1. In this problem we will check that $x^n - x - 1$ has Galois group S_n (i.e, the splitting field of $x^n - x - 1$ has Galois group S_n over $\mathbb{Q}$) for $n = 2$, 3, and 4.

(a) Show the case $n = 2$.

For $n = 3$, 4 you may assume $x^n - x - 1$ is irreducible, without proving it. (Although proving it for $n = 3$ is something we know how to do.)

(b) Show the case $n = 3$.

(c) Show the case $n = 4$.

Reminders : (1) We have algorithms for computing the Galois groups of irreducible polynomials. (2) The formula for the discriminant of a cubic is in **H9** Q2. (3) given a quartic $f = x^4 + bx^3 + cx^2 + dx + e$ then the resolvent cubic of f is $p(t) = t^3 - ct^2 + (bd - 4e)t + (4ce - d^2 - b^2e)$. (4) The discriminant of a quartic polynomial is the same as the discriminant of its resolvent cubic.

Solution.

(a) The discriminant of $x^2 - x - 1$ is $1 - 4(1)(-1) = 5$, and $\sqrt{5} \notin \mathbb{Q}$. Therefore $x^2 - x - 1$ is irreducible over $\mathbb{Q}$ and the splitting field of $x^2 - x - 1$ has degree 2 over $\mathbb{Q}$. As we have seen (when the characteristic isn't 2), every degree 2 extension is a Galois extension, with Galois group $\mathbb{Z}/2\mathbb{Z} = S_2$.

(b) Let $f = x^3 - x - 1$, then $\Delta(f) = -23$, and $\delta(f) = \sqrt{-23} \notin \mathbb{Q}$. Therefore the Galois group of $L/\mathbb{Q}$ is S_3 (as opposed to C_3).

(c) Now let $f = x^4 - x - 1$. Then $\Delta(f) = -283$, and so $\delta(f) = \sqrt{-283} \notin \mathbb{Q}$. The resolvent cubic of f is $p(t) = t^3 + 4t - 1$. The resolvent cubic is irreducible over $\mathbb{Q}$. (Here are two ways to see that $p(t)$ is irreducible over $\mathbb{Q}$. One, $p(t)$ has no roots in $\mathbb{F}_7$, and hence is irreducible. Two, $p(6) = 239$ is prime, and $6 \geqslant \max\{|4/1|, |-1/1|\} + 2 = 6$.) By our algorithm, this means that the Galois group is S_3.

2. In this question we will investigate the norm in quadratic extensions. Let d be an integer which isn't a square, and set $L = \mathbb{Q}(\sqrt{d})$.

(a) Let $\gamma = a + b\sqrt{d} \in \mathrm{L}$, with $a, b \in \mathbb{Q}$. Write out the 2×2 matrix for the map "multiplication by γ" and compute its determinant. I.e., compute $\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma)$.

(b) $L/\mathbb{Q}$ is a Galois extension of degree 2, with Galois group $G = \mathbb{Z}/2\mathbb{Z} = C_2$. Let τ be the nontrivial element of G. How does τ act on L? (You don't have to prove your answer, we already did that in **H4** Q3, you just need to recall it for use below.)

(c) Given $\gamma = a + b\sqrt{d}$ as above, compute $\gamma \cdot \tau(\gamma)$, i.e., compute $N_{L/\mathbb{Q}}(\gamma)$ according to the alternate formula in Galois extensions.

For the rest of the question let us consider the case $d = 3$, and set $\gamma = 2 + \sqrt{3}$.

(d) Check that $N_{L/\mathbb{Q}}(\gamma) = 1$.

(e) Explain why $N_{L/\mathbb{Q}}(\gamma^n) = 1$ for all $n \geqslant 1$.

(f) Compute γ^2 and γ^3, and check directly that their norms are 1.

(g) Prove that the equation $x^2 - 3y^2 = 1$ has infinitely many solutions in positive integers x, y.

(h) Is there $a + b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ such that $\gamma = (a + b\sqrt{3})/\tau(a + b\sqrt{3})$? (You don't have to find such a, b, but you do have to argue whether such a, b exist.)

Solution.

