1. Suppose that K is a field of characteristic zero, and $p(x) \in K[x]$ an irreducible polynomial of degree d over K. Let α_1, α_2, $\ldots$, α_d be the roots of $p(x)$, and $L = K(\alpha_1, \ldots, \alpha_d)$ the field obtained by adjoining all the roots of $p(x)$.

Let S be the set $S = \{\alpha_1, \ldots, \alpha_d\}$ of the roots.

(a) If σ is an element of $\mathrm{Aut}(L/K)$ explain why, for any root $\alpha_i \in S$, $\sigma(\alpha_i) \in S$ too, so that the group $G = \mathrm{Aut}(L/K)$ acts on the set S.

(b) If $\sigma \in G$, and $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, d$, explain why σ is actually the identity map $\sigma : L \longrightarrow L$ on L.

(c) An action of a group G on a set S is the same as a homomorphism $G \longrightarrow \mathrm{Perm}(S)$ from G to the group of permutations of S. Explain why the action from part (a) gives an *injective* homomorphism.

(d) Explain why the group G acts *transitively* on S. [Hint: Lifting lemma!]

(e) Explain why G can be realized as a subgroup of S_d, the symmetric group on d elements, such that the subgroup acts transitively on the set $\{1, \ldots, d\}$.

Solution.

(a) We recall the following result (from the class on Wednesday, January 20th, the 8th class of the semester) which we have used frequently:

Lemma — *Suppose that $K \subseteq L$ is an extension of fields, that α is an element of L algebraic over K, and let $q(x) \in K[x]$ be the minimal polynomial of α over K. Then for any $\sigma \in \mathrm{Aut}(L/K)$, $\sigma(\alpha)$ is also a root of $q(x)$.*

Let α_i be any root of $p(x)$. Let $q(x) \in K[x]$ be the minimal polynomial of α_i over K. Since $p(\alpha_i) = 0$ we have that $q(x)$ divides $p(x)$. By the lemma, for any $\sigma \in \mathrm{Aut}(L/K)$, we have that $\sigma(\alpha_i)$ is a root of $q(x)$, and hence also a root of $p(x)$ since $q(x)$ divides $p(x)$. Therefore, $\sigma(\alpha_i)$ is also in S.

Remarks. (1) The argument above shows that the lemma implies something apparently stronger : that if $p(x) \in K[x]$ is any polynomial with α as a root, and $\sigma \in \mathrm{Aut}(L/K)$ then $\sigma(\alpha)$ is a root of $p(x)$. (2) We didn't actually need this extension in the problem. Since $p(x)$ is irreducible over K, and divisible by the nonconstant polynomial $q(x)$, we must have $p(x) = cq(x)$ where $c \in K$ is the leading coefficient of $p(x)$ (and so equal to 1 if $p(x)$ is also monic). I.e, $p(x)$ is, up to scaling to make it monic, the minimal polynomial of α_i (and since α_i was arbitrary, it is the minimal polynomial of any of its other roots as well).

(b) Since $L = K(\alpha_1, \ldots, \alpha_d)$, we have that L is generated over K by $\alpha_1, \ldots, \alpha_d$, each of which is algebraic over K. By our theorem on simple extensions and the proof of the tower law, this means that every element of $\gamma \in L$ can be written as a finite sum

$$\gamma = \sum c_{m_1,m_2,\ldots,m_d} \alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_d^{m_d}$$

with the coefficients $c_{m_1,\ldots,m_d} \in K$. Thus for any $\sigma \in \mathrm{Aut}(L/K)$ we have

$$\begin{aligned} \sigma(\gamma) &= \sum \sigma(c_{m_1,m_2,\ldots,m_d}) \sigma(\alpha_1)^{m_1} \sigma(\alpha_2^{m_2}) \cdots \sigma(\alpha_d)^{m_d} \\ &= \sum c_{m_1,m_2,\ldots,m_d} \sigma(\alpha_1)^{m_1} \sigma(\alpha_2^{m_2}) \cdots \sigma(\alpha_d)^{m_d}. \end{aligned}$$

Where the last equality is because σ fixes K. If, in addition, $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \ldots, d$, then this becomes

$$\begin{aligned} \sigma(\gamma) &= \sum c_{m_1,m_2,\ldots,m_d} \sigma(\alpha_1)^{m_1} \sigma(\alpha_2^{m_2}) \cdots \sigma(\alpha_d)^{m_d} \\ &= \sum c_{m_1,m_2,\ldots,m_d} \alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_d^{m_d} = \gamma, \end{aligned}$$

in other words, $\sigma(\gamma) = \gamma$. Since γ was an arbitrary element of L, we conclude that σ fixes all of L, so that $\sigma = \mathrm{Id}_L$.

