1 (a)

Since α_1, α_2, α_3, α_4 are the roots, we have

$$f(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4). \quad (1)$$

Expanding out and collecting terms, the coefficient of X^3 is $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$. Equating the coefficients we have the result.

(b)

$$\beta + \gamma + \delta = 3\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 2\alpha_1 + (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) = 2\alpha_1,$$

using (a).

$$\beta - \gamma - \delta = \alpha_2 - \alpha_3 - \alpha_1 - \alpha_4 = 2\alpha_1 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) = 2\alpha_2,$$

using (a).

Others similar.

(c)

Using (a) repeatedly,

$$\begin{aligned}
\beta^2 &= (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4),\\
\gamma^2 &= (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\alpha_1\alpha_2 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_3\alpha_4),\\
\delta^2 &= (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) = -(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4).
\end{aligned}$$

Adding we get

$$\beta^2 + \gamma^2 + \delta^2 = -2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4).$$

Expanding out (1), the coefficient p of X^2 is $(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4)$.

Others similar.

(d)

$$(Y - \beta^2)(Y - \gamma^2)(Y - \delta^2) = Y^3 - (\beta^2 + \gamma^2 + \delta^2)Y^2 + (\beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2)Y - \beta^2\gamma^2\delta^2.$$

So, using (c), this is

$$Y^3 + 2pY^2 + (p^2 - 4r)Y - q^2.$$

(e)

Write r_1, r_2, r_3 for the roots of the cubic in (d).

Choose square roots of r_1 and r_2 and write $\beta = \sqrt{r_1}$ and $\gamma = \sqrt{r_2}$.

Then $\delta = -\frac{q}{\beta\gamma}$. (If β or γ is zero then $Y = 0$ is a solution and the cubic reduces to a quadratic.)

Now determine α_1, α_2, α_3, α_4 from (b).

(f)

We have $p = 2$, $q = 4$, $r = 2$ so the resolvent cubic is

$$Y^3 + 4Y^2 - 4Y - 16 = (Y - 2)(Y^2 + 6Y + 8) = (Y - 2)(Y + 2)(Y + 4).$$

The roots are $2, -2, -4$.

Take $\beta^2 = 2$, $\gamma^2 = -4$, $\delta^2 = -2$ and

$$\beta = \sqrt{2}, \qquad \gamma = 2i, \qquad \delta = i\sqrt{2}.$$

Then

$$\alpha_1 = \tfrac{1}{2}(\sqrt{2} + i(2 + \sqrt{2})), \quad \alpha_2 = \tfrac{1}{2}(\sqrt{2} - i(2 + \sqrt{2})),$$
$$\alpha_3 = \tfrac{1}{2}(-\sqrt{2} + i(2 - \sqrt{2})), \quad \alpha_4 = \tfrac{1}{2}(-\sqrt{2} - i(2 - \sqrt{2})).$$

Q2 (a), (b)

First, $\alpha^2 = 4 + \sqrt{7}$ and then $(\alpha^2 - 4)^2 = 7$ so α is a root of $x^4 - 8x^2 + 9$.

Now $(x+1)^4 - 8(x+1)^2 + 9 = x^4 + 4x^3 - 2x^2 - 12x + 2$ so by shifted Eisenstein at 2, we have that $x^4 - 8x^2 + 9$ is irreducible.

Thus the minimal polynomial is $x^4 - 8x^2 + 9$.

Regarding $x^4 - 8x^2 + 9 = 0$ as a quadratic in x^2, the roots are $\pm\alpha$ and $\pm\beta$.

(c)

$\alpha\beta = \sqrt{16 - 7} = 3$ (not -3 since $\alpha, \beta > 0$).

So $\beta = \frac{3}{\alpha} \in \mathbb{Q}(\alpha) = L$.

Hence L is a splitting field for $x^4 - 8x^2 + 9$ and is therefore Galois.

Degree is $4 =$ degree of minimal polynomial.

(d)

Automorphisms permute roots, so the elements of the Galois group are as follows.

	id	φ	ψ	θ
α	α	β	$-\alpha$	$-\beta$
β	β	α	$-\beta$	$-\alpha$

The action of φ, ψ, θ on $-\alpha$ and $-\beta$ is determined, since φ, ψ, θ are field automorphisms.

