Galois theory — All exam questions

(1) Put $L = \mathbb{Q}(\sqrt{7}, \sqrt{13})$ and $\alpha = \sqrt{7} + \sqrt{13} \in L$.

(a) Give a basis for L over $\mathbb{Q}$. **(2 marks)**

(b) Define the Galois group $G(L/\mathbb{Q})$, and list all its elements. **(3 marks)**

(c) Let $\alpha_0, \dots, \alpha_r$ be the images of α under all the automorphisms of L. Calculate the sum $\alpha_0 + \dots + \alpha_r$ and the product $\alpha_0\alpha_1 \cdots \alpha_r$. **(4 marks)**

(d) Find a monic polynomial $f(x)$ of degree four over $\mathbb{Q}$ such that $f(\alpha) = 0$. **(3 marks)**

(e) Consider an element $a = w + x\sqrt{7} + y\sqrt{13} + z\sqrt{91} \in L$, and suppose that $a^2 \in \mathbb{Q}$. By considering the action of automorphisms on a and a^2, prove that

$$a \in \mathbb{Q} \cup \mathbb{Q}.\sqrt{7} \cup \mathbb{Q}.\sqrt{13} \cup \mathbb{Q}.\sqrt{91}.$$

(7 marks)

(f) Describe all the subfields K with $\mathbb{Q} \subseteq K \subseteq L$, justifying your answer briefly. For each such field K, state the values of $[L : K]$ and $[K : \mathbb{Q}]$. **(6 marks)**

Solution: Parts (a), (b), (d) and (f) are standard, and very similar to examples in the notes and exercises. Part (c) will not be familiar but nonetheless is easy. Part (e) is intended to be more challenging.

(a) The list $1, \sqrt{7}, \sqrt{13}, \sqrt{7}\sqrt{13}$ is a basis for L over $\mathbb{Q}$. [2]

(b) $G(L/\mathbb{Q})$ is the group of automorphisms of L (that act as the identity on $\mathbb{Q}$). [1]There are four such automorphisms, as follows:

$$\begin{aligned}
\sigma_0(w + x\sqrt{7} + y\sqrt{13} + z\sqrt{7}\sqrt{13}) &= w + x\sqrt{7} + y\sqrt{13} + z\sqrt{7}\sqrt{13} \\
\sigma_1(w + x\sqrt{7} + y\sqrt{13} + z\sqrt{7}\sqrt{13}) &= w - x\sqrt{7} + y\sqrt{13} - z\sqrt{7}\sqrt{13} \\
\sigma_2(w + x\sqrt{7} + y\sqrt{13} + z\sqrt{7}\sqrt{13}) &= w + x\sqrt{7} - y\sqrt{13} - z\sqrt{7}\sqrt{13} \\
\sigma_3(w + x\sqrt{7} + y\sqrt{13} + z\sqrt{7}\sqrt{13}) &= w - x\sqrt{7} - y\sqrt{13} + z\sqrt{7}\sqrt{13}.[2]
\end{aligned}$$

(c) The relevant images are

$$\begin{aligned}
\alpha_0 &= +\sqrt{7} + \sqrt{13} & \alpha_1 &= -\sqrt{7} + \sqrt{13} \\
\alpha_2 &= +\sqrt{7} - \sqrt{13} & \alpha_3 &= -\sqrt{7} - \sqrt{13}.[1]
\end{aligned}$$

From this it is clear that $\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 = 0$ [1]. We also have $\alpha_0\alpha_1 = (\sqrt{7})^2 - (\sqrt{13})^2 = 7 - 13 = -6$ and similarly $\alpha_2\alpha_3 = -6$ so $\alpha_0\alpha_1\alpha_2\alpha_3 = 36$. [2]

(d) We have $\alpha^2 = 7 + 2\sqrt{7}\sqrt{13} + 13 = 20 + 2\sqrt{91}$ [1], so $(\alpha^2 - 20)^2 = 4 \times 91 = 364$ [1]. Thus, if we put $f(x) = (x^2 - 20)^2 - 364 = x^4 - 40x^2 + 36$ then $f(\alpha) = 0$ [1].

(e) Consider an element $a = w + x\sqrt{7} + y\sqrt{13} + z\sqrt{91} \in K$ with $a^2 \in \mathbb{Q}$. For any automorphism σ_i, we then have $\sigma_i(a)^2 = \sigma_i(a^2) = a^2$, so $\sigma_i(a) = \pm a$ [2]. Recall that

$$\sigma_1(a) = w - x\sqrt{7} + y\sqrt{13} - z\sqrt{7}\sqrt{13}.$$

This is only equal to a if $x = z = 0$, and is only equal to $-a$ if $w = y = 0$ [1]. From this and the parallel arguments for σ_2 and σ_3, we see that

(1) either $w = y = 0$, or $x = z = 0$;

(2) either $w = x = 0$, or $y = z = 0$;

(3) either $w = z = 0$, or $x = y = 0$. [2]

Suppose that $w \neq 0$; then we see from (1) that $x = z = 0$, and from (2) that $y = z = 0$, so $x = y = z = 0$, so $a \in \mathbb{Q}$. Similarly, if $x \neq 0$ we see from (1) that $w = y = 0$, and from (2) that $y = z = 0$, so $w = y = z = 0$ and $a \in \mathbb{Q}.\sqrt{7}$. In the same way, if $y \neq 0$ then $w = x = z = 0$ and $a \in \mathbb{Q}.\sqrt{13}$, and if $z \neq 0$ then $w = x = y = 0$ and $a \in \mathbb{Q}.\sqrt{91}$. [2]

