1. Let L/K be a finite extension and $G = \mathrm{Aut}(L/K)$. Even if L/K is not a Galois extension we always have order-reversing maps of lattices

$$\left\{\text{lattice of subgroups } H \text{ of } G\right\} \underset{\mathrm{Aut}(L/M) \,\longleftarrow\!\dashv\, M}{\overset{H \,\longmapsto\, L^H}{\rightleftarrows}} \left\{\text{lattice of intermediate fields } M\right\}$$

However, if L/K is not a Galois extension, there is no reason that these maps have to be bijections. In this problem we will see this in a very simple example. (In some sense the example may be too small to be convincing, but it does show that the correspondence doesn't work out in general.)

Let $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$.

(a) Is L/K a Galois extension?

(b) Find $[L : K]$.

(c) Find all intermediate fields M, $K \subseteq M \subseteq L$. (Suggestion: Consider the tower law $[L : K] = [L : M] \cdot [M : K]$ and find the possible degrees of the intermediate fields first.)

(d) Write down the lattice of intermediate fields.

(e) Let $G = \mathrm{Aut}(L/K)$. If $\sigma \in G$ explain where σ must send $\sqrt[3]{2}$. (Suggestion: As usual you should start with the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$.)

(f) Compute G (i.e., find all elements of G).

(g) Write down the lattice of all subgroups of G. (This will be quite small.)

(h) For each subgroup H of G, find L^H.

(i) For each intermediate field M, find $\mathrm{Aut}(L/M)$.

Solution.

(a) No, L/K is not a Galois extension. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $q(x) = x^3 - 2$ with roots $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$, where $\omega = e^{2\pi i/3}$. The last two roots are not in L, so $L/\mathbb{Q}$ is not a normal extension, and hence not a Galois extension.

(b) $[L : K] = \deg(x^3 - 2) = 3$.

(c) Let M be an intermediate field. Then we have

$$3 = [L : K] = [L : M] \cdot [M : K]$$

since 3 is a prime number, the only possible factorization is $3 \cdot 1$ or $1 \cdot 3$, giving either $[M : K] = 1$ and so $M = K$ or $[L : M] = 1$ and so $L = M$. That is, the only intermediate fields are L and M.

(d) The lattice of intermediate fields is $\boxed{\begin{array}{c} L \\ | \\ K \end{array}}$.

(e) Let σ be any element of $G = \mathrm{Aut}(L/K)$, then $\sigma(\sqrt[3]{2})$ must be another root of $q(x) = x^3 - 2$. The only root of $q(x)$ in L is $\sqrt[3]{2}$, so we conclude that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$. In other words, every element of $\mathrm{Aut}(L/K)$ must take $\sqrt[3]{2}$ to itself.

(f) The element $\sqrt[3]{2}$ generates L over $\mathbb{Q}$, and in fact (from (b)) we have

$$L = \left\{ a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \;\middle|\; a, b, c \in \mathbb{Q} \right\}.$$

By part (e), if $\sigma \in \mathrm{Aut}(L/K)$ we have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ and so for an arbitrary $\gamma = a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \in L$ we have

$$\sigma(\gamma) = \sigma\left(a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2\right) = a\sigma(1) + b\sigma(\sqrt[3]{2}) + c\left(\sigma(\sqrt[3]{2})\right)^2 = a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 = \gamma.$$

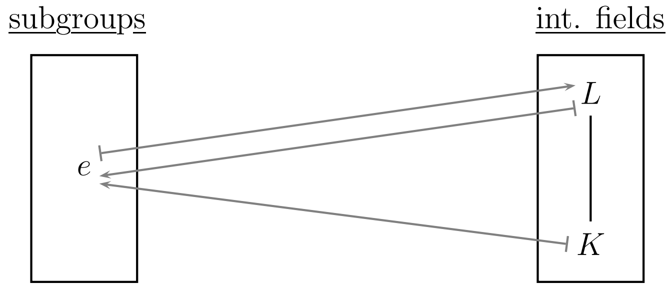
Thus σ acts as the identity on L. Since this is true for all $\sigma \in \mathrm{Aut}(L/K)$, we conclude that the only element of $\mathrm{Aut}(L/K)$ is e, i.e., that $G = \{e\}$.