Note that applying each of φ, ψ, θ to $\alpha\beta$ must result in $3 \in \mathbb{Q}$.

Each element of the Galois group has order 2, so the group must be isomorphic to $C_2 \times C_2$.

(e)

	id	φ	ψ	θ
α^2	α^2	β^2	α^2	β^2
$\alpha + \beta$	$\alpha + \beta$	$\alpha + \beta$	$-\alpha - \beta$	$-\alpha - \beta$
$\alpha - \beta$	$\alpha - \beta$	$\beta - \alpha$	$\beta - \alpha$	$\alpha - \beta$

The subgroup which preserves each element of $\mathbb{Q}(\alpha^2)$ is $\{\mathrm{id}, \psi\}$.

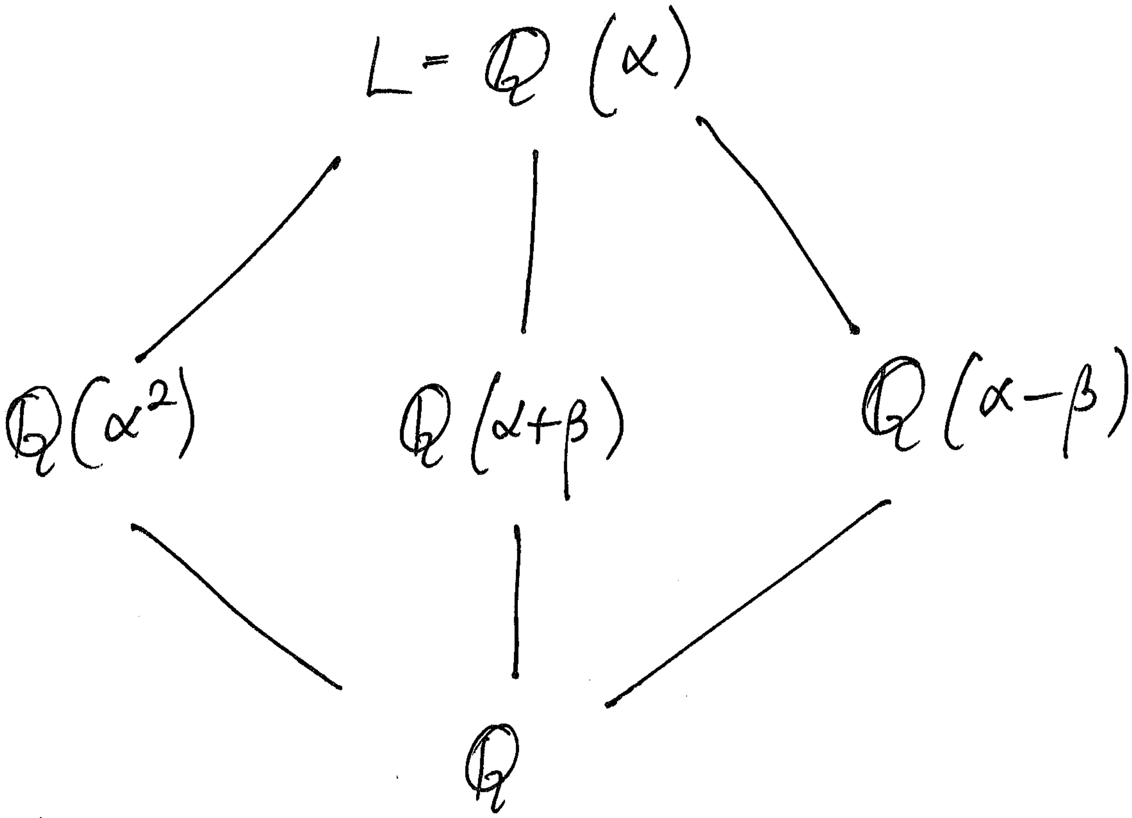
The subgroup which preserves each element of $\mathbb{Q}(\alpha + \beta)$ is $\{\mathrm{id}, \varphi\}$.

The subgroup which preserves each element of $\mathbb{Q}(\alpha - \beta)$ is $\{\mathrm{id}, \theta\}$.