(a) since 1, $\sqrt{d}$ is a basis of $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$, and $(a + b\sqrt{d}) \cdot 1 = a + b\sqrt{d}$, and $(a + b\sqrt{d}) \cdot \sqrt{d} = bd + a\sqrt{d}$, the matrix for multiplication by $\gamma = a + b\sqrt{d}$ (with $a, b \in \mathbb{Q}$) is

$$\begin{bmatrix} a & bd \\ b & a \end{bmatrix},$$

which has determinant $a^2 - db^2$, so $N_{L/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2$.

(b) By **H4** Q3, if $a, b \in \mathbb{Q}$ then $\tau(a + b\sqrt{d}) = a - b\sqrt{d}$.

(c) Therefore, if $\gamma = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$, $\gamma \cdot \tau(\gamma) = (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - db^2$, just as in part (a).

(d) Since $d = 3$, we have $N_{L/\mathbb{Q}}(a + b\sqrt{3}) = a^2 - 3b^2$. Therefore if $\gamma = 2 + 1 \cdot \sqrt{3}$, $N_{L/\mathbb{Q}}(\gamma) = 2^3 - 3 \cdot 1^2 = 4 - 3 \cdot 1 = 1$.

(e) The norm is multiplicative, for any α, $\beta \in L$, $N_{L/\mathbb{Q}}(\alpha\beta) = N_{L/\mathbb{Q}}(\alpha) \cdot N_{L/\mathbb{Q}}(\beta)$. Therefore for all $n \geqslant 1$ (and even all $n \in \mathbb{Z}$) we have $N_{L/\mathbb{Q}}(\gamma^n) = \big(N_{L/\mathbb{Q}}(\gamma)\big)^n = 1^n = 1$.

(f) We have

$$\begin{aligned}\gamma^2 &= (2+\sqrt{3})\cdot(2+\sqrt{3}) = \left(4+\sqrt{3}^2\right)+2\cdot 2\cdot 1\sqrt{3} &&= 7+4\sqrt{3}, \text{ and}\\ \gamma^3 &= \gamma^2\cdot\gamma = (7+4\sqrt{3})\cdot(2+\sqrt{3})\\ &= (7\cdot 2+4\cdot 1\cdot 3)+(7\cdot 1+4\cdot 2)\sqrt{3} &&= 26+15\sqrt{3}.\end{aligned}$$

Their norms are

$$\begin{aligned}\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(7+4\sqrt{3}) &= 7^2-3\cdot 4^2 = 49-3\cdot 16 = 49-48 &&= 1, \text{ and}\\ \mathrm{N}_{\mathrm{L}/\mathbb{Q}}(26+15\sqrt{3}) &= 26^2-3\cdot 15^2 = 676-3\cdot 225 = 676-675 &&= 1,\end{aligned}$$

just as part (e) guarantees.

(g) For each $n \geqslant 1$ define rational numbers x_n and y_n by the formula $x_n + y_n\sqrt{3} = \gamma^n$. I.e., x_n and y_n are the coefficients of 1 and $\sqrt{3}$ respectively when expressing γ^n in the basis 1, $\sqrt{3}$ of L over $\mathbb{Q}$. So, for example, $(x_1, y_1) = (2, 1)$, $(x_2, y_2) = (7, 4)$, and $(x_3, y_3) = (26, 15)$.

By parts (e) and (a) we have $1 = \mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma^n) = \mathrm{N}_{\mathrm{L}/\mathbb{Q}}(x_n + y_n\sqrt{3}) = x_n^2 - 3y_n^2$ for all $n \geqslant 1$. Therefore if we show that x_n and y_n are always positive integers, and always different pairs of positive integers, we will have shown that $x^2 - 3y^2 = 1$ has infinitely many different solutions in positive integers.

One way to see this is to note that since

$$x_{n+1}+y_{n+1}\sqrt{3} = \gamma^{n+1} = \gamma^n\cdot\gamma = (x_n+y_n\sqrt{3})\cdot(2+\sqrt{3}) = (2x_n+3y_n)+(x_n+2y_n)\sqrt{3}$$

we have the recursions $x_{n+1} = 2x_n + 3y_n$ and $y_{n+1} = x_n + 2y_n$. Starting with $(x_1, y_1) = (2, 1)$ the recursions show that x_{n+1}, y_{n+1} are always positive integers, and increasing. Since they are increasing, they must all be different.