Remark. This question is asking about a principle (and the argument behind it) that we have used several times : if L is generated over K by a set S, and if $\sigma \in \mathrm{Aut}(L/K)$ fixes all the elements in S, then σ must fix all of L, and hence $\sigma = \mathrm{Id}_L$.

(c) The kernel of the homomorphism $\varphi \colon G \longrightarrow \mathrm{Perm}(G)$ consists of those automorphism which permute S trivially, i.e, those $\sigma \in G$ such that $\sigma(\alpha_i) = \alpha_i$ for all $\alpha_i \in S$. By part (b) the only such $\sigma \in G$ is $\sigma = \mathrm{Id}_L$, which is the identity of G. Therefore $\ker \varphi = \{\mathrm{Id}_L\}$, and so φ is injective.

(d) Let α_i and α_j be any two roots. As noted above, $p(x)$ is irreducible and (up to scaling to make it monic) is the minimal polynomial of both α_i and α_j. By the theorem on simple extensions we therefore have an isomorphism

$$\varphi \colon K(\alpha_i) \cong \frac{K[x]}{(p(x))} \cong K(\alpha_j),$$

which takes α_i to α_j and acts as the identity on K. We lift this automorphism to a map $\sigma \colon L \longrightarrow L$ by using the lifting lemma.

$$\begin{tikzcd} L \arrow[r, dashed, "\sigma"] \arrow[d, dash] & L \arrow[d, dash] \\ K(\alpha_i) \arrow[r, "\sim"', "\varphi"] & K(\alpha_j) \end{tikzcd}$$

We need to check that the hypothesis of the lifting lemma is satisfied. Since L is generated over K by $\alpha_1, \ldots, \alpha_d$, it is certainly true that $\alpha_1, \ldots, \alpha_d$ generate L over the larger field $K(\alpha_i)$. Pick α_ℓ, and let $q_\ell(x) \in K(\alpha_i)$ be the minimal polynomial of α_ℓ over $K(\alpha_i)$. Since α_ℓ is also root of $p(x)$, we have $q_\ell(x) \mid p(x)$. Therefore $\varphi(q_\ell(x))$ divides $\varphi(p(x)) = p(x)$. (The equality $\varphi(p(x)) = p(x)$ follows since all coefficients of $p(x)$ are in K, and φ fixes K.) Since $p(x)$ splits completely in L, $\varphi(q_\ell(x))$ also must split completely in L and so the hypothesis of the lifting lemma is satisfied.

Thus by the lifting lemma there exists $\sigma \colon L \longrightarrow L$ lifting φ.
The map ψ must be an isomorphism since it is an injective
map between K vector spaces of the same dimension. Thus σ is an automorphism of L, and $\sigma(\alpha_i) = \alpha_j$. Since α_i and α_j were arbitrary, this shows that G acts transitively on S.

Remarks. (1) This argument, using the lifting lemma to find an automorphism which takes one root of an irreducible polynomial to another, is also one which we have been using when studying Galois groups in particular examples. (2) As part of this argument, we have verified something which has previously been passed over in silence : when using the inductive part of the lifting lemma, how do we know that the new larger field still satisfies the hypothesis of the lifting lemma? The argument here shows how to use the fact that the new minimal polynomial in the larger field will have to divide the old minimal polynomial from the smaller field, and the fact that the hypothesis held for the smaller field, to deduce that the hypothesis holds for the larger field.

