

Galois and Class Field Theory for Quantum Chemists

Ichio Kikuchi¹, Akihito Kikuchi^{1*}

¹*Internationales Forschungszentrum für Quantentechnik*

June 30, 2020

Abstract

Quantum mechanics could be studied through polynomial algebra, as has been demonstrated by a work (“An approach to first-principles electronic structure calculation by symbolic-numeric computation” by A. Kikuchi). We carry forward the algebraic method of quantum mechanics through algebraic number theory; the basic equations are represented by the multivariate polynomial ideals; the symbolic computations process the ideal and disentangle the eigenstates as the algebraic variety; upon which one can build the Galois extension of the number field, in analogy with the univariate polynomial case, to investigate the hierarchy of solutions; the Galois extension is accompanied with the group operations, which permute the eigenstates from one to another, and furnish the quantum system with a non-apparent symmetry. Besides, this sort of algebraic quantum mechanics is an embodiment of the class field theory; some of the important consequences of the latter emerge in quantum mechanics. We shall demonstrate these points through simple models; we will see the use of computational algebra facilitates such sort of analysis, which might often be complicated if we try to solve them manually.

Keywords— quantum mechanics; algebraic geometry; algebraic number theory; commutative algebra; Gröbner basis; primary ideal decomposition, eigenvalue problem in quantum mechanics; molecular orbital theory; quantum chemistry; quantum chemistry in algebraic variety; symbolic computation; algebraic molecular orbital theory; Galois theory; class field theory

*akihito.kikuchi@gakushikai.jp (The corresponding author; a visiting researcher in IFQT)

1 Introduction

The purpose of this article is to acquaint the readers with the algebraic viewpoint to study quantum mechanics, utilizing computer algebra. Indeed, quantum mechanics has the feature that one could investigate through the ideas of ideal theory in commutative algebra [Kik13]. In this article, we demonstrate the following points using model computations.

- Quantum mechanics is the subject of the research of algebraic geometry. We can analyze the secular equation from the standpoint of ideal theory because the quantum states are represented by the polynomial ideals.
- We can execute the primary ideal decomposition for the ideal that represents quantum states. Through symbolic computations, we get the univariate polynomial equation, the roots of which give the energy spectrum. We determine wavefunctions in sequence from the polynomials which lie in the decomposed ideals.
- Thereupon quantum mechanics is the subject of the research of algebraic number theory. We analyze it through Galois and class field theory.
- The polynomial for the energy spectrum splits in the Galois extension of the base number field. The splitting of this polynomial consequently induces the decomposition of the prime ideal for the quantum states. The automorphism in the Galois field permutes not only the energy spectra but the corresponding quantum states which are conjugate. It is a kind of symmetry operation – indeed that of the hidden symmetry, which permutes the quantum states from one to another.
- If quantum mechanics is furnished with the algebraic representation by polynomial ideals, there emerge some of the profound consequences of class field theory, such as the reciprocity law and the density theorem.

The readers shall see the use of computer algebra could facilitate this sort of computations.

2 Preliminaries

In the elementary lectures of quantum mechanics, the matrix algebra is an essential tool of quantum mechanics [SO12, Fey65], as the energy and the wave-function are the eigenvalue and the eigenvector of the secular equation:

$$(\mathbf{H} - E) \psi = 0, \quad (1)$$

or,

$$\sum_j (H_{ij} - ES_{ij}) \psi_j = 0. \quad (2)$$

The equation is the set of polynomial equations, which generate an ideal J in commutative polynomial algebra. For example, the secular equation (for a simple molecular orbital model of the diatomic molecule) is written as

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = e \begin{pmatrix} x \\ y \end{pmatrix},$$

with the *normalization condition*

$$x^2 + y^2 = 1.$$

This set of the polynomial equations is represented by the ideal

$$J = (x + ey, y + ex, x^2 + y^2 - 1).$$

The roots of the secular equation are the common zeros of the polynomials in J , which is called the *Affine algebraic set* (*Affine algebraic variety*) and denoted by $V(J)$.

One can apply an operation (similar to Gauss elimination in linear algebra) to the polynomial set and generate the *Gröbner basis*:

$$J_{GB} = \{x + ey, -2y^2 + 1, e^2 - 1\}$$

The Gröbner basis (as an ideal) defines the Affine algebraic variety, exactly identical to that of the ideal J . As one can see, the variables in the polynomials in J_{GB} are eliminated one by one: the first contains x, y, e ; the second, y ; the third, e . Hence it is more convenient to use the Gröbner basis for the study the algebraic variety. However, one can proceed more; one applies the *primary ideal decomposition* to the ideal and obtain:

$$J = p_1 \cap p_2 = (x + y, -2y^2 + 1, e - 1) \cap (x - y, -2y^2 + 1, e + 1).$$

The ideal J is the intersection of two larger ideals p_1 and p_2 , and these two ideals cannot be decomposed anymore; from the viewpoint of commutative algebra, they are primary (indeed prime) ideals. (Here we find the similarity to the elementary number theory, concerning the factorization of an integer into primes, say, $M = p_1^{e_1} \dots p_n^{e_n}$. The prime ideals correspond to primes p_1, \dots, p_n ; the primary ideals, then, to the power of primes $p_1^{e_1}, \dots, p_n^{e_n}$.) In accordance with the prime ideals, the Affine algebraic variety is decomposed to the union of two sub-varieties:

$$V(J) = V(p_1) \cup V(p_2).$$

Observe that the primary ideal decomposition is essentially the computation of eigenstates of the given Hamiltonian.ⁱ

ⁱIn algebraic geometry, the term *spectrum* points to the set of all prime ideals of a commutative ring R , meanwhile, in quantum mechanics, it stands for the energy. In our formulation of algebraic quantum mechanics, we label each prime ideal representing a quantum state through its eigenenergy. Herein might not we use the term *spectrum* in a somewhat equivocal way to nominate the eigenstate and the corresponding prime ideal at the same time?

As for the mathematical concepts concerning this sort of algebraic method, see [KK19] and the references therein. In [Kik13], the secular equation, derived from the first-principles molecular orbital theory, is transformed into the set of polynomial equations, which are chosen to be the generators of an ideal. For this purpose, the matrix elements, analytically given by transcendental functions, are recapped into polynomials through Taylor expansion. The searching the zero set of the ideal is executed by a hybrid method of numeric and symbolic computation, through which the computer algebra enables us to conduct a various range of simulations, including the simultaneous determination of wave-function and the atomic structure, the inverse problem (from the assumed Homo-Lumo gap to the inference of the molecular structure), etc.

Provided that the polynomial representation of quantum eigenstates is obtained, the next work is to analyze and extract useful information from them. Regarding this, recall this fact: it is the central theme of Galois theory to solve univariate polynomials equations [McC91, AM98, Mil17]. Galois theory reveals an elegant mathematical structure with hierarchy, related to the extension of the field and the permutation group. (Be careful that we use the term *field* in the context of mathematics, not of physics.) We give simple examples.

Let f be a polynomial with the coefficient of rational numbers, say,

$$f = e^4 - 5e^2 + 6 = (e^2 - 3)(e^2 - 2).$$

It could not be factorized in \mathbb{Q} (the field of rational numbers). But if one extends \mathbb{Q} by adding $\sqrt{2}$ and creates a new field $\mathbb{Q}(\sqrt{2})$, the polynomial factorizes as follows:

$$f = (e^2 - 3)(e - \sqrt{2})(e + \sqrt{2}).$$

By extending the field again, in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the polynomial splits fully:

$$f = (e - \sqrt{3})(e + \sqrt{3})(e - \sqrt{2})(e + \sqrt{2}).$$

We can decompose the equation by climbing another side: $\mathbb{Q}(\sqrt{3})$.

Remark 2.1. When a polynomial is irreducible in \mathbb{Q} , one might do the factorization of the polynomial through successive extensions of \mathbb{Q} by the addition of irrational numbers which lie outside of \mathbb{Q} : in general, a base field could be extended by the addition of one of the roots of the polynomial equation

$$f = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_0 = \prod_i^n (x - \alpha_j),$$

which has the coefficients lying in the base field. The elements of the extension field are generated from two types of resources: a part of the roots of this polynomial and the elements of the base field. If all of the roots of the polynomial are included in the extension field, one can construct the automorphism of this field, which shall exchange the roots by permutations. This automorphism evolves a group and keeps invariant the elements of the base field.

The above example permits two operations ($a : \sqrt{2} \longleftrightarrow -\sqrt{2}$ and $b : \sqrt{3} \longleftrightarrow -\sqrt{3}$). They generate the automorphism in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. The corresponding group is $C_2 \times C_2$, given by

$$\{e, a, b \mid a^2 = b^2 = e, ab = ba\}$$

The elements in \mathbb{Q} is invariant by this group operation, but the elements in $\mathbb{Q}(\sqrt{2})$, represented as $a + b\sqrt{2}$, turns into $a - b\sqrt{2}$. The group operation in $\mathbb{Q}(\sqrt{3})$ behaves likewise.

Let us summarise the situation.

- In \mathbb{Q} , the polynomial is $(x^2 - 2)(x^2 - 3)$. The operations a and b , namely, the group $C_2 \times C_2$, keep the polynomial invariant.
- In $\mathbb{Q}(\sqrt{2})$, the polynomial splits as $(x - \sqrt{2})(x + \sqrt{2})(x^2 - 3)$. The group operation b , namely, the subgroup $\langle b \rangle$ fixes each component of this factorization.
- In $\mathbb{Q}(\sqrt{3})$, the polynomial splits as $(x^2 - 2)(x - \sqrt{3})(x + \sqrt{3})$. The group operation a , namely, the subgroup $\langle a \rangle$ fixes each component in the factorization.
- In $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, the polynomial splits as $(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$. The group operation which fixes each component is e (the identity).

These things could be restated more abstractly.

- Once the base field is extended by a suitable element, the splitting process of the polynomial can proceed more.
- Each extension field has a corresponding subgroup that fixes the elements in that field.
- There is a maximal field in which the given polynomial split completely.

In the present example, the subgroups and the subfields are illustrated in figures 2.2 and 2.1.

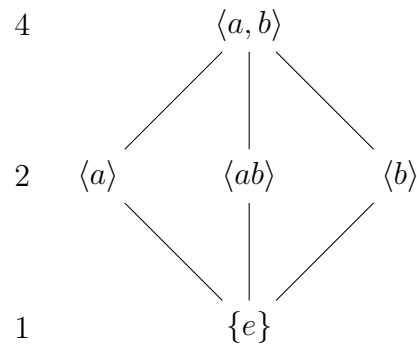


Figure 2.1: The graphical representation of the subgroup lattice for $C_2 \times C_2$. Each node shows the subgroups; The inclusion relations as subgroups are denoted by edges. The column of the numbers in the left side of the graph are the orders of the subgroups.

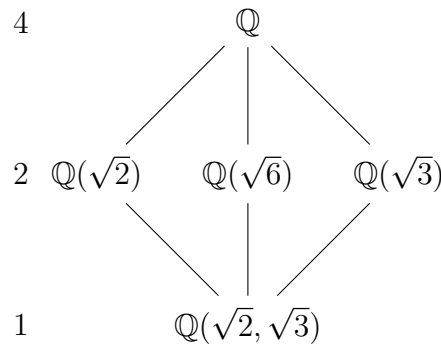


Figure 2.2: The graphical representation of the subfields that are fixed by the subgroups of $C_2 \times C_2$. Observe that this is the same graph as is presented for the subgroups. Each subfield is fixed by the Galois group situated at the corresponding node of the graph.

Let us consider another example: $g = x^4 + x^3 + x^2 + 1$. It has four roots $\alpha, \beta = \alpha^2, \gamma = \alpha^4 = -\alpha^3 - \alpha^2 - \alpha - 1, \delta = \alpha^3$. We can construct four operations which permute the roots and construct the group C_4 . They are given by

$$\begin{aligned} e &: \alpha \longrightarrow \alpha && (\text{Identity}) \\ a &: \alpha \longrightarrow \gamma && (1, 2, 3, 4) \\ a^2 &: \alpha \longrightarrow \beta && (1, 3)(2, 4) \\ a^4 &: \alpha \longrightarrow \delta && (1, 4, 3, 2) \end{aligned}$$

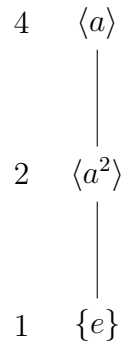


Figure 2.3: The graphical representation of the subgroup lattice for C_4 . Each node shows the subgroups; The inclusion relations as subgroups are denoted by edges. The column of the numbers in the left side of the graph are the orders of the subgroups.

- In \mathbb{Q} , the polynomial does not split.
- In $\mathbb{Q}(y)$, namely, in the extension by y such that $y^2 + y - 1 = 0$, the polynomial splits into $(x^2 - yx + 1)(x^2 + (y + 1)x + 1)$.
- In $\mathbb{Q}(\alpha)$, the polynomial splits as $(x - \alpha)(x - \beta)(x - \gamma)(x - \delta)$.

These examples are of the incorporation of the fundamental theorem of Galois theory.

Theorem 2.1. (FUNDAMENTAL THEOREM OF GALOIS THEORY) Let E be a Galois extension of F with Galois group G (which is denoted by $\text{Gal}(E/F)$). There is a one-to-one correspondence between these two sets.

- The set of subgroups of G
- The set of sub-extensions of $F \subset M \subset E$
- Let E^H be the subfield corresponding to the subgroup H of $\text{Gal}(E/F)$. E^H is the set of elements of E which are fixed by every automorphism in H .
- $H_1 \supset H_2 \iff E^{H_2} \supset E^{H_1}$.
- $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$: the index of the subgroup and the degree of the extension is equal in the correspondence of the subgroups and subfields.
- For the automorphism σ in F , $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$, and, $\text{Gal}(E/\sigma M) = \sigma \text{Gal}(E/M) \sigma^{-1}$.
- If H is normal in G , E^H is the normal extension of F and $\text{Gal}(E^H/F) \simeq G/H$.

In the first example, the Galois group is $C_2 \times C_2$ and the Galois extension is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. In the second, the Galois group is C_4 and the Galois extension is $\mathbb{Q}(\zeta_5)$. The subgroups and the subfields have a one-to-one correspondence.

Remark 2.2. Here we should recall the basic definitions concerning the Galois theory.

An algebraic field extension is the pair of a field K and a larger field L which contains K , being made by the addition of extra elements to K . Such a circumstance is denoted by L/K (L over K). L is a K -vector space and its dimension is called the degree of L over K and denoted by $[L : K]$.

A normal extension is an algebraic field extension L/K , in which every polynomial (irreducible over K) either has no root in L or splits completely into linear factors in L .

A separable extension is an algebraic field extension E/F , in which the minimal polynomial of $\alpha (\in E)$ over F has distinct roots. For α , we might find the polynomials with coefficients in F , to which α is a root. The minimal polynomial is of the minimal degrees among them. The conjugate roots of α might not always lie in F .

A Galois extension E/F is an extension which is normal and separable. E is a splitting field of a separable polynomial with coefficients in F .

$\text{Aut}(E/F)$ (the automorphism in E which fixes each element of F) is called the Galois group of E/F .

A prime \mathfrak{p} in K factors (decomposes) into the product of the prime ideals in an extension L of K in this way: $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$, where $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$. When $e_i > 1$, the prime \mathfrak{p} is said to ramify in L . Let n be the degree of L over K , and let f_i be the degree of the residue field extension $([\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}])$. Then $e_1f_1 + \cdots + e_gf_g = [L : K]$. In the case of Galois extension, the splitting occurs in this way: $\mathfrak{p} = (\mathfrak{B}_1 \cdots \mathfrak{B}_g)^e$, with $n = efg$.

An extension L of a number field K is said to be unramified over K if there is no prime ideal of \mathcal{O}_K which ramifies in \mathcal{O}_L .

A local field is the field which has a unique maximal ideal. (Caveat: for a field to be local, it requires more detailed conditions.) An extension L/K of local fields is unramified if $[L : K] = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$ where \mathfrak{P} (resp. \mathfrak{p}) is the maximal ideal of L (resp. K). In this case, the ramification index is $e = 1$.

In the next section, let us construct a simple model of molecules, represented by the set of multivariate polynomials. We represent quantum mechanics using polynomial equations. We apply the primary ideal decomposition to the corresponding ideal. Then we investigate the obtained equations using Galois theory. The analysis reveals a kind of symmetry (guaranteed by the Galois group). In [Kik18], the author has suggested such a kind of hidden symmetry in analytic equations of simple model Hamiltonian of the C_{60} molecule. In this article, we shall see how to analyze it in detail with the aid of computer algebra. As for computational algebraic number theory, the book by Cohen [Coh13] is recommendable.

3 Exemplar computations by model molecules

Let us compute some examples. We assume molecules made of n -atoms forming networks; each of atoms has a π orbital and interacts with neighbors.

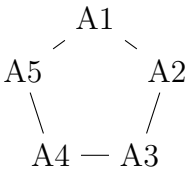
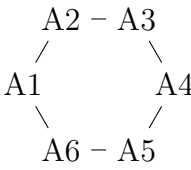
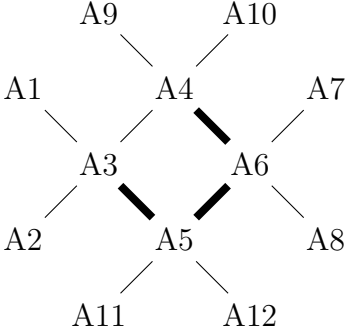
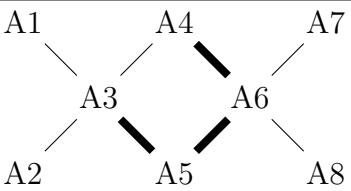
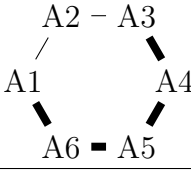
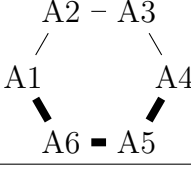
Structure	Eigenvalue	Galois Group
	$-e^5 + 5 * e^3 - 5 * e - 2$	C_2
	$(e - 2)(e - 1)^2(e + 1)^2(e + 2)$	Trivial
	e^4 $\times (e^4 - 3 * e^3 - 6 * e^2 + 6 * e + 4)$ $\times (e^4 + 3 * e^3 - 6 * e^2 - 6 * e + 4)$	D_4
	$e^5 - 17 * e^3 + 34 * e$	D_4
	$(e^4 - 14 * e^2 + 16)(e + 2)(e - 2)$	$C_2 \times C_2$
	$(e^3 - 3 * e^2 - 3 * e + 6)$ $\times (e^3 + 3 * e^2 - 3 * e - 6)$	S_3

Table 3.1: The model molecules to be examined in the study. In the rows, the structures are graphically represented, and along with them, the determinant of $H - eI$ and the corresponding Galois group are given. The widths of the segments of the molecular models distinguish the strength of the electron hopping: $H_{ij} = -1$ at thin ones; -2 at thick ones; if not connected, no interaction.

As are exemplified in Fig. 3.1, one can generate various model structures; then one

can analyze the determinant and the polynomials in the ideals, which are derived from the secular equations. We shall study some of them: those of pentagon and hexagon, and a molecule with the Galois group D_4 . The results of others are shown in the appendix (the supplemental part of the article). If one would get acquainted with the way to study the polynomials by computer algebra through these three chosen examples, it is easy to practice the analysis for others.

3.1 Simple model structures: two types of Galois group of C_2 and the trivial one.

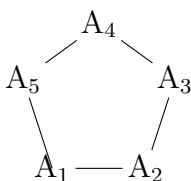


Figure 3.1: The framework of a molecule of pentagonal structure. The atoms are indexed as A_1, \dots, A_5 and they interact between nearest neighbors, as are indicated by the bonds.

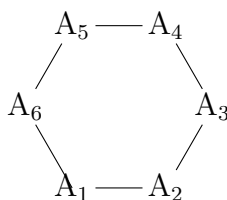


Figure 3.2: The framework of a hexagonal molecule. The atoms are indexed as A_1, \dots, A_6 .

Let us compute the simple model of molecules. We place one orbital at each site and assume the interaction between neighboring orbitals, connected by the bonds (which are indicated by broad segments).

For the pentagonal and hexagonal models, as are given in the figures (3.1, 3.2), the *algebraic molecular orbital computations* could be done by the computer algebra system SINGULAR [DGPS]. The results are given below. The spectrum is represented by the variable 'e'; the wavefunction ψ is given by the vector $(y(1), \dots, y(n))$. We give the secular equation as the defining ideal. From this, we generate the standard bases (by eliminating the variables in this order: $y(1), y(2), \dots, y(n), e$, through the Buchberger algorithm [CLO06, CLO13, Buc65]). Then we execute the primary ideal decomposition [Eis13, GTZ88, Möl93].

For the pentagonal model molecule, the result is as follows.