(f) The intermediate fields between $\mathbb{Q}$ and K biject with the subgroups of $G(K/\mathbb{Q})$ [1]. If we put $H_i = \{\sigma_0, \sigma_i\}$ then the full list of subgroups is $\{1\}, H_1, H_2, H_3$ and $G(K/\mathbb{Q})$ itself [2], so the intermediate fields are

$$\begin{aligned} K^{\{1\}} &= K \\ K^{H_1} &= \mathbb{Q}(\sqrt{13}) \\ K^{H_2} &= \mathbb{Q}(\sqrt{7}) \\ K^{H_3} &= \mathbb{Q}(\sqrt{7}\sqrt{13}) \\ K^{G(K/\mathbb{Q})} &= \mathbb{Q}.\end{aligned}$$ [2]

The degrees are $[K : \mathbb{Q}] = 4$ and $[K : K^{H_i}] = [K^{H_i} : \mathbb{Q}] = 2$. [1]

(2)

(a) Define what is meant by an *automorphism* of a field. **(3 marks)**

(b) Let K be an extension field of $\mathbb{Q}$, and let ϕ be an automorphism of K. Prove that $\phi(q) = q$ for all $q \in \mathbb{Q}$. **(5 marks)**

(c) Define the *Galois group* $G(L/K)$ for a field extension $K \leq L$. **(2 marks)**

(d) Show that $G(\mathbb{Q}(i)/\mathbb{Q})$ is a cyclic group of order two. (Your proof should be complete and self-contained, except that you may assume part (b).) **(9 marks)**

(e) Give an example of an extension $K \leq L$ where $[L : K] = 4$ but $|G(L/K)| = 2$. Justify your answer. **(6 marks)**

Solution:

(a) **(Bookwork)** An automorphism of a field K is a bijective [1]map $\phi\colon K \to K$ such that

- $\phi(0) = 0$ and $\phi(1) = 1$. [1]
- $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in K$.
- $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in K$. [1]

(b) **(Bookwork)** Let $\phi\colon K \to K$ be an automorphism, where $\mathbb{Q} \leq K$. We first claim that $\phi(n) = n$ for all $n \in \mathbb{N}$. Indeed, this is true for $n = 0$ and $n = 1$ by the definition of a homomorphism.[1]If $\phi(n) = n$ for some n, it follows that

$$\phi(n + 1) = \phi(n) + \phi(1) = n + 1.$$ [1]

We therefore see by induction that $\phi(n) = n$ for all $n \in \mathbb{N}$. From this, we see that

$$n + \phi(-n) = \phi(n) + \phi(-n) = \phi(n + (-n)) = \phi(0) = 0,$$

which gives $\phi(-n) = -n$ for all $n \in \mathbb{N}$, so $\phi(m) = m$ for all $m \in \mathbb{Z}$ [1]. Now suppose that $n, m \in \mathbb{Z}$ with $n > 0$, and put $q = m/n \in \mathbb{Q}$. As $nq = m$ and $n, m \in \mathbb{Z}$ we have

$$n\,\phi(q) = \phi(n)\phi(q) = \phi(nq) = \phi(m) = m,$$

so $\phi(q) = m/n = q$ [2]. As every element of $\mathbb{Q}$ can be written as m/n for some such m and n, we deduce that $\phi|_{\mathbb{Q}} = 1_{\mathbb{Q}}$ as required.

(c) **(Bookwork)** $G(L/K)$ is defined to be the set of all automorphisms $\theta\colon L \to L$ [1]that satisfy $\theta(a) = a$ for all $a \in K$ [1].

(d) **(This is a rearrangement/specialisation of standard material.)** $\mathbb{Q}(i)$ is the set of complex numbers of the form $a = x + iy$ with $x, y \in \mathbb{Q}$. We can define $\sigma\colon \mathbb{Q}(i) \to \mathbb{Q}(i)$ by $\sigma(x + iy) = x - iy$ [1]. This has $\sigma(0) = 0$ and $\sigma(1) = \sigma(1 + 0i) = 1 - 0i = 1$. If $b = u + iv$ (with $u, v \in \mathbb{Q}$) then it is clear that $\sigma(a + b) = \sigma(a) + \sigma(b)$ [1]. We also have

$$\begin{aligned}\sigma(ab) &= \sigma(xu - yv + (xv + yu)i) = xy - yv - (xv + yu)i \\ &= (x - iy)(y - iv) = \sigma(a)\sigma(b).\text{[1]}\end{aligned}$$

This proves that σ is a homomorphism from $\mathbb{Q}(i)$ to $\mathbb{Q}(i)$. it is also clear that $\sigma^2(a) = \sigma(x - iy) = x + iy = a$ for all a, so σ is its own inverse, so it is an automorphism [1].

Now let $\tau\colon \mathbb{Q}(i) \to \mathbb{Q}(i)$ be an arbitrary automorphism. Note that $\tau(i)^2 + 1 = \tau(i^2 + 1) = \tau(0) = 0$ [1]. From this it is clear that $\tau(i) \in \{i, -i\}$. Note also that $\tau(x) = x$ for all $x \in \mathbb{Q}$ by part (b) [1]. Thus, if $\tau(i) = i$ we have $\tau(x + iy) = \tau(x) + \tau(i)\tau(y) = x + iy$, so $\tau = 1_{\mathbb{Q}(i)}$ [1]. On the other hand, if $\tau(i) = -i$ we have $\tau(x + iy) = \tau(x) + \tau(i)\tau(y) = x - iy = \sigma(x + iy)$ for all x and y, so $\tau = \sigma$ [1]. This proves that $G(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \sigma\}$, which is a cyclic group of order two [1].

(e) **(Unseen)** Take $K = \mathbb{Q}$ and $L = \mathbb{Q}(2^{1/4}) \leq \mathbb{R}$ [3]. As $L \simeq \mathbb{Q}[x]/(x^4 - 2)$ we see that automorphisms of L biject with roots of $x^4 - 2$ in L [2], of which there are precisely two (namely $2^{1/4}$ and $-2^{1/4}$) so $|G(L/K)| = 2$ [1].