(f)

The Galois group $C_2 \times C_2$ has exactly five subgroups, namely the three identified in (e) plus the trivial subgroup and $C_2 \times C_2$ itself.

The subfield lattice is therefore



Q3(i)

(a)

Note that $\alpha^2 + 4 = 3\sqrt{2} = \sqrt{18}$, and squaring again shows that $\alpha^4 + 8\alpha^2 + 16 = 18$, as required.

Thus α is a root. Further, as f is a polynomial in x^2, $-\alpha$ must also be a root.

Write $\pm\beta$ for the other roots. Because the product of all the roots is -2, it follows that $\pm\beta = \pm\frac{i\sqrt{2}}{\alpha}$, as required.

(b) The extension is Galois (since it is a splitting field) and is of degree 8. So the Galois group has order 8.

Any automorphism is uniquely determined by its action on α and $i\sqrt{2}$.

α must be mapped to another root of $f(x)$, by APR.

$i\sqrt{2}$ must be mapped to another root of $x^2 + 2$, its minimal polynomial; that is, to $\pm i\sqrt{2}$.

effect on α	effect on $i\sqrt{2}$
α	$i\sqrt{2}$
α	$-i\sqrt{2}$
$-\alpha$	$i\sqrt{2}$
$-\alpha$	$-i\sqrt{2}$
$\frac{i\sqrt{2}}{\alpha}$	$i\sqrt{2}$
$\frac{i\sqrt{2}}{\alpha}$	$-i\sqrt{2}$
$-\frac{i\sqrt{2}}{\alpha}$	$i\sqrt{2}$
$-\frac{i\sqrt{2}}{\alpha}$	$-i\sqrt{2}$

This determines 8 possibilities and so is the complete list of elments of $\mathrm{Gal}(L/\mathbb{Q})$.

(c) Let φ be the automorphism sending α to $\frac{i\sqrt{2}}{\alpha}$ and $i\sqrt{2}$ to $-i\sqrt{2}$.

Claim that φ has order 4.

$$\varphi^2(\alpha) = \varphi(\tfrac{i\sqrt{2}}{\alpha}) = \tfrac{\varphi(i\sqrt{2})}{\varphi(\alpha)} = \tfrac{-i\sqrt{2}}{i\sqrt{2}/\alpha} = -\alpha$$
$$\varphi^2(i\sqrt{2}) = \varphi(-i\sqrt{2}) = -\varphi(i\sqrt{2}) = i\sqrt{2}$$

so φ^2 fixes $i\sqrt{2}$ and sends α to $-\alpha$.

Then $\varphi^4 = (\varphi^2)^2$ is the identity. So φ has order 4.

Let ψ be any element of order 2 not equal to φ^2, such as the automorphism sending α to α and $i\sqrt{2}$ to $-i\sqrt{2}$.

The group generated by φ and ψ contains a subgroup of order 4, and so by Lagrange must have order $4n$ for some n. It also contains ψ, so the order must be greater than 4, and therefore must be 8. So $\mathrm{Gal}(M/\mathbb{Q}) = \langle\varphi, \psi\rangle$.

(d) Note that

$$\psi\varphi\psi^{-1}(\alpha) = \psi\varphi(\alpha) = \psi(\tfrac{i\sqrt{2}}{\alpha}) = \tfrac{\psi(i\sqrt{2})}{\psi(\alpha)} = -\tfrac{i\sqrt{2}}{\alpha}$$
$$\psi\varphi\psi^{-1}(i\sqrt{2}) = \psi\varphi(-i\sqrt{2}) = \psi(i\sqrt{2}) = -i\sqrt{2}.$$

One easily sees that now $\psi\varphi\psi^{-1} = \varphi^{-1}$.

It follows that the group is isomorphic to D_4, the group of symmetries of a square.

Other choices are possible for φ and ψ in (c) and will mean that the detail of (d) is different; however the argument will be very similar.

Q4(i)

(a) A group G is *soluble* if there is a chain of subgroups

$$G = G_0 > G_1 > \cdots > G_n = \{1\}$$

with each G_{i+1} normal in G_i and G_i/G_{i+1} abelian.