N=5 (Matrix H) Five atoms.

```
0, -1, 0, 0, -1,
-1, 0, -1, 0, 0,
0, -1, 0, -1, 0,
0, 0, -1, 0, -1,
-1, 0, 0, -1, 0
```

Defining Ideal

```
-y(1)*e-y(2)-y(5),
-y(1)-y(2)*e-y(3),
-y(2)-y(3)*e-y(4),
-y(3)-y(4)*e-y(5),
-y(1)-y(4)-y(5)*e,
y(1)^2+y(2)^2+y(3)^2+y(4)^2+y(5)^2-1
```

The determinant of (H-eI)

```
-e^5+5*e^3-5*e-2
```

Standard Basis

```
_ [1]=e^3+e^2-3*e-2
_ [2]=5*y(5)^2*e^2-5*y(5)^2*e-5*y(5)^2-e^2+e+1
_ [3]=y(4)*e^2-y(4)*e-y(4)-y(5)*e^2+y(5)*e+y(5)
_ [4]=10*y(4)^2-2*y(4)*y(5)*e^3+14*y(4)*y(5)*e
      +2*y(4)*y(5)-y(5)^2*e^3+2*y(5)^2*e^2+9*y(5)^2+e-3
_ [5]=y(3)+y(4)*e+y(5)
_ [6]=y(2)+y(3)*e+y(4)
_ [7]=y(1)+y(4)+y(5)*e
```

Primary Ideal Decomposition

[1]:

[1]: !Primary ideal

```
_ [1]=e^2-e-1
_ [2]=10*y(4)^2+10*y(4)*y(5)*e+10*y(5)^2+e-3
_ [3]=y(3)+y(4)*e+y(5)
_ [4]=y(2)-y(4)*e-y(5)*e^2+y(5)
_ [5]=y(1)+y(4)+y(5)*e
```

[2]: !Corresponding prime ideal.

```
_ [1]=e^2-e-1
_ [2]=10*y(4)^2+10*y(4)*y(5)*e+10*y(5)^2+e-3
_ [3]=y(3)+y(4)*e+y(5)
_ [4]=y(2)-y(4)*e-y(5)*e^2+y(5)
_ [5]=y(1)+y(4)+y(5)*e
```

[2] :

[1] :

```
_ [1]=e+2
_ [2]=5*y(5)^2-1
_ [3]=y(4)-y(5)
_ [4]=y(3)+y(4)*e+y(5)
_ [5]=y(2)-y(4)*e-y(5)*e^2+y(5)
_ [6]=y(1)+y(4)+y(5)*e
```

[2] :

```
_ [1]=e+2
_ [2]=5*y(5)^2-1
_ [3]=y(4)-y(5)
_ [4]=y(3)+y(4)*e+y(5)
_ [5]=y(2)-y(4)*e-y(5)*e^2+y(5)
_ [6]=y(1)+y(4)+y(5)*e
```

For the hexagonal model molecule, the result is as follows.

N=6 (Matrix H) Six atoms.

```
0, -1, 0, 0, 0, -1,
-1, 0, -1, 0, 0, 0,
0, -1, 0, -1, 0, 0,
0, 0, -1, 0, -1, 0,
0, 0, 0, -1, 0, -1,
-1, 0, 0, 0, -1, 0
```

Defining Ideal

```
-y(1)*e-y(2)-y(6),
-y(1)-y(2)*e-y(3),
-y(2)-y(3)*e-y(4),
-y(3)-y(4)*e-y(5),
-y(4)-y(5)*e-y(6),
-y(1)-y(5)-y(6)*e,
y(1)^2+y(2)^2+y(3)^2+y(4)^2+y(5)^2+y(6)^2-1
```

Standard Basis

```
_ [1]=e^4-5*e^2+4
_ [2]=6*y(6)^2*e^2-6*y(6)^2-e^2+1
_ [3]=2*y(5)*e^2-2*y(5)+y(6)*e^3-y(6)*e
_ [4]=8*y(5)^2-2*y(5)*y(6)*e^5+9*y(5)*y(6)*e^3+
y(5)*y(6)*e-2*y(6)^2*e^4+12*y(6)^2*e^2-2*y(6)^2-2
_ [5]=y(4)+y(5)*e+y(6)
_ [6]=y(3)+y(4)*e+y(5)
_ [7]=y(2)+y(3)*e+y(4)
```

$$_ [8]=y(1)+y(5)+y(6)*e$$

Primary Ideal Decomposition

[1]:

[1]:

$$\begin{aligned}_ [1] &= e-1 \\ _ [2] &= 4*y(5)^2+4*y(5)*y(6)+4*y(6)^2-1 \\ _ [3] &= y(4)+y(5)*e+y(6) \\ _ [4] &= y(3)+1/2*y(6)*e^3-3/2*y(6)*e \\ _ [5] &= y(2)-y(5)*e-y(6)*e^2+y(6) \\ _ [6] &= y(1)+y(5)+y(6)*e\end{aligned}$$

[2]:

$$\begin{aligned}_ [1] &= e-1 \\ _ [2] &= 4*y(5)^2+4*y(5)*y(6)+4*y(6)^2-1 \\ _ [3] &= y(4)+y(5)*e+y(6) \\ _ [4] &= y(3)+1/2*y(6)*e^3-3/2*y(6)*e \\ _ [5] &= y(2)-y(5)*e-y(6)*e^2+y(6) \\ _ [6] &= y(1)+y(5)+y(6)*e\end{aligned}$$

[2]:

[1]:

$$\begin{aligned}_ [1] &= e+1 \\ _ [2] &= 4*y(5)^2-4*y(5)*y(6)+4*y(6)^2-1 \\ _ [3] &= y(4)+y(5)*e+y(6) \\ _ [4] &= y(3)+1/2*y(6)*e^3-3/2*y(6)*e \\ _ [5] &= y(2)-y(5)*e-y(6)*e^2+y(6) \\ _ [6] &= y(1)+y(5)+y(6)*e\end{aligned}$$

[2]:

$$\begin{aligned}_ [1] &= e+1 \\ _ [2] &= 4*y(5)^2-4*y(5)*y(6)+4*y(6)^2-1 \\ _ [3] &= y(4)+y(5)*e+y(6) \\ _ [4] &= y(3)+1/2*y(6)*e^3-3/2*y(6)*e \\ _ [5] &= y(2)-y(5)*e-y(6)*e^2+y(6) \\ _ [6] &= y(1)+y(5)+y(6)*e\end{aligned}$$

[3]:

[1]:

$$\begin{aligned}_ [1] &= e+2 \\ _ [2] &= 6*y(6)^2-1 \\ _ [3] &= y(5)-y(6) \\ _ [4] &= y(4)+y(5)*e+y(6) \\ _ [5] &= y(3)+1/2*y(6)*e^3-3/2*y(6)*e \\ _ [6] &= y(2)-y(5)*e-y(6)*e^2+y(6) \\ _ [7] &= y(1)+y(5)+y(6)*e\end{aligned}$$

[2]:

```

    _[1]=e+2
    _[2]=6*y(6)^2-1
    _[3]=y(5)-y(6)
    _[4]=y(4)+y(5)*e+y(6)
    _[5]=y(3)+1/2*y(6)*e^3-3/2*y(6)*e
    _[6]=y(2)-y(5)*e-y(6)*e^2+y(6)
    _[7]=y(1)+y(5)+y(6)*e
[4]:
[1]:
    _[1]=e-2
    _[2]=6*y(6)^2-1
    _[3]=y(5)+y(6)
    _[4]=y(4)+y(5)*e+y(6)
    _[5]=y(3)+1/2*y(6)*e^3-3/2*y(6)*e
    _[6]=y(2)-y(5)*e-y(6)*e^2+y(6)
    _[7]=y(1)+y(5)+y(6)*e
[2]:
    _[1]=e-2
    _[2]=6*y(6)^2-1
    _[3]=y(5)+y(6)
    _[4]=y(4)+y(5)*e+y(6)
    _[5]=y(3)+1/2*y(6)*e^3-3/2*y(6)*e
    _[6]=y(2)-y(5)*e-y(6)*e^2+y(6)
    _[7]=y(1)+y(5)+y(6)*e

```

Observe that in the case of the six-membered hexagonal model, the eigenvalues are obtained as integers, while in the case of the five-membered pentagonal model, some eigenvalues are unsolved and kept in a polynomial equation. To solve the equation, we should add an irrational number. In this case, the equation is given by

$$e^2 - e - 1 = 0, \quad (3)$$

to which, the solutions are

$$e_{1,2} = \frac{1 \pm \sqrt{5}}{2}. \quad (4)$$

Let a be one of the roots of $e^2 - e - 1 = 0$. In $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{5})$, the solutions for the given problem are given by the two sets of equations (A and B below).

A: $(y_1(e_1), y_2(e_1), y_3(e_1), y_4(e_1), y_5(e_1), e_1)$ is defined by

$$\begin{aligned} e + (a - 1) &= 0 \\ 10 * y(4)^2 + (-10 * a + 10) * y(4) * y(5) + 10 * y(5)^2 + (-a - 2) &= 0 \\ y(3) + (-a + 1) * y(4) + y(5) &= 0 \\ y(2) + y(3) + (a) * y(5) &= 0 \\ y(1) + y(4) + (-a + 1) * y(5) &= 0 \end{aligned}$$

B: $(y_1(e_2), y_2(e_2), y_3(e_2), y_4(e_2), y_5(e_2))$ is defined by

$$\begin{aligned} e + (-a) &= 0 \\ 10 * y(4)^2 + (10 * a) * y(4) * y(5) + 10 * y(5)^2 + (a - 3) &= 0 \\ y(3) + (a) * y(4) + y(5) &= 0 \\ y(2) + y(3) + (-a + 1) * y(5) &= 0 \\ y(1) + y(4) + (a) * y(5) &= 0 \end{aligned}$$

According to the Galois theory (as we have seen in the former section), the extension of \mathbb{Q} evokes the automorphism, which fixes the polynomial equation with the coefficients in \mathbb{Q} . The solutions A and B are interchangeable through the map

$$a \longleftrightarrow 1 - a,$$

or, equivalently,

$$\sqrt{5} \longleftrightarrow -\sqrt{5}$$

3.2 Galois group D_4

Next let us see an example for the Galois group D_4 . This example is given by the structure presented in Fig. 3.3.

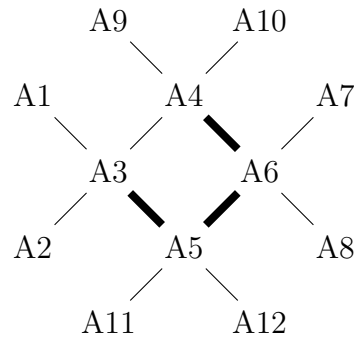


Figure 3.3: A model molecule. The hopping integrals H_{ij} are set to be -2 on the bonds denoted by broad edges; and $H_{ij} = -1$ on others.

The result of the computation for this molecule is given below.

Matrix H

```

0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0,
-1, -1, 0, -1, -2, 0, 0, 0, 0, 0, 0, 0,
0, 0, -1, 0, 0, -2, 0, 0, -1, -1, 0, 0,
0, 0, -2, 0, 0, -2, 0, 0, 0, 0, -1, -1,
0, 0, 0, -2, -2, 0, -1, -1, 0, 0, 0, 0,
0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0,
0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0

```

The polynomial equation for spectra.

[Determinant of $H - e I$]

$e^{12} - 21e^{10} + 80e^8 - 84e^6 + 16e^4$

Defining Ideal

```

-y(1)*e-y(3),
-y(2)*e-y(3),
-y(1)-y(2)-y(3)*e-y(4)-2*y(5),
-y(3)-y(4)*e-2*y(6)-y(9)-y(10),
-2*y(3)-y(5)*e-2*y(6)-y(11)-y(12),
-2*y(4)-2*y(5)-y(6)*e-y(7)-y(8),
-y(6)-y(7)*e,
-y(6)-y(8)*e,

```

$-y(4)-y(9)*e,$
 $-y(4)-y(10)*e,$
 $-y(5)-y(11)*e,$
 $-y(5)-y(12)*e,$
 $y(1)^2+y(2)^2+y(3)^2+y(4)^2+y(5)^2+y(6)^2+y(7)^2$
 $+y(8)^2+y(9)^2+y(10)^2+y(11)^2+y(12)^2-1$

Standard Basis

$_{[1]}=e^9-21*e^7+80*e^5-84*e^3+16*e$
 $_{[2]}=70176*y(12)^2*e+97*e^7-2059*e^5+8266*e^3-11608*e$
 $_{[3]}=8*y(11)+y(12)*e^8-21*y(12)*e^6+80*y(12)*e^4$
 $-84*y(12)*e^2+8*y(12)$
 $_{[4]}=24*y(10)*e+y(12)*e^7-21*y(12)*e^5+76*y(12)*e^3-36*y(12)*e$
 $_{[5]}=48*y(9)+48*y(10)+9*y(12)*e^8-185*y(12)*e^6+636*y(12)*e^4$
 $-452*y(12)*e^2$
 $_{[6]}=12*y(8)*e+y(12)*e^8-20*y(12)*e^6+61*y(12)*e^4-38*y(12)*e^2$
 $_{[7]}=6*y(7)+6*y(8)+y(12)*e^7-20*y(12)*e^5+61*y(12)*e^3-38*y(12)*e$
 $_{[8]}=12*y(6)-y(12)*e^8+20*y(12)*e^6-61*y(12)*e^4+38*y(12)*e^2$
 $_{[9]}=y(5)+y(12)*e$
 $_{[10]}=24*y(4)-y(12)*e^7+21*y(12)*e^5-76*y(12)*e^3+36*y(12)*e$
 $_{[11]}=48*y(3)+y(12)*e^8-17*y(12)*e^6+4*y(12)*e^4+76*y(12)*e^2$
 $_{[12]}=48*y(2)*e-y(12)*e^8+17*y(12)*e^6-4*y(12)*e^4-76*y(12)*e^2$
 $_{[13]}=1376*y(2)^2+1376*y(8)^2+1376*y(10)^2+1376*y(12)^2$
 $-e^8+23*e^6-126*e^4+336*e^2-688$
 $_{[14]}=24*y(1)+24*y(2)-y(12)*e^7+17*y(12)*e^5-4*y(12)*e^3-76*y(12)*e$

Primary Ideal Decomposition

[1]:

[1]: !Primary ideal

$_{[1]}=e$
 $_{[2]}=2*y(2)^2+2*y(8)^2+2*y(10)^2+2*y(12)^2-1$
 $_{[3]}=y(11)+1/8*y(12)*e^8-21/8*y(12)*e^6+10*y(12)*e^4$
 $-21/2*y(12)*e^2+y(12)$
 $_{[4]}=y(9)+y(10)+3/16*y(12)*e^8-185/48*y(12)*e^6$
 $+53/4*y(12)*e^4-113/12*y(12)*e^2$
 $_{[5]}=y(7)+y(8)+1/6*y(12)*e^7-10/3*y(12)*e^5$
 $+61/6*y(12)*e^3-19/3*y(12)*e$
 $_{[6]}=y(6)-1/12*y(12)*e^8+5/3*y(12)*e^6$
 $-61/12*y(12)*e^4+19/6*y(12)*e^2$
 $_{[7]}=y(5)+y(12)*e$
 $_{[8]}=y(4)-1/24*y(12)*e^7+7/8*y(12)*e^5-19/6*y(12)*e^3+3/2*y(12)*e$
 $_{[9]}=y(3)+1/48*y(12)*e^8-17/48*y(12)*e^6+1/12*y(12)*e^4$
 $+19/12*y(12)*e^2$

```

    _[10]=y(1)+y(2)-1/24*y(12)*e^7+17/24*y(12)*e^5
           -1/6*y(12)*e^3-19/6*y(12)*e
[2]: !Corresponding prime ideal
    _[1]=e
    _[2]=2*y(2)^2+2*y(8)^2+2*y(10)^2+2*y(12)^2-1
    _[3]=y(11)+1/8*y(12)*e^8-21/8*y(12)*e^6+10*y(12)*e^4
           -21/2*y(12)*e^2+y(12)
    _[4]=y(9)+y(10)+3/16*y(12)*e^8-185/48*y(12)*e^6
           +53/4*y(12)*e^4-113/12*y(12)*e^2
    _[5]=y(7)+y(8)+1/6*y(12)*e^7-10/3*y(12)*e^5
           +61/6*y(12)*e^3-19/3*y(12)*e
    _[6]=y(6)-1/12*y(12)*e^8+5/3*y(12)*e^6-61/12*y(12)*e^4
           +19/6*y(12)*e^2
    _[7]=y(5)+y(12)*e
    _[8]=y(4)-1/24*y(12)*e^7+7/8*y(12)*e^5-19/6*y(12)*e^3
           +3/2*y(12)*e
    _[9]=y(3)+1/48*y(12)*e^8-17/48*y(12)*e^6+1/12*y(12)*e^4
           +19/12*y(12)*e^2
    _[10]=y(1)+y(2)-1/24*y(12)*e^7+17/24*y(12)*e^5
           -1/6*y(12)*e^3-19/6*y(12)*e
[2]:
[1]:
    _[1]=e^4+3*e^3-6*e^2-6*e+4
    _[2]=5848*y(12)^2+54*e^3+209*e^2-205*e-766
    _[3]=4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12)
    _[4]=y(8)-y(12)
    _[5]=4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12)
    _[6]=y(11)+1/8*y(12)*e^8-21/8*y(12)*e^6+10*y(12)*e^4
           -21/2*y(12)*e^2+y(12)
    _[7]=y(9)+y(10)+3/16*y(12)*e^8-185/48*y(12)*e^6
           +53/4*y(12)*e^4-113/12*y(12)*e^2
    _[8]=y(7)+y(8)+1/6*y(12)*e^7-10/3*y(12)*e^5+61/6*y(12)*e^3
           -19/3*y(12)*e
    _[9]=y(6)-1/12*y(12)*e^8+5/3*y(12)*e^6-61/12*y(12)*e^4
           +19/6*y(12)*e^2
    _[10]=y(5)+y(12)*e
    _[11]=y(4)-1/24*y(12)*e^7+7/8*y(12)*e^5-19/6*y(12)*e^3
           +3/2*y(12)*e
    _[12]=y(3)+1/48*y(12)*e^8-17/48*y(12)*e^6+1/12*y(12)*e^4
           +19/12*y(12)*e^2
    _[13]=y(1)+y(2)-1/24*y(12)*e^7+17/24*y(12)*e^5
           -1/6*y(12)*e^3-19/6*y(12)*e
[2]:

```

```

_[1]=e^4+3*e^3-6*e^2-6*e+4
_[2]=5848*y(12)^2+54*e^3+209*e^2-205*e-766
_[3]=4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12)
_[4]=y(8)-y(12)
_[5]=4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12)
_[6]=y(11)+1/8*y(12)*e^8-21/8*y(12)*e^6+10*y(12)*e^4
    -21/2*y(12)*e^2+y(12)
_[7]=y(9)+y(10)+3/16*y(12)*e^8-185/48*y(12)*e^6
    +53/4*y(12)*e^4-113/12*y(12)*e^2
_[8]=y(7)+y(8)+1/6*y(12)*e^7-10/3*y(12)*e^5
    +61/6*y(12)*e^3-19/3*y(12)*e
_[9]=y(6)-1/12*y(12)*e^8+5/3*y(12)*e^6
    -61/12*y(12)*e^4+19/6*y(12)*e^2
_[10]=y(5)+y(12)*e
_[11]=y(4)-1/24*y(12)*e^7+7/8*y(12)*e^5-19/6*y(12)*e^3
    +3/2*y(12)*e
_[12]=y(3)+1/48*y(12)*e^8-17/48*y(12)*e^6+1/12*y(12)*e^4
    +19/12*y(12)*e^2
_[13]=y(1)+y(2)-1/24*y(12)*e^7+17/24*y(12)*e^5
    -1/6*y(12)*e^3-19/6*y(12)*e

```

[3]:

[1]:

```

_[1]=e^4-3*e^3-6*e^2+6*e+4
_[2]=5848*y(12)^2-54*e^3+209*e^2+205*e-766
_[3]=4*y(10)-y(12)*e^3+3*y(12)*e^2+4*y(12)*e-2*y(12)
_[4]=y(8)+y(12)
_[5]=4*y(2)+y(12)*e^3-3*y(12)*e^2-4*y(12)*e+2*y(12)
_[6]=y(11)+1/8*y(12)*e^8-21/8*y(12)*e^6+10*y(12)*e^4
    -21/2*y(12)*e^2+y(12)
_[7]=y(9)+y(10)+3/16*y(12)*e^8-185/48*y(12)*e^6
    +53/4*y(12)*e^4-113/12*y(12)*e^2
_[8]=y(7)+y(8)+1/6*y(12)*e^7-10/3*y(12)*e^5+61/6*y(12)*e^3
    -19/3*y(12)*e
_[9]=y(6)-1/12*y(12)*e^8+5/3*y(12)*e^6-61/12*y(12)*e^4
    +19/6*y(12)*e^2
_[10]=y(5)+y(12)*e
_[11]=y(4)-1/24*y(12)*e^7+7/8*y(12)*e^5-19/6*y(12)*e^3
    +3/2*y(12)*e
_[12]=y(3)+1/48*y(12)*e^8-17/48*y(12)*e^6+1/12*y(12)*e^4
    +19/12*y(12)*e^2
_[13]=y(1)+y(2)-1/24*y(12)*e^7+17/24*y(12)*e^5
    -1/6*y(12)*e^3-19/6*y(12)*e

```

[2]:

$$\begin{aligned}
_ [1] &= e^4 - 3e^3 - 6e^2 + 6e + 4 \\
_ [2] &= 5848y(12)^2 - 54e^3 + 209e^2 + 205e - 766 \\
_ [3] &= 4y(10) - y(12)e^3 + 3y(12)e^2 + 4y(12)e - 2y(12) \\
_ [4] &= y(8) + y(12) \\
_ [5] &= 4y(2) + y(12)e^3 - 3y(12)e^2 - 4y(12)e + 2y(12) \\
_ [6] &= y(11) + 1/8y(12)e^8 - 21/8y(12)e^6 + 10y(12)e^4 \\
&\quad - 21/2y(12)e^2 + y(12) \\
_ [7] &= y(9) + y(10) + 3/16y(12)e^8 - 185/48y(12)e^6 \\
&\quad + 53/4y(12)e^4 - 113/12y(12)e^2 \\
_ [8] &= y(7) + y(8) + 1/6y(12)e^7 - 10/3y(12)e^5 \\
&\quad + 61/6y(12)e^3 - 19/3y(12)e \\
_ [9] &= y(6) - 1/12y(12)e^8 + 5/3y(12)e^6 - 61/12y(12)e^4 \\
&\quad + 19/6y(12)e^2 \\
_ [10] &= y(5) + y(12)e \\
_ [11] &= y(4) - 1/24y(12)e^7 + 7/8y(12)e^5 \\
&\quad - 19/6y(12)e^3 + 3/2y(12)e \\
_ [12] &= y(3) + 1/48y(12)e^8 - 17/48y(12)e^6 \\
&\quad + 1/12y(12)e^4 + 19/12y(12)e^2 \\
_ [13] &= y(1) + y(2) - 1/24y(12)e^7 + 17/24y(12)e^5 \\
&\quad - 1/6y(12)e^3 - 19/6y(12)e
\end{aligned}$$

We can reshape the decomposed components so that they should be *reduced*. Besides, we can compute the dimensions of them. The reshaped primary (indeed prime) ideals P_1 , P_2 , and P_3 are given below. The ideal P_1 is of dimension 3, and P_1 and P_2 are of dimension 0. Hence the ideal P_1 delineates an object (an algebraic variety) of dimension 3 in the affine space $\mathbb{Q}[y(1), \dots, y(12), e]$; from which we can choose four representatives of the orthonormalized quantum states (at the spectrum $e=0$), with degeneracy 4, as is suggested by the determinant of $H - eI$. On the other hand, the ideal P_2 and P_3 delineate the algebraic varieties of dimension 0, which are the isolated points, and we choose one representative of the quantum state respectively.

$$\begin{aligned}
P_1 = & \\
& (e, y(11) + y(12), y(9) + y(10), y(7) + y(8), \\
& y(6), y(5), y(4), y(3), \\
& 2y(2)^2 + 2y(8)^2 + 2y(10)^2 + 2y(12)^2 - 1, \\
& y(1) + y(2)) \\
& \dim(P_1) = 3
\end{aligned}$$

$$\begin{aligned}
P_2 = & \\
& (e^4 + 3e^3 - 6e^2 - 6e + 4, \\
& 5848y(12)^2 + 54e^3 + 209e^2 - 205e - 766, \\
& y(11) - y(12), \\
& 4y(10) + y(12)e^3 + 3y(12)e^2 - 4y(12)e - 2y(12), \\
& 4y(9) + y(12)e^3 + 3y(12)e^2 - 4y(12)e - 2y(12),
\end{aligned}$$

```

y(8)-y(12),
y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12))
dim(P2)=0

```

```

P3=(e^4-3*e^3-6*e^2+6*e+4,
5848*y(12)^2-54*e^3+209*e^2+205*e-766,
y(11)-y(12),
4*y(10)-y(12)*e^3+3*y(12)*e^2+4*y(12)*e-2*y(12),
4*y(9)-y(12)*e^3+3*y(12)*e^2+4*y(12)*e-2*y(12),
y(8)+y(12),
y(7)+y(12),
y(6)-y(12)*e,
y(5)+y(12)*e,
2*y(4)+y(12)*e^2-2*y(12)*e-2*y(12),
2*y(3)-y(12)*e^2+2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3-3*y(12)*e^2-4*y(12)*e+2*y(12),
4*y(1)+y(12)*e^3-3*y(12)*e^2-4*y(12)*e+2*y(12))
dim(P3)=0

```

The decomposed ideals could split more if we place them in the extension field in which the univariate polynomials of the variable 'e' shall split.