(3)

(a) Explain what is meant by the following. **(7 marks)**

(1) A *homomorphism* of fields.

(2) The *degree* of a homomorphism.

(3) An *automorphism* of a field.

(4) The *Galois group* of a field extension.

(b) Show that any homomorphism of fields is injective. **(5 marks)**

(c) Let N/K be a field extension of finite degree. Explain what it means for N to be *normal* over K. You should give one criterion in terms of roots of polynomials, and another criterion in terms of numbers of homomorphisms. **(5 marks)**

(d) Which of the following fields are normal over $\mathbb{Q}$? Justify your answers briefly. **(8 marks)**

$$\begin{aligned}L_1 &= \mathbb{Q}(\sqrt{11}, \sqrt{13}) \\ L_2 &= \mathbb{Q}(e^{2\pi i/11}) \\ L_3 &= \mathbb{Q}(2^{1/11}) \\ L_4 &= \mathbb{Q}\left(\sqrt{3 + \sqrt{7}}\right)\end{aligned}$$

Solution:

(a) **Bookwork**

(1) Let K and L be fields. A *homomorphism* from K to L is a function $\phi\colon K \to L$ such that

$$\begin{aligned}\phi(0_K) &= 0_L \\ \phi(1_K) &= 1_L \\ \phi(a + b) &= \phi(a) + \phi(b) && \text{for all } a, b \in K \\ \phi(ab) &= \phi(a)\phi(b) && \text{for all } a, b \in K.\text{[2]}\end{aligned}$$

(The first condition here could be omitted as it follows from the third. However, the second condition does not follow from the fourth one, because ϕ could be zero.)

(2) The *degree* of a homomorphism ϕ as above is the dimension of L considered as a vector space over the subfield $\phi(K)$. [2]

(3) An *automorphism* of K is a bijective homomorphism from K to itself. [1]

(4) Let L be a field extension of K. The *Galois group* $G(L/K)$ is the group of all automorphisms $\phi\colon L \to L$ that satisfy $\phi(a) = a$ for all $a \in K$. [2]

(b) **I will give the students a list of 8-10 proofs to learn, of which this will be one.** Let $\phi\colon K \to L$ be a homomorphism of fields. We first claim that if $a \in K$ and $a \neq 0$ then $\phi(a) \neq 0$. [1]Indeed, as $a \neq 0$ there exists $b \in K$ with $ab = 1$, so $\phi(a)\phi(b) = \phi(ab) = \phi(1) = 1$. However, if $\phi(a)$ were 0 we would instead have $\phi(a)\phi(b) = 0 \times \phi(b) = 0$, which is impossible because $0 \neq 1$. [2]

Now suppose we have $u, v \in K$ with $u \neq v$. This means that $u - v \neq 0$, so by the previous paragraph the element $\phi(u) - \phi(v) = \phi(u - v)$ is nonzero, so $\phi(u) \neq \phi(v)$. Thus, ϕ is injective. [2]

(c) **Bookwork** Let N/K be a field extension of finite degree. We say that N is *normal* over K if for every monic irreducible polynomial $f(x) \in K[x]$, either f has no roots in N or f splits properly over N [3]. One can show that this is equivalent to the following criterion: for any other extension L/K, either $E_K(L, N) = \emptyset$ or $|E_K(L, N)| = [L : K]$ (where $E_K(L, N) = \{\phi\colon L \to N \mid \phi|_K = 1\}$). [2] (Alternatively, it is equivalent to say that $|G(N/K)| = [N : K]$; two marks will also be given for this answer.)

(d) **Similar to examples in the notes and problem sheets.** The field L_1 is the splitting field for $(x^2 - 11)(x^2 - 13)$ over $\mathbb{Q}$, [1]so it is normal [1]. Similarly, L_2 is the splitting field for $x^{11} - 1$ (or for the cyclotomic polynomial $\varphi_{11}(x)$) [1]and so is normal over $\mathbb{Q}$ [1]. However, L_3 contains the unique real root of the polynomial $x^{11} - 2$ but none of the non-real roots (such as $e^{2\pi i/11}2^{1/11}$) [1], so it cannot be normal [1]. Similarly, L_4 contains the number $\alpha = \sqrt{3 + \sqrt{7}}$ which is a root of the irreducible polynomial $f(x) = (x^2 - 3)^2 - 7 = x^4 - 6x^2 + 2$, but it does not contain the number $\beta = \sqrt{3 - \sqrt{7}}$ which is another root of $f(x)$ [1]. This means that $f(x)$ has a root in L_3 but does not split, so L_3 is not normal over $\mathbb{Q}$ [1]. (The polynomial $f(x)$ is irreducible by Eisenstein's criterion at the prime 2, but candidates are not required to prove this. They are also not required to prove that $\beta \notin \mathbb{Q}(\alpha)$. Some such facts have been proved in lectures, but in most cases we have merely remarked that they can be proved by congruence arguments that have not been given.)