(b)

$$1 \triangleleft C_2 \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$$

where $V_4 = \{(1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3),\ \mathrm{id}\}$.

The first quotient is C_2, cyclic so abelian.

For the second quotient, V_4 has order 4 and C_2 has order 2, so C_2 has index 2 in V_4 and is therefore normal. And V_4/C_2 has order 2 so is cyclic and therefore abelian.

For the third quotient, recall that conjugation in S_n preserves the cycle structure. Since V_4 contains every transposition pair in A_4, every conjugate of an element of V_4 is in V_4. Therefore V_4 is normal in A_4 (and in fact is normal in S_4). And A_4/V_4 has order $12/4 = 3$ so is cyclic and therefore abelian.

For the final quotient, A_4 has index 2 in S_4 and is therefore a normal subgroup. And S_4/A_4 has order $24/12 = 2$ so is cyclic and therefore abelian.

(ii)

(a) First, transposition pairs $(a\,b)(c\,d)$ where a, b, c, d are all distinct.

Next, 3-*cycles* $(a\,b\,c)$ where a, b, c are all distinct.

Lastly, 5-*cycles* $(a\,b\,c\,d\,e)$ where a, b, c, d, e are all distinct.

(b) Since g and g' have the same cycle type, they are conjugate in S_5; that is, there is a $y \in S_5$ such that $ygy^{-1} = g'$. If $y \in A_5$ then there is nothing further to prove.

If $y \notin A_5$ then $xy \in A_5$ since both x and y are odd. And

$$(yx)g(yx)^{-1} = y(xgx^{-1})y^{-1} = ygy^{-1} = g'.$$

So g and g' are conjugate in A_5.

(c) Consider any two transposition pairs, $(a\,b)(c\,d)$ and $(a'\,b')(c'\,d')$. The transposition $(a\,b)$ commutes with $(a\,b)(c\,d)$, so, using (b), we get that $(a\,b)(c\,d)$ and $(a'\,b')(c'\,d')$ are conjugate in A_5.

Consider any two 3-cycles $(a\,b\,c)$ and $(a'\,b'\,c')$. Take d and e such that a, b, c, d, e are all distinct. Then $(d\,e)$ commutes with $(a\,b\,c)$ so by (b), $(a\,b\,c)$ and $(a'\,b'\,c')$ are conjugate in A_5.

(d) Suppose N contains a 3-cycle. Then since it is normal, N contains all 3-cycles, in particular $n = (1\,2\,3)$. Write $g = (1\,2)(3\,4) \in A_5$. Then

$$gng^{-1}n^{-1} = (1\,3)(2\,4).$$

But $gng^{-1} \in N$ since N is normal, so $(1\,3)(2\,4) \in N$. By (c), N contains all transposition pairs.

(e) Suppose N contains a transposition pair. Then since it is normal, it contains all transposition pairs. So with $n = (1\,2)(3\,4)$ and $n' = (1\,2)(3\,5)$, we have

$$nn' = (3\,5\,4) \in N$$

and since N is normal, it contain all 3-cycles.

(f) Suppose that N contains a 5-cycle. Relabel the symbols so that $n = (1\,2\,3\,4\,5) \in N$.

With $g = (1\,2\,3) \in A_5$ we have

$$ngn^{-1}g^{-1} = (1\,4\,2)$$

and $ngn^{-1}g^{-1} = n(gn^{-1}g^{-1}) \in N$.

(g) Since N is nontrivial it must contain a transposition pair or a 3-cycle or a 5-cycle.
By (d), (e) and the given information, it follows that N contains all transposition pairs and all 3-cycles.

Now consider any element g of A_5. It is a product of an even number of transpositions. Group these in pairs, so that

$$g = t_1 t_1' \, t_2 t_2' \dots t_r t_r'$$

for some r.

Now for each pair $t_i t_i'$ there are three possibilities.

If $t_i = t_i'$ then the product is the identity and this pair can be removed.

If t_i and t_i' are disjoint then their product is a transposition pair and is therefore in N.

If t_i and t_i' are not disjoint then their product is a 3-cycle and is therefore in N.

So g is a product of elements of N and is therefore in N. This proves that $N = A_5$.