Let us take one of the components in the primary ideal decomposition and inspect the Galois correspondence. For the component P2, the eigenvalues are the root of this polynomial:

$$f = x^4 + 3x^3 - 6x^2 - 6x + 4.$$

The Galois group of the polynomial is D_4 . In this case, therefore, it is sufficient to use the extension field with the Galois group D_4 .

Remark 3.1. It is not trivial how to determine the Galois group; The book by Milne [Mil18] explains how to do it, and computer algebra programs [PARI/GP [The19] and GAP [The17]] can compute it.

The roots of the equation are given by

$$x = -\frac{\sqrt{\frac{3\sqrt{17}}{2} + \frac{29}{2}}}{2} - \frac{\sqrt{17}}{4}, \frac{\sqrt{\frac{3\sqrt{17}}{2} + \frac{29}{2}}}{2} - \frac{\sqrt{17}}{4},$$

$$\frac{\sqrt{17}}{4} - \frac{\sqrt{\frac{29}{2} - \frac{3\sqrt{17}}{2}}}{2}, \frac{\sqrt{17}}{4} + \frac{\sqrt{\frac{29}{2} - \frac{3\sqrt{17}}{2}}}{2}$$

The Galois extension for D_4 is illustrated in Fig. 3.4. The group D_4 contains 9 subgroups and there are two pairs of conjugated subgroups.

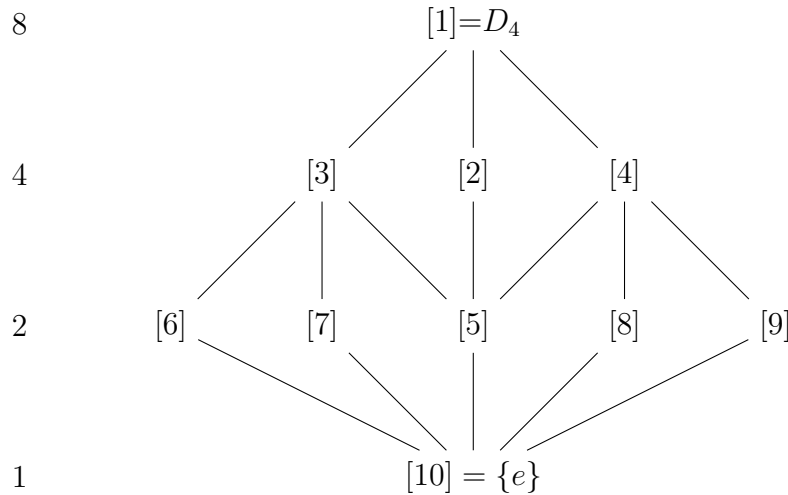


Figure 3.4: The graphical representation of the subgroup lattice for D_4 . Each node shows the subgroups; The inclusion relations as subgroups are denoted by edges. Two pairs of subgroups ($[6]$ and $[7]$, $[8]$ and $[9]$) are conjugated in the same classes. The column of the numbers in the left side of the graph are the orders of the subgroups.

Let us analyze the equation using PARI/GP. A short computer program is presented in the appendix E. At first one should prepare the splitting field of f to study the Galois extension. Usually one has only to add four distinct roots to \mathbb{Q} to generate it. However, the splitting field proposed by PARI/GP is not of this kind, as the defining polynomial is

$$K = x^8 - 46 * x^6 + 461 * x^4 - 1360 * x^2 + 1156.$$

This polynomial is different to f , although the Galois group operation in the splitting field for K shall evolve the permutation of four roots of f . In addition, the Galois group of this polynomial is D_4 . The use of the alternative polynomial K makes the treatment simpler, as the splitting field of f is constructed by the addition of only one of the root of the polynomial K to \mathbb{Q} .

The list of subfields (computed by PARI/GP) in the splitting field defined by K is presented below. They are designated by the defining polynomials of their own.

	Defining Polynomial	
No.1	—	\mathbb{Q}
No.2	$x^2 - 26316$	$\mathbb{Q}(\sqrt{17 \cdot 43})$
No.3	$x^2 - 68$	$\mathbb{Q}(\sqrt{17})$
No.4	$x^2 - 92 * x + 1428$	$\mathbb{Q}(\sqrt{43})$
No.5	$x^4 - 92 * x^3 + 2796 * x^2 - 31280 * x + 103904$	
No.6	$x^4 - 63 * x^2 + 102 * x - 32$	
No.7	$x^4 - 63 * x^2 - 102 * x - 32$	
No.8	$x^4 - 92 * x^3 + 1844 * x^2 - 10880 * x + 18496$	
No.9	$x^4 - 58 * x^2 + 153$	
No.10	$x^8 - 46 * x^6 + 461 * x^4 - 1360 * x^2 + 1156$	The splitting field

Table 3.2: The list of subfields in the Galois extension. One can construct each of them by adding one of the roots of the defining polynomial to \mathbb{Q} .

In these subfields, the polynomial equation f for the spectrum e splits in the following way. All polynomials share the four common roots, indexed by 1, 2, 3, and 4. The number-lists between the square brackets stand for the roots given by this index.

NO.1

$$(1) \ x^4 + 3x^3 - 6x^2 - 6x + 4 \quad [1,2,3,4]$$

NO.2

$$(2) \ x^4 + 3x^3 - 6x^2 - 6x + 4 \quad [1,2,3,4]$$

NO.3

$$(1) \ x^2 + \text{Mod}(-1/4*y + 3/2, y^2 - 68)*x - 2 \quad [1,4]$$

$$(2) \ x^2 + \text{Mod}(1/4*y + 3/2, y^2 - 68)*x - 2 \quad [2,3]$$

NO.4

$$(1) \ x^4 + 3x^3 - 6x^2 - 6x + 4 \quad [1,2,3,4]$$

NO.5

$$(1) \ x^2 + \text{Mod}(-1/620*y^3 + 69/620*y^2 - 11/5*y + 1992/155, \\ y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x - 2 \\ [1,4]$$

$$(2) \ x^2 + \text{Mod}(1/620*y^3 - 69/620*y^2 + 11/5*y - 1527/155, \\ y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x - 2 \\ [2,3]$$

NO.6

- (1) $x + \text{Mod}(-2/49*y^3 - 3/98*y^2 + 213/98*y - 69/49, y^4 - 63*y^2 + 102*y - 32)$ [1]
 (2) $x + \text{Mod}(6/49*y^3 + 9/98*y^2 - 737/98*y + 354/49, y^4 - 63*y^2 + 102*y - 32)$ [4]
 (3) $x^2 + \text{Mod}(-4/49*y^3 - 3/49*y^2 + 262/49*y - 138/49, y^4 - 63*y^2 + 102*y - 32)*x - 2$ [2,3]
-

NO.7

- (1) $x + \text{Mod}(-6/49*y^3 + 9/98*y^2 + 737/98*y + 354/49, y^4 - 63*y^2 - 102*y - 32)$ [3]
 (2) $x + \text{Mod}(2/49*y^3 - 3/98*y^2 - 213/98*y - 69/49, y^4 - 63*y^2 - 102*y - 32)$ [2]
 (3) $x^2 + \text{Mod}(4/49*y^3 - 3/49*y^2 - 262/49*y - 138/49, y^4 - 63*y^2 - 102*y - 32)*x - 2$ [1,4]
-

NO.8

- (1) $x^2 + \text{Mod}(-5/6528*y^3 + 247/3264*y^2 - 725/408*y + 119/12, y^4 - 92*y^3 + 1844*y^2 - 10880*y + 18496)*x + \text{Mod}(-7/1088*y^3 + 305/544*y^2 - 156/17*y + 55/2, y^4 - 92*y^3 + 1844*y^2 - 10880*y + 18496)$ [3,4]
 (2) $x^2 + \text{Mod}(5/6528*y^3 - 247/3264*y^2 + 725/408*y - 83/12, y^4 - 92*y^3 + 1844*y^2 - 10880*y + 18496)*x + \text{Mod}(-3/2176*y^3 + 121/1088*y^2 - 197/136*y + 17/4, y^4 - 92*y^3 + 1844*y^2 - 10880*y + 18496)$ [1,2]
-

NO.9

- (1) $x^2 + \text{Mod}(-1/2*y + 3/2, y^4 - 58*y^2 + 153)*x + \text{Mod}(-1/24*y^3 + 1/8*y^2 + 49/24*y - 33/8, y^4 - 58*y^2 + 153)$ [1,3]
 (2) $x^2 + \text{Mod}(1/2*y + 3/2, y^4 - 58*y^2 + 153)*x + \text{Mod}(1/24*y^3 + 1/8*y^2 - 49/24*y - 33/8, y^4 - 58*y^2 + 153)$ [2,4]
-

NO.10

- (1) $x + \text{Mod}(5/1632*y^6 - 247/1632*y^4 + 725/408*y^2 - 1/2*y - 83/24, y^8 - 46*y^6 + 461*y^4 - 1360*y^2 + 1156)$ [1]
 (2) $x + \text{Mod}(5/1632*y^6 - 247/1632*y^4 + 725/408*y^2 + 1/2*y - 83/24, y^8 - 46*y^6 + 461*y^4 - 1360*y^2 + 1156)$ [2]

$$\begin{aligned}
(3) \quad & x + \text{Mod}(-7/544*y^7 - 5/1632*y^6 + 305/544*y^5 \\
& + 247/1632*y^4 - 78/17*y^3 - 725/408*y^2 + 55/8*y + 119/24, \\
& y^8 - 46*y^6 + 461*y^4 - 1360*y^2 + 1156) [3] \\
(4) \quad & x + \text{Mod}(7/544*y^7 - 5/1632*y^6 - 305/544*y^5 + 247/1632*y^4 \\
& + 78/17*y^3 - 725/408*y^2 - 55/8*y + 119/24, \\
& y^8 - 46*y^6 + 461*y^4 - 1360*y^2 + 1156) [4]
\end{aligned}$$

Notice that we use a special notation to represent the coefficients in the subfields: when a coefficient is given by modulo, say,

$$\text{Mod}(-1/4 * y + 3/2, y^2 - 68),$$

it implies a number $-1/4y + 3/2$, defined by y such that $y^2 - 68 = 0$. This is the notation adopted by PARI/GP.

One might feel the necessity to know in what way these irreducible polynomials in the subfields encapsulate the four root of the polynomial f . We can check it after some algebra as follows.

- Let $\mathbb{Q}(a)$ is the splitting field of K .
- For each subfield of $\mathbb{Q}(a)$, its defining polynomial splits in $\mathbb{Q}(a)$. The roots β_i are given by polynomials $\beta_i(a)$.
- The polynomial f splits into the set of polynomials in the subfields. The latter polynomials have the coefficients composed of 'y' which is one of the roots of the defining polynomial of the subfield.
- By the substitution $y \rightarrow \beta_i(a)$ (with an available β_i) for these polynomials factorized in the subfield, we get the representations in $\mathbb{Q}(a)$ that split.

We present additional information on the subgroups. They are given by the permutations. We could use the GAP system [The17] to get the representation by the minimal generators 'a' and 'b'.

No.1	[(1,2)(3,7)(4,6)(5,8), (1,7,6,5)(2,8,4,3)]; [a, b]
No.2	[(1,7,6,5)(2,8,4,3)]; [b]
No.3	[(1,2)(3,7)(4,6)(5,8), (1,6)(2,4)(3,8)(5,7)]; [a, b ⁻²]
No.4	[(1,8)(2,7)(3,6)(4,5), (1,6)(2,4)(3,8)(5,7)]; [b ⁻¹ a, b ⁻²]
No.5	[(1,6)(2,4)(3,8)(5,7)]; [b ⁻²]
No.6	[(1,2)(3,7)(4,6)(5,8)]; [a]
No.7	[(1,4)(2,6)(3,5)(7,8)]; [a*b ⁻²]
No.8	[(1,8)(2,7)(3,6)(4,5)]; [b ⁻¹ a]
No.9	[(1,3)(2,5)(4,7)(6,8)]; [a*b ⁻¹]
No.10	[()]; [e]

Table 3.3: The Galois groups and the subgroups corresponding to the Galois extension, represented by the generators of D_4 . ($a^2 = b^4 = e, ab = b^{-1}a$).

Remark 3.2. If one would like to see the Galois group operations on the roots of f , one should make use of the automorphisms of the splitting field. Let y be one of the roots of the polynomial K . The automorphism is composed of polynomials of y in this way:

$$y \rightarrow -y,$$

$$y \rightarrow y,$$

$$y \rightarrow -7/272*y^7 + 305/272*y^5 - 156/17*y^3 + 55/4*y,$$

$$y \rightarrow -7/544*y^7 - 5/816*y^6 + 305/544*y^5 + 247/816*y^4 \\ - 78/17*y^3 - 725/204*y^2 + 59/8*y + 101/12,$$

$$y \rightarrow -7/544*y^7 + 5/816*y^6 + 305/544*y^5 - 247/816*y^4 \\ - 78/17*y^3 + 725/204*y^2 + 59/8*y - 101/12,$$

$$y \rightarrow 7/544*y^7 - 5/816*y^6 - 305/544*y^5 + 247/816*y^4 \\ + 78/17*y^3 - 725/204*y^2 - 59/8*y + 101/12,$$

$$y \rightarrow 7/544*y^7 + 5/816*y^6 - 305/544*y^5 - 247/816*y^4 \\ + 78/17*y^3 + 725/204*y^2 - 59/8*y - 101/12,$$

$$y \rightarrow 7/272*y^7 - 305/272*y^5 + 156/17*y^3 - 55/4*y$$

In the next section, we shall discuss more the significance of the result presented in this section.

4 Review of the computation

4.1 From the simple model to the realistic system

We have worked in the rational number field \mathbb{Q} . However, in general cases, the matrix elements in the secular equations are real numbers and the corresponding polynomials have the coefficients of real numbers. Hence we should conduct the study not in \mathbb{Q} , but in

$$\mathbb{Q}(\{H_{ij}\}, \{S_{ij}\}),$$

that is an extension of \mathbb{Q} , to which the matrix elements $\{H_{ij}\}$ and $\{S_{ij}\}$ are added. One could extend this field and study the equations involved therein using the Galois theory. Notice that it is not obligatory to compute in the field of real numbers; $\{H_{ij}\}$ and $\{S_{ij}\}$ might be replaced with the approximations with rational numbers; then one can work in \mathbb{Q} .

4.2 Quantum mechanics as the objects of number theory

In this section, we make a review of the computation executed hitherto. As the eigenstates of quantum mechanics are represented by polynomials, one may expect the splitting of polynomial ideals in the extension of the fields, as is customary in the number theory:

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_n^{e_n}$$

Let us see how the splitting occurs. When the monomial order (for the Gröbner bases) is properly chosen, we obtain the set of polynomials to which the variables are added one by one. An example of this is the ideal \mathfrak{p} which we have obtained in the exemplary computation of a model molecule with the Galois group D_4 . The generators of \mathfrak{p} are given below.

```

_[1]=e^4+3*e^3-6*e^2-6*e+4
_[2]=5848*y(12)^2+54*e^3+209*e^2-205*e-766
_[3]=4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12)
_[4]=y(8)-y(12)
_[5]=4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12)
_[6]=y(11)+1/8*y(12)*e^8-21/8*y(12)*e^6+10*y(12)*e^4
    -21/2*y(12)*e^2+y(12)
_[7]=y(9)+y(10)+3/16*y(12)*e^8-185/48*y(12)*e^6
    +53/4*y(12)*e^4-113/12*y(12)*e^2
_[8]=y(7)+y(8)+1/6*y(12)*e^7-10/3*y(12)*e^5
    +61/6*y(12)*e^3-19/3*y(12)*e
_[9]=y(6)-1/12*y(12)*e^8+5/3*y(12)*e^6
    -61/12*y(12)*e^4+19/6*y(12)*e^2
_[10]=y(5)+y(12)*e
_[11]=y(4)-1/24*y(12)*e^7+7/8*y(12)*e^5-19/6*y(12)*e^3
    +3/2*y(12)*e
_[12]=y(3)+1/48*y(12)*e^8-17/48*y(12)*e^6+1/12*y(12)*e^4
    +19/12*y(12)*e^2
_[13]=y(1)+y(2)-1/24*y(12)*e^7+17/24*y(12)*e^5
    -1/6*y(12)*e^3-19/6*y(12)*e

```

If the polynomial for the energy spectrum, given at first as $_{-}[1]$, is split, we can decompose the corresponding algebraic variety into four subsets:

$$V(\mathfrak{p}) = V(\mathfrak{P}_1) \cup V(\mathfrak{P}_2) \cup V(\mathfrak{P}_3) \cup V(\mathfrak{P}_4)$$

where the subsets are defined by four ideals $\mathfrak{P}_i (i = 1, \dots, 4)$ such that

$$\mathfrak{p} = \mathfrak{P}_1 \cap \mathfrak{P}_2 \cap \mathfrak{P}_3 \cap \mathfrak{P}_4$$

Observe that the representation concerning the decomposition is given by the intersection; but the intersection is replaced with the product, as the four decomposed ideals are coprime with each other. (Recall the definition: two ideals a and b are coprime if and only if $a + b = (1)$; for such a pair, $a \cdot b = a \cap b$.) These four ideals are obtained only by replacing the first polynomial by a linear one:

$$e - \alpha_i.$$

The situation occurring in this computation would be illustrated by Fig.4.1. As the four quantum state have generators almost identical, except the linear polynomial of the variable 'e', the automorphism of $\mathbb{Q}(a)$ permutes them among themselves.

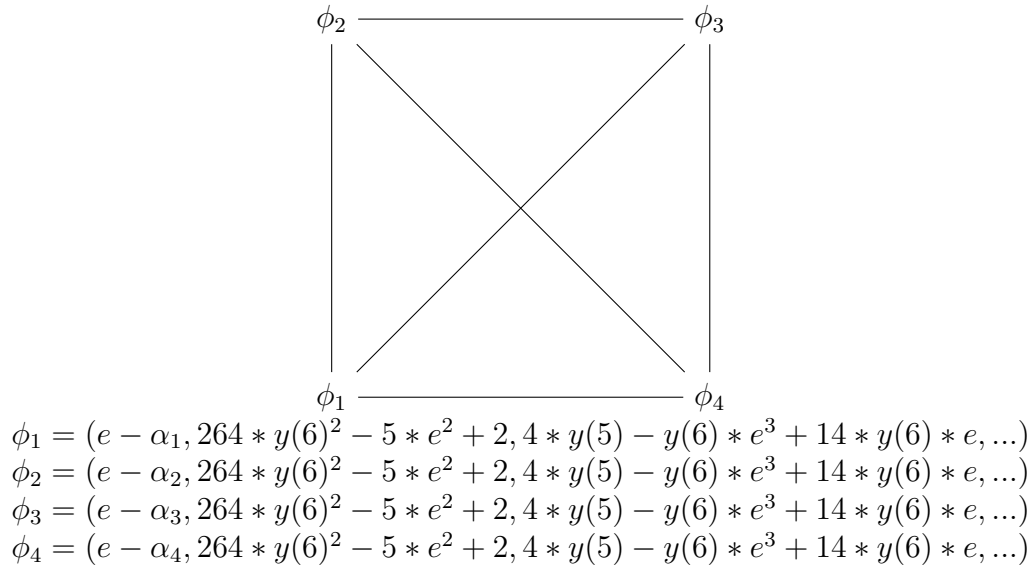


Figure 4.1: The permutation of the quantum states induced by the extension of field.