A similar argument is that since $\alpha \approx 3.732050808\ldots > 1$, we see that the sequence $\{\gamma^n\}_{n\geqslant 1}$ is a strictly increasing sequence of real numbers, and so are all distinct. Since the (x_n, y_n) is the coefficients of γ^n in a basis for L over $\mathbb{Q}$, these coefficients must also all be distinct. We then need to see that they are all positive integers. Using the binomial theorem we have

$$x_n + y_n\sqrt{3} = \gamma^n = (2+\sqrt{3})^n = \sum_{m=0}^{n}\binom{n}{m}2^{n-m}\left(\sqrt{3}\right)^m$$

So that

$$x_n = \sum_{\substack{m=0\\ m \text{ even}}}^{n}\binom{n}{m}2^{n-m}\left(\sqrt{3}\right)^m \quad \text{and} \quad y_n = \sum_{\substack{m=1\\ m \text{ odd}}}^{n}\binom{n}{m}2^{n-m}m\left(\sqrt{3}\right)^{m-1}.$$

These explicit expressions show that x_n and y_n are positive integers (since each of the terms we are adding are positive integers).

(h) Since $\mathrm{N}_{\mathrm{L}/\mathbb{Q}}(\gamma) = 1$, and since $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ is a cyclic group generated by τ, Hilbert's Theorem 90 tells us that there is a $\beta \in \mathrm{L}$, $\beta \neq 0$, such that $\gamma = \beta/\tau(\beta)$. Since $\beta \in \mathrm{L}$ we can write $\beta = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$, and therefore the answer to the question is yes — there are nonzero $a, b \in \mathbb{Q}$ so that $\gamma = \frac{a+b\sqrt{3}}{\tau(a+b\sqrt{3})}$.

Explicitly, $\beta = 3 + \sqrt{3}$ is such an element since

$$\begin{aligned} \frac{3+\sqrt{3}}{\tau(3+\sqrt{3})} &= \frac{3+\sqrt{3}}{3-\sqrt{3}} = \left(\frac{3+\sqrt{3}}{3-\sqrt{3}}\right) \cdot \left(\frac{3+\sqrt{3}}{3+\sqrt{3}}\right) \\ &= \frac{(3\cdot 3 + 1\cdot 3) + (2\cdot 3\cdot 1)\sqrt{3}}{9-3} = \frac{12+6\sqrt{3}}{6} = 2+\sqrt{3}. \end{aligned}$$

Such a β is unique up to multiplying by a nonzero element of $\mathbb{Q}$, and so the solution above is the "smallest" possible β with positive integer coefficients.

3. Suppose that K is a field of characteristic zero, and that $f(x) \in K[x]$ is an irreducible polynomial of degree 4 with splitting field L. Further suppose that $G = \mathrm{Gal}(L/K) = A_4$. The purpose of this question is to write down all the intermediate fields of L/K, without having a concrete polynomial to work with. The idea is to demonstrate that the Galois group not only controls the "shape" of the diagram of intermediate fields (since this lattice is the reverse of the subgroup lattice), but that once the Galois group is fixed, there are "universal formulae" for these intermediate fields.

Let α_1, α_2, α_3, and α_4 be the four roots of f, and $\gamma_{12|34}$, $\gamma_{13|24}$, and $\gamma_{14|23}$ the three roots of the resolvent cubic g, as described in class.

(a) List and name the subgroups of A_4. You should have four subgroups of order 3, one subgroup of order 4, and three subgroups of order 2.

(By "name" I mean : if the subgroup has a well-known name that we've seen before, use that, if not give it your own name [e.g., "H_7"], whatever name you want, so that below when we match intermediate fields to subgroups you'll have a way to describe which subgroup, something better than "the third subgroup on the list from part (a)...".)

(b) Find the fixed fields associated to the subgroups of order 3 (this should be fairly easy).

(c) Find the fixed field of the subgroup of order 4.

(d) Explain why $K(\gamma_{12|34}) = K(\gamma_{13|24}) = K(\gamma_{14|23})$. (An indirect argument is best, and there is more than one possible such argument.)

(e) And now the challenge problem: find the fixed fields for the groups of order 2. Explain your answer, and your reasoning, as clearly as you can.

Solution.