(4)

(a) Define the cyclotomic polynomial $\varphi_n(x)$ (where n is a positive integer). **(2 marks)**

(b) Explain the recursive method for calculating $\varphi_n(x)$. **(2 marks)**

(c) You may assume that $\varphi_8(x) = x^4 + 1$. Determine the relationship between $x^{24} - 1$, $x^{12} - 1$, $\varphi_8(x)$ and $\varphi_{24}(x)$, and thus calculate $\varphi_{24}(x)$. **(5 marks)**

(d) Put $\zeta = e^{2\pi i/24}$. Use de Moivre's Theorem to calculate ζ^2, ζ^3, ζ^6, $\zeta^2 + \zeta^{-2}$ and $\zeta^3 + \zeta^{-3}$ in terms of $\sqrt{2}$, $\sqrt{3}$ and i. **(5 marks)**

(e) Using (d), calculate $(1+i)(\sqrt{3}-i)/\sqrt{2}$ in terms of ζ. Deduce that $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i)$. **(3 marks)**

(f) Using the general theory of cyclotomic fields, list the elements of $G(\mathbb{Q}(\zeta)/\mathbb{Q})$. **(3 marks)**

(g) There is an automorphism τ of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = \mathbb{Q}(\zeta)$ given by

$$\tau(\sqrt{2}) = -\sqrt{2} \qquad \tau(\sqrt{3}) = \sqrt{3} \qquad \tau(i) = i.$$

Calculate $\tau(\zeta)$ and thus determine which of the automorphisms in (f) is equal to τ. **(5 marks)**

Solution: The notes and exercises contain many examples similar to parts (a) to (f), but (g) will be less familiar.

(a) $\varphi_n(x)$ is defined to be the product $\prod_{\zeta\in\mu_n^\times}(x-\zeta)$, where $\mu_n^\times\subset\mathbb{C}$ is the set of primitive n'th roots of unity. [2]

(b) It is a standard fact that

$$x^n-1=\prod_{d|n}\varphi_d(x).$$

Thus, if we already know $\varphi_d(x)$ for all $d|n$ with $d<n$, then we can divide x^n-1 by the product of all these to find $\varphi_n(x)$. [2]

(c) We have

$$\begin{aligned} x^{12}-1 &= \varphi_1(x)\varphi_2(x)\varphi_3(x)\varphi_4(x)\varphi_6(x)\varphi_{12}(x)\\ x^{24}-1 &= \varphi_1(x)\varphi_2(x)\varphi_3(x)\varphi_4(x)\varphi_6(x)\varphi_8(x)\varphi_{12}(x)\varphi_{24}(x)[2]\\ &= (x^{12}-1)\varphi_8(x)\varphi_{24}(x)=(x^{12}-1)(x^4+1)\varphi_{24}(x)\\ \varphi_{24}(x) &= \frac{x^{24}-1}{(x^{12}-1)(x^4+1)}=\frac{x^{12}+1}{x^4+1}=x^8-x^4+1.[3] \end{aligned}$$

(d) We have

$$\begin{aligned} \zeta^2 &= e^{\pi i/6}=\cos(\pi/6)+i\sin(\pi/6)=(\sqrt{3}+i)/2[1]\\ \zeta^3 &= e^{\pi i/4}=\cos(\pi/4)+i\sin(\pi/4)=(1+i)/\sqrt{2}[1]\\ \zeta^6 &= e^{\pi i/2}=\cos(\pi/2)+i\sin(\pi/2)=i[1]\\ \zeta^2+\zeta^{-2} &= (\sqrt{3}+i)/2+(\sqrt{3}-i)/2=\sqrt{3}[1]\\ \zeta^3+\zeta^{-3} &= (1+i)/\sqrt{2}+(1-i)/\sqrt{2}=2/\sqrt{2}=\sqrt{2}[1]. \end{aligned}$$

(e) We now have $(1+i)/\sqrt{2}=\zeta^3$ and $\sqrt{3}-i=2\zeta^{-2}$ so $(1+i)(\sqrt{3}-i)/\sqrt{2}=2\zeta$ [2]. It follows that $\zeta\in\mathbb{Q}(\sqrt{2},\sqrt{3},i)$, so $\mathbb{Q}(\zeta)\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3},i)$. On the other hand, it is clear from (d) that $\sqrt{2}$, $\sqrt{3}$ and i lie in $\mathbb{Q}(\zeta)$, so $\mathbb{Q}(\sqrt{2},\sqrt{3},i)\subseteq\mathbb{Q}(\zeta)$, so $\mathbb{Q}(\sqrt{2},\sqrt{3},i)=\mathbb{Q}(\zeta)$. [1]

(f) The general theory says that for each

$$k\in(\mathbb{Z}/24)^\times=\{1,5,7,11,13,17,19,23\}$$

there is a unique automorphism $\sigma_k\in G(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma_k(\zeta)=\zeta^k$, and that the map $k\mapsto\sigma_k$ gives an isomorphism $(\mathbb{Z}/24)^\times\to G(\mathbb{Q}(\zeta)/\mathbb{Q})$. [3]

(g) The automorphism τ must be equal to σ_k for some k. We have

$$\tau(\zeta)=\tau\left(\frac{(1+i)(\sqrt{3}-i)}{2\sqrt{2}}\right)=\frac{(1+i)(\sqrt{3}-i)}{-2\sqrt{2}}=-\zeta,[2]$$

and $\zeta^{12}=e^{i\pi}=-1$ [1], so we can rewrite this as $\tau(\zeta)=\zeta^{13}$ [1]. We must therefore have $\tau=\sigma_{13}$. [1]

(5) Put $L=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$.

(a) Give a basis for L over $\mathbb{Q}$. (You need not prove that your answer is correct.) **(3 marks)**

(b) List the elements of the group $G(L/\mathbb{Q})$, and show that $|G(L/\mathbb{Q})|=[L:\mathbb{Q}]$. To which well-known group is $G(L/\mathbb{Q})$ isomorphic? **(5 marks)**

(c) For each of the following fields K_i, determine the subgroup $H_i\leq G(L/\mathbb{Q})$ that corresponds to K_i under the Galois correspondence.

$$K_1=\mathbb{Q}(\sqrt{10})\qquad K_2=\mathbb{Q}(\sqrt{6},\sqrt{15})\qquad K_3=\mathbb{Q}(\sqrt{2}+\sqrt{5})\qquad K_4=\mathbb{Q}(\sqrt{30})$$

(6 marks)

(d) Use the Galois correspondence to show that $K_1 \leq K_3$, then prove the same thing by a direct calculation. **(4 marks)**

(e) How many fields M are there with $\mathbb{Q} < M < L$ and $[M : \mathbb{Q}] = 4$? **(4 marks)**

(f) Show that if $f(x) \in \mathbb{Q}[x]$ is an irreducible monic polynomial of degree 3, then $f(x)$ has no roots in L. **(3 marks)**

Solution:

(a) **(Examples of this type have been seen.)** The set

$$B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$$

is a basis for L over $\mathbb{Q}$ [3].