Let us clarify the points.

- The prime ideal \mathfrak{p} in \mathbb{Q} contains the polynomial of four degrees P_E , univariate of the variable of the energy spectrum. In the splitting field, it splits into four linear polynomials, and the ideal also splits into four prime ideals. As the other variables are linking to the energy spectrum 'e', the automorphism, (namely, the permutation of the roots of that equation) causes the permutation of the four prime ideals.
- In the splitting field, the four ideals that represent four quantum states are conjugate. In the subfields, these ideals would merge into prime ideals that encapsulate several quantum states.
- It is easy to write down the generators of prime ideals in the subfields. We have the prime ideal \mathfrak{p} in the base ring, and \mathfrak{p} has the univariate polynomial p_E which gives the energy spectra. In the subfields, this polynomial p_E shall split into $q_E^1 \cdots q_E^g$, as is demonstrated in the preceding section. In the generating set of \mathfrak{p} , we replace p_E with any of q_E^1, \dots, q_E^g to make the set of prime ideals P_1, \dots, P_g in the subfield.
- Fig. 4.2 visualizes the splittings of \mathfrak{p} in all of the subfields. Both in the sixth and seventh subfields, we find the sets of three prime ideals. These two sets share a feature: one prime ideal encloses two quantum states, while the remaining two prime ideals enclose only one quantum state. (These ideals are denoted by $P_{6,i}$ and $P_{7,i}$ in the figure.) This similarity arises from the conjugacy of the subfields and the subgroups in the Galois correspondence.

- Consider the prime ideals in one subfield. The operation of the subgroups permutes the conjugate pair of the quantum states belonging to the same prime ideal. And it does not intermingle the quantum states between represented by different prime ideals. On the other hand, if the subgroup N is normal in the Galois group G , the factor group G/N shall permute the quantum states belonging to different prime ideals.

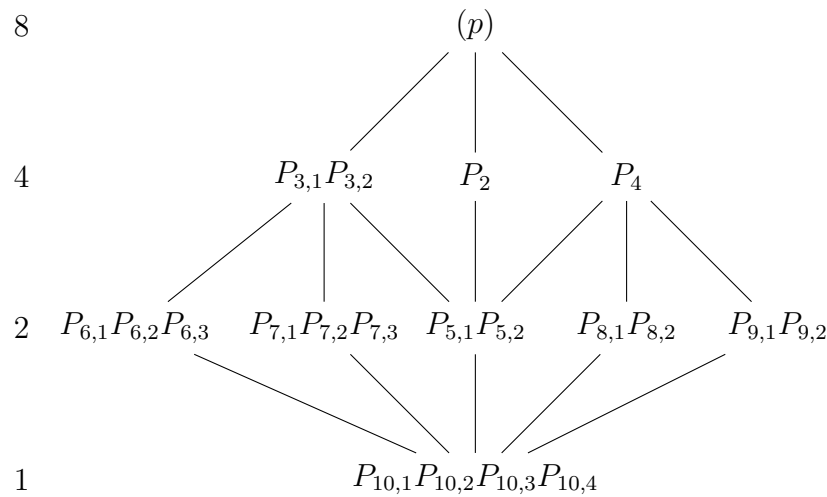


Figure 4.2: The graphical representation of the splitting of the ideals D_4 . Each node stands for the subfield, upon which transcribed are the factorized prime ideals enclosing quantum states. The inclusion relations as subfields are denoted by edges. The column of the numbers in the left side of the graph are the degrees of extensions.

The model molecule under investigation has two prime ideals other than \mathfrak{p} in $\mathbb{Q}[y(1), \dots, y(12), e]$. Let us go back to Section 3.2 and ascertain what they are. According to the list in that section, the first \mathfrak{p}_1 is of dimension 3 with spectrum $e = 0$; the second \mathfrak{p}_2 is \mathfrak{p} used above; the third \mathfrak{p}_3 is of dimension 0 with spectra $e^4 - 3e^3 - 6e^2 + 4 = 0$. These three prime ideals are interchanged by an operation as follows.

$$\begin{aligned} e &\longleftrightarrow -e \\ \mathfrak{p}_1 &\longleftrightarrow \mathfrak{p}_1 \\ \mathfrak{p}_2 &\longleftrightarrow \mathfrak{p}_3 \end{aligned}$$

The change of the sign of 'e' fixes \mathfrak{p}_1 while it interchanges \mathfrak{p}_2 and \mathfrak{p}_3 . \mathfrak{p}_3 is the replica of \mathfrak{p}_2 , similarly under the action of the Galois group D_4 .

Although we have labeled the quantum states by the energy spectrum, we could designate the quantum states by one of the variables $y(1), \dots, y(n)$ representing the

amplitude of the wave function. The new labels are the roots of the univariate polynomial equation of $y(i)$. The splitting field for this polynomial is larger than that for the polynomial of the energy spectrum. This is because of the double-fold degeneracy of $y(i)$; indeed ϕ and $-\phi$ are equivalent quantum states from the viewpoint of quantum mechanics, although they are distinguishable in the algebraic variety.

We dare say there is a hidden symmetry, which originates from the automorphism of the number field. Traditionally we have analyzed the symmetry in molecules using the point group that acts upon the atomic configuration, which fixes the secular equation and the energy spectrum [Wey50, Tin03, DDJ08]. However, the Galois theory provides the quantum system with another sort of symmetry, as we have seen now. (We use the term symmetry, so long as group-theoretic operations mutate the wavefunctions.) The apparent difference is that the energy spectrum is not fixed but changeable through the automorphism of the extended field. Note that the quantum states, exchangeable by the Galois theoretic automorphism, are included in the same irreducible representations of the molecular point group because they satisfy the same set of equations.

Concerning the point group operation, one should keep in mind this: the residue ring by a 0-dimensional ideal is denoted by

$$\mathbb{Q}[y_1, y_2, \dots, y_n, e]/\mathfrak{p}.$$

It stands for a field

$$\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n, \beta),$$

where $(\alpha_1, \alpha_2, \dots, \alpha_n, \beta) \in V(\mathfrak{p})$. (That is to say, $(\alpha_1, \alpha_2, \dots, \alpha_n, \beta)$ is the solution of the polynomial equations defined by \mathfrak{p} .) One can construct the automorphism of the former large field, which contains the point-group operation on the wavefunctions. In this wise, our exemplar computation is the study of the part of the automorphism in this field, as we have worked in $\mathbb{Q}(e)$ modestly. The unified modeling of the Galois group and the point group would be possible.

5 Class field theory and quantum mechanics

5.1 Preliminaries

The aim of *class field theory* is to establish the correspondence between a type of group generated by ideals and the Galois group in the extension of the field [Mil17, Con01, AT68, Ser79, Gra13].

As we know, one of the fundamental items in number theory is the ideal, which is the set closed by the multiplication and the addition. Besides, in a similar way to the integers, the division between two ideals is defined. The consequence of this extension is the *fractional ideal*, in which a kind of group structure is built.

In general number fields K , we can define the ideal class group I_K/P_K in K as the quotient of the fractional ideal group I_K by a subgroup P_K , the latter of which is

composed of the principal ideals in K which satisfy a certain condition. It is proved that the number of classes in a number field is limited.

In the extension field, the ideal class group and that of the Galois group are deeply related; to establish the correspondence between these two objects is the principal concern of the *class field theory*.

To construct the *class field theory*, we have to define several things. Let L be a separable extension of degree n over K , with K -homomorphisms $(\sigma_1, \dots, \sigma_n)$. The rings of integers for these fields are denoted by \mathcal{O}_L and \mathcal{O}_K . The prime ideal in K is denoted by \mathfrak{p} and the prime ideal in L that divide \mathfrak{p} is denoted by \mathfrak{B} .

- [Ring of integer] An element of the field is F integral over \mathbb{Z} if it satisfies the equation

$$x^m + a_1 x^{m-1} + \dots + a_m = 0,$$

with $a_1, \dots, a_m \in \mathbb{Z}$. The ring of elements of L integral over \mathbb{Z} is called the integral closure of \mathbb{Z} in L . The integral closure of \mathbb{Z} in an algebraic number field L is called the ring of integers \mathcal{O}_L in L .

- [Trace and Norm] The trace and norm maps are defined in the following way. $\text{Tr}_{L/K}(\beta) := \sigma_1(\beta) + \dots + \sigma_n(\beta)$; $\text{Nm}_{L/K} := \sigma_1(\beta) \times \dots \times \sigma_n(\beta)$
- [Fractional ideal] A fractional ideal I in K is a set of elements such that there exists a non-zero $r \in \mathcal{O}_K$ and $rI \subseteq \mathcal{O}_K$
- [Modulus] A modulus of a number field K is the formal product of ideals: $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$, where \mathfrak{m}_0 is the products of finite primes; \mathfrak{m}_∞ is that of infinite real primes. (The definition of the latter is complicated. It is a kind of sign condition which we use for the real numbers.) We denote by $S(\mathfrak{m})$ the set of prime ideals which divide \mathfrak{m} .
- [The group of fractional ideals with a modulus] Let I^S be the group of fractional ideals generated the prime ideals of K which do not lie in S .
- [Ray class group] Let $C_{\mathfrak{m}}$ be the quotient $I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$. We define $K_{\mathfrak{m},1}$ to be the set generated by the element a such that

$$\text{ord}_{\mathfrak{p}}(a - 1) \geq \text{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$$

for all prime ideals \mathfrak{p} dividing \mathfrak{m}_0 , and,

$$a_{\mathfrak{p}} > 0$$

at all primes dividing \mathfrak{m}_∞ . Regarding the latter condition, readers should check what it would mean exactly from textbooks because it involves a quantity of explanation on number theory. In the case of the \mathbb{Q} , it means $a > 0$. i is the map from $K_{\mathfrak{m},1}$ to $I^{S(\mathfrak{m})}$, defined by $a \mapsto (a)$. For any $a \in K_{\mathfrak{m},1}$, the principal ideal (a) belongs to $I^{S(\mathfrak{m})}$. Hence $i(K_{\mathfrak{m},1})$ is the subgroup of $I^{S(\mathfrak{m})}$ and generated by principal ideals.

- [Frobenius map] Frobenius element, denoted by $(\mathfrak{P}, L/K)$ is the unique element σ of $\text{Gal}(L/K)$ satisfying the following two conditions:

$$\sigma\mathfrak{P} = \mathfrak{P}$$

and for all $\alpha \in \mathfrak{O}_L$

$$\sigma(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}$$

where q is the number of elements the residue field $\mathfrak{O}_K/\mathfrak{p}$. For an extension L of K , let $S'(\mathfrak{m})$ be the prime ideals of L lying over the prime ideals in $S(\mathfrak{m})$. We have a norm map $\text{Nm} : I^{S'(\mathfrak{m})} \rightarrow I^{S(\mathfrak{m})}$ such that $\text{Nm}(\mathfrak{P}) = \mathfrak{p}^f$ where $\mathfrak{p} = \mathfrak{O}_K \cap \mathfrak{P}$. Let f is the residue class degree $[\mathfrak{O}_L/\mathfrak{P} : \mathfrak{O}_K/\mathfrak{p}]$. Then we have

$$(\text{Nm}(\mathfrak{P}), L/K) = (\mathfrak{p}^f, L/K) \stackrel{\text{def}}{=} (\mathfrak{p}, L/K)^f = 1.$$

Hence $\text{Nm}(I^{S'(\mathfrak{m})})$ is contained in the kernel of $I^{S(\mathfrak{m})} \rightarrow C_{\mathfrak{m}}$.

Theorem 5.1 (ARTIN, Reciprocity law). Let L be an abelian extension of K ; let S be the set of prime ideals that ramify in L . For some modulus \mathfrak{m} such that $S(\mathfrak{m}) = S$, the homomorphism

$$I^S \rightarrow \text{Gal}(L/K),$$

or,

$$p \mapsto (p, L/K)$$

factors through $C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$.

It induces an isomorphism

$$I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \cdot \text{Nm}(I^{S'(\mathfrak{m})}) \rightarrow \text{Gal}(L/K)$$

where $S'(\mathfrak{m})$ are the prime ideals of L lying over the prime ideals in $S(\mathfrak{m})$. In particular, the prime ideals splitting in L exactly belong to the subgroup of I^S , given by

$$\tilde{H} = i(K_{\mathfrak{m},1}) \cdot \text{Nm}(I^{S'(\mathfrak{m})}).$$

Theorem 5.2 (LOCAL RECIPROCITY LAW). For every non-archimedean local field K , there exists a unique homomorphism

$$\phi_K : K^\times \rightarrow \text{Gal}(K^{\text{ab}}/K)$$

with the following properties:

- (a) for every prime element π of K and every finite unramified extension L of K , $\phi_K(\pi)$ acts on L as the Frobenius map $(\text{Frob}_{L/K})$;
- (b) for every finite abelian extension L of K , $\text{Nm}_{L/K}(L^\times)$ is contained in the kernel of $a \mapsto \phi_K(a)|_L$, and ϕ_K induces an isomorphism

$$\phi_K : K^\times / \text{Nm}_{L/K}(L^\times) \rightarrow \text{Gal}(L/K)$$

In particular, we have

$$(K^\times : \text{Nm}_{L/K}(L^\times)) = [L : K].$$

Let us denote $\text{Nm}_{L/K}(L^\times)$ by $\text{Nm}(L^\times)$. The statement (b) says that, for every finite abelian extension L of K , the map K factors as follows:

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_K} & \text{Gal}(K^{ab}/K) \\ \text{quotient map} \downarrow & & \downarrow \tau \mapsto \tau|_L \\ K^\times/\text{Nm}(L^\times) & \xrightarrow[\simeq]{\phi_{L/K}} & \text{Gal}(L/K) \end{array}$$

In the above diagram, ϕ_K and $\phi_{L/K}$ are the local Artin maps (the local reciprocity maps) for K and L/K . $\phi_{L/K}$ is often called the norm residue map and denoted by $a \mapsto (a, L/K)$. The subgroups of K^\times , given by $\text{Nm}(L^\times)$ for some finite abelian extension L of K , are called the norm groups in K .

Theorem 5.3 (EXISTENCE THEOREM). For every congruence subgroup H modulo \mathfrak{m} , there exists a finite abelian extension L/K such that $H = i(K_{\mathfrak{m},1})\text{Nm}_{L/K}(I_L^{\mathfrak{m}})$.

At a glance, it is unclear how to constitute a class field. However, This fact is affirmed.

- Every abelian extension of \mathbb{Q} is a class field. (Another version of the statement goes as follows: according to the Kronecker-Weber theorem (the primitive version of the existence theorem), every abelian extension of \mathbb{Q} is contained in a cyclotomic extension.

In the following sections, we execute heuristic computations to comprehend these concepts and statements.

5.2 Feasibility of class field theory in quantum mechanics

As far as we concern ourselves about the computation of quantum mechanics, which is accomplished by the decomposition of ideals, this sort of statement is quite touching for us. We use the prime ideals \mathfrak{p} in the base ring $R = \mathbb{Q}[y_1, \dots, y_n, e]$ to represent a quantum state. If the polynomial representation is possible, anything related to this quantum state is given symbolically by the ideal I in the ring of integers of the quotient field $R/\mathfrak{p}R$. (Also one might employ an extension ring: $(R/\mathfrak{p}R)[x_1, \dots, x_m]$ with the new set of indeterminate variables.) Once the class field is constructed over $R/\mathfrak{p}R$, we could expect the reciprocity relation, which regulates the splitting of the ideal through the Norm map. Now let us inspect what the merit of ideal representation should be. Recall that an ideal is a quite different object from the ordinary numbers: several elements could generate one ideal. In contrast, the observable in quantum mechanics would be represented by a single function, which generates a principal ideal if it is expressed by

a polynomial. In class field theory, however, as the ray class group is the quotient of the group of fractional ideals by a certain class of principal ideals, there are principal ideals which reduce to the identity. Hence the observable as the principal ideal might be the trivial element in the class group, from which we could not expect any useful application. Then what shall be a non-principal ideal? In a sense, it is the line of mass production of mathematical objects from a set of generators. If one is engaged in a bunch of computations using the elements in an ideal I , the factorization of the ideal might economize the cost of computation, as it would serve as a kind of Karatsuba algorithm. However, it is not of the interest of quantum mechanics.

Besides, it seems that there would be technical difficulties to construct the class field for the polynomial algebra. One has to prove the existence of the maximum abelian extension that should be the class field. At the same time, one has to substantiate it by polynomials, establishing the maps between the class group and the Galois group. As far as the authors investigate the references, the existence of class field has been proven for the function field, as well as for the number field; for these two objects, the concrete construction of the class field should be possible. Hence the class field theory over the algebra of polynomials would be practicable. However, the general-purpose algorithm to build the class field seems to be unknown for the latter case.

If \mathfrak{p} is 0-dimensional, $R/\mathfrak{p}R$ is an extension of \mathbb{Q} and the class field theory might be applicable. However, this number field appears to be too large; it might not be an abelian extension. We know that the entries in the solutions of the equation $\mathfrak{p} = 0$ are mutually dependent, owing to the specific forms of the defining polynomials. (As for the dependence of the variables, review the generators of prime ideals given in Section 3.2.) However, once they are lifted to the extension field, such dependence is hardly discerned. We prefer to work on a smaller scale, always keeping in mind the feature of the polynomial ideal.

For these reasons, at present, we postpone the plan to construct the class field over the polynomial algebra. Instead, we seek another channel from which the outcome of class field theory could be conducted into quantum mechanics.

5.3 Consequence of class field theory in quantum mechanics

Let us see a consequence of the theorem concerning the class field theory. In this section, we choose a model molecule with the Galois group $C_2 \times C_2$, the analysis of which is given in the appendix B. One of the entries of the primary ideal decomposition is given as follows.

$$\begin{aligned} P1 = & (e^4 - 14e^2 + 16, \\ & 264y(6)^2 - 5e^2 + 2, \\ & 4y(5) - y(6)e^3 + 14y(6)e, \\ & y(4) - y(6), \end{aligned}$$

$$\begin{aligned} &4*y(3)+y(6)*e^3-12*y(6)*e, \\ &2*y(2)-y(6)*e^2+12*y(6), \\ &4*y(1)+y(6)*e^3-12*y(6)*e \end{aligned}$$

It contains four quantum states, distinguished by four energy spectra, which are the roots of the first univariate polynomial of the variable 'e': $e^4 - 14e^2 + 16$. Let us compute the Galois extension and factorize the polynomial, using PARI/GP. We must recall these things: as we have seen, the factorization of the polynomial causes that of the ideal; the permutation of the roots of the polynomial is equivalent to that of the quantum states.

```
/* Define the polynomial f. */
f=Pol([1,0,-14,0,16])
/* Compute the splitting field and get the defining polynomial L*/
L=nfsplitting(f) /*In this case L=f */
nf=nfinit(L);
/* Make the Galois extension. */
gal=galoisinit(L);
```

Under the decomposition of the polynomial, the ideal P_1 decomposes into P_{11} , P_{12} , P_{13} , and P_{14} in the extension field $L = \mathbb{Q}(a)$, where a is a root of the polynomial f .

Let us try an experiment: choose a prime integer p (in \mathbb{Z}) and decompose it in L . One finds the set of prime ideals $(\mathfrak{P}[1] \dots \mathfrak{P}[g])$ in $\mathbb{Q}(a)$ lying over p . Therein p might be decomposed into the different numbers of prime ideals. From each of these prime ideals, one could manage to make the so-called Frobenius map, which has this property:

$$\sigma(x) == x^{\#N[p]} \bmod \mathfrak{P}[i],$$

where simply $\#N[p] = p$ for a prime. This is an automorphism in $\mathbb{Q}(a)/\mathbb{Q}$. (In general, for the extension L over K , the Frobenius map is denoted by $(\mathfrak{P}, L/K)$.) How it would be? Once it is built, it also acts as the transmuting map among the four quantum states P_{12} , P_{12} , P_{13} , and P_{14} .

Remark 5.1. The proof of the existence of the Frobenius element requires a short argument, as is given in Chapter 8 of [Mil17]. One can find the Frobenius element by symbolic computations.