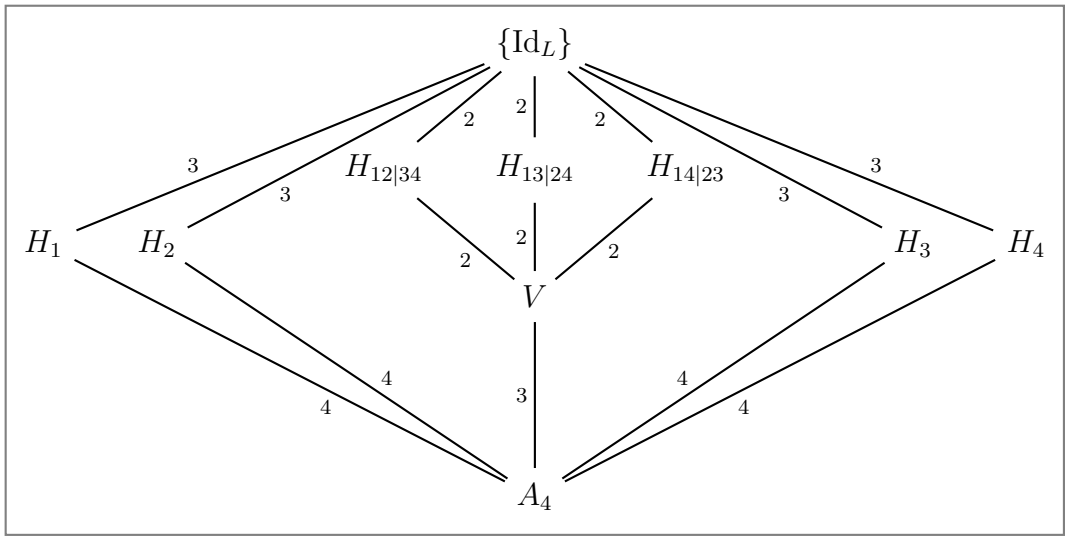
(a) Besides A_4 and $\{\mathrm{Id}_L\}$ the subgroups of A_4 are :

Subgroups of order 3
$H_1 = \langle(2\,3\,4)\rangle$; $H_2 = \langle(1\,3\,4)\rangle$; $H_3 = \langle(1\,2\,4)\rangle$; $H_4 = \langle(1\,2\,3)\rangle$.

Subgroup of order 4
$V = \{\mathrm{Id}_L, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

Subgroups of order 2
$H_{12|34} = \{\mathrm{Id}_L, (1\,2)(3\,4)\}$; $H_{13|24} = \{\mathrm{Id}_L, (1\,3)(2\,4)\}$; $H_{14|23} = \{\mathrm{Id}_L, (1\,4)(2\,3)\}$.

For use in the rest of the question, here is the reversed lattice of subgroups of A_4.



To see that these are all the subgroups, we make the following observations. Since $|A_4| = 12$, the size of any subgroup has to divide 12. Subgroups of orders 2 and 3 must be cyclic, generated by elements of order 2 and 3. Listing all the elements of orders 2 and 3 in A_4 gives the subgroups of orders 2 and 3 above. (NOTE: Different elements of order 2 generate different subgroups. However, if σ is of order 3 then so is $\sigma^2 = \sigma^{-1}$, and σ and σ^{-1} generate the same subgroup.) Any group of order 4 is either cyclic generated by an element of order 4, or the Klein four-group, where all elements other than the identity are of order 2. The group A_4 has no elements of order 4, so the first possibility is out. However, A_4 does have three elements of order 2, and together with the identity give V. The remaining divisor of 12

(other than 1 and 12) is 6. Any group of order 6 has an element of order 2 and an element of order 3. However, direct calculation shows that in A_4, any elements of order 2 and order 3 generate all of A_4, so there is no subgroup of order 6.

(b) A subgroup of A_4 of order 3 corresponds to an extension of $\mathbb{Q}$ of degree $\frac{12}{3} = 4$. We started with an irreducible degree 4 equation f with four roots. Each of those roots generates a degree 4 extension. We can now check that these are all the degree 4 extensions of $\mathbb{Q}$ in L.