(b) **(Examples of this type have been seen.)** We can define automorphisms $\phi, \psi, \chi \in G(L/\mathbb{Q})$ by

$$\begin{array}{lll} \phi(\sqrt{2}) = -\sqrt{2} & \phi(\sqrt{3}) = \sqrt{3} & \phi(\sqrt{5}) = \sqrt{5} \\ \psi(\sqrt{2}) = \sqrt{2} & \psi(\sqrt{3}) = -\sqrt{3} & \psi(\sqrt{5}) = \sqrt{5} \\ \chi(\sqrt{2}) = \sqrt{2} & \chi(\sqrt{3}) = \sqrt{3} & \chi(\sqrt{5}) = -\sqrt{5}.[3] \end{array}$$

More explicitly, we have

$$\phi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{5} + e\sqrt{6} + f\sqrt{10} + g\sqrt{15} + h\sqrt{30}) = \\ a - b\sqrt{2} + c\sqrt{3} + d\sqrt{5} + -e\sqrt{6} - f\sqrt{10} + g\sqrt{15} - h\sqrt{30}$$

and so on. These automorphisms commute with each other and satisfy $\phi^2 = \psi^2 = \chi^2 = 1$. The full group is

$$G(L/\mathbb{Q}) = \{1,\ \phi,\ \psi,\ \chi,\ \phi\psi,\ \phi\chi,\ \psi\chi,\ \phi\psi\chi\} \simeq C_2 \times C_2 \times C_2.[2]$$

(c) **(Broadly similar examples have been seen.)** H_i is the set of automorphisms $\theta \in G(L/\mathbb{Q})$ satisfying $\theta|_{K_i} = 1$. For example, this means that H_1 is the group of those $\theta \in G(L/K)$ for which $\theta(\sqrt{10}) = \sqrt{10}$, or equivalently $\theta(\sqrt{2})\theta(\sqrt{5}) = \sqrt{2}\sqrt{5}$. This gives the list

$$H_1 = \{1, \phi\chi, \psi, \phi\psi\chi\}.[2]$$

Similarly, we have

$$H_2 = \{1, \phi\psi\chi\}[1]$$
$$H_4 = \{1, \phi\psi, \phi\chi, \psi\chi\}[1].$$

For H_3, we note that any $\theta \in G(L/\mathbb{Q})$ has $\theta(\sqrt{2} + \sqrt{5}) = \pm\sqrt{2} \pm \sqrt{5}$. As $\sqrt{2}$ and $\sqrt{5}$ are linearly independent over $\mathbb{Q}$, we see that $\theta(\sqrt{2} + \sqrt{5})$ can only be equal to $\sqrt{2} + \sqrt{5}$ if $\theta(\sqrt{2}) = \sqrt{2}$ and $\theta(\sqrt{5}) = \sqrt{5}$ [1], which means that θ cannot involve ϕ or χ. We conclude that

$$H_3 = \{1, \psi\}.[1]$$

(d) **(Unseen)** As the Galois correspondence is an order-reversing bijection, we have $K_1 \leq K_3$ iff $H_1 \geq H_3$, which is true by part (c) [2]. More explicitly, we have

$$\sqrt{10} = \tfrac{1}{2}\,(\sqrt{2} + \sqrt{5})^2 - \tfrac{7}{2},$$

so $\sqrt{10} \in \mathbb{Q}(\sqrt{2} + \sqrt{5})$, so $K_1 = \mathbb{Q}(\sqrt{10}) \leq \mathbb{Q}(\sqrt{2} + \sqrt{5}) = K_3$. [2]

(e) **(Unseen)** If a field M (with $\mathbb{Q} < M < L$) corresponds to a subgroup $H \leq G(L/\mathbb{Q})$, we have

$$|H| = [L : M] = [L : \mathbb{Q}]/[M : \mathbb{Q}] = 8/[M : \mathbb{Q}].$$

Thus, the intermediate fields with $[M : \mathbb{Q}] = 4$ biject with subgroups of order 2 in $G(L/\mathbb{Q})$ [2]. There are 7 non-identity elements $\theta \in G(L/K)$ [1], and each of these satisfies $\theta^2 = 1$ so it gives a subgroup $\{1, \theta\}$ of order 2, and this gives all such subgroups [1]. Thus, there are 7 intermediate fields of degree 4 over $\mathbb{Q}$.

(f) **(Fairly standard)** Let $f(x)$ be a monic irreducible polynomial of degree d over $\mathbb{Q}$, and suppose that $f(x)$ has a root $\alpha \in L$. Then $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[x]/f(x)$ so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = d$ [1]. We also have $[L : \mathbb{Q}(\alpha)]d = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [L : \mathbb{Q}] = 8$, so d is a divisor of 8 [1], so d cannot be equal to 3 [1].