Let us define a small function of PARI/GP.

```
procmakefrobenius(p)=
{
  prs=idealprimedec(nf,p);
  g = vector(#prs,k,idealfrobenius(nf,gal,prs[k]));
  polmap=vector(#g,k,galoispermtopol(gal,g[k]));
  return(polmap);
}
```

The function does the prime ideal decomposition of the given prime number in the extension field; then, for each of the prime ideals obtained by the decomposition, it computes the Frobenius map. The result is a table, in which the Frobenius maps are transcribed. (Hence the length of the table is the number of the decomposed factors; it might be 1, 2, or 4.) Let us try the computation with the list of primes in \mathbb{Z} . As the discriminant of the polynomial f is $4460504 = 2^{12} \cdot 3^2 \cdot 11$, the primes that shall ramify in $\mathbb{Q}(a)$ are only three: 2, 3, and 11. From these primes, one could not make the Frobenius map, and we omit them from the experiment. The result given below shows the primes and the corresponding Frobenius maps. The Frobenius maps are given by the polynomials $Frb(x)$, which maps the generator 'a' of $\mathbb{Q}(a)$ by $a \mapsto Frb(a)$. The permutations of the four roots of the polynomial f (viz., the permutation in four quantum states), induced by the Frobenius map, are also shown.

```
prime->[Frobenius maps]
5->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]      !(1,2)(3,4)
7->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]    !(1,3)(2,4)
13->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
17->[-x, -x]                                !(1,4)(2,3)
19->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
23->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
29->[x, x, x, x]                            !()
31->[-x, -x]
37->[-x, -x]
41->[-x, -x]
43->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
47->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
53->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
59->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
61->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
67->[x, x, x, x]
71->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
73->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
79->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
83->[-x, -x]
89->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
97->[x, x, x, x]
101->[x, x, x, x]
103->[-x, -x]
107->[-x, -x]
109->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
113->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
127->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
131->[-x, -x]
137->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
```

139-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 149-> $[x, x, x, x]$
 151-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 157-> $[-x, -x]$
 163-> $[x, x, x, x]$
 167-> $[x, x, x, x]$
 173-> $[x, x, x, x]$
 179-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 181-> $[-x, -x]$
 191-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 193-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 197-> $[x, x, x, x]$
 199-> $[-x, -x]$
 211-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 223-> $[-x, -x]$
 227-> $[-x, -x]$
 229-> $[-x, -x]$
 233-> $[-x, -x]$
 239-> $[x, x, x, x]$
 241-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 251-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 257-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 263-> $[x, x, x, x]$
 269-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 271-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 277-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 281-> $[-x, -x]$
 283-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 293-> $[x, x, x, x]$
 307-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 311-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 313-> $[x, x, x, x]$
 317-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 331-> $[x, x, x, x]$
 337-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$
 347-> $[-x, -x]$
 349-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 353-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 359-> $[x, x, x, x]$
 367-> $[-x, -x]$
 373-> $[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]$
 379-> $[x, x, x, x]$
 383-> $[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]$

```

389->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
397->[-x, -x]
401->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
409->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
419->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
421->[-x, -x]
431->[x, x, x, x]
433->[x, x, x, x]
439->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
443->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
449->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
457->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
461->[x, x, x, x]
463->[-x, -x]
467->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
479->[x, x, x, x]
487->[-x, -x]
491->[-x, -x]
499->[x, x, x, x]
503->[x, x, x, x]
509->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
521->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]
523->[1/4*x^3 - 7/2*x, 1/4*x^3 - 7/2*x]
541->[-1/4*x^3 + 7/2*x, -1/4*x^3 + 7/2*x]

```

We observe these remarkable phenomena:

- Four patterns are discernible in the images of the maps. One prime always generates one unique Frobenius map, even if it splits into distinct prime ideals.
- When four identical Frobenius maps are obtained, i.e., when the prime splits completely into four components, the map is always the identity ($x \rightarrow x$);
- Otherwise, the map is not the identity.

The first phenomenon results from the feature of the chosen Galois group: one can prove that, in the case of abelian extension, in other words, if the Galois group is abelian, the Frobenius map is unique for all of the prime ideals lying over one prime. Hence one denotes the map by $(p, L/K)$. (To collaborate this statement, please experiment with the molecule with the Galois group D_4 : in the latter case, the prime ideals decomposed from one prime might generate different maps. And you shall find that when p splits completely into eight components, the Frobenius map is the identity ($x \rightarrow x$).)

The second and third phenomena are quite intriguing. One can assert this:

a prime p in K splits completely in L if and only if $(p, L/K)$ is the identity.

This is ascribed to the reciprocity law, which is the consequence of the class field theory.

According to the statement of class field theory, one can claim more subtle things about the Frobenius maps between the primes and the Galois group. Recall that the prime ideals in \mathbb{Q} that ramify in splitting field L of the polynomial $f = x^4 - 14x^2 + 16$ are 2, 3, and 11. Let us check the reminders of primes modulo the powers of 2, 3, 11, and compare them to the corresponding images of the Frobenius map. We notice the following.

[A] If $p \bmod 3 == 1$ and $p \bmod 11 == 1$, then $(p, L/\mathbb{Q})(x) = x$ or $-x$.

[B] If $p \bmod 3 == 1$ and $p \bmod 11 == 1$
and $p \bmod 2*2*2 = (1 \text{ or } 3)$
then
 $(p, L/\mathbb{Q})(x) = x$.

[C] If $p \bmod 3 == 1$ and $p \bmod 11 == 1$
and $p \bmod 2*2*2 = (5 \text{ or } 7)$
then
 $(p, L/\mathbb{Q})(x) = -x$.

These observations suggest that the primes are partitioned into several subsets, each of which has a common image by the Frobenius map. (This is the namesake of *class field theory*.) The partitioning of primes would be done according to the modulo by a finite set of unramified primes. If the partitioning is done according to the condition [A], it is insufficient to make a map from the class group to the Galois group, as one subset has two images. In contrast, if the partitioning is done according to the conditions [B] and [C], we could distinguish two subsets by the different images and could make the well-defined map upon them. This sort of argument is related to the necessity of the ray class group, which renders the statements of class field theory abstruse, in accumulating the troublesome definitions such as “modulus”, “congruence subgroup modulo m ”, “conductor”, or “the homomorphism which admits a modulus”, etc.

Let us conduct one more numerical experiment. In a range of primes that not ramify in $L = \mathbb{Q}(a)$, we compute the Frobenius map of primes p and evaluate the residues of p modulo 3, 11, 8. We store the result in the list $[[p \bmod 3, p \bmod 11, p \bmod 8], (p, L/\mathbb{Q})]$; the first three remainders attach the label to the prime p . Then we accumulate the computation, remove the duplication, and sort the set to extract the distinct classes. As a result, we get 80 classes of primes.

Frobenius Map	The number of related classes	Typical class
$[x]$	20	$[1,1,1]$
$[-x]$	20	
$[-1/4 * x^3 + 7/2 * x]$	20	
$[1/4 * x^3 - 7/2 * x]$	20	

One-quarter of those distinct classes contains 20 entries, and each of the four quarters maps itself exactly into a unique element of the Galois group $C_2 \times C_2$. Besides, other than the class $([1, 1, 1])$, there are more classes mapped to the identity. It means that the kernel of the map is larger than the *unit* in the quotient. This is a collaboration of the reciprocal law, wherein we shall recognize the reason d'être of modulus; it is required to impart the sufficiently fine classification to the primes so that the correspondence between the ideal class group and the Galois group could be built.

Note that the classification given above uses the modulus $(2^3)(3)(11)(\infty)$. One might understand what the real prime (∞) means, from the following statements. In modulo 8, the ideal $(7) \equiv (-7) \equiv (1)$, because $-7-1 \equiv 0 \pmod{8}$. However, the remainders 7 and 1 are distinguished concerning the images by the Frobenius map. We utilize the infinite real prime (∞) to take into account the sign condition for finer distinction.

Remark 5.2. As the element in the fractional ideal is represented by the product of the powers of primes, we define the Artin map:

$$\phi_{L/K} : \mathfrak{p}_1^{n_1} \cdot \mathfrak{p}_t^{n_t} \mapsto \prod (\mathfrak{p}_i, L/K)^{n_i}.$$

This map, in the reciprocal law, relates the fractional ideal to the Galois group. As the norm map $\text{Nm}(I_L^S)$ is included in the kernel of the Artin map, the latter induces the homomorphism

$$\phi_{L/K} : I_K^S / \text{Nm}(I_L^S) \mapsto \text{Gal}(L/K).$$

Remark 5.3. The principal ideal in a number field shall split into non-principal ones in the extension of that field. Let $L = \mathbb{Q}(a)$ be the extension of \mathbb{Q} by a root of $y^4 - 14y^2 + 16$, as above. The integers in L (denoted by \mathcal{O}_L) are represented by the following basis set:

$$Zk = (1, 1/4 * a^3 - 5/2 * a, a, 1/2 * a^2 - 4).$$

Therefore the generators of ideals are represented by $Zk \cdot M$ with the matrices. Some of the primes in \mathbb{Z} split as follows.

$$(2)\mathcal{O}_L = \mathfrak{B}_1 \mathfrak{B}_2.$$

with

$$\mathfrak{B}_1 = Zk \cdot \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\mathfrak{B}_2 = Zk \cdot \begin{bmatrix} 2 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

$$(11)\mathcal{O}_L = \mathfrak{B}^2$$

with

$$\mathfrak{P} = Zk \cdot \begin{bmatrix} 11 & 0 & 0 & 6 \\ 0 & 11 & 5 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Remark 5.4. Regarding the ray class field, Milner, in his book [Mil13], jotted down this comment:

To prove the Existence Theorem we must construct a ray class field for each modulus. Unfortunately, we don't know how to construct the ray class field directly. Rather we construct enough extensions to force the theorem to be true.

The situation emerging this computation would be illustrated by Fig.5.1. The Frobenius maps $(p, \mathbb{Q}(a)/\mathbb{Q})$ induces the permutation of the four quantum states $\{\phi_i\}$. In other words, the Frobenius map in the underlying number fields induces the permutation of the prime ideals representing $\{\phi_i\}$ in the polynomial ring. For this reason, the consequence of class field theory in the underlying number fields emerges in the polynomial rings.

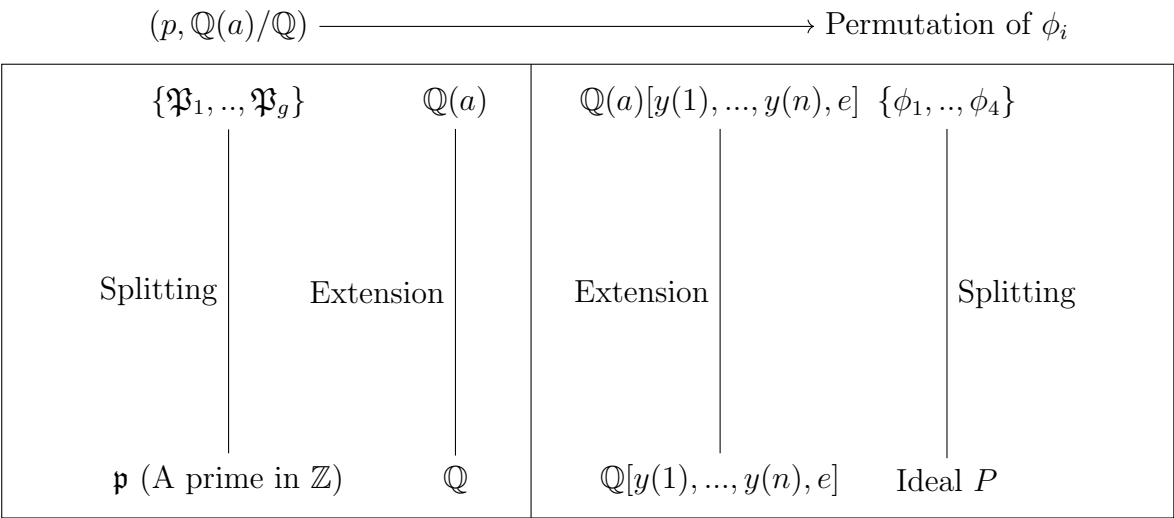


Figure 5.1: The extension and the splitting in the computed model.

5.4 Chebotarev density theorem

The primes are factorized and transformed into the Frobenius maps according to a certain pattern. The occurrence of each pattern seems to be random – is it not a kind of quantum fluctuation? Let us compute the density of each pattern in the accumulated result. This experiment shall reveal another consequence of the class field theory, which is stated as follows.

Let L be the finite Galois extension of the number field K with the Galois group G . And let C be the subset of G stable under the conjugation. It has the following property: if $\sigma \in C, \tau \in G$, then $\tau\sigma\tau^{-1} \in C$. (Usually, C is called the *conjugacy class*.) Moreover, let $T(C)$ be the set of prime ideals in K , being unramified prime in K , and accompanied by a certain type of Frobenius map such that $(p, L/K) \subset C$. Each $T(C)$ shall occupy a certain amount of density in the infinite number of primes. This quantity is called the *Dirichlet density*. Then, according to the Chebotarev density theorem, the Dirichlet density for $T(C)$ is related to two factors: the size of the conjugacy class and the order of the Group. It is given by the equation:

$$\delta(T(C)) = \frac{\#C}{\#G}$$

Note that this equation is not the definition; the left-hand side is the density of the subsets in the infinite number of primes, classified by the conjugacy classes; on the other hand, the right-side pertains to the Galois group; the relation between them is not trivial.

In the case of the model molecule with the Galois group $C_2 \times C_2$ (defined by $\langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle$), there are four types of $C[i]$ ($i = 1, 2, 3, 4$), i.e.,

$$\{\{1\}, \{a\}, \{b\}, \{ab\}\}.$$

As the group is abelian, each conjugacy class contains only one element and

$$\delta(C[i]) = 1/4, \text{ for } i = 1, \dots, 4.$$

The numerical check verifies the statement. Using the finite set of primes (which contains every prime from 2 to a maximum, except those which ramify), one can compute the corresponding Frobenius elements, and evaluate the density for each conjugacy class. Fig. 5.2a is the plot of the variation of the densities of four Frobenius elements with the increase of the number of the sampled primes. Indeed, each density converges to 1/4. In the case of non-abelian extension, the density theorem is also valid. For the case of the model molecule with the Galois group D_4 , the definition of which is $\langle r, s \mid r^4 = s^2 = 1, (rs)^2 = 1 \rangle$. This group has five conjugacy classes:

$$\{\{1\}, \{r^2\}, \{r, r^3\}, \{s, r^2s\}, \{rs, r^3s\}\}.$$

These classes have the density

$$1/8, 1/8, 1/4, 1/4, 1/4,$$

and that is collaborated by the numeric simulation, shown in Fig. 5.2b.

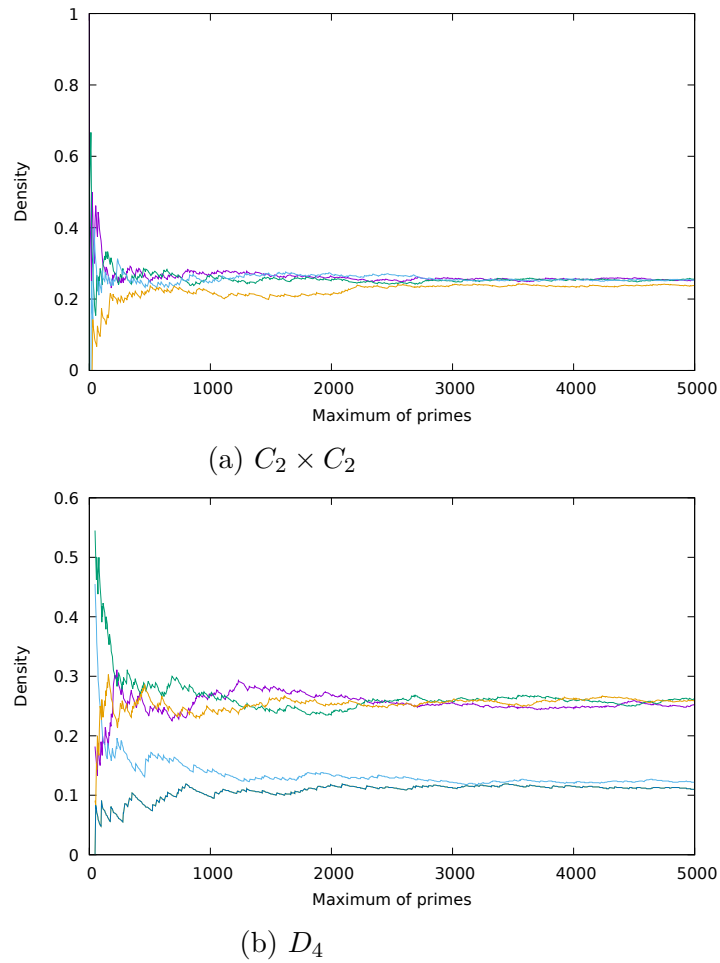


Figure 5.2: The numerical check of Chebotarev density theorem, using the computation of the model molecules: (a) the model with the Galois group $C_2 \times C_2$; (b) the one with the Galois group D_4 . The densities are computed in the finite set of the first N primes (counted from 2). The vertical and the horizontal axis represent the density and the maximum one in the set of primes used in the estimation, respectively.

6 Conclusion

We have presented a template of computation in algebraic molecular orbital theory. Once quantum mechanics get the algebraic representation, we could study problems from an algebraic standpoint, wherein algebraic geometry is essential. We have affirmed that Galois and class field theory would have no small significance. To this end, computer algebra is an excellent means. We hope this sort of study shall be profitable for the progress of quantum theory.

7 Acknowledgement

The computer programs used in this work are available at <https://github.com/kikuchiichio/GaloisClassFieldTheoryQ>.

Appendices

A The splitting of the polynomial $x^8 - 46 * x^6 + 461 * x^4 - 1360 * x^2 + 1156$ (for the study of a model molecule with D_4 Galois group)

In the main part of this article, to solve the eigenvalue problem for a model molecule with the Galois group D_4 , we used an extension of \mathbb{Q} , defined by $K = x^8 - 46 * x^6 + 461 * x^4 - 1360 * x^2 + 1156$. In this section, we see the splitting of K in the subfields (No.1...No.10), which are indexed in the main part of the article.

No.1	$x^8 - 46 * x^6 + 461 * x^4 - 1360 * x^2 + 1156$
No.2	$x^4 - 23 * x^2 - 1/3 * y_2 * x - 34, x^4 - 23 * x^2 + 1/3 * y_2 * x - 34$
No.3	$x^4 - y_3 * x^3 + 11 * x^2 + 3 * y_3 * x - 34,$ $x^4 + y_3 * x^3 + 11 * x^2 - 3 * y_3 * x - 34$
No.4	$x^4 - 1/2 * y_4 * x^2 + (3/2 * y_4 - 17),$ $x^4 + (1/2 * y_4 - 46) * x^2 + (-3/2 * y_4 + 121)$
No.5	$x^2 + (-1/310 * y_5^3 + 69/310 * y_5^2 - 22/5 * y_5 + 3519/155) * x$ $+ (1/620 * y_5^3 - 69/620 * y_5^2 + 17/10 * y_5 - 442/155),$ $x^2 + (1/310 * y_5^3 - 69/310 * y_5^2 + 22/5 * y_5 - 3519/155) * x$ $+ (-1/620 * y_5^3 + 69/620 * y_5^2 - 17/10 * y_5 - 488/155),$ $x^2 + (-1/310 * y_5^3 + 69/310 * y_5^2 - 22/5 * y_5 + 3519/155) * x$ $+ (-1/620 * y_5^3 + 69/620 * y_5^2 - 17/10 * y_5 - 488/155),$ $x^2 + (1/310 * y_5^3 - 69/310 * y_5^2 + 22/5 * y_5 - 3519/155) * x$ $+ (1/620 * y_5^3 - 69/620 * y_5^2 + 17/10 * y_5 - 442/155)$
No.6	$x^2 - y_6 * x + (3/49 * y_6^3 + 29/98 * y_6^2 - 393/98 * y_6 - 19/49),$ $x^2 + y_6 * x + (3/49 * y_6^3 + 29/98 * y_6^2 - 393/98 * y_6 - 19/49),$ $x^2 + (16/49 * y_6^3 + 12/49 * y_6^2 - 999/49 * y_6 + 846/49) * x$ $+ (9/49 * y_6^3 - 11/98 * y_6^2 - 1179/98 * y_6 + 1070/49),$ $x^2 + (-16/49 * y_6^3 - 12/49 * y_6^2 + 999/49 * y_6 - 846/49) * x$ $+ (9/49 * y_6^3 - 11/98 * y_6^2 - 1179/98 * y_6 + 1070/49)$

No.7	$x^2 - y_7 * x + (-3/49 * y_7^3 + 29/98 * y_7^2 + 393/98 * y_7 - 19/49),$ $x^2 + (-16/49 * y_7^3 + 12/49 * y_7^2 + 999/49 * y_7 + 846/49) * x +$ $(-9/49 * y_7^3 - 11/98 * y_7^2 + 1179/98 * y_7 + 1070/49),$ $x^2 + (16/49 * y_7^3 - 12/49 * y_7^2 - 999/49 * y_7 - 846/49) * x +$ $(-9/49 * y_7^3 - 11/98 * y_7^2 + 1179/98 * y_7 + 1070/49),$ $x^2 + y_7 * x + (-3/49 * y_7^3 + 29/98 * y_7^2 + 393/98 * y_7 - 19/49)$
No.8	$x^2 - 1/2 * y_8,$ $x^2 + (-5/3264 * y_8^3 + 247/1632 * y_8^2 - 725/204 * y_8 + 101/6) * x$ $+ (-1/128 * y_8^3 + 43/64 * y_8^2 - 85/8 * y_8 + 143/4),$ $x^2 + (-1/64 * y_8^3 + 43/32 * y_8^2 - 83/4 * y_8 + 85/2),$ $x^2 + (5/3264 * y_8^3 - 247/1632 * y_8^2 + 725/204 * y_8 - 101/6) * x$ $+ (-1/128 * y_8^3 + 43/64 * y_8^2 - 85/8 * y_8 + 143/4)$
No.9	$x^2 - y_9 * x + (1/4 * y_9^2 - 17/4),$ $x^2 + (-1/6 * y_9^3 + 1/4 * y_9^2 + 29/3 * y_9 - 75/4),$ $x^2 + y_9 * x + (1/4 * y_9^2 - 17/4),$ $x^2 + (1/6 * y_9^3 + 1/4 * y_9^2 - 29/3 * y_9 - 75/4)$
No.10	$x - y_{10},$ $x + (-7/544 * y_{10}^7 - 5/816 * y_{10}^6 + 305/544 * y_{10}^5 + 247/816 * y_{10}^4 - 78/17 * y_{10}^3$ $- 725/204 * y_{10}^2 + 59/8 * y_{10} + 101/12),$ $x + (7/272 * y_{10}^7 - 305/272 * y_{10}^5 + 156/17 * y_{10}^3 - 55/4 * y_{10}),$ $x + (-7/544 * y_{10}^7 + 5/816 * y_{10}^6 + 305/544 * y_{10}^5 - 247/816 * y_{10}^4 - 78/17 * y_{10}^3$ $+ 725/204 * y_{10}^2 + 59/8 * y_{10} - 101/12),$ $x + (7/544 * y_{10}^7 + 5/816 * y_{10}^6 - 305/544 * y_{10}^5 - 247/816 * y_{10}^4 + 78/17 * y_{10}^3$ $+ 725/204 * y_{10}^2 - 59/8 * y_{10} - 101/12),$ $x + y_{10},$ $x + (7/544 * y_{10}^7 - 5/816 * y_{10}^6 - 305/544 * y_{10}^5 + 247/816 * y_{10}^4 + 78/17 * y_{10}^3$ $- 725/204 * y_{10}^2 - 59/8 * y_{10} + 101/12),$ $x + (-7/272 * y_{10}^7 + 305/272 * y_{10}^5 - 156/17 * y_{10}^3 + 55/4 * y_{10})$

Remark A.1. CAVEAT. The permutations (given as the generators of the groups in the main part of the article) do not exchange the factorized linear polynomials (in No.10) according to the sequential ordering in the list, despite one's expectation. The Galois group contains the element $(1, 2)(3, 7)(4, 6)(5, 8)$, which represents $y \rightarrow -y$; indeed polynomials of the first and the second are interchanged, but the third and the seventh are not; in fact, the pair to the third is the fourth. Therefore, if one would like to know the Galois group operations on polynomials, one should at first get the automorphism of the splitting field and then apply it to the polynomials: The computation of the automorphism is simply to modify the coefficients by substitutions that represent the map. Elsewhere in the appendix, we shall see how to do it.