(e) By picking a bijection of $\alpha_1, \ldots, \alpha_d$ (for instance, $\alpha_i \leftrightarrow i$) we obtain an isomorphism of $\mathrm{Perm}(S)$ with S_d. Combining this with the homomorphism $G \longrightarrow \mathrm{Perm}(S)$ from the action of G on S, we get a homomorphism $G \longrightarrow S_d$. By part (c) this homomorphism is injective. By part (d) G acts transitively on S and hence its image in S_d acts transitively on $\{1, \ldots, d\}$.

Remark. In trying to identify and understand Galois groups, one of our tools has been looking for ways to represent the group concretely. For instance, each $\sigma \in \mathrm{Gal}(L/K)$ is a K-linear transformation, so we could write down the matrix associated to σ. On the other hand, when studying extensions like $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ and $\mathbb{Q}(5^{\frac{1}{4}}, i)/\mathbb{Q}$ it was convenient to understand G by studying how G permuted the generators and the other roots of their minimal polynomials. This problem is applying that idea to the case that L/K is generated by the roots of a single irreducible polynomial. Then we know that G can be realized as a transitive subgroup of S_d, a result we will use in developing algorithms for finding Galois groups.

2. Let $K = \mathbb{Q}$, and $\zeta = e^{2\pi i/7}$. By **H3** Q1, the minimal polynomial of ζ over $\mathbb{Q}$ is $q(x) = x^6 + x^5 + x^5 + x^3 + x^2 + x + 1 = \frac{x^7-1}{x-1}$.

(a) Show that all other roots of $q(x)$ are powers of ζ, and explain why this shows that $L = \mathbb{Q}(\zeta)$ is the splitting field for $q(x)$.

(b) Let $G = \mathrm{Gal}(L/\mathbb{Q})$. For $\sigma \in G$, explain why σ is completely determined by what it does to ζ. (i.e., once you know what $\sigma(\zeta)$ is, you know how σ acts on all of L.)

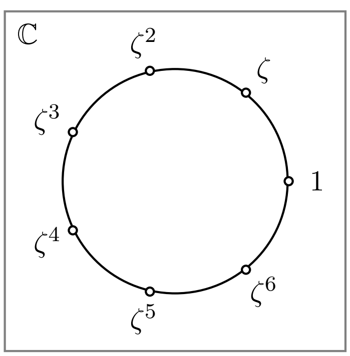
(c) Compute the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$. (Keeping in mind part (b) of this question, and part (d) of question 1 may help, but don't get hung up on it if it doesn't.)

(d) Describe the subgroups of G, and draw the corresponding diagram of intermediate fields between $\mathbb{Q}$ and L.

(e) Compute the Galois groups for the extensions $\mathbb{Q}(\cos(\frac{2\pi}{7}))/\mathbb{Q}$ and $\mathbb{Q}(i\sin(\frac{2\pi}{7}))/\mathbb{Q}$, where $i = \sqrt{-1}$. (Note: These are subfields of L.)

Solution.

(a) For any $m \in \mathbb{Z}$, we have $(\zeta^m)^7 = (e^{2m\pi i/7})^7 = e^{2m\pi i} = 1$, that is, all powers of ζ satisfy the equation $x^7 - 1 = 0$. For $m = 1, \ldots, 6$ these powers are distinct, and not equal to 1.



In fact, as we know, the powers ζ^m, $m = 0, \ldots, 6$ are all of the 7-th roots of unity, distributed in a 7-gon (i.e, a heptagon) with one of the vertices at $1 \in \mathbb{C}$.

Since the ζ^m, $m = 1, \ldots, 6$ are not equal to 1, they are roots of $\frac{x^7-1}{x-1} = q(x)$. Since $q(x)$ has degree 6, the elements $\zeta^1, \ldots, \zeta^6$ are all the roots of $q(x)$.

Thus $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^1, \zeta^2, \ldots, \zeta^6)$ is generated by the roots of $q(x)$, and so is the splitting field for $q(x)$ over $\mathbb{Q}$.

(b) Since ζ generates L over $\mathbb{Q}$, once we know what $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ does to ζ, we can deduce what σ does to any element of L. Specifically, since $q(x)$ has degree 6, we know that $1, \zeta, \zeta^2, \ldots, \zeta^5$ is a basis for L over $\mathbb{Q}$, so that any $\gamma \in L$ can be written $\gamma = c_0 \cdot 1 + c_1\zeta + c_2\zeta^2 + \cdots c_5\zeta^5$ with $c_0, \ldots, c_5 \in \mathbb{Q}$. Then $\sigma(\gamma) = c_0 \cdot 1 + c_1\sigma(\zeta) + \cdots + c_5\sigma(\zeta)^5$, i.e, what σ does to ζ completely determines what σ does to any other element of L.