(g) The lattice of subgroups of G is $\boxed{e}$ (quite small!).

(h) The only subgroup of G is $G = \{e\} = G$ with fixed field $L^G = L$.

(i) For $M = K$ we have already computed that $\mathrm{Aut}(L/K) = \{e\}$. For $M = L$ we also have $\mathrm{Aut}(L/L) = \{e\}$.

Thus, in this case the order-reversing maps of lattices are



Unlike the case of a Galois extension, these maps are not bijections!

2. Suppose that (α_1, β_1), ..., (α_k, β_k) are points of $\mathbb{C}^2$ (i.e, $\alpha_i, \beta_i \in \mathbb{C}$), and that the set $S = \{(\alpha_1, \beta_1), \dots, (\alpha_k, \beta_k)\}$ is stable under complex conjugation. (This means that if $(\alpha_i, \beta_i) \in S$ then $(\overline{\alpha_i}, \overline{\beta_i}) \in S$ too). For any $d \geqslant 0$, consider the $\mathbb{C}$-vector space V_d of polynomials of degree $\leqslant d$ in $\mathbb{C}[x, y]$ which are zero at all (α_i, β_i), $i = 1, \dots, k$. Show that V_d has a basis consisting of polynomials with real coefficients.

Solution. Let $G = \{\mathrm{Id}_{\mathbb{C}}, \tau\}$, where τ is complex conjugation. Let V be the vector space of polynomials of degree $\leqslant d$. The vector space V has a basis of monomials $\{x^a y^b\}$ such that $a + b \leqslant d$, and is isomorphic to $\mathbb{C}^N$, with $N = \binom{d+2}{2}$. We let G act on a polynomial $f \in V$ by acting on the coefficients : for any $\sigma \in G$, $f = c_{00} + c_{10}x + c_{01}y + \cdots + c_{ab}x^a y^b + \cdots c_{0,d}y^d \in V$, we have

$$\sigma(f) = \sigma(c_{00}) + \sigma(c_{10})x + \sigma(c_{01})y + \cdots + \sigma(c_{ab})x^a y^b + \cdots \sigma(c_{0,d})y^d.$$

Now let V_d be the subspace of V consisting of those polynomials which vanish at the points of S. We claim that V_d is stable under the action of G, and so (by the descent lemma) has a basis with coefficients in $\mathbb{C}^G = \mathbb{R}$.

Let $f \in V_d$ be any polynomial. We need to show that $\sigma(f) \in V_d$ for all $\sigma \in G$. This is clear for $\sigma = \mathrm{Id}_{\mathbb{C}}$ since $\mathrm{Id}_{\mathbb{C}}(f) = f$, so we only need to check for $\sigma = \tau$. By definition, $\tau(f)$ is in V_d if and only if $\tau(f)(\alpha_i, \beta_i) = 0$ for all $(\alpha_i, \beta_i) \in S$. However,

$$\tau(f)(\alpha_i, \beta_i) = \overline{f}(\alpha_i, \beta_i) = \overline{f(\overline{\alpha_i}, \overline{\beta_i})}.$$

Since S is stable under complex conjugation, $(\overline{\alpha_i}, \overline{\beta_i}) \in S$, and since f is in V_d, $f(\overline{\alpha_i}, \overline{\beta_i}) = 0$. Thus

$$\tau(f)(\alpha_i, \beta_i) = \overline{f(\overline{\alpha_i}, \overline{\beta_i})} = \overline{0} = 0.$$

Since this holds for all $(\alpha_i, \beta_i) \in S$, we conclude that $\tau(f) \in V_d$, and hence that V_d is stable under the action of G.

Thus, by the descent lemma, V_d has a basis with coefficients in $\mathbb{R}$.

3. In this problem we will work out the Galois correspondence in the case $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $K = \mathbb{Q}$. Recall that from **H3** Q2(d) we know that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis of L/K.