B An example of molecule with the Galois group $C_2 \times C_2$

It is not difficult to find example of molecule with the Galois group other than D_4 . For example, the following structure is equipped with $C_2 \times C_2$.

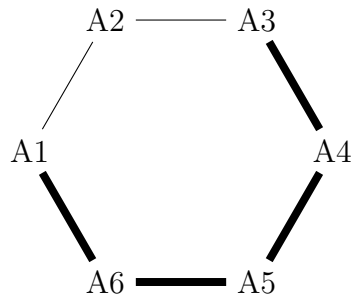


Figure B.1: A model molecule. The hopping integrals H_{ij} are set to be -2 on the bonds denoted by broad edges; and $H_{ij} = -1$ on others.

The primary ideal decomposition for the secular equation is given below.

```
P1=
(e^4-14*e^2+16,
 264*y(6)^2-5*e^2+2,
 4*y(5)-y(6)*e^3+14*y(6)*e,
 y(4)-y(6),
 4*y(3)+y(6)*e^3-12*y(6)*e,
 2*y(2)-y(6)*e^2+12*y(6),
 4*y(1)+y(6)*e^3-12*y(6)*e )
dim(P1)=0
```

```
P2=
( e+2,
 2*y(6)-1,
 y(5),
 2*y(4)+1,
 2*y(3)+1,
 y(2),
 2*y(1)-1 )
dim(P2)=0
```

```
P3=
( e-2,
```



```

2*y(6)+1,
y(5),
2*y(4)-1,
2*y(3)+1,
y(2),
2*y(1)-1 )
dim(P3)=0

```

The determinant of $H - eI$ is given by

$$(e^4 - 14 * e^2 + 16)(e + 2)(e - 2)$$

The Galois group of the first component of the factorization of the determinant,

$$f = e^4 - 14 * e^2 + 16,$$

is $C_2 \times C_2$. The polynomial has four roots:

$$\begin{aligned}
 e_1 &= \frac{\sqrt{6} + \sqrt{22}}{2} \\
 e_2 &= \frac{-\sqrt{6} + \sqrt{22}}{2} \\
 e_3 &= \frac{\sqrt{6} - \sqrt{22}}{2} \\
 e_4 &= \frac{-\sqrt{6} - \sqrt{22}}{2}
 \end{aligned}$$

By adding one of the roots of this polynomial to \mathbb{Q} , we can make the Galois extension. The correspondence between subfields and the subgroups is given in Table B.1, and the factorization of the polynomial is given in Table B.2. The subgroups are defined by the permutation of four roots of the polynomial, which are given in the last row of Table refC2C2GALOISFACTOR.

The automorphism in the splitting field is given by these four maps, by means of the primitive element y , such that $f(y)=0$. The maps are listed in the box brackets on the right-hand side.

$y \rightarrow [-y, y, -1/4*y^3 + 7/2*y, 1/4*y^3 - 7/2*y]$

	Defining Polynomial	Field	Subgroup
No.1	—	\mathbb{Q}	Group((1, 2)(3, 4), (1, 3)(2, 4))
No.2	$x^2 - 22$	$\mathbb{Q}(\sqrt{22})$	Group((1, 2)(3, 4))
No.3	$x^2 - 6$	$\mathbb{Q}(\sqrt{6})$	Group((1, 4)(2, 3))
No.4	$x^2 - 28x + 64$	$\mathbb{Q}(\sqrt{33})$	Group((1, 2)(3, 4))
No.5	$x^4 - 14x^2 + 16$	$\mathbb{Q}(\sqrt{6}, \sqrt{22})$	Group(())

Table B.1: The Galois extension for $x^4 - 14x^2 + 16$ and the corresponding subgroups.

No.1	$x^4 - 14 * x^2 + 16$
No.2	$x^2 - y_2 * x + 4$ $x^2 + y_2 * x + 4$
No.3	$x^2 - y_3 * x - 4$ $x^2 + y_3 * x - 4$
No.4	$x^2 - 1/2 * y_4$ $x^2 + (1/2 * y_4 - 14)$
No.5	$x - y_5$ $x + (1/4 * y_5^3 - 7/2 * y_5)$ $x + (-1/4 * y_5^3 + 7/2 * y_5)$ $x + y_5$

Table B.2: The factorization of $x^4 - 14 * x^2 + 16$.

C An example of molecule with the Galois group S_3

The following structure is equipped with the Galois group S_3 .

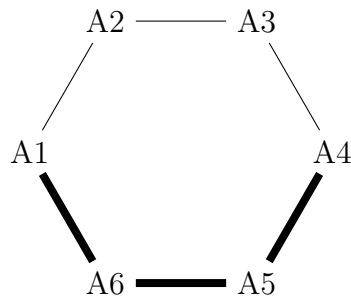


Figure C.1: A model molecule. The hopping integrals H_{ij} are set to be -2 on the bonds denoted by broad edges; and $H_{ij} = -1$ on others.

The primary ideal decomposition of the secular equation is given below.

$$\begin{aligned}
 P1 = & (e^3 + 3 * e^2 - 3 * e - 6, \\
 & 186 * y(6)^2 - 5 * e^2 - e - 7, \\
 & y(5) - y(6), \\
 & 2 * y(4) + y(6) * e + 2 * y(6), \\
 & 2 * y(3) - y(6) * e^2 - 2 * y(6) * e + 4 * y(6), \\
 & 2 * y(2) - y(6) * e^2 - 2 * y(6) * e + 4 * y(6), \\
 & 2 * y(1) + y(6) * e + 2 * y(6))
 \end{aligned}$$

$\dim(P1)=0$

$P2=(e^3-3*e^2-3*e+6,$
 $186*y(6)^2-5*e^2+e-7,$
 $y(5)+y(6),$
 $2*y(4)-y(6)*e+2*y(6),$
 $2*y(3)+y(6)*e^2-2*y(6)*e-4*y(6),$
 $2*y(2)-y(6)*e^2+2*y(6)*e+4*y(6),$
 $2*y(1)+y(6)*e-2*y(6))$
 $\dim(P2)=0$

The determinant of $H - eI$ is given by

$$(e^3 - 3 * e^2 - 3 * e + 6)(e^3 + 3 * e^2 - 3 * e - 6)$$

The Galois group of two components of the factorized determinant is S_4 . Choose the one:

$$f = (e^3 - 3 * e^2 - 3 * e + 6)$$

(The study of another branch in the determinant is the imitation of the following, only with the replacement $e \rightarrow -e$.) To factorize f , we have to use the splitting field defined by

$$K = x^6 - 36 * x^4 + 324 * x^2 - 837.$$

The latter polynomial is factorized as follows.

$$\begin{aligned} K &= (x + y)(x - y) \\ &\times (x + (-1/6 * y^4 + 5 * y^2 - 1/2 * y - 24)) \\ &\times (x + (-1/6 * y^4 + 5 * y^2 + 1/2 * y - 24)) \\ &\times (x + (1/6 * y^4 - 5 * y^2 - 1/2 * y + 24)) \\ &\times (x + (1/6 * y^4 - 5 * y^2 + 1/2 * y + 24)), \end{aligned}$$

provided that y is one of the roots of K . (The other roots are represented by y .) By adding one the roots of this polynomial, e.g., y to \mathbb{Q} , we can make the Galois extension for the factorization of f . The correspondence between subfields and the subgroups is given in Table C.1, and the factorization of the polynomial is given in Table C.2. The subgroups are defined by the permutation of six roots of the polynomial K .

The automorphism in the splitting field is given by these six maps, by means of the primitive element y , such that $K(y)=0$. The maps are listed in the box brackets in the right hand side.

$y \rightarrow [-y, y,$
 $-1/6*y^4 + 5*y^2 - 1/2*y - 24,$
 $-1/6*y^4 + 5*y^2 + 1/2*y - 24,$
 $1/6*y^4 - 5*y^2 - 1/2*y + 24,$
 $1/6*y^4 - 5*y^2 + 1/2*y + 24]$

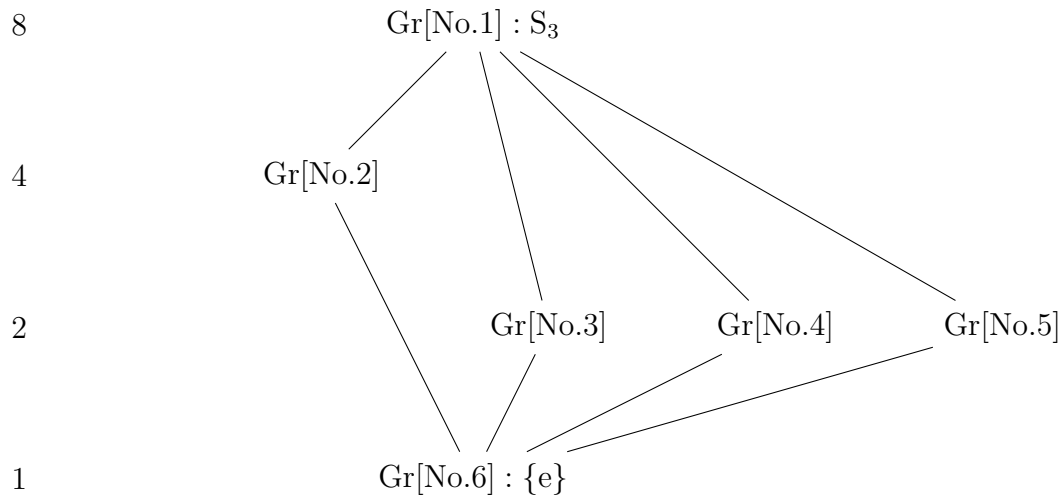


Figure C.2: The graphical representation of the subgroup lattice for S_3 ; Each node shows the subgroups; The inclusion relations as subgroups are denoted by edges. The column of the numbers in the left side of the graph are the orders of the subgroups.

	Defining Polynomial	Field	Subgroup
No.1	—	\mathbb{Q}	Group((1, 2, 4)(3, 5, 6), (1, 3)(2, 6)(4, 5))
No.2	$x^2 - 7533$		Group((1, 2, 4)(3, 5, 6))
No.3	$y^3 - 54 * y - 27$		Group((1, 3)(2, 6)(4, 5))
No.4	$y^3 - 72 * y^2 + 1296 * y - 6696$		Group((1, 6)(2, 5)(3, 4))
No.5	$y^3 - 54 * y + 27$		Group((1, 5)(2, 3)(4, 6))
No.6	$y^6 - 36 * y^4 + 324 * y^2 - 837$		Group(())

Table C.1: The Galois extension for $f = e^3 - 3 * e^2 - 3 * e + 6$ and the corresponding subgroups.

No.1	$x^3 - 3 * x^2 - 3 * x + 6$
No.2	$x^3 - 3 * x^2 - 3 * x + 6$
No.3	$x + (1/3 * y_3 - 1)$ $x^2 + (-1/3 * y_3 - 2) * x + (1/9 * y_3^2 + 1/3 * y_3 - 5)$
No.4	$x + (1/36 * y_4^2 - 5/3 * y_4 + 15)$ $x^2 + (-1/36 * y_4^2 + 5/3 * y_4 - 18) * x + (1/36 * y_4^2 - 11/6 * y_4 + 19)$
No.5	$x + (-1/3 * y_5 - 1)$ $x^2 + (1/3 * y_5 - 2) * x + (1/9 * y_5^2 - 1/3 * y_5 - 5)$
No.6	$x + (-1/18 * y_6^4 + 5/3 * y_6^2 - 1/2 * y_6 - 9)$ $x + (-1/18 * y_6^4 + 5/3 * y_6^2 + 1/2 * y_6 - 9)$ $x + (1/9 * y_6^4 - 10/3 * y_6^2 + 15)$

Table C.2: The factorization of $x^4 - 14 * x^2 + 16$

D Another example of molecule with D_4 Galois group

It is not difficult to find example of molecule with D_4 Galois group. For example, there is another of this.

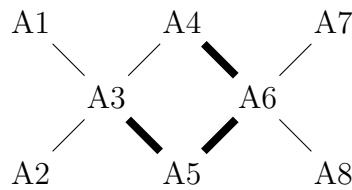


Figure D.1: A model molecule. The hopping integrals H_{ij} are set to be -2 on the bonds denoted by broad edges; and $H_{ij} = -1$ on others.

The determinant of $H - eI$ is given by

$$e^5 - 17 * e^3 + 34 * e$$

The primary ideal decomposition of the secular equation is composed of two components, the energy spectra of which are given by

$$e = 0,$$

and

$$e^4 - 17 * e^2 + 34 = 0,$$

respectively. The Galois group of the latter equation is D_4 . The splitting field is the extension of \mathbb{Q} by a root of

$$K = x^8 + 170 * x^6 + 9061 * x^4 + 156060 * x^2 + 93636 = 0.$$

A similar analysis, as is conducted in the main part of the article, can be done for this spectrum-ideal.

The automorphism in the splitting field is given by eight polynomials, represented by the primitive element y , such that $K(y)=0$. These maps are listed below in the box brackets in the right hand side.

```

y->[-y,
    y,
    -35/172584*y^7 + 2525/86292*y^5 - 11905/10152*y^3 + 6973/564*y,
    -7/43146*y^7 + 505/21573*y^5 - 2381/2538*y^3 + 1310/141*y,
    -7/57528*y^7 + 505/28764*y^5 - 2381/3384*y^3 + 1545/188*y,
    7/57528*y^7 - 505/28764*y^5 + 2381/3384*y^3 - 1545/188*y,
    7/43146*y^7 - 505/21573*y^5 + 2381/2538*y^3 - 1310/141*y,
    35/172584*y^7 - 2525/86292*y^5 + 11905/10152*y^3 - 6973/564*y]

```

E Tools of molecular orbital computation

To do the computation concerning algebraic geometry by Singular, the authors used the program provided below.

```

// You should save this part in a file, say, "mol.txt".
// In order to load and execute that file,
// Give the command (terminated by a semi-colon)
//    <"mol.txt";
// to the command prompt of Singular.
LIB "primdec.lib";
option(redSB);
proc molsolver()
{
// At first we define the ring in which we work.
    int n=12;
    ring r=0,(y(1..n),e),lp;
//
// The topology of the molecule is this.
//      9      10
//    1      4      7
//      3      6
//    2      5      8
//      11     12
// We make the link of atoms by means of the matrix v[12][2]:
    matrix v[12][2]=1,3,2,3,3,4,3,5,4,6,5,6,
                    6,7,6,8,9,4,10,4,11,5,12,5;
// The defined matrix should be read to be the set of juxtaposed rows,
// which goes as [[1,3],[2,3],[3,4],...[12,5]]
// where each row indicates the linked atom pairs.
//
// p[n][1] is the matrix which holds the wave-function [y(1)...y(12)]
// H[n][n] is the matrix representation of the Hamiltonian.
// The indeterminate e is the energy.

```

```

//
// We conduct the experiment in Q [The field of rational numbers].
//
// You can modify the setting according to your plan!
//
matrix p[n][1];
matrix HH[n][n];
int i,i1,i2;
for (i=1; i<=n;i++)
{
    p[i,1]=y(i);
}
print(v);
int k1,k2;
// Set value to the Hamiltonian on each link.
for (i=1;i<=12;i++)
{
    k1=int(v[i,1]);
    k2=int(v[i,2]);
    HH[k1,k2]=-1;
    HH[k2,k1]=-1;
}
// Set special values for chosen links.
for (i=4;i<=6;i++)
{
    k1=int(v[i,1]);
    k2=int(v[i,2]);
    HH[k1,k2]=-2;
    HH[k2,k1]=-2;
}
// The identity matrix MI: for the convenience of computation.
matrix MI[n][n];
for(i=1;i<=12;i++){ MI[i,i]=1;}
print(HH);
// Determinant.
print(det(HH-e*MI));
// The definition of ideal:
// The secular equation (HH-e)*y=0,
// and
// The normalization condition (y,y)=1.
ideal J=HH*p-e*p,transpose(p)*p-1;
print("Defining Ideal");
print(J);

```

```

        print("Standard Bases");
        std(J);
// Observe this:
// the first entry of the standard bases is
// the polynomial equation for the energy e.
// Now we apply primary ideal decomposition to the ideal.
// We shall have the list indexed by [1],[2],[3].
// Each entry of the list contains two sub-items.
// [1]: the primary ideal and
// [2]: the corresponding prime ideal.
        list A=primdecGTZ(J);
        print("Primary Ideal Decomposition");
        print(A);
// We check the Krull dimension of the decomposed components,
// after formatting them into standard bases.
// Krull-dimension might not be zero, owing to the degeneracy.
        ideal ps;
        for(int s=1;s<=size(A);s++)
        {
            ps=A[s][2];
            printf("Decomposed component:");
            print(std(ps));
            printf("Compute Krull dimension:");
            print(dim(std(ps)));
        }
        return(0);
    }
}
molsolver()
quit;

```

To do the computation concerning algebraic number theory PARI/GP, the authors used the program provided below.

```

/* THIS IS A PROGRAM OF PARI/GP COMPUTATION */
/* Logfile preparation*/
default(logfile,"c:/Users/Public/Downloads/parilog.txt")
default(log,3)

print("Define the polynomial f")
/* f=x+3*x^3-6*x^2-6*x+4*/
f=Pol([1,3,-6,-6,4])

/*
Compute the splitting field and get the defining polynomial K.

```



```

*/
K=nfsplitting(f)

/* Make the Galois extension.*/
gal=galoisinit(K)

/* Get the subgroups of the Galois group. */
subs=galoissubgroups(gal)

/*
Compute properties of the subgroups.
The computations are done for the indexed subgroups: subs[i].
The results are stored in the vectors.
*/

/* Get the fixed field by the subgroups.
The following is the list of the defining polynomials.
*/
v=vector(#subs,i,galoisfixedfield(gal,subs[i],2))
print(v)

/* Represent the subgroups by means of permutations. */
v2=vector(#subs,i,galoisexport(subs[i]))

/* Identify them with the permutations. */
v3=vector(#subs,i,galoisidentify(subs[i]))

/*
Example:
We have already done the factorization of
the defining polynomial K.
v[10] is the list of information on the splitting field.
*/
print(v[10][3])

/*
Example:
The permutation representation of the fifth subgroup.
*/
print(v2[5])

/* Hereupon let us Work in the splitting field.*/
nf=nfinit(subst(K,x,y))

```

```

/* Get the subfields. */
nfs=nfsubfields(subst(K,x,y))

/*Factorization of f in the subfields*/
v4=vector(#subs,i, nffactor(nfs[i][1],f))
/*Rearrange the result.*/
v5=vector(#v4,i,v4[i][,1])

/* Get automorphism on the splitting field. */
autos=nfgaloisconj(nf)

/* Compute the composition of the automorphisms. */
vij=vector(#autos,i, vector(#autos,j,nfgaloisapply(nf,autos[i],autos[j])))

/* Compute the basis of the splitting field K. */
nfbasis(K)

/* Give the automorphism with respect to the basis. */
w=vector(#autos,i,nfalgtobasis(nf,autos[i]))

/*
Let us check the automorphism upon factorized polynomials,
say, v5[10][1..4].
*/
for(i=1,4,print(v5[10][i]))
print(v5[10][1])
/* What is 'lift'? */
print(lift(v5[10][1]))
vector(#autos,i,subst(lift(v5[10][1]),y,autos[i])*Mod(1,nf.pol));
print(%)

/*
The conjugation in v5[5] :
the factorized polynomials in the fifth subfield.
*/
print(v5[5][1])
print(v5[5][2])

/*
The list of subfields, computed in another way.
*/
nfsfield=vector(#nfs, i,nfinit(nfs[i][1]))

```

```

/* Define the automorphism in the fifth subfield */
autos5=nfgaloisconj(nfsfield[5])

/* Compare the <subfields> and the <fixed fields>,
   computed just now and previously.
   Are they sorted in the same order? */
print(nfs[1][1]);print(v[1][1])
print(nfs[2][1]);print(v[2][1])
print(nfs[3][1]);print(v[3][1])
print(nfs[4][1]);print(v[4][1])
print(nfs[5][1]);print(v[5][1])
print(nfs[6][1]);print(v[6][1])
print(nfs[7][1]);print(v[7][1])
print(nfs[8][1]);print(v[8][1])
print(nfs[9][1]);print(v[9][1])
print(nfs[10][1]);print(v[10][1])

/*
It is a quite natural question:
How are the roots of the irreducible factors in the subfield?
OR,
How are the four roots of the polynomial 'f' situated in the irreducible factors?

The check requires a little algebra, described below.

Let us pick up two fields:
    v[3] and the splitting field v[10].

Let Z and W be the irreducible components
after the factorization of 'f' in these two fields.

*/

nums=3;
Z=nffactor(nfinit(v[nums][1]),f);
W=nffactor(nfinit(v[10][1]),f);
Z=Z[,1];
W=W[,1];

/*
How is the third subfield?

