a31^2-a31*a45-a31*a65,
a21*a31-a26*a41+a31^2+a31*a41-a31*a44+a31*a61-a41*a66-a42*a46,
a22*a31-a24*a41+a31^2+a31*a42-a31*a44+a31*a62-a41*a64-a42*a44+a31-a46,
-a22*a41+a23*a31+a31^2+a31*a41-a31*a44+a31*a63-a41*a62-a42^2-a45,
-a23*a41+a24*a31+a31^2+a31*a64-a41*a42-a41*a63+a31,
-a21*a41+a25*a31+a31^2-a31*a44+a31*a45+a31*a65-a41*a42-a41*a61,
-a25*a41+a26*a31+a31^2-a31*a44+a31*a46+a31*a66-a41*a65-a42*a45,
-a26*a63-a31*a64-a46*a62-a61*a66+a21,
-a24*a63-a31*a64-a44*a62-a61*a64+a22-a66,
-a22*a63-a31*a64-a42*a62-a61*a62+a23-a65,
-a23*a63-a31*a64-a41*a62-a61*a63+a24,
-a21*a63-a31*a64-a41*a62-a61^2+a25,
-a25*a63-a31*a64-a45*a62-a61*a65+a26
>;
TriangularDecomposition(I);
```

Magma gives the solutions:

```
Ideal of Polynomial ring of rank 16 over Multivariate rational function field
  of rank 2 over Rational Field
Order: Lexicographical
Variables: a22, a23, a24, a25, a26, a41, a42, a44, a45, a46,
           a63, a66, a61, a62, a64, a65
Inhomogeneous, Dimension 0
Groebner basis:
[
    a22 + (-a21*a31 - a21 - a31 - 1)/a31,
    a23 - a21 - 1,
    a24 - a21,
    a25 - a21 - 1,
    a26 + (-a21*a31 - a21 - a31 - 1)/a31,
    a41 + (2*a21*a31 + a31^2 + a31)/(a21 + 2*a31 + 1),
    a42 + (2*a21*a31 + a21 + a31^2 + 3*a31 + 1)/(a21 + 2*a31 + 1),
    a44 + (2*a21*a31 + 2*a21 + a31^2 + 2*a31 + 1)/(a21 + 2*a31 + 1),
    a45 + (2*a21*a31 + a21 + a31^2 + 3*a31 + 1)/(a21 + 2*a31 + 1),
    a46 + (2*a21*a31 + 2*a21 + a31^2 + 2*a31 + 1)/(a21 + 2*a31 + 1),
    a63 + (a21^2 + a21*a31 + 2*a21 + a31^2 + 2*a31 + 1)/(a21 + 2*a31 + 1),
    a66 + (a21^2*a31 + a21^2 + a21*a31^2 + 2*a21*a31 + a21 + a31^3 + a31^2)
    /(a21*a31 + 2*a31^2 + a31),
    a61 + (a21^2 + a21*a31 + a21 + a31^2)/(a21 + 2*a31 + 1),
    a62 + (a21^2*a31 + a21^2 + a21*a31^2 + 4*a21*a31 + 2*a21 + a31^3 +
    2*a31^2 + 3*a31 + 1)/(a21*a31 + 2*a31^2 + a31),
    a64 + (a21^2 + a21*a31 + a31^2 + a31)/(a21 + 2*a31 + 1),
    a65 + (a21^2 + a21*a31 + a21 + a31^2)/(a21 + 2*a31 + 1)
]
```

If $a_{3,1} \neq 0$ and $a_{2,1} + 2a_{3,1} + 1 \neq 0$, this can be used to find solutions to our original system of equations over $\mathbb{Q}$.

Let $N := \{(r,t) \in \mathbb{Q} \times \mathbb{Q} : \ r + 2t + 1 \neq 0 \text{ and } t \neq 0\}$.

For $(r,t) \in N$, we let

$$B_{r,t} := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ r & \frac{(r+1)(t+1)}{t} & r+1 & r & r+1 & \frac{(r+1)(t+1)}{t} \\ t & t & t & t & t & t \\ -\frac{t(t+2r+1)}{r+2t+1} & -\frac{2rt+r+t^2+3t+1}{r+2t+1} & -\frac{t(t+2r+1)}{r+2t+1} & -\frac{(2r+t+1)(t+1)}{r+2t+1} & -\frac{2rt+r+t^2+3t+1}{r+2t+1} & -\frac{(2r+t+1)(t+1)}{r+2t+1} \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -\frac{r^2+rt+r+t^2}{r+2t+1} & -\frac{r^2t+r^2+rt^2+4rt+2r+t^3+2t^2+3t+1}{(r+2t+1)\,t} & -\frac{r^2+rt+2r+(t+1)^2}{r+2t+1} & -\frac{r^2+rt+t^2+t}{r+2t+1} & -\frac{r^2+rt+r+t^2}{r+2t+1} & -\frac{(t+1)(r^2+rt+t^2+r)}{(r+2t+1)t} \end{pmatrix}.$$

We have $\det B_{r,t} = 1$ for $(r,t) \in N$.

So we can summarize as follows.

Remark 37 We have

$$\{\, B_{r,t} : \ (r,t) \in N \,\} \ \subseteq \ \{\, A \in \mathrm{GL}_6(\mathbb{Q}) : \ A^{S_1} \cdot A = A \cdot A^{S_1} \text{ and } A^{S_2} \cdot A = A \cdot A^{S_2} \,\}\,.$$

So given $(r,t) \in N$ and provided that the matrix $B_{r,t}$ has an irreducible characteristic polynomial $\chi_{B_{r,t}}(X) \in \mathbb{Q}[X]$, then the field extension $\mathbb{Q}[B_{r,t}]|\mathbb{Q}$ is galois with Galois group isomorphic to S_3.

Example 38 We have $B_{-2,1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -2 & -2 & -1 & -2 & -1 & -2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 4 & 1 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & -2 & -4 & -1 & -2 \end{pmatrix}$.

It has the characteristic polynomial $\chi_{B_{-2,1}}(X) = X^6 - X^5 + 6X^4 + 7X^3 + 6X^2 - X + 1$.

We verify with Maple that this characteristic polynomial is irreducible:

```
A := matrix([[0,1,0,0,0,0],[-2,-2,-1,-2,-1,-2],[1,1,1,1,1,1],[2,1,2,4,1,4],
[0,0,0,1,0,0],[-1,-1,-2,-4,-1,-2]]);
factor(charpoly(A,X));
```

We obtain a single factor. Thus $\chi_{B_{-2,1}}(X)$ is irreducible in $\mathbb{Q}[X]$.

We test with Magma whether $\mathrm{Gal}(\mathbb{Q}[B_{-2,1}]|\mathbb{Q}) \simeq \mathrm{S}_3$:

```
P<X> := PolynomialRing(Rationals());
f := X^6-X^5+6*X^4+7*X^3+6*X^2-X+1;
G := GaloisGroup(f);
print "Order(G) =", Order(G);
print "IsAbelian(G):", IsAbelian(G);
```

Magma gives:

```
Order(G) = 6
IsAbelian(G): false
```

Thus $\mathrm{Gal}(\mathbb{Q}[B_{-2,1}]|\mathbb{Q}) \simeq \mathrm{S}_3$.

Example 39 We have $B_{0,1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ -2/3 & -5/3 & -2/3 & -4/3 & -5/3 & -4/3 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -1/3 & -7/3 & -4/3 & -2/3 & -1/3 & -2/3 \end{pmatrix}$.

It has the characteristic polynomial $\chi_{B_{0,1}}(X) = X^6 - X^5 + \frac{10}{3}X^4 + \frac{5}{3}X^3 + \frac{10}{3}X^2 - X + 1$.

We verify with Maple that this characteristic polynomial is irreducible:

```
A := matrix([[0, 1, 0, 0, 0, 0], [0, 2, 1, 0, 1, 2], [1, 1, 1, 1, 1, 1],
[-2/3, -5/3, -2/3, -4/3, -5/3, -4/3], [0, 0, 0, 1, 0, 0],
[-1/3, -7/3, -4/3, -2/3,-1/3, -2/3]]);
factor(charpoly(A,X));
```

We obtain a single factor. Thus $\chi_{B_{0,1}}(X)$ is irreducible in $\mathbb{Q}[X]$.

We test with Magma whether $\mathrm{Gal}(\mathbb{Q}[B_{0,1}]|\mathbb{Q}) \simeq \mathrm{S}_3$:

```
P<X> := PolynomialRing(Rationals());
f := X^6-X^5+10/3*X^4+5/3*X^3+10/3*X^2-X+1;
G := GaloisGroup(f);
print "Order(G) =", Order(G);
print "IsAbelian(G):", IsAbelian(G);
```

Magma gives:

```
Order(G) = 6
IsAbelian(G): false
```

Thus $\mathrm{Gal}(\mathbb{Q}[B_{0,1}]|\mathbb{Q}) \simeq \mathrm{S}_3$.

Example 40 We have $B_{-1,1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & 0 & 0 & -1 & -0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 & 0 \end{pmatrix}$.

It has the characteristic polynomial $\chi_A(X) = X^6 - X^5 + 2X^4 - X^3 + 2X^2 - X + 1$.

We verify with Maple that this characteristic polynomial is reducible:

```
A := matrix([[0, 1, 0, 0, 0, 0], [-1, 0, 0, -1, 0, 0], [1, 1, 1, 1, 1, 1],
[0, -1, 0, 0, -1, 0], [0, 0, 0, 1, 0, 0],
[0, -1, -1, -1,0, 0]]);
factor(charpoly(A,X));
```

We obtain `(X^2+X+1)*(X^2-X+1)^2`. Thus $\chi_{B_{0,1}}(X)$ is reducible in $\mathbb{Q}[X]$.

So in fact the condition on the characteristic polynomial to be irreducible in $\mathbb{Q}[X]$ cannot be omitted.

References

[1] Blessenohl D., Johnsen, K., *Eine Verschärfung des Satzes von der Normalbasis*, J. Alg. 103, p. 141–159, 1986.

[2] Bosma W., Cannon, J., Playoust, C., *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24, 235–265, 1997.

[3] Lang, S., *Algebra,* Graduate Texts in Mathematics 211, Springer-Verlag, 2002.

[4] Maple, *Maple User Manual*, Toronto: Maplesoft, a division of Waterloo Maple Inc., 2005-2019.

[5] Wang, D., *Elimination practice. Software tools and applications*, Imperial College Press, London, 2004. Cf. also `http://wang.cc4cm.org/epsilon/`, where `http://wang.cc4cm.org/epsifun.pdf` provides a handbook for the package Epsilon.

Zusammenfassung

Sei G eine endliche Gruppe mit $|G| =: n$. Weiter sei ein Körper Q von Charakteristik 0 gegeben. Dieser Körper ist unser Grundkörper.

Sei eine Galoiserweiterung $K|Q$ gegeben mit einer Galoisgruppe, welche isomorph zu G ist.

Wir bilden die verschränkte Gruppenalgebra $K \wr G$, welche als K-Vektorraum mit der Basis G und der Multiplikation $\sigma a \cdot \rho b = \sigma\rho a^{\rho} b$ für $\sigma, \rho \in G$ und $a, b \in K$ definiert ist.

Diese verschränkte Gruppenalgebra ist eine Q-Algebra, welche isomorph zu $Q^{n\times n}$ ist.

Wir wählen nun ein Element $z \in K$ so, dass $(z^{\sigma} : \sigma \in G)$ eine Normalbasis von K über Q ist. Dadurch ist auch $K = Q(z) = Q[z]$.

Wir haben einen Isomorphismus von $K \wr G$ nach $Q^{n\times n}$, welcher das Element z auf eine Matrix $A \in Q^{n\times n}$ abbildet. Folglich wird $K = Q[z]$ isomorph auf die Teilalgebra $Q[A]$ von $Q^{n\times n}$ abgebildet.

Für $\rho \in G$ ist das Bild $S_\rho \in Q^{n\times n}$ eine Permutationsmatrix. Es wird z^{ρ} abgebildet auf A^{S_ρ}. Es gilt somit $A^{S_\rho} \in Q[A]$. Da $Q[A]$ kommutativ ist, haben wir die Gleichung $A^{S_\rho} \cdot A = A \cdot A^{S_\rho}$ für $\rho \in G$.

Seien nun Erzeuger $\rho_1, \ldots, \rho_m$ von G gewählt, sodass $G = \langle \rho_1, \ldots, \rho_m \rangle$. Wir schreiben $S_i := S_{\rho_i} \in \mathrm{GL}_n(Q)$ für $i \in [1, m]$. Dabei sind $S_1, \ldots, S_m$ von der Gruppe G abhängig, aber nicht von der Galoiserweiterung.