(c) By part (b), to understand $G = \mathrm{Gal}(L/\mathbb{Q})$ we only need to pay attention to what σ does to ζ. By Q1(d), for each m, $m = 1, \ldots, 6$, there is a $\sigma_m \in G$ such that $\sigma_m(\zeta) = \zeta^m$. Since these elements do different things to ζ, they must all be distinct, and so we have 6 different elements of G. Since $|G| = [L : \mathbb{Q}] = \deg q(x) = 6$, these are all the elements of G.

For reference, here is what each of the σ_m to do the powers $\zeta, \ldots, \zeta^6$ of ζ :

	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6
σ_1	ζ	ζ^2	ζ^3	ζ^4	ζ^5	ζ^6
σ_2	ζ^2	ζ^4	ζ^6	ζ	ζ^3	ζ^5
σ_3	ζ^3	ζ^6	ζ^2	ζ^5	ζ	ζ^4
σ_4	ζ^4	ζ	ζ^5	ζ^2	ζ^6	ζ^3
σ_5	ζ^5	ζ^3	ζ	ζ^6	ζ^4	ζ^2
σ_6	ζ^6	ζ^5	ζ^4	ζ^3	ζ^2	ζ

In making the table we used the rule that $\zeta^m = \zeta^{m'}$ if $m \equiv m' \pmod 7$.

Now which group is G? Let us try and figure out the rule of composition. For any m and n, we have $\sigma_m(\sigma_n(\zeta)) = \sigma_m(\zeta^n) = \zeta^{mn}$. Let r be the element of $\{1, \ldots, 6\}$ which is congruent to mn mod 7. We then have

$$\sigma_m(\sigma_n(\zeta)) = \zeta^{mn} = \zeta^r = \sigma_r(\zeta).$$

Since any element of G is completely determined by what it does to ζ, this tells us we must have $\sigma_m\sigma_n = \sigma_r$. Thus the law of composition in G is

$$\sigma_m\sigma_n = \sigma_{mn \bmod 7}.$$

From this we can write down the multiplication table for the group :

$\circ$	$\boldsymbol{\sigma_1}$	$\boldsymbol{\sigma_2}$	$\boldsymbol{\sigma_3}$	$\boldsymbol{\sigma_4}$	$\boldsymbol{\sigma_5}$	$\boldsymbol{\sigma_6}$
$\boldsymbol{\sigma_1}$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
$\boldsymbol{\sigma_2}$	σ_2	σ_4	σ_6	σ_1	σ_3	σ_5
$\boldsymbol{\sigma_3}$	σ_3	σ_6	σ_2	σ_5	σ_1	σ_4
$\boldsymbol{\sigma_4}$	σ_4	σ_1	σ_5	σ_2	σ_6	σ_3
$\boldsymbol{\sigma_5}$	σ_5	σ_3	σ_1	σ_6	σ_4	σ_2
$\boldsymbol{\sigma_6}$	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

We can also recognize the group. The law of composition is telling us that G is isomorphic to the group of units mod 7, i.e., to the multiplicative group of $\mathbb{F}_7$. We know that this group is cyclic, and hence our group G is the cyclic group of order 6.

A cyclic group of order 6 has two generators. In this case, σ_3 and σ_5 are generators (i.e., have order 6). The elements of order 3 are σ_2 and σ_4, the element of order 2 is σ_6, and the identity is σ_1.

(d) A cyclic group of order 6 has proper subgroups of orders 2 and 3. By looking at the orders of the elements from (c), we see that the subgroups are $\{\sigma_1, \sigma_5\}$ and $\{\sigma_1, \sigma_2, \sigma_4\}$. Here are the lattices of subgroups and intermediate fields.