```

```

*/
print(v[nums][2]);

/*
The second component of the output v[3] is
the root <ym> of the defining polynomial of v[3],
represented by the root <y> of the polynomial 'K'.
*/
ym=subst(lift(v[nums][2]),x,y);

/*
By substitution, we get the representations of
the irreducible factors in the subfield v[3] by <y>
which could be factorized in the splitting field Q(y).
*/

ZR=vector(#Z,i, subst(lift(Z[i]),y,ym)*Mod(1,subst(K,x,y)));

/*
The function given below does the factorization in Q(y) explained above
and gives back the corresponding sequential numbers
as the roots of <K> stored in the set 'W'.
*/

procfactorization()={
for(i=1,#ZR,nfs=nfinit(subst(K,x,y));
FZR=nfactor(nfs,ZR[i]);print(FZR);
FZR=FZR[,1];
WIND=vector(#FZR,j,setsearch(Set(W),FZR[j]));
print(WIND);
}

```

F Decomposition of an ideal in the extension field of \mathbb{Q} , using SINGULAR

In SINGULAR, one can extend the coefficient field of the ring; then one can decompose some ideal in this extended ring. The following is an example of the computation. We study the prime ideal in $\mathbb{Q}[y(1), \dots, y(12), e]$, which is the result of the primary ideal decomposition of the secular equation for the model molecule with the Galois group D_4 . We change the coefficient field from \mathbb{Q} to the splitting field of $a^8 - 46 * a^6 + 461 * a^4 - 1360 * a^2 + 1156$, namely, $\mathbb{Q}(a)$, where the primary ideal decomposition can be done

further.

```
LIB "primdec.lib";
int n=12;
ring r=(0,a),(y(1..n),e),lp; minpoly=a^8 - 46*a^6 + 461*a^4 - 1360*a^2 + 1156;
ideal J=e^4+3*e^3-6*e^2-6*e+4,
5848*y(12)^2+54*e^3+209*e^2-205*e-766,
y(11)-y(12),
4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(9)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
y(8)-y(12),
y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12);
primdecGTZ(std(J));
```

We obtain four prime ideals ($P[1], P[2], P[3], P[4]$) in the extended ring; their generators are presented below. Observe that only the linear polynomials constitute the ideal; if one solve these linear polynomials from the top to the bottom one by one, one can get the solutions. (One determines e , then $y(12)$, then $y(11), \dots$, finally $y(1)$.)

```
P[1]:
_[1]=1632*e+(21*a^7-5*a^6-915*a^5+247*a^4
+7488*a^3-2900*a^2-11220*a+8092)
_[2]=561408*y(12)^2+(41*a^7+53*a^6-1867*a^5
-2167*a^4+17708*a^3+12692*a^2-31708*a-35020)
_[3]=y(11)-y(12)
_[4]=1088*y(10)+
(-7*a^7+305*a^5-2496*a^3+4012*a+272)*y(12)
_[5]=y(9)-y(10)
_[6]=y(8)-y(12)
_[7]=y(7)-y(12)
_[8]=1632*y(6)+(-21*a^7+5*a^6+915*a^5-247*a^4
-7488*a^3+2900*a^2+11220*a-8092)*y(12)
_[9]=y(5)-y(6)
_[10]=3264*y(4)+(-21*a^7+5*a^6+915*a^5-247*a^4
-7488*a^3+2900*a^2+11220*a-4828)*y(6)+3264*y(12)
_[11]=y(3)-y(4)
_[12]=y(2)-y(9)
_[13]=y(1)-y(2)
```

P[2]:

```

_[1]=1632*e+(5*a^6-247*a^4+2900*a^2-816*a-5644)
_[2]=58480*y(12)^2+(5006*a+1802)*e
      +(-81*a^5-47*a^4+3105*a^3-623*a^2-8568*a-9894)
_[3]=y(11)-y(12)
_[4]=1088*y(10)
      +(-7*a^7+305*a^5-2496*a^3+4012*a+272)*y(12)
_[5]=y(9)-y(10)
_[6]=y(8)-y(12)
_[7]=y(7)-y(12)
_[8]=1632*y(6)
      +(-5*a^6+247*a^4-2900*a^2+816*a+5644)*y(12)
_[9]=y(5)-y(6)
_[10]=3264*y(4)
      +(-5*a^6+247*a^4-2900*a^2+816*a+8908)*y(6)
      +3264*y(12)
_[11]=y(3)-y(4)
_[12]=y(2)-y(9)
_[13]=y(1)-y(2)

```

P[3]:

```

_[1]=1632*e
      +(-21*a^7-5*a^6+915*a^5+247*a^4-7488*a^3-2900*a^2+11220*a+8092)
_[2]=561408*y(12)^2+
      (-41*a^7+53*a^6+1867*a^5-2167*a^4-17708*a^3+12692*a^2+31708*a-35020)
_[3]=y(11)-y(12)
_[4]=1088*y(10)
      +(7*a^7-305*a^5+2496*a^3-4012*a+272)*y(12)
_[5]=y(9)-y(10)
_[6]=y(8)-y(12)
_[7]=y(7)-y(12)
_[8]=1632*y(6)
      +(21*a^7+5*a^6-915*a^5-247*a^4+7488*a^3+2900*a^2-11220*a-8092)*y(12)
_[9]=y(5)-y(6)
_[10]=3264*y(4)
      +(21*a^7+5*a^6-915*a^5-247*a^4+7488*a^3
      +2900*a^2-11220*a-4828)*y(6)
      +3264*y(12)
_[11]=y(3)-y(4)
_[12]=y(2)-y(9)
_[13]=y(1)-y(2)

```

```

P[4]:
_[1]=1632*e+(5*a^6-247*a^4+2900*a^2+816*a-5644)
_[2]=58480*y(12)^2+(-5006*a+1802)*e
      +(81*a^5-47*a^4-3105*a^3-623*a^2+8568*a-9894)
_[3]=y(11)-y(12)
_[4]=1088*y(10)
      +(7*a^7-305*a^5+2496*a^3-4012*a+272)*y(12)
_[5]=y(9)-y(10)
_[6]=y(8)-y(12)
_[7]=y(7)-y(12)
_[8]=1632*y(6)
      +(-5*a^6+247*a^4-2900*a^2-816*a+5644)*y(12)
_[9]=y(5)-y(6)
_[10]=3264*y(4)
      +(-5*a^6+247*a^4-2900*a^2-816*a+8908)*y(6)
      +3264*y(12)
_[11]=y(3)-y(4)
_[12]=y(2)-y(9)
_[13]=y(1)-y(2)

```

Using another library, one can try the factorization of polynomials. Try the following.

```

LIB "primdec.lib";
LIB "primitiv.lib";
int n=12;
ring r=(0,a),(y(1..n),e),lp;
ring r1=splitring(e^4+3*e^3-6*e^2-6*e+4);
setring r1;
ideal J=e^4+3*e^3-6*e^2-6*e+4,
5848*y(12)^2+54*e^3+209*e^2-205*e-766,
y(11)-y(12),
4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(9)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
y(8)-y(12),
y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12);
primdecGTZ(std(J));
minpoly;

```

You shall observe the factorization is imperfect; indeed there is one component in which the polynomial of the variable e is still quadratic.

```

_[1]=y(11)-y(12)
_[2]=4*y(10)+(-a^3-3*a^2+4*a+4)*y(12)
_[3]=4*y(9)+(-a^3-3*a^2+4*a+4)*y(12)
_[4]=y(8)-y(12)
_[5]=y(7)-y(12)
_[6]=y(5)-y(6)
_[7]=4*y(4)+(-a^3-3*a^2+4*a+4)*y(6)
_[8]=4*y(3)+(-a^3-3*a^2+4*a+4)*y(6)
_[9]=4*y(2)+(-a^3-3*a^2+4*a+4)*y(12)
_[10]=4*y(1)+(-a^3-3*a^2+4*a+4)*y(12)
_[11]=2*e^2+(a^3+3*a^2-4*a)*e-4
_[12]=y(6)+y(12)*e
_[13]=2*y(6)*e+(a^3+3*a^2-4*a)*y(6)+4*y(12)
_[14]=11696*y(12)^2+(-47*a^3-141*a^2+188*a+22)*e+(-108*a^3-324*a^2+432*a-696)
_[15]=5848*y(6)*y(12)+(-11*a^3-33*a^2+44*a+254)*e+(47*a^3+141*a^2-188*a-22)
_[16]=5848*y(6)^2+(47*a^3+141*a^2-188*a-22)*e+(22*a^3+66*a^2-88*a-508)

```

It is on account of the defining polynomial of the splitting ring, which is $e^4 + 3e^3 - 6e^2 - 6e + 4$; you shall check it by the command “minpoly”.

In addition, try the following.

```

LIB "primdec.lib";
LIB "primitiv.lib";
int n=12;
ring r=(0,a),(y(1..n),e),lp;
ideal J=e^4+3*e^3-6*e^2-6*e+4,
5848*y(12)^2+54*e^3+209*e^2-205*e-766,
y(11)-y(12),
4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(9)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
y(8)-y(12),
y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12);
primitive(J);

```

As the result of the last command, you shall get a list composed of 14 elements. The first entry is the defining polynomial of the primitive element α , so that we shall have

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\hat{y}(1), \hat{y}(2), \dots, \hat{y}(12), \hat{e}),$$

where we denote the coordinates of the isolated points of $V(J)$ [the solutions to $J = 0$] by $(\hat{y}(1), \hat{y}(2), \dots, \hat{y}(12), \hat{e})$. The entries from the second to the fourteenth shows the polynomial representations of $(y(1), \dots, y(12), e)$ by means of α . The defining polynomial of α is determined by a probabilistic method so that the result would vary in each run.

G Computation of automorphism

If one would like to ascertain the action of the automorphism on the polynomial f (that initially given) and K (that defines the splitting field), try the computation presented below. The procedure presented here computes the automorphism on the polynomials through the substitutions to the coefficients and gives back the corresponding matrix representations of the permutations. Indeed, the validation is necessary, and it is because of these reasons: the computation of PARI/GP returns the Galois group as the permutations of the roots of the defining polynomial of the splitting field; However, there is no guarantee that the result of the factorization shall arrange the factored linear polynomials in the same ordering of the roots on which the Galois group is constituted.

```
/* Define the polynomial f. */
f=Pol([1,3,-6,-6,4])
/* Compute the splitting field and get the defining polynomial K.*/
K=nfsplitting(f)
/* Make Galis extension. */
gal=galoisinit(subst(K,x,y));

/*Automorphism. */
nf=nfinit(subst(K,x,y));
autos=nfgaloisconj(nf);

/* Factorization of f. */
factoredf=nffactor(nf,f)[,1];

/* Factorization of K. */
factoredK=nffactor(nf,K)[,1];

/* Define a function which apply l-th automorphism to the factors. */
procautocal(factors,autos,l)=
{
ev=vector(#factors,i,lift(factors[i]-x));
for(j=1,#ev,opr=(Mod(subst(ev[j],y,autos[l]),subst(K,x,y))));
print(vector(#ev,i,opr==ev[i])););
}

/* Apply the automorphism to the factors of f. */
```

```

for(l=1,8,print("auto",l);procautocal(factoredf,autos,l));

/* Apply the automorphism to the factors of K. */
for(l=1,8,print("auto",l);procautocal(factoredK,autos,l));

/* Check the invariance of the subfields. */
/* Get the subfields*/
subfs=galoissubfields(gal);

watchinvariance(subf,autos,l)=
{
/* Watch the invariance of the defining element of the subfield,
when l-th automorphism is applied.
Query: let subfield := Q(z). Then Auto(z)==z? */
definingy=lift(subf[2]);
dest=subst(definingy,y,autos[l])*Mod(1,gal.pol);
/* If invariant, return 1; else return 0*/
return (dest==subf[2]);
}
for(k=1,#subf,print("subfield",k);
print(vector(#autos,l,watchinvariance(subf[k],autos,l))));

```

The computation shall return these results. (In some places, for clarity, several comments are inserted, although the program does not issue them.)

```

aut1 !(1,2)(3,8)(4,6)(5,7)
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1]
[0, 0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0]
aut2 !()
[1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 1, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1]
aut3 !(1,8)(2,3)(4,5)(6,7)

```

```

[0, 0, 0, 0, 0, 0, 0, 0, 1]
[0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0]
aut4 !(1,7)(2,4)(3,5)(6,8)
[0, 0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1]
[1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0]
aut5 !(1,6)(2,5)(3,4)(7,8)
[0, 0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1]
[0, 0, 0, 0, 0, 0, 0, 1, 0]
aut6 !(1,5,8,4)(2,6,3,7)
[0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 0]
[1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1]
[0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0]
aut7 !(1,4,8,5)(2,7,3,6)
[0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1]
[1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0]

```

```

[0, 0, 0, 0, 1, 0, 0, 0]
aut8 !(1,3)(2,8)(4,7)(5,6)
[0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1]
[1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0]
aut1 !(1,2)(3,4)
[0, 1, 0, 0]
[1, 0, 0, 0]
[0, 0, 0, 1]
[0, 0, 1, 0]
aut2 !()
[1, 0, 0, 0]
[0, 1, 0, 0]
[0, 0, 1, 0]
[0, 0, 0, 1]
aut3 !(1,4)(2,3)
[0, 0, 0, 1]
[0, 0, 1, 0]
[0, 1, 0, 0]
[1, 0, 0, 0]
aut4 !(2,3)
[1, 0, 0, 0]
[0, 0, 1, 0]
[0, 1, 0, 0]
[0, 0, 0, 1]
aut5 !(1,4)
[0, 0, 0, 1]
[0, 1, 0, 0]
[0, 0, 1, 0]
[1, 0, 0, 0]
aut6 !(1,2,4,3)
[0, 1, 0, 0]
[0, 0, 0, 1]
[1, 0, 0, 0]
[0, 0, 1, 0]
aut7 !(1,3,4,2)
[0, 0, 1, 0]
[1, 0, 0, 0]

```

```
[0, 0, 0, 1]
[0, 1, 0, 0]
aut8 !(1,3)(2,4)
[0, 0, 1, 0]
[0, 0, 0, 1]
[1, 0, 0, 0]
[0, 1, 0, 0]
```

```
subfield 1 !Invariant by all automorphisms.
[1, 1, 1, 1, 1, 1, 1, 1]
subfield 2 !Invariant by the automorphisms No.2,3,6,7.
[0, 1, 1, 0, 0, 1, 1, 0]
subfield 3 !Invariant by the automorphisms No.2,3,4,5.
[0, 1, 1, 1, 1, 0, 0, 0]
subfield 4 !Invariant by the automorphisms No.1,2,3,8.
[1, 1, 1, 0, 0, 0, 0, 1]
subfield 5 !Invariant by the automorphisms No.2,3
[0, 1, 1, 0, 0, 0, 0, 0]
subfield 6 !Invariant by the automorphisms No.2,4.
[0, 1, 0, 1, 0, 0, 0, 0]
subfield 7 !Invariant by the automorphisms No.2,5.
[0, 1, 0, 0, 1, 0, 0, 0]
subfield 8 !Invariant by the automorphisms No.1,2.
[1, 1, 0, 0, 0, 0, 0, 0]
subfield 9 !Invariant by the automorphisms No.2,8.
[0, 1, 0, 0, 0, 0, 0, 1]
subfield 10 !Invariant by the automorphism No.2.
[0, 1, 0, 0, 0, 0, 0, 0]
```

Hence we get two groups (GK, Gf) which are generated by the permutations of the roots of K and f. These two groups belong to D_4 .

```
GK:=Group((1,2)(3,8)(4,6)(5,7),(),
(1,8)(2,3)(4,5)(6,7),
(1,7)(2,4)(3,5)(6,8),(1,6)(2,5)(3,4)(7,8),
(1,5,8,4)(2,6,3,7),(1,4,8,5)(2,7,3,6),
(1,3)(2,8)(4,7)(5,6));
```

```
Gf:=Group((1,2)(3,4),(),(1,4)(2,3),(2,3),(1,4),
(1,2,4,3),(1,3,4,2),(1,3)(2,4));
```

Using the command of PARI/GP, one can know the correspondence between the permutation generator of the Galois group and the automorphism. To this end, try the following.

```
for(i=1,8, print(galoispermtpol(gal,gal.group[i]))
```

In the following, we give an example of computation to check the automorphism. We work in the subfield (No.5) in Section 3.2). The notations are as follows: `pol1` and `pol2` be the factors of f ; `polcoeff(pol1,1)` returns the coefficient of x^1 ; `Mod(A, B)` is the remainder of A with respect to the modulus B ; `lift(Mod(A, B))` gives back A ; `nfinit(pol)` is the initialization of a number field by a polynomial pol ; `nfgaloisconj(nfs)` returns the automorphisms of the field nfs ; the command `subst(REF,y,z)` is used to do the substitution of 'z' to the variable 'y' in some representation REF , etc... As the automorphism is given by a polynomial ($y \mapsto y^n + \dots$), the computation is simply done by the substitution in polynomials $p(y) \mapsto p(y^n + \dots)$. Employing computations of this sort, we know that some of the automorphism interchange `pol1` and `pol2`; and that others not. If we are dubious of the result, we should check the integrity of the algebra in that way.

```
gp> pol1=x^2 + Mod(-1/620*y^3 + 69/620*y^2 - 11/5*y + 1992/155,
y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x - 2
```

```
gp> pol2=x^2 + Mod(1/620*y^3 - 69/620*y^2 + 11/5*y - 1527/155,
y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x - 2
```

```
gp> pol1*pol2
```

```
Mod( 1, y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x^4
+ Mod( 3, y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x^3
+ Mod(-6, y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x^2
+ Mod(-6, y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)*x
+ Mod( 4, y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)
```

```
gp>polcoeff(pol1,1)
```

```
Mod(-1/620*y^3 + 69/620*y^2 - 11/5*y + 1992/155,
y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)
```

```
gp> lift(polcoeff(pol1,1))
```

```
-1/620*y^3 + 69/620*y^2 - 11/5*y + 1992/155
```

```
gp> defpol= y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904
```

```
gp> nfs5=nfinit(defpol);
```

```
gp> autos5=nfgaloisconj(nfs5,1)
```

```

[-y + 46, y, -1/155*y^3 + 69/155*y^2 - 39/5*y + 7038/155,
1/155*y^3 - 69/155*y^2 + 39/5*y + 92/155]~

gp > subst(lift(polcoeff(pol1,1)),y,autos5[2])

-1/620*y^3 + 69/620*y^2 - 11/5*y + 1992/155

gp> subst(lift(polcoeff(pol1,1)),y,autos5[3])

1/2308802500*y^9 - 207/2308802500*y^8 + 1791/230880250*y^7 -
419727/1154401250*y^6 + 5772753/577200625*y^5 -
94341492/577200625*y^4 + 3536326739/2308802500*y^3 -
17356359567/2308802500*y^2 + 300569217/18619375*y -
4955080773/577200625

gp> Mod(subst(lift(polcoeff(pol1,1)),y,autos5[3]),nfs5.pol)

Mod(1/620*y^3 - 69/620*y^2 + 11/5*y - 1527/155,
y^4 - 92*y^3 + 2796*y^2 - 31280*y + 103904)

gp> lift(polcoeff(pol2,1))

1/620*y^3 - 69/620*y^2 + 11/5*y - 1527/155

```

H Validation of Frobenius map

```

/*
Let us check the validity of the Frobenius map,
computed by PARI/GP.
The check is done only 'element by element'.
*/
f=Pol([1,0,-14,0,16])
nf=nfinit(f)
gal=galoisinit(nf)

/*
Factorize p=89.
*/
p=89
/*
Take one prime ideal 'pr', lying over p.
We get the Frobenius map frob:=(p, L/K).
*/

```

```

pr=idealprimedec(nf,p)[1]
g=idealfrobenius(nf,gal,pr)
frob=galoispermtpol(gal,g)

/*
In addition, we prepare Auto(L/K).
*/
autos=nfgaloisconj(nf)

/* We compute the Hermite normal form of pr.*/
A=ideálnormalform(nf,pr)

elm=x^5+x^2+1

/*
We compute the  $x^p - \text{Frob}(x)$  in L;
then get the Hermite normal form of this.
*/

B=nfalgtobasis(nf, lift(elm^p*Mod(1,gal.pol)-nfgaloisapply(nf,frob,elm)))

/*
Let us compute the ideal (pr) + ( $x^p - \text{Frob}(x)$ )
If ( $x^p - \text{Frob}(x)$ ) is included in (pr), the addition returns (pr)!
*/

A==idealadd(nf,A,B)

/*
For comparison, a similar check is done for the automorphisms (autos[i])
*/
BV=vector(#autos,i,
nfalgtobasis(nf, lift(elm^p*Mod(1,gal.pol)-nfgaloisapply(nf,autos[i],elm))))
vector(#BV,i,A==idealadd(nf,A,BV[i]))

```


I Decomposition of an ideal in the extension field of \mathbb{Q} , using SINGULAR

In SINGULAR, one can extend the coefficient field of the ring; then one can decompose some ideal in this extended ring. The following is an example of the computation. We study the prime ideal in $\mathbb{Q}[y(1), \dots, y(12), e]$, which is the result of the primary ideal decomposition of the secular equation for the model molecule with the Galois group D_4 . We change the coefficient field from \mathbb{Q} to the splitting field of $a^8 - 46 * a^6 + 461 * a^4 - 1360 * a^2 + 1156$, namely, $\mathbb{Q}(a)$, where the primary ideal decomposition can be done further.

```
LIB "primdec.lib";
int n=12;
ring r=(0,a),(y(1..n),e),lp; minpoly=a^8 - 46*a^6 + 461*a^4 - 1360*a^2 + 1156;
ideal J=e^4+3*e^3-6*e^2-6*e+4,
5848*y(12)^2+54*e^3+209*e^2-205*e-766,
y(11)-y(12),
4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(9)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
y(8)-y(12),
y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12);
primdecGTZ(std(J));
```