The root α_1 is fixed by H_1 (H_1 acts by $\alpha_2 \mapsto \alpha_3 \mapsto \alpha_4 \mapsto \alpha_2$), and therefore $K(\alpha_1) \subseteq L^{H_1}$. Since both $K(\alpha_1)$ and L^{H_1} have degree 4 over K, we conclude that $L^{H_1} = K(\alpha_1)$.

Similarly, $L^{H_2} = K(\alpha_2)$, $L^{H_3} = K(\alpha_3)$, and $L^{H_4} = K(\alpha_4)$. Since $H_1,\ldots, H_4$ are all the subgroups of index 4 in A_4, $K(\alpha_1),\ldots, K(\alpha_4)$ are all the degree 4 extensions of K contained in L. (They are also distinct degree 4 extensions, since the subgroups $H_1,\ldots, H_4$ are all different.)

(c) The fixed field corresponding to V has degree $\frac{12}{4} = 3$ over K. Since the Galois group is A_4, our algorithm for Galois groups of irreducible quartics tells us that the resultant cubic $p(t)$ is irreducible over K. Therefore each of its roots give a degree 3 extension of K.

The root $\gamma_{12|34}$ is fixed by V, and so $K(\gamma_{12|34}) \subseteq L^V$. Since both fields have degree 3 over K, we conclude that $K(\gamma_{12|34}) = L^V$.

(d) The argument in (c) works just as well for $\gamma_{13|24}$ and $\gamma_{14|23}$ and shows that $K(\gamma_{13|24}) = L^V$ and $K(\gamma_{14|23}) = L^V$, and therefore we have that $K(\gamma_{12|34}) = K(\gamma_{13|24}) = K(\gamma_{14|23})$.

Another versions of the same argument is to note that $K(\gamma_{12|34})$, $K(\gamma_{13|24})$, and $K(\gamma_{14|23})$ are degree 3 extensions of K, and so correspond to subgroups of A_4 with index 3, i.e., subgroups of A_4 with 4 elements. Since A_4 only has one subgroup with 4 elements, and since the Galois correspondence is a bijection, these fields must be the same.

(e) To solve this question let us first write down what we can observe from the groups and the Galois correspondence. We will use $H_{12|34}$ as an example, but similar reasoning applies to the other groups.

- Since $H_{12|34}$ is a normal subgroup of V of index 2 , $L^{H_{12|34}}$ is a Galois extension of L^V of degree 2, with Galois group $V/H_{12|34} \cong C_2$.
- As long as Char $\neq 2$, any quadratic extension is obtained by adding an element which the nontrivial element of the Galois group sends to its negative. (E.g., Q2(b) of this assignment, **H4** Q3, many examples in class.)

Therefore $L^{H_{12|34}}$ is obtained by adjoining a single element to L^V. That element must be fixed by $H_{12|34}$ and sent to its negative by the nontrivial element of $V/H_{12|34}$. (Since the cosets of $H_{12|34}$ in V are $\{\mathrm{Id}_L, (1\,2)(3\,4)\}$ and $\{(1\,3)(2\,4), (1\,4)(2\,3)\}$, this is the same as asking the element we are adjoining to be sent to its negative by $(1\,3)(2\,4)$ and $(1\,4)(2\,3)$.) Let us look for such an element.

After thinking for a bit, here are two natural candidates :

$$\begin{aligned} \delta_{12|34} &= (\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4) \text{ or} \\ \epsilon_{12|34} &= \alpha_1\alpha_2 - \alpha_3\alpha_4. \end{aligned}$$

From their descriptions, we see that both are fixed by (1 2)(3 4), and both are sent to their negatives by (1 3)(2 4) and (1 4)(2 3). At this point there are also two natural questions :

$\mathbf{Q}_1$: How do we know that these elements aren't zero? (Being zero is compatible with the two properties above, but adjoining zero isn't going to get us anywhere).

$\mathbf{Q}_2$: If neither are zero, which one do we pick?

Here are the answers.

$\mathbf{A}_1$: First suppose that $\delta_{12|34} = 0$, i.e., that $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$. Acting by $(1\,2\,3) \in A_4$ gives $\alpha_2 + \alpha_3 = \alpha_1 + \alpha_4$. Adding these two together gives $\alpha_1 + 2\alpha_2 + \alpha_3 = \alpha_1 + \alpha_3 + 2\alpha_4$, or $2\alpha_2 = 2\alpha_4$, and so (since Char $\neq 2$) $\alpha_2 = \alpha_4$. But $f(x)$ is an irreducible quadratic equation in characteristic zero, so it must have distinct roots. This contradiction shows that $\delta_{12|34} \neq 0$.