(a) Show that L/K is a Galois extension.

Let $G = \mathrm{Gal}(L/K)$. In this case it turns out that G is the Klein four-group, $G = \{e, \tau_1, \tau_2, \tau_1\tau_2\}$ where all elements except e have order 2, and τ_1 and τ_2 commute. The action of G on L may be deduced from the information :

$$\boxed{\begin{array}{l}\tau_1\\ \sqrt{2} \longmapsto -\sqrt{2}\\ \sqrt{3} \longmapsto \sqrt{3}\end{array}} \quad \text{and} \quad \boxed{\begin{array}{l}\tau_2\\ \sqrt{2} \longmapsto \sqrt{2}\\ \sqrt{3} \longmapsto -\sqrt{3}\end{array}} .$$

(b) Deduce the action of τ_1, τ_2 on $\sqrt{6}$.

(c) Deduce the action of τ_1, τ_2, and $\tau_1\tau_2$ on an arbitrary element $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ of L (with $a, b, c, d \in \mathbb{Q}$).

(d) Find all subgroups of G and write down the (reversed) lattice of subgroups of G

(e) For each subgroup H of G, find the fixed field L^H.

SUGGESTION: To find the elements of L fixed by an element σ of G, start with a general element $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ of L, write down the equation $\sigma(\alpha) = \alpha$, and consider it as a system of linear equations in the unknowns a, b, c, and d. Solutions to the equations are elements of L fixed by σ. (Here you will need to use your formula from (c) to see what $\sigma(\alpha)$ is.)

(f) Write down the lattice of intermediate fields of L/K.

Solution.

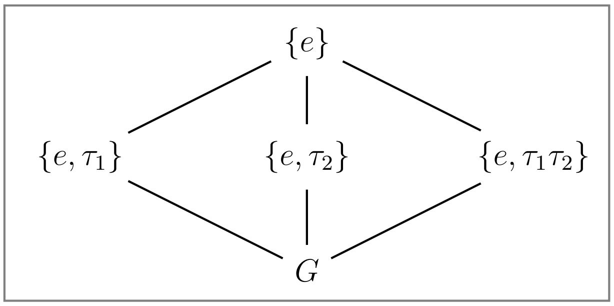
(a) The generators of $L/\mathbb{Q}$ are $\sqrt{2}$, $\sqrt{3}$ with minimal polynomials $x^2 - 2$ and $x^2 - 3$ respectively. The roots of these polynomials are $\pm\sqrt{2}$ and $\pm\sqrt{3}$, all of which are in L. Thus $L/\mathbb{Q}$ is a normal extension. Since we are in characteristic zero, $L/\mathbb{Q}$ is automatically a separable extension, and so $L/\mathbb{Q}$ is a Galois extension.

(b)
$$\begin{aligned}\tau_1(\sqrt{6}) &= \tau_1(\sqrt{2}\cdot\sqrt{3}) = \tau_1(\sqrt{2})\cdot\tau_1(\sqrt{3}) = (-\sqrt{2})\cdot(\sqrt{3}) = -\sqrt{6}.\\ \tau_2(\sqrt{6}) &= \tau_2(\sqrt{2}\cdot\sqrt{3}) = \tau_2(\sqrt{2})\cdot\tau_2(\sqrt{3}) = (\sqrt{2})\cdot(-\sqrt{3}) = -\sqrt{6}.\end{aligned}$$

(c) We have

$$\begin{aligned}
\tau_1\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) &= a+b\tau_1(\sqrt{2})+c\tau_1(\sqrt{3})+d\tau_1(\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}.\\
\tau_2\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) &= a+b\tau_2(\sqrt{2})+c\tau_2(\sqrt{3})+d\tau_2(\sqrt{6}) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}.\\
\tau_1\tau_2\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) &= a+b\tau_1\tau_2(\sqrt{2})+c\tau_1\tau_2(\sqrt{3})+d\tau_1\tau_2(\sqrt{6}) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}.
\end{aligned}$$

(d) Since G has order 4, any subgroup of G other than G and $\{e\}$ has order 2, and so corresponds to an element of order 2. The reversed lattice of subgroups is therefore



.