We obtain four prime ideals ($P[1], P[2], P[3], P[4]$) in the extended ring; their generators are presented below. Observe that only the linear polynomials constitute the ideal; if one solve these linear polynomials from the top to the bottom one by one, one can get the solutions. (One determines e , then $y(12)$, then $y(11), \dots$, finally $y(1)$.)

```
P[1]:
_[1]=1632*e+(21*a^7-5*a^6-915*a^5+247*a^4
+7488*a^3-2900*a^2-11220*a+8092)
_[2]=561408*y(12)^2+(41*a^7+53*a^6-1867*a^5
-2167*a^4+17708*a^3+12692*a^2-31708*a-35020)
_[3]=y(11)-y(12)
_[4]=1088*y(10)+
(-7*a^7+305*a^5-2496*a^3+4012*a+272)*y(12)
_[5]=y(9)-y(10)
```

```

_ [6]=y(8)-y(12)
_ [7]=y(7)-y(12)
_ [8]=1632*y(6)+(-21*a^7+5*a^6+915*a^5-247*a^4
      -7488*a^3+2900*a^2+11220*a-8092)*y(12)
_ [9]=y(5)-y(6)
_ [10]=3264*y(4)+(-21*a^7+5*a^6+915*a^5-247*a^4
      -7488*a^3+2900*a^2+11220*a-4828)*y(6)+3264*y(12)
_ [11]=y(3)-y(4)
_ [12]=y(2)-y(9)
_ [13]=y(1)-y(2)

```

P [2] :

```

_ [1]=1632*e+(5*a^6-247*a^4+2900*a^2-816*a-5644)
_ [2]=58480*y(12)^2+(5006*a+1802)*e
      +(-81*a^5-47*a^4+3105*a^3-623*a^2-8568*a-9894)
_ [3]=y(11)-y(12)
_ [4]=1088*y(10)
      +(-7*a^7+305*a^5-2496*a^3+4012*a+272)*y(12)
_ [5]=y(9)-y(10)
_ [6]=y(8)-y(12)
_ [7]=y(7)-y(12)
_ [8]=1632*y(6)
      +(-5*a^6+247*a^4-2900*a^2+816*a+5644)*y(12)
_ [9]=y(5)-y(6)
_ [10]=3264*y(4)
      +(-5*a^6+247*a^4-2900*a^2+816*a+8908)*y(6)
      +3264*y(12)
_ [11]=y(3)-y(4)
_ [12]=y(2)-y(9)
_ [13]=y(1)-y(2)

```

P [3] :

```

_ [1]=1632*e
      +(-21*a^7-5*a^6+915*a^5+247*a^4-7488*a^3-2900*a^2+11220*a+8092)
_ [2]=561408*y(12)^2+
      (-41*a^7+53*a^6+1867*a^5-2167*a^4-17708*a^3+12692*a^2+31708*a-35020)
_ [3]=y(11)-y(12)
_ [4]=1088*y(10)
      +(7*a^7-305*a^5+2496*a^3-4012*a+272)*y(12)
_ [5]=y(9)-y(10)
_ [6]=y(8)-y(12)
_ [7]=y(7)-y(12)
_ [8]=1632*y(6)

```

```

      +(21*a^7+5*a^6-915*a^5-247*a^4+7488*a^3+2900*a^2-11220*a-8092)*y(12)
_[9]=y(5)-y(6)
_[10]=3264*y(4)
      +(21*a^7+5*a^6-915*a^5-247*a^4+7488*a^3
      +2900*a^2-11220*a-4828)*y(6)
      +3264*y(12)
_[11]=y(3)-y(4)
_[12]=y(2)-y(9)
_[13]=y(1)-y(2)

P[4]:
_[1]=1632*e+(5*a^6-247*a^4+2900*a^2+816*a-5644)
_[2]=58480*y(12)^2+(-5006*a+1802)*e
      +(81*a^5-47*a^4-3105*a^3-623*a^2+8568*a-9894)
_[3]=y(11)-y(12)
_[4]=1088*y(10)
      +(7*a^7-305*a^5+2496*a^3-4012*a+272)*y(12)
_[5]=y(9)-y(10)
_[6]=y(8)-y(12)
_[7]=y(7)-y(12)
_[8]=1632*y(6)
      +(-5*a^6+247*a^4-2900*a^2-816*a+5644)*y(12)
_[9]=y(5)-y(6)
_[10]=3264*y(4)
      +(-5*a^6+247*a^4-2900*a^2-816*a+8908)*y(6)
      +3264*y(12)
_[11]=y(3)-y(4)
_[12]=y(2)-y(9)
_[13]=y(1)-y(2)

```

Using another library, one can try the factorization of polynomials. Try the following.

```

LIB "primdec.lib";
LIB "primitiv.lib";
int n=12;
ring r=(0,a),(y(1..n),e),lp;
ring r1=splitring(e^4+3*e^3-6*e^2-6*e+4);
setring r1;
ideal J=e^4+3*e^3-6*e^2-6*e+4,
5848*y(12)^2+54*e^3+209*e^2-205*e-766,
y(11)-y(12),
4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(9)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
y(8)-y(12),

```

```

y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12);
primdecGTZ(std(J));
minpoly;

```

You shall observe the factorization is imperfect; indeed there is one component in which the polynomial of the variable e is still quadratic.

```

_[1]=y(11)-y(12)
_[2]=4*y(10)+(-a^3-3*a^2+4*a+4)*y(12)
_[3]=4*y(9)+(-a^3-3*a^2+4*a+4)*y(12)
_[4]=y(8)-y(12)
_[5]=y(7)-y(12)
_[6]=y(5)-y(6)
_[7]=4*y(4)+(-a^3-3*a^2+4*a+4)*y(6)
_[8]=4*y(3)+(-a^3-3*a^2+4*a+4)*y(6)
_[9]=4*y(2)+(-a^3-3*a^2+4*a+4)*y(12)
_[10]=4*y(1)+(-a^3-3*a^2+4*a+4)*y(12)
_[11]=2*e^2+(a^3+3*a^2-4*a)*e-4
_[12]=y(6)+y(12)*e
_[13]=2*y(6)*e+(a^3+3*a^2-4*a)*y(6)+4*y(12)
_[14]=11696*y(12)^2+(-47*a^3-141*a^2+188*a+22)*e+(-108*a^3-324*a^2+432*a-696)
_[15]=5848*y(6)*y(12)+(-11*a^3-33*a^2+44*a+254)*e+(47*a^3+141*a^2-188*a-22)
_[16]=5848*y(6)^2+(47*a^3+141*a^2-188*a-22)*e+(22*a^3+66*a^2-88*a-508)

```

It is on account of the defining polynomial of the splitting ring, which is $e^4 + 3 * e^3 - 6 * e^2 - 6 * e + 4$; you shall check it by the command “minpoly”.

In addition, try the following.

```

LIB "primdec.lib";
LIB "primitiv.lib";
int n=12;
ring r=(0,a),(y(1..n),e),lp;
ideal J=e^4+3*e^3-6*e^2-6*e+4,
5848*y(12)^2+54*e^3+209*e^2-205*e-766,
y(11)-y(12),
4*y(10)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(9)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
y(8)-y(12),

```

```

y(7)-y(12),
y(6)+y(12)*e,
y(5)+y(12)*e,
2*y(4)-y(12)*e^2-2*y(12)*e+2*y(12),
2*y(3)-y(12)*e^2-2*y(12)*e+2*y(12),
4*y(2)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12),
4*y(1)+y(12)*e^3+3*y(12)*e^2-4*y(12)*e-2*y(12);
primitive(J);

```

As the result of the last command, you shall get a list composed of 14 elements. The first entry is the defining polynomial of the primitive element α , so that we shall have

$$\mathbb{Q}(\alpha) = \mathbb{Q}(\hat{y}(1), \hat{y}(2), \dots, \hat{y}(12), \hat{e}),$$

where we denote the coordinates of the isolated points of $V(J)$ [the solutions to $J = 0$] by $(\hat{y}(1), \hat{y}(2), \dots, \hat{y}(12), \hat{e})$. The entries from the second to the fourteenth shows the polynomial representations of $(y(1), \dots, y(12), e)$ by means of α . The defining polynomial of α is determined by a probabilistic method so that the result would vary in each run.

J Computations related to the reciprocal law in class field theory

```

/*
We can get in touch with a bit of class field theory.
*/

/* Define the polynomial f. */
f=Pol([1,0,-14,0,16])
/* Compute the splitting field and get the defining polynomial K.*/
K=nfsplitting(f) /*In this case, K=f.*/

/*
We have defined nf = Q(a), the splitting field.
which is the extension by the element 'a' such that f(a)=K(a)=0.
*/
nf=nfinit(K);
/* Make the Galois extension. */
gal=galoisinit(K);

setofprime=primes(10000)
for(i=1,10000,print(setofprime[i], " ", #idealprimedec(nf, setofprime[i])));

/*

```

Let us decompose a prime integer p (in \mathbb{Z}) in the extension field $\mathbb{Q}(a)$.
 One finds the set of primes in $\mathbb{Q}(a)$ lying over p , $(B_1 \dots B_n)$
 From each of them, one manages to make the so-called Frobenius map :

$\sigma(x) = (\text{equivalent}) = x^{\#N[p]} \bmod B[i]$, with $\#N[p] = p$.

This is an automorphism in $\mathbb{Q}(a)$.
 When the Galois group is abelian, it is independent of the choice of $B[i]$;
 hence one assumes the prime p is the label of this map.
 We denote it by $(p, \mathbb{Q}(a)/\mathbb{Q})$.

How this automorphism would be?

Let us compute the Frobenius map of primes and compare the cases,
 in which p might be decomposed into different numbers of prime ideals.

One find this:

if $\#B=4$ (i.e. when p splits completely),
 the automorphism is the identity $(x \rightarrow x)$;
 else, the automorphism might not the identity.

This is an outcome of the reciprocity law,
 which is the consequence of the class field theory.
 */

/*

The function below

(1) receives the prime k in \mathbb{Q} ,
 (2) computes the factorization of k
 in the extension field 'nf' of \mathbb{Q} ,
 (3) and gives back the Frobenius elements
 for the prime ideals lying over k .

Note that a Frobenius map $(p, \mathbb{Q}(x)/\mathbb{Q})$ is represented
 by a polynomial to which 'x' (the generating element of $\mathbb{Q}(x)$) is mapped.

*/

```
procmakefrobenius(k)=
{
  prs=idealprimedec(nf,k);
  return(vector(#prs,k, galoispermtopol(gal,idealfrobenius(nf,gal,prs[k]))));
}
```

/*

```

Let us conduct a numerical experiment.
We compute the Frobenius map from primes p in a certain range.
And we put the label on each prime p, using the reminders:
[p mod 3, p mod 11, p mod 11].
We collect the pairs of the label and the corresponding Frobenius map in a list.
Then we remove the duplication to extract the distinct classes.
*/

L=List();
for(i=10,10000,p=prime(i);v=[p%3,p%11,p%8,Set(procmakefrobenius(p))]);
print(v);listput(L,v));
A=Set(L);
#A      /* = 80, the size of the list containing distinct classes.*/
#[p|p<-A,p[4]==[x]]
      /* = 20, the size of the classes mapped to a Frobenius element. */
#[p|p<-A,p[4]==[-x]]      /* = 20 */
#[p|p<-A,p[4]==[ 1/4*x^3 - 7/2*x]] /* = 20 */
#[p|p<-A,p[4]==[-1/4*x^3 + 7/2*x]] /* = 20 */

/*
We get 80 classes of primes.
One-quarter of them, therefore, contains 20 classes,
and each of the quarters maps itself exactly into
a unique element of the Galois group C2*C2.
It is the collaboration of the reciprocal raw,
wherein we shall perceive what the use of the modulus is.
*/

```

K Computation of Chebotarev density theorem

```

/* The following is the computation to numerically validate the density theorem.*/

/*
Define the number field 'nf', and the Galois field 'gal'.
*/
f=Pol([1,0,-14,0,16]);
K=nfsplitting(f);
nf=nfinit(K);
gal=galoisinit(nf);

/*
Function procrob(p).

```

```

(1) Receives a prime 'p' in Z.
(2) Decomposes p into primes 'pr' in the number field 'nf'.
(3) For each of pr, Frobenius map (pr[i],nf/Q) is computed.
(4) The result returns as a list,
(4) If p ramifies (pr.e>1), an empty list returns.
*/

procfrob(p)={
my(pr,v);
pr=idealprimedec(nf,p);
v=[];
if(pr[1].e==1,
v=vector(#pr,i,galoispermtopol(gal,idealfrobenius(nf,gal,pr[i]))));
);
return(v);
}

/*
Get the representatives of Frobenius maps (p,nf/Q),
which lies below 1000th prime.
*/
classes= Set([Set(procfrob(p))| p<-primes(1000)]);

/* Enough number of primes is prepared. */
setofprimes=primes(100000);
/*
Function procdensity(N)
(1) It counts the number of the Frobenius maps of each type,
    using the computation which involves up to the first Nth prime.
(2) Then it evaluates the density.
(3) For simplicity, we allot a dummy set to the empty list,
    which is issued from the primes that ramify.
    Hence we neglect this dummy set,
    which shall come ahead (at the leftmost entry) in the evaluation.
*/
procdensity(N)={
my(p,foundclasses,foundnumber);
foundclasses= [Set(procfrob(p))| p<-setofprimes[1..N]];
foundnumber=vector(#classes,i,#[p|p<-foundclasses,p==classes[i] ]);
foundnull=#[p|p<-foundclasses,p==[]];
print(setofprimes[N]);
print(foundnumber);
print(foundnumber*1./(N-foundnull));

```



```

}

/*
The density computations up to 10th, 100th, 1000th, and 4000th primes are done.
*/
procdensity(10);
procdensity(100);
procdensity(1000);
procdensity(4000);

```

L Some computations using the GAP system

We could use the GAP system[The17] to compute the properties of the group D_4 .

```

OutputLogTo("galoislatticeout.txt");

# At first we define the group D4 and the subgroups
# by permutations.
# The generators are computed by PARI/GP
# concerning the problem of Galois group
# in the examples in the main article.
# subs[1] is D4; others are subgroups.

subs:=
Group((1, 6)(2, 4)(3, 8)(5, 7),
(1, 7, 6, 5)(2, 8, 4, 3),
(1, 2)(3, 7)(4, 6)(5, 8)),
Group((1, 6)(2, 4)(3, 8)(5, 7), (1, 7, 6, 5)(2, 8, 4, 3)),
Group((1, 6)(2, 4)(3, 8)(5, 7), (1, 2)(3, 7)(4, 6)(5, 8)),
Group((1, 6)(2, 4)(3, 8)(5, 7), (1, 8)(2, 7)(3, 6)(4, 5)),
Group((1, 6)(2, 4)(3, 8)(5, 7)),
Group((1, 2)(3, 7)(4, 6)(5, 8)),
Group((1, 4)(2, 6)(3, 5)(7, 8)),
Group((1, 8)(2, 7)(3, 6)(4, 5)),
Group((1, 3)(2, 5)(4, 7)(6, 8)),
Group(());

# Is this a subgroup of another?
# The answer [true/false] returns.
inc:=List(subs,i->List(subs,j->IsSubgroup(i,j)));

# Is this a normal subgroup of another?
# The answer [true/false] returns.

```

```

for i in [1..10] do
for j in [1..10] do
if inc[i][j]=true then
Print(i);Print("-");Print(j);Print(IsNormal(subs[i],subs[j]));Print("\n");
fi;
od;
od;

# Are two subgroups conjugate?
# The answer [true] returns.
IsConjugate(subs[1],subs[6],subs[7]);
IsConjugate(subs[1],subs[8],subs[9]);

# Define D4 as an abstract group.
D4:=DihedralGroup(8);

# The isomorphism
# between the Abstract group D4 and subs[1].
# The answer is the correspondence of generators:
# [ f1, f2, f3 ]
# -> [ (1,2)(3,7)(4,6)(5,8), (1,7,6,5)(2,8,4,3),
#      (1,6)(2,4)(3,8)(5,7) ].

IsomorphismGroups(D4,subs[1]);

# g0 is equivalent to subs[1],
# except that the group is minimally generated.

g0:=Group(MinimalGeneratingSet(subs[1]));

# We use this group
# to represent the generators of subgroups minimally.

hom:=EpimorphismFromFreeGroup(g0:names=["a","b"]);
for i in [1..10] do
mingens:=MinimalGeneratingSet(subs[i]);
Print("NO");Print(i);Print(mingens);Print("\n");
for gen in mingens do
preim:=PreImagesRepresentative(hom,gen);
Print(preim);Print("->");Print(gen);Print("\n");
od;
od;

```

```

for i in [1..10] do
mingens:=MinimalGeneratingSet(subs[i]);
Print("N0");Print(i);
genlist:=List(mingens,gen->PreImagesRepresentative(hom,gen));
Print(mingens);Print(genlist);
Print("\n");
od;

```

We shall get the following output, in which the generators of the subgroups are represented by 'a' and 'b', which are the generators of the group g_0 .

```

N01[ (1,2)(3,7)(4,6)(5,8), (1,7,6,5)(2,8,4,3) ]
a^-1->(1,2)(3,7)(4,6)(5,8)
b->(1,7,6,5)(2,8,4,3)
N02[ (1,7,6,5)(2,8,4,3) ]
b->(1,7,6,5)(2,8,4,3)
N03[ (1,2)(3,7)(4,6)(5,8), (1,6)(2,4)(3,8)(5,7) ]
a^-1->(1,2)(3,7)(4,6)(5,8)
b^-2->(1,6)(2,4)(3,8)(5,7)
N04[ (1,8)(2,7)(3,6)(4,5), (1,6)(2,4)(3,8)(5,7) ]
b^-1*a^-1->(1,8)(2,7)(3,6)(4,5)
b^-2->(1,6)(2,4)(3,8)(5,7)
N05[ (1,6)(2,4)(3,8)(5,7) ]
b^-2->(1,6)(2,4)(3,8)(5,7)
N06[ (1,2)(3,7)(4,6)(5,8) ]
a^-1->(1,2)(3,7)(4,6)(5,8)
N07[ (1,4)(2,6)(3,5)(7,8) ]
a^-1*b^-2->(1,4)(2,6)(3,5)(7,8)
N08[ (1,8)(2,7)(3,6)(4,5) ]
b^-1*a^-1->(1,8)(2,7)(3,6)(4,5)
N09[ (1,3)(2,5)(4,7)(6,8) ]
a^-1*b^-1->(1,3)(2,5)(4,7)(6,8)
N010[ ]

```

References

- [AM98] Emil Artin and Arthur Norton Milgram. *Galois theory*, volume 2. Courier Corporation, 1998.
- [AT68] Emil Artin and John Torrence Tate. *Class field theory*, volume 366. American Mathematical Soc., 1968.

- [Buc65] Bruno Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. *PhD thesis, Universitat Innsbruck*, 1965.
- [CLO06] David A Cox, John Little, and Donal O'shea. *Using algebraic geometry*, volume 185. Springer Science & Business Media, 2006.
- [CLO13] David Cox, John Little, and Donal OShea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media, 2013.
- [Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.
- [Con01] Keith Conrad. History of class field theory. *This unpublished essay is available online as a PDF file at [www. math. uconn. edu/~ kconrad/blurbs/gradnumthy/cfthistory. pdf](http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf)*, 2001.
- [DDJ08] M. S. Dresselhaus, G. Dresselhaus, and A. Jorio. *Group Theory: Application to the Physics of Condensed Matter*. Springer-Verlag, 2008.
- [DGPS] W. Decker, G.-M. Greuel, G. Pfister, and H. Schoenemann. Computer algebra system SINGULAR. Available at <http://www.singular.uni-kl.de/>.
- [Eis13] David Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.
- [Fey65] Richard P Feynman. Feynman lectures on physics. Volume 3: Quantum mechanics. *Reading, Ma.: Addison-Wesley, 1965, edited by Feynman, Richard P.; Leighton, Robert B.; Sands, Matthew*, 1965.
- [Gra13] Georges Gras. *Class Field Theory: from theory to practice*. Springer Science & Business Media, 2013.
- [GTZ88] Patrizia Gianni, Barry Trager, and Gail Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2-3):149–167, 1988.
- [Kik13] Akihito Kikuchi. An approach to first principles electronic structure computation by symbolic-numeric computation. *QScience Connect*, 2013:14, 2013. <http://dx.doi.org/10.5339/connect.2013.14>.
- [Kik18] Akihito Kikuchi. *Computer Algebra and Materials Physics: A Practical Guidebook to Group Theoretical Computations in Materials Science*, volume 272. Springer, 2018.
- [KK19] A Kikuchi and I Kikuchi. Computational Algebraic Geometry and Quantum Mechanics: An Initiative toward Post Contemporary Quantum Chemistry. *J Multidis Res Rev*, 1:47–79, 2019.

- [McC91] Paul J McCarthy. *Algebraic extensions of fields*. Courier Corporation, 1991.
- [Mil13] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.
- [Mil17] James S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.
- [Mil18] James S Milne. Fields and Galois theory (v4. 60). *order*, 3:138, 2018.
- [Möl93] H Michael Möller. On decomposing systems of polynomial equations with finitely many solutions. *Applicable Algebra in Engineering, Communication and Computing*, 4(4):217–230, 1993.
- [Ser79] Jean-Pierre Serre. Local class field theory. In *Local Fields*, pages 188–203. Springer, 1979.
- [SO12] Attila Szabo and Neil S Ostlund. *Modern quantum chemistry: introduction to advanced electronic structure theory*. Courier Corporation, 2012.
- [The17] The Gap Group. GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra. Available at <http://www.gap-system.org/>, 2017.
- [The19] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.11.2*, 2019. available from <http://pari.math.u-bordeaux.fr/>.
- [Tin03] M. Tinkham. *Group Theory and Quantum Dynamics*. Dover Books on Chemistry, 2003.
- [Wey50] H. Weyl. *The Theory of Groups and Quantum Mechanics*. Dover, 1950.