(6)

(a) Let p be a prime number, and let $f(x)$ be an irreducible monic polynomial of degree p over $\mathbb{Q}$. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Suppose that $f(x)$ has precisely $p - 2$ real roots. Prove that the Galois group $G(K/\mathbb{Q})$ contains a transposition. **(2 marks)**

(b) Let R be the set of complex roots of $f(x)$, and define a relation on R by declaring that $\alpha \sim \beta$ if either $\alpha = \beta$ or the transposition $(\alpha\ \beta)$ lies in $G(K/\mathbb{Q})$. Show that this is an equivalence relation, and that all equivalence classes have the same size. **(10 marks)**

(c) Deduce that $G(K/\mathbb{Q})$ is isomorphic to the whole symmetric group Σ_p. **(3 marks)**

(d) Now let $L \subseteq \mathbb{C}$ be a normal extension of $\mathbb{Q}$ such that $G(L/\mathbb{Q}) \simeq C_5$. Let α be any element of L that does not lie in $\mathbb{Q}$, and let $g(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Show that $g(x)$ must have degree 5, and that it must split over L. **(5 marks)**

(e) Now show (using ideas from (a), or otherwise) that $g(x)$ must have five real roots. **(5 marks)**

Solution: I will give the students a list of 8-10 proofs to learn. Parts (a) to (c) will be one of these.

We will write G for the Galois group $G(K/\mathbb{Q})$.

(a) As f has rational coefficients we see that complex conjugation defines an element $\tau \in G$. This must fix the $p - 2$ real roots and exchange the two non-real roots, so τ is a transposition [2].

(b) As $\alpha \sim \alpha$ by definition, we see that $\sim$ is reflexive [1]. As $(\alpha\ \beta) = (\beta\ \alpha)$ we see that it is also symmetric [1]. Now suppose that $\alpha \sim \beta$ and $\beta \sim \gamma$; we claim that $\alpha \sim \gamma$ [1]. If any two of α, β and γ are the same, then this is trivial [1]. We may therefore assume that α, β and γ are distinct, and that $(\alpha\ \beta)$ and $(\beta\ \gamma)$ are in G. As G is a group it follows that the product $(\beta\ \gamma)(\alpha\ \beta)(\beta\ \gamma)$ lies in G, but this is equal to $(\alpha\ \gamma)$, so $\alpha \sim \gamma$ as claimed [2]. This proves that $\sim$ is an equivalence relation on R. We next claim that any two equivalence classes have the same size [1]. To see this, consider equivalence classes $[\alpha]$ and $[\alpha']$. As G acts transitively on R [1], we can choose $\sigma \in G$ with $\sigma(\alpha) = \alpha'$. Now if $\beta \in [\alpha]$ with $\beta \neq \alpha$ then the transposition $\tau = (\alpha\ \beta)$ must lie in G, so the conjugate $\tau' = \sigma\tau\sigma^{-1}$ must also lie in G. However, this conjugate is just $(\alpha'\ \sigma(\beta))$, so we see that $\sigma(\beta) \in [\alpha']$. This shows that $\sigma([\alpha]) \subseteq [\alpha']$ and essentially the same argument shows that $\sigma^{-1}([\alpha']) \subseteq [\alpha]$, so $|[\alpha]| = |[\alpha']|$ as claimed [2].

(c) Now suppose we have n different equivalence classes each of size m. We must then have $nm = |R| = p$. Moreover, as G contains at least one transposition we see that one of the equivalence classes has size larger than one, so they all do, so $m > 1$ [1]. As $nm = p$ with $m > 1$ we must have $m = p$ and $n = 1$. This means that there is only one equivalence class, so for all $\alpha, \beta \in R$ with $\alpha \neq \beta$ we have $\alpha \sim \beta$ and thus $(\alpha\ \beta) \in G$ [1]. However, Σ_R is generated by the transpositions, so we must have $G = \Sigma_R$ as claimed [1].

(d) **Unseen.** As $\alpha \notin \mathbb{Q}$ we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 1$ [1]. We also have $[L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ so we must have $[L : \mathbb{Q}(\alpha)] = 1$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ [2]. This means that $\mathbb{Q}(\alpha) = L$. It is also standard that the degree of the minimal polynomial $g(x)$ is the same as $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, which is 5 [1]. As L is normal over $\mathbb{Q}$ and $g(x)$ has a root in L we see that $g(x)$ must split over L [1].

(e) **Unseen.** We see from (b) that L is the splitting field of the polynomial $g(x) \in \mathbb{Q}[x]$, so it is preserved by complex conjugation [1]. The conjugation map therefore gives an element of $G(L/\mathbb{Q})$, which is either the identity (if all roots of g are real) or of order 2 (otherwise) [2]. As $G(L/\mathbb{Q})$ has order 5, it cannot contain any elements of order 2, so all the roots must be real [2].

(7)

(a) Let H be a transitive subgroup of the symmetric group Σ_5 that contains a transposition. Prove that $H = \Sigma_5$. **(12 marks)**

(b) Let $f(x)$ be an irreducible polynomial of degree five over $\mathbb{Q}$, and let $L \subseteq \mathbb{C}$ be the splitting field. Let n be the number of real roots of $f(x)$. Prove that $n \in \{1, 3, 5\}$. **(3 marks)**

(c) Suppose that $n = 3$. Prove that $G(L/\mathbb{Q}) \simeq \Sigma_5$. **(3 marks)**

(d) Deduce that if $n = 3$ there is no field K with $\mathbb{Q} \subseteq K \subseteq L$ such that K is normal over $\mathbb{Q}$ and $[K : \mathbb{Q}] = 60$. **(7 marks)**

Solution: Part (a) is bookwork. I will give the students a list of perhaps six or eight proofs to learn, including this one. The deduction of (c) from (a) is standard, and (b) is just a small extension of that argument. Part (d) is unseen.

(a) We introduce a relation on the set $N = \{1, 2, 3, 4, 5\}$ by declaring that $i \sim j$ iff ($i = j$ or the transposition $(i\ j)$ lies in H) [1]. This is clearly reflexive and symmetric [1]. We claim that it is also transitive [1]. To see this, suppose that $i \sim j$ and $j \sim k$. There are various cases to consider:

(1) If $i = j$ then the relation $j \sim k$ gives $i \sim k$. [1]

(2) If $j = k$ then the relation $i \sim j$ gives $i \sim k$.