Similarly, suppose that $\epsilon_{12|34} = 0$, or $\alpha_1\alpha_2 = \alpha_3\alpha_4$. Acting by $(1\,2\,3)$ gives $\alpha_2\alpha_3 = \alpha_1\alpha_4$, and multiplying these gives $\alpha_1\alpha_2^2\alpha_3 = \alpha_1\alpha_3\alpha_4^2$ or (since none of the roots of $f(x)$ are zero) $\alpha_2^2 = \alpha_4^2$. Acting by (1 3 4) gives $\alpha_2^2 = \alpha_1^2$, and acting once more by (1 3 4) gives $\alpha_2^2 = \alpha_3^2$. Thus $\alpha_1^2 = \alpha_2^2 = \alpha_3^2 = \alpha_4^2$. Set $c = \alpha_1^2$, then $\alpha_1 = \pm\sqrt{c}$, $\alpha_2 = \pm\sqrt{c}$, $\alpha_3 = \pm\sqrt{c}$, and $\alpha_4 = \pm\sqrt{c}$, and this implies some of the roots must be the same (there are only two possibilities for the sign, and four roots — at least two of them must share the same sign). This is again a contradiction (as above the roots of $f(x)$ are distinct) and shows that $\epsilon_{12|34} \neq 0$.

$\mathbf{A}_2$: It doesn't matter — both generate the same extension. Each of $\delta_{12|34}$ and $\epsilon_{12|34}$ are in $L^{H_{12|34}}$ but not in L^V (since they are each fixed by $H_{12|34}$ but not fixed by V). Thus $L^V(\delta_{12|34})$ and $L^V(\epsilon_{12|34})$ are nontrivial extensions of L^V contained in $L^{H_{12|34}}$. Since $[L^{H_{12|34}} : L^V] = [V : H_{12|34}] = 2$, there is not much room for a nontrivial extension! The only possibility is $L^V(\delta_{12|34}) = L^{H_{12|34}}$ and $L^V(\epsilon_{12|34}) = L^{H_{12|34}}$, i.e., they both generate the same extension.

We can actually be more precise : since $\delta_{12|34}$ and $\epsilon_{12|34}$ are each sent to their negatives by the nontrivial element of $V/H_{12|34}$, they must be scalar multiples of each other, with the scalar coming from L^V (CHALLENGE : Can you find such an element?)

Thus, $L^{H_{12|34}} = L^V(\delta_{12|34}) = K(\gamma_{12|34}, \delta_{12|34})$ and $L^{H_{12|34}} = L^V(\epsilon_{12|34}) = K(\gamma_{12|34}, \epsilon_{12|34})$.

Note that $\delta_{12|34}$ and $\epsilon_{12|34}$ are not the only possibilities we could add. Any nonzero element of L which is fixed by (1 2)(3 4) and sent to its negative by (1 3)(2 4) (and so also by (1 4)(2 3)) will do. E.g., $\alpha_1^2+\alpha_2^2-\alpha_3^2-\alpha_4^2$, if nonzero, would work.

Identical arguments, with permuted notation, work for $H_{13|24}$ and $H_{14|23}$, so for example

$$\begin{aligned} L^{H_{13|24}} &= K(\gamma_{13|24}, \alpha_1+\alpha_3-\alpha_2-\alpha_4) = K(\gamma_{13|24}, \alpha_1\alpha_3-\alpha_2\alpha_4), \text{ and} \\ L^{H_{14|23}} &= K(\gamma_{14|23}, \alpha_1+\alpha_4-\alpha_2-\alpha_3) = K(\gamma_{14|23}, \alpha_1\alpha_4-\alpha_2\alpha_3). \end{aligned}$$

Setting $M = K(\gamma_{12|34}) = K(\gamma_{13|24}) = K(\gamma_{14|23})$, $\delta_{13|24} = \alpha_1+\alpha_3-\alpha_2-\alpha_4$, and $\delta_{14|23} = \alpha_1+\alpha_4-\alpha_2-\alpha_3$, the lattice of intermediate fields is :