(Reversed) lattice of subgroups

$$\begin{tikzcd}[column sep=small]
 & \{\sigma_1\} \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\{\sigma_1,\sigma_6\} \arrow[dr, dash, "3"'] & & \{\sigma_1,\sigma_2,\sigma_4\} \arrow[dl, dash, "2"] \\
 & G &
\end{tikzcd}$$

and

Lattice of intermediate fields

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\zeta) \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\mathbb{Q}(\zeta+\zeta^6) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\sqrt{7}i) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Let us now check that these intermediate fields are correct. Set $H_1 = \{\sigma_1, \sigma_5\}$. From the table we see that σ_5 exchanges ζ and ζ^6, ζ^2 and ζ^5, ζ^3 and ζ^4. (in fact, since $\zeta^6 = \zeta^{-1} = \overline{\zeta}$, we see that σ_6 is the restriction of complex conjugation to $\mathbb{Q}(\zeta)$). Using the formula $\zeta^6 = -(\zeta^5 + \zeta^4 + \cdots + \zeta + 1)$ (deduced from $p(\zeta) = 0$), we see that the action of σ_5 on an element $\gamma = c_0 + \cdots + c_5\zeta^5 \in \mathbb{Q}(\zeta)$ is :

$$c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3+c_4\zeta^4+c_5\zeta^5 \xrightarrow{\sigma_6}$$

$$(c_0-c_1)-c_1\zeta+(c_5-c_1)\zeta^2+(c_4-c_1)\zeta^3+(c_3-c_1)\zeta^4+(c_2-c_1)\zeta^5.$$

Comparing coefficients gives the equations

$$\begin{array}{rclrclrcl}
c_0 & = & c_0 - c_1; & c_1 & = & -c_1; & c_2 & = & c_5 - c_1; \\
c_3 & = & c_4 - c_1; & c_4 & = & c_3 - c_1; & c_5 & = & c_2 - c_1.
\end{array}$$

These equations reduce to $c_1 = 0$, $c_2 = c_5$ and $c_3 = c_4$, showing us that a basis for L^{H_1} over $\mathbb{Q}$ is 1, $\zeta^2 + \zeta^5$, and $\zeta^3 + \zeta^4$. Since $(\zeta^2 + \zeta^5)^2 - 2 = (\zeta^4 + 2\zeta^7 + \zeta^{10}) - 2 = \zeta^3 + \zeta^4$, we see that $\zeta^2 + \zeta^5$ generates L^{H_1} over $\mathbb{Q}$. Therefore $L^{H_1} = \mathbb{Q}(\zeta^2 + \zeta^5)$.

There are other possible generators for this field which are useful to know. For instance, $\zeta + \zeta^6$ is an element of L^{H_1}. Using the relation for ζ^6 above, we have $\zeta + \zeta^6 = 1 - (\zeta^2 + \zeta^5) - (\zeta^3 + \zeta^4) \in L^{H_1}$. Since $(\zeta + \zeta^6)^2 - 2 = \zeta^2 + \zeta^5$, we see that $\zeta + \zeta^6$ also generates L^{H_1} over $\mathbb{Q}$, i.e., $L^{H_1} = \mathbb{Q}(\zeta + \zeta^6)$. Since this description will be useful for question (e) below, this is the description used in the lattice above. Finally, $(\zeta^3 + \zeta^4)^2 - 2 = \zeta + \zeta^6$, so $\zeta^3 + \zeta^4$ is another generator of L^{H_1}.

Now let $H_2 = \{\sigma_1, \sigma_2, \sigma_4\}$. Being fixed by H_2 is the same as being fixed by σ_2, which generates H_2. Acting on the powers of ζ, σ_2 cycles them in groups of 3: $\zeta \mapsto \zeta^2 \mapsto \zeta^4 \mapsto \zeta$ and $\zeta^3 \mapsto \zeta^6 \mapsto \zeta^5 \mapsto \zeta^3$. Once again using the relation for ζ^6, this means that σ_2 has the following effect on a general $\gamma \in L$:

$$c_0+c_1\zeta+c_2\zeta^2+c_3\zeta^3+c_4\zeta^4+c_5\zeta^5 \xrightarrow{\sigma_2}$$

$$(c_0 - c_3) + c_4\zeta + c_1\zeta^2 + (c_5 - c_3)\zeta^3 + c_2\zeta^4 - c_3\zeta^5.$$