(3) If neither (1) nor (2) holds, then the transpositions $(i\ j)$ and $(j\ k)$ both lie in H, and H is a subgroup so $(i\ j)(j\ k)(i\ j) \in H$, but this composite is just $(i\ k)$, so again $i \sim k$. [1]

We now see that we have an equivalence relation, so we can divide N into equivalence classes. We next claim that if $i \sim j$ and $\sigma \in H$ then $\sigma(i) \sim \sigma(j)$ [1]. Indeed, if $i = j$ then $\sigma(i) = \sigma(j)$, so certainly $\sigma(i) \sim \sigma(j)$. Otherwise, the transposition $(i\ j)$ must lie in H, so $\sigma(i\ j)\sigma^{-1} \in H$, but $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$, so $\sigma(i) \sim \sigma(j)$ as claimed [1]. By applying the same logic to σ^{-1}, we see that $i \sim j$ iff $\sigma(i) \sim \sigma(j)$, so σ gives a bijection from the equivalence class $[i]$ to the equivalence class $[\sigma(i)]$, so these equivalence classes have the same size [1]. As H is transitive, it follows that all equivalence classes have the same size, say m [1]. As H contains a transposition we see that at least one equivalence class has size larger than one, so $m > 1$ [1]. If there are n equivalence classes, this means that $nm = 5$. As $m > 1$, we must have $n = 1$ and $m = 5$, so N is a single equivalence class [1]. This means that for all $i \neq j$, the transposition $(i\ j)$ lies in H. As Σ_5 is generated by transpositions, this means that $H = \Sigma_5$ [1].

(b) Let $f(x)$ be an irreducible polynomial of degree five over $\mathbb{Q}$. It is then standard that $f(x)$ has 5 distinct roots, say $\alpha_1, \ldots, \alpha_5$ [1]. As the coefficients of $f(x)$ are real we see that $f(\overline{\alpha_i}) = \overline{f(\alpha_i)} = \overline{0} = 0$, so $\overline{\alpha_i} = \alpha_j$ for some j [1]. We can thus group the non-real roots in complex conjugate pairs, so there are an even number of them. As there are 5 roots in total, the number of real ones must be 1, 3 or 5. [1]

(c) Suppose that there are precisely 3 real roots, and thus two non-real ones. Let L be the splitting field, and put $H = G(L/K)$. It is standard that this can be identified with a transitive subgroup of the group of permutations of the roots [1]. Complex conjugation gives an element of H which exchanges the two non-real roots and fixes the real ones, so it is a transposition [1]. It therefore follows from (a) that $H = \Sigma_5$ [1].

(d) Now suppose as above that $H = \Sigma_5$, and that we have a field K with $\mathbb{Q} \subseteq K \subseteq L$ and $[K : \mathbb{Q}] = 60$ and K is normal over $\mathbb{Q}$. Note that $[L : \mathbb{Q}] = |H| = |\Sigma_5| = 5! = 120$ [1]. By the Galois correspondence, there is a subgroup $A \leq H$ with $K = L^A$ [1]and $|A| = [L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}] = 120/60 = 2$ [1]. As K is normal over $\mathbb{Q}$, we also see that A is a normal subgroup of Σ_5 [1]. On the other hand, we must have $A = \{1, \sigma\}$ for some permutation σ with $\sigma^2 = 1$, so σ must be a transposition or a transposition pair [1]. In either case, σ is conjugate to every other permutation of the same cycle type [1], so A is not normal in H [1].

(8)

(a) Define the cyclotomic polynomial $\phi_n(x)$. **(2 marks)**

(b) State the rule relating the polynomials $\phi_n(x)$ to the polynomials $x^m - 1$. **(2 marks)**

(c) Find $\phi_2(x)$, $\phi_4(x)$ and $\phi_8(x)$, then state and prove a general formula for $\phi_{2^k}(x)$. **(6 marks)**

(d) Put

$$\zeta = \frac{\sqrt{2+\sqrt{2}} + \sqrt{2-\sqrt{2}}\, i}{2}.$$

Show that $\phi_{16}(\zeta) = 0$, and thus that $\mathbb{Q}(\zeta) = \mathbb{Q}(\mu_{16})$. **(6 marks)**

(e) Prove that $\mathbb{Q}(i) \leq \mathbb{Q}(\zeta)$ and that $G(\mathbb{Q}(\zeta)/\mathbb{Q}(i))$ is a cyclic group of order 4. You may assume general facts about cyclotomic fields and their Galois groups, provided that you state them clearly. **(9 marks)**

Solution:

(a) **(Bookwork)** $\phi_n(x) = \prod_k (x - e^{2\pi i k/n})$, where k runs over all integers with $0 \leq k < n$ that are coprime to n. [2]

(b) **(Bookwork)** $x^n - 1 = \prod_{d|n} \phi_d(x)$. [2]

(c) **(The specific cases are standard. The general case is an exercise in the notes.)** It is clear from the definitions that $\phi_1(x) = x - 1$ and $\phi_2(x) = x + 1$ [1]. Next note that

$$\phi_1(x)\phi_2(x)\phi_4(x) = x^4 - 1,$$

so

$$\phi_4(x) = \frac{x^4 - 1}{\phi_1(x)\phi_2(x)} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1.\text{[1]}$$

Similarly, we have

$$\phi_1(x)\phi_2(x)\phi_4(x)\phi_8(x) = x^8 - 1,$$

so

$$\phi_8(x) = \frac{x^8 - 1}{\phi_1(x)\phi_2(x)\phi_4(x)} = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1.\text{[1]}$$