Das Minimalpolynom von z ist irreduzibel von Grad n. Es stimmt mit dem Minimalpolynom von A und mit dem charakteristischen Polynom $\chi_A(X) \in Q[X]$ überein. Insbesondere ist $\chi_A(X)$ irreduzibel.

Folglich ist K isomorph zu $Q[A]$ als Körpererweiterung von Q. Dabei erfüllt A die Gleichung $A^{S_i} \cdot A = A \cdot A^{S_i}$ für $i \in [1, n]$, und $\chi_A(X) \in Q[X]$ ist irreduzibel.

Nun wollen wir dieses Verfahren umdrehen.

Hierfür behalten wir die Permutationsmatrizen $S_1, \ldots, S_m \in \mathrm{GL}_n(Q)$.

Die Teilmenge

$$\{\, A \in \mathrm{GL}_n(Q) :\ A^{S_i} \cdot A = A \cdot A^{S_i} \text{ for } i \in [1, m] \,\} \ \subseteq\ \mathrm{GL}_n(Q) \ \subseteq\ Q^{n\times n}$$

wird Galoisvarietät von G genannt, bezüglich der gewählten Erzeuger.

Sei nun A aus der Galoisvarietät von G. Habe zudem A ein irreduzibles charakteristisches Polynom $\chi_A(X) \in Q[X]$.

Das Gruppenelement ρ_i liefert einen Automorphismus auf $Q[A]$, welcher eine Matrix $B \in Q[A]$ auf $B^{S_i} \in Q[A]$ abbildet.

So erhält man dann eine Galoiserweiterung $Q[A]|Q$ mit der Galoisgruppe $\mathrm{Gal}(Q[A]|Q) \simeq G$.

Sei nun $Q := \mathbb{Q}$.

Wir betrachten die Galoisvarietät im Fall $G = \mathrm{C}_3$. Zunächst stellen wir fest, dass der Schnitt dieser Varietät mit dem affinen Teilraum der Matrizen der Form $\begin{pmatrix} 0 & 1 & 0 \\ * & * & * \\ * & * & * \end{pmatrix}$ immer noch alle Galoiserweiterungen mit Galoisgruppe isomorph zu C_3 liefert. Wir berechnen diesen Schnitt:

$$\begin{aligned} \mathcal{L} &:= \{A = \begin{pmatrix} 0 & 1 & 0 \\ d & e & f \\ g & h & i \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Q}) : A^S \cdot A = A \cdot A^S\} \\ &= \{\begin{pmatrix} 0 & 1 & 0 \\ 1 & e & -1 \\ 0 & -1 & -1 \end{pmatrix} : e \in \mathbb{Q}\} \cup \{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\} \cup \{ \begin{pmatrix} 0 & 1 & 0 \\ -\frac{g^2+g+1}{i} & -\frac{(g^2+g+1)^2+i^3}{gi^2} & -g-1 \\ g & \frac{g^2+g+1}{i} & i \end{pmatrix} : g, i \in \mathbb{Q} \setminus \{0\}\}. \end{aligned}$$

Damit $A \in \mathcal{L}$ tatsächlich eine Galoiserweiterung $\mathbb{Q}[A]|\mathbb{Q}$ mit Galoisgruppe isomorph zu C_3 gibt, muss man noch an das charakteristsche Polynom $\chi_A(X)$ die Bedingung stellen, irreduzibel zu sein.

Im Fall $G = \mathrm{C}_4$ liefern die gebräuchlichen Computeralgebrasysteme nur eine große Teilmenge des Schnitts der Galoisvarietät mit $\begin{pmatrix} 0 & 1 & 0 & 0 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{pmatrix}$. Diese Teilmenge setzt sich zusammen als Vereinigungsmenge von 25 kleineren Teilmengen, die mit 0 bis 3 Variablen parametrisiert sind. Auch hier muss man jeweils noch das charakteristische Polynom auf Irreduzibilität testen.

Im Fall $G = \mathrm{S}_3$ finden wir nur noch eine von zwei Variablen parametrisierte kleine Teilmenge der Galoisvarietät. Aber auch hier muss man noch bei den Matrizen das charakteristische Polynom auf Irreduzibilität testen.

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, den 19.03.2020

Katrin Leitner