Comparing coefficients gives the equations

$$\begin{array}{rclrclrcl} c_0 &=& c_0 - c_3; & c_1 &=& c_4; & c_2 &=& c_1; \\ c_3 &=& c_5 - c_3; & c_4 &=& c_2; & c_5 &=& -c_3. \end{array}$$

These equations reduce to : $c_1 = c_2 = c_4$, $c_3 = c_5 = 0$, showing us that a basis for L^{H_2} over $\mathbb{Q}$ is 1, $\zeta + \zeta^2 + \zeta^4$. In particular we have $\mathrm{L}^{H_2} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$.

We can try and simplify this expression. Let $\gamma = \zeta + \zeta^2 + \zeta^4$. Then $\gamma^2 = \zeta+\zeta^2+2\zeta^3+\zeta^4+2\zeta^5+2\zeta^6 = 2(\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6)-\gamma = 2(-1)-\gamma = -\gamma-2$. Therefore $\gamma^2 + \gamma + 2 = 0$, and γ is a root of $p(x) = x^2 + x + 2$. By the quadratic formula, the roots of $p(x)$ are $\frac{1}{2}\left(-1 \pm \sqrt{-7}\right)$. Therefore, L^{H_2} is also the field $\mathbb{Q}(\sqrt{-7}) = \mathbb{Q}(\sqrt{7}i)$.

Remark. Some of the computations above could have been simplified slightly with a choice of a different basis for L over $\mathbb{Q}$. Using the relation for ζ^6, the elements ζ, ζ^2, ζ^3, ζ^4, ζ^5, and ζ^6 are a basis for L over $\mathbb{Q}$. The advantage of this basis is that G permutes the elements, so it is easy to find fixed elements — they correspond to sums of basis elements in orbits of the subgroup. For instance the action of σ_6 in this basis is

$$c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 + c_5\zeta^5 + c_6\zeta^6 \xrightarrow{\sigma_6}$$
$$c_6\zeta + c_5\zeta^2 + c_4\zeta^3 + c_3\zeta^4 + c_2\zeta^5 + c_1\zeta^6,$$

from which it is clear that $\zeta+\zeta^6$, $\zeta^2+\zeta^5$, and $\zeta^3+\zeta^4$ are a basis of L^{H_1} over $\mathbb{Q}$. Similarly the action of σ_2 in this basis is

$$c_1\zeta + c_2\zeta^2 + c_3\zeta^3 + c_4\zeta^4 + c_5\zeta^5 + c_6\zeta^6 \xrightarrow{\sigma_6}$$
$$c_4\zeta + c_1\zeta^2 + c_5\zeta^3 + c_2\zeta^4 + c_6\zeta^5 + c_3\zeta^6,$$

from which we see that $\zeta + \zeta^2 + \zeta^4$ and $\zeta^3 + \zeta^5 + \zeta^6$ are a basis for L^{H_2} over $\mathbb{Q}$.

(e) From complex analysis we have the identities $\cos(\theta) = \frac{e^{i\theta}+e^{-i\theta}}{2}$ and $\sin(\theta) = \frac{e^{i\theta}-e^{-i\theta}}{2i}$. With $\theta = \frac{2\pi}{7}$, this gives

$$\cos\left(\tfrac{2\pi}{7}\right) = \frac{e^{\frac{2\pi i}{7}} + e^{-\frac{2\pi i}{7}}}{2} = \frac{\zeta + \zeta^{-1}}{2} = \frac{\zeta + \zeta^6}{2}.$$

and

$$i\sin\left(\tfrac{2\pi}{7}\right) = i\left(\frac{e^{\frac{2\pi i}{7}} - e^{-\frac{2\pi i}{7}}}{2i}\right) = \frac{\zeta - \zeta^{-1}}{2} = \frac{\zeta - \zeta^6}{2}.$$

Therefore $\mathbb{Q}(\cos(\frac{2\pi}{7})) = \mathbb{Q}(\zeta + \zeta^6)$ and $\mathbb{Q}(i\sin(\frac{2\pi}{7})) = \mathbb{Q}(\zeta - \zeta^6)$.