(e) To find the fixed field L^{H_i} for any of the subgroups H_i of order 2, it is enough to find the elements of L fixed under the generator of H_i. Using the formulae from (c), we have

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = \tau_1\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$

only if $b=-b$ and $d=-d$, i.e, $b=d=0$ so that the element is of the form $a+c\sqrt{3}$ and so $L^{\{e,\tau_1\}}=\mathbb{Q}(\sqrt{3})$.

Similarly, we have

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = \tau_2\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) = a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$

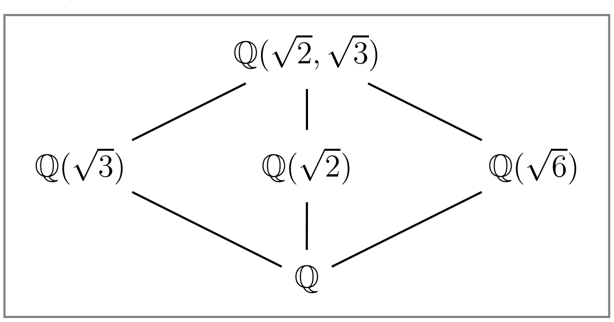
if and only if $d=0$ and $c=0$, so that the element is of the form $a+b\sqrt{2}$, and $L^{\{e,\tau_2\}}=\mathbb{Q}(\sqrt{2})$.

Finally,

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = \tau_1\tau_2\left(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\right) = a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$

if and only if $b=0$ and $c=0$, so that the element is of the form $a+d\sqrt{6}$, and $L^{\{e,\tau_1\tau_2\}}=\mathbb{Q}(\sqrt{6})$.

(f) Thus the corresponding lattice of intermediate fields is



.

4. Let L/K be a Galois extension, $G = \mathrm{Gal}(L/K)$, and set $d = |G| = [L : K]$. Let $\sigma_1, \ldots, \sigma_d$ be the elements of G, and choose any basis $\alpha_1, \ldots, \alpha_d$ of L over K. Explain why the determinant

$$\begin{vmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \sigma_1(\alpha_3) & \cdots & \sigma_1(\alpha_d) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \sigma_2(\alpha_3) & \cdots & \sigma_2(\alpha_d) \\ \sigma_3(\alpha_1) & \sigma_3(\alpha_2) & \sigma_3(\alpha_3) & \cdots & \sigma_3(\alpha_d) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_d(\alpha_1) & \sigma_d(\alpha_2) & \sigma_d(\alpha_3) & \cdots & \sigma_d(\alpha_d) \end{vmatrix} \neq 0.$$

(SUGGESTION : Consider the matrix as giving a linear map $L^d \longrightarrow L^d$ and use part of the argument from the proof of Artin's lemma.)

Solution. Consider the map $L^d \longrightarrow L^d$ given by the matrix above, and let W be the kernel of this map. If the determinant of the matrix is zero, then $\dim_L(W) \geqslant 1$. In the proof of Artin's lemma we have seen that the kernel is stable under the action of G, and hence by the descent lemma, W has a basis consisting of elements whose coordinates are in K. Since $\dim_L(W) \geqslant 1$ there is at least one such basis element, say $w = (c_1, c_2, \ldots, c_d)$. I.e., we now have $(c_1, \ldots, c_d) \in W$ with the $c_i \in K$, and not all $c_i = 0$.

Since w is in the kernel of the matrix, for each j we have

$$\sigma_j(\alpha_1) \cdot c_1 + \sigma_j(\alpha_2) \cdot c_2 + \cdots + \sigma_j(\alpha_d) \cdot c_d = 0.$$

One of the elements in the group is the identity. For that element the equation above becomes

$$c_1\alpha_1 + c_2\alpha_2 + \cdots + c_d\alpha_d = 0,$$

with all the $c_i \in K$ and at least one nonzero. This contradicts the assumption that $\alpha_1, \ldots, \alpha_d$ are linearly independent over K.

The contradiction shows that the determinant above must be nonzero.