From the Galois correspondence in (d), $\mathbb{Q}(\zeta+\zeta^6)$ is the intermediate field corresponding to H_1 (a normal subgroup, since G is abelian), and hence the Galois group of $\mathbb{Q}(\cos(\frac{2\pi}{7}))/\mathbb{Q}$ is G/H_1, the cyclic group of order 3.

Which intermediate field is $M = \mathbb{Q}(i\sin(\frac{2\pi}{7})) = \mathbb{Q}(\zeta-\zeta^6)$? Perhaps the easiest way to see, which also would have worked for $\mathbb{Q}(\cos(\frac{2\pi}{7}))$, is to ask which subgroups of L fix this field, and use the Galois correspondence. Since $\sigma_6(\zeta-\zeta^6) = \zeta^6-\zeta = -(\zeta-\zeta^6)$, we see that M is not fixed by H_1. Since $\sigma_2(\zeta-\zeta_6) = \zeta^2-\zeta^5 \neq \zeta-\zeta^6$, we see that M is also not fixed by H_2. (And so M also cannot be fixed by G, which contains both.) Therefore, in the lattice of subgroups, the only subgroup left to fix M is $\{\sigma_1\}$. The subgroup $\{\sigma_1\}$ corresponds to the field L, so $\mathbb{Q}\left(\sin(\frac{2\pi}{7})\right) = L = \mathbb{Q}(\zeta)$.

In the next two problems we will explore some further aspects of the Galois correspondence.

3. Recall that a group G is a product $G = H_1 \times H_2$ if and only if there are *normal* subgroups $H_1 \subset G$ and $H_2 \subset G$ such that $H_1 \cap H_2 = \{e\}$ and $H_1 \cdot H_2$ (the subgroup generated by H_1 and H_2) is equal to G.

Suppose that $K \subseteq L$ is a finite Galois extension, and M_1 and M_2 are two intermediate fields such that:

1. Both $K \subseteq M_1$ and $K \subseteq M_2$ are Galois extensions.
2. $M_1 \cap M_2 = K$.
3. The smallest subfield of L containing both M_1 and M_2 is L itself.

(a) If H_1 and H_2 are the subgroups of $G = \mathrm{Aut}(L/K)$ corresponding to M_1 and M_2 under the Galois correspondence, show that $G = H_1 \times H_2$.

(b) Conversely, if the Galois group G is a product $G = H_1 \times H_2$, then show that there are two intermediate fields M_1 and M_2 having properties (1)–(3) above.

(c) Consider again the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ and its intermediate fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. Use (a) to find the Galois group $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. (This justifies the claim about this Galois group from **H6** Q3.)

Solution.

Let L/K be a Galois extension with Galois group G, M_1 and M_2 intermediate fields corresponding to subgroups H_1 and H_2 By the Galois correspondence, we have the following equivalencies :

1.	M_i/K is a Galois extension	if and only if	H_i is a normal subgroup of K
2.	$\min(M_1, M_2) = M_1 \cap M_2 = K$	if and only if	$\max(H_1, H_2) = \langle H_1, H_2 \rangle = G$
3.	$\max(M_1, M_2) = \langle M_1, M_2 \rangle = L$	if and only if	$\min(H_1, H_2) = H_1 \cap H_2 = \{e\}$

In items 2 and 3 we have used the definitions of max and min in the lattices of intermediate fields and subgroups respectively. That is, in the lattice of subgroups, $\min(H_1, H_2) = H_1 \cap H_2$ and $\max(H_1, H_2) = \langle H_1, H_2 \rangle$, the subgroup generated by H_1 and H_2. In the lattice of intermediate fields we have $\min(M_1, M_2) = M_1 \cap M_2$ and $\max(M_1, M_2) = \langle M_1, M_2 \rangle$, i.e., the field generated by M_1 and M_2, or the smallest intermediate field containing M_1 and M_2. In 2 and 3 the equivalencies follow since, being an order-reversing bijection of lattices, the Galois correspondence switches the max and min.

(a) By the above equivalencies, the conditions stated are equivalent to the conditions that H_1 and H_2 are normal subgroups of G, that $H_1 \cap H_2 = \{e\}$, and that H_1 and H_2 generate G. In turn, this is equivalent to the statement that $G = H_1 \times H_2$.

(b) On the other hand, if $G = H_1 \times H_2$ then we have normal subgroups H_1 and H_2 which generate G and such that $H_1 \cap H_2 = \{e\}$. By the equivalencies above, the corresponding intermediate fields M_1 and M_2 satisfy $M_1 \cap M_2 = K$, L is the smallest subfield containing M_1 and M_2, and that both M_1/K and M_2/K are Galois extensions.

(c) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, with intermediate fields $M_2 = \mathbb{Q}(\sqrt{2})$, $M_1 = \mathbb{Q}(\sqrt{3})$ over $K = \mathbb{Q}$. The smallest field containing M_1 and M_2 will have to contain $\sqrt{2}$, $\sqrt{3}$, and $\mathbb{Q}$, and so contain $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conversely, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ contains both M_1 and M_2, so L is the smallest field containing M_1 and M_2. Both $M_1/\mathbb{Q}$ and $M_2/\mathbb{Q}$ are degree 2 extensions, and hence Galois extensions (in characteristic $\neq 2$). Finally, we have checked several times that $M_1 \cap M_2 = \mathbb{Q}$. For instance, if $M_1 \cap M_2 \neq \mathbb{Q}$, then $M_1 \cap M_2$ is a subfield of each of M_1 and M_2 larger than $\mathbb{Q}$, and so for degree reasons we would have to have $M_1 = M_1 \cap M_2 = M_2$. But we have shown in **H1** Q3(c) that $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$.

Therefore, M_1 and M_2 satisfy the conditions above. Setting $H_1 = \mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and $H_2 = \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, we therefore have that $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = H_1 \times H_2$.

The composition $H_1 \hookrightarrow G \longrightarrow G/H_2$ is an isomorphism, and $G/H_2 = \mathrm{Gal}(M_2/\mathbb{Q})$. Let σ_1 be the generator of $\mathrm{Gal}(M_2/\mathbb{Q})$ (so that $\sigma_1(\sqrt{2}) = -\sqrt{2}$), also use the name

σ_1 for the corresponding element of H_1 under the isomorphism. Similarly, we let σ_2 be the generator of $H_2 \cong G/H_1 \cong \mathrm{Gal}(M_1/\mathbb{Q})$ (so that $\sigma_2(\sqrt{3}) = -\sqrt{3}$). We then have that the elements of G are :

$$\begin{aligned} e &= (e_1, e_2), \\ \tau_1 &= (\sigma_1, e_2), \\ \tau_2 &= (e_1, \sigma_2), \\ \tau_1\tau_2 &= (\sigma_1, \sigma_2), \end{aligned}$$

exactly as claimed in **H6** Q3. Note that, since H_1 fixes M_1 and H_2 fixes M_2, we also know that $\tau_1(\sqrt{3}) = \sqrt{3}$ and $\tau_2(\sqrt{2}) = \sqrt{2}$.

4. Suppose that L/K is a Galois extension with Galois group G, and let $M_1 \subseteq M_2$ be intermediate fields, corresponding to subgroups H_1 and H_2 of G.

(a) What condition on H_1 and H_2 is equivalent to the condition that "M_2/M_1 is a Galois extension"?

(b) Given that this condition on groups holds, what is $\mathrm{Gal}(M_2/M_1)$, i.e., how do you compute $\mathrm{Gal}(M_2/M_1)$ from H_1 and H_2?

Solution.

(a) Since $M_1 \subset M_2$ we have $H_2 \subset H_1$ be the Galois correspondence. In fact, restricting the intermediate fields to those intermediate fields containing M_1, we have that L/M_1 is a Galois extension with Galois group H_1, and the intermediate field $M_1 \subseteq M_2 \subseteq L$ corresponds to the subgroup H_1. By the Galois correspondence, M_2/M_1 is a Galois extension if and only if H_2 is a normal subgroup of H_1.

(b) If M_2/M_1 is a Galois extension (so that H_2 is a normal subgroup of H_1), then by the Galois correspondence $\mathrm{Gal}(M_2/M_1) = H_1/H_2$.