More generally, for any $k > 0$ we can divide the equation

$$\phi_1(x)\phi_2(x)\cdots\phi_{2^k}(x) = \prod_{j=0}^{k} \phi_{2^j}(x) = x^{2^k} - 1$$

by the equation

$$\phi_1(x)\phi_2(x)\cdots\phi_{2^{k-1}}(x) = \prod_{j=0}^{k-1} \phi_{2^j}(x) = x^{2^{k-1}} - 1$$

to get

$$\phi_{2^k}(x) = \frac{x^{2^k} - 1}{x^{2^{k-1}} - 1} = \frac{(x^{2^{k-1}})^2 - 1}{x^{2^{k-1}} - 1} = \frac{(x^{2^{k-1}} - 1)(x^{2^{k-1}} + 1)}{x^{2^{k-1}} - 1} = x^{2^{k-1}} + 1.\text{[3]}$$

(d) **(Unseen, but requires no creativity.)** By straightforward algebra we have

$$\begin{aligned} 4\zeta^2 &= (2+\sqrt{2}) + 2\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}}i - (2-\sqrt{2}) \\ &= 2\sqrt{2} + 2\sqrt{2^2 - \sqrt{2}^2}\, i = 2\sqrt{2}(1+i) \\ \zeta^2 &= \frac{2\sqrt{2}(1+i)}{4} = \frac{1+i}{\sqrt{2}}[3] \\ \zeta^4 &= (\zeta^2)^2 = \frac{1+2i-1}{2} = i[1] \\ \zeta^8 &= (\zeta^4)^2 = i^2 = -1 \\ \phi_{16}(\zeta) &= \zeta^8 + 1 = 0.[1] \end{aligned}$$

This means that ζ is a generator of the group μ_{16}, so $\mathbb{Q}(\zeta) = \mathbb{Q}(\mu_{16})$. [1]

(e) **($G(\mathbb{Q}(\mu_{16})/\mathbb{Q})$ is standard. Changing the ground field to $\mathbb{Q}(i)$ is new.)** First, we saw in (d) that $i = \zeta^4$ so $\mathbb{Q}(i) \leq \mathbb{Q}(\zeta)$. [1]

It is a standard fact that for every $a \in (\mathbb{Z}/n)^\times$ there is a unique automorphism ϕ_a of $\mathbb{Q}(\mu_n)$ satisfying $\phi_a(\xi) = \xi^a$ for all $\xi \in \mu_n$, and that the map $a \mapsto \phi_a$ gives an isomorphism $(\mathbb{Z}/n)^\times \to G(\mathbb{Q}(\mu_n)/\mathbb{Q})$ [2]. Thus, if we put $L = \mathbb{Q}(\mu_{16}) = \mathbb{Q}(\zeta)$, we have

$$G(K/\mathbb{Q}) = \{\phi_1, \phi_3, \phi_5, \phi_7, \phi_9, \phi_{11}, \phi_{13}, \phi_{15}\}.[1]$$

Note that $i \in \mu_{16}$ so $\phi_a(i) = i^a$. The group $G(K/\mathbb{Q}(i))$ is the subgroup consisting of those ϕ_a for which $\phi_a(i) = i$ [1], or equivalently $a = 1 \pmod 4$ [1]. We thus have

$$G(K/\mathbb{Q}(i)) = \{\phi_1, \phi_5, \phi_9, \phi_{13}\}.[1]$$

Moreover, we have

$$\begin{aligned} \phi_5^2 &= \phi_{25} = \phi_9 \\ \phi_5^3 &= \phi_{5\times 9} = \phi_{45} = \phi_{13} \\ \phi_5^4 &= \phi_{5\times 13} = \phi_{65} = \phi_1.[1] \end{aligned}$$

It follows that $G(K/\mathbb{Q}(i))$ is cyclic of order 4, generated by ϕ_5. [1]

(9) Consider the polynomial $f(x) = x^4 - 24x^2 + 4$. Some of the values of f are as follows:

x	0	1	2	3	4	5
$f(x)$	4	-19	-76	-131	-124	29

(a) Use the above table to show that f has four real roots and no integer roots. **(4 marks)**

(b) Suppose we have a factorisation $f(x) = (x^2 + ax + b)(x^2 + cx + d)$. Show that $c = -a$ and either $a = 0$ or $b = d$. By continuing this analysis further, show that a, b, c and d cannot all be integers. **(7 marks)**

(c) Deduce that $f(x)$ is irreducible over $\mathbb{Q}$, stating carefully any general results that you use. **(5 marks)**

(d) Now let α be the largest real root of $f(x)$. Put $\beta = \frac{1}{2}\alpha^2 - 6$ and $\gamma = \frac{1}{4}\alpha(\alpha^2 - 22)$. Simplify β^2 and γ^2, and show that they are integers. **(6 marks)**

(e) Use (d) to find primes p and q such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. **(3 marks)**

Solution:

(a) **Similar to examples in the notes and problem sheets.** As $f(4) < 0$ and $f(5) > 0$, the Intermediate Value Theorem tells us that there is a root α with $4 < \alpha < 5$ [1]. As $f(0) > 0$ and $f(1) < 0$, the IVT also tells us that there is a root α' with $0 < \alpha' < 1$ [1]. As $f(x) = f(-x)$ we see that $-\alpha'$ and $-\alpha$ are also roots [1]. As f has degree four there can be no more roots, so we have four real roots as required, and none of them are integers [1]. It is also clear that α is the largest root, so our naming is consistent with part (d).

Alternatively, we can use the quadratic formula to see that the roots satisfy $x^2 = 12 \pm 2\sqrt{35} \simeq 0.168$ or 23.832, so $x \simeq \pm 0.410$ or $x \simeq \pm 4.882$. These kinds of approximations will be accepted as a proof that the roots are real and not integral.

(b) **Essentially unseen.** By direct expansion we have

$$(x^2 + ax + b)(x^2 + cx + d) - f(x) = (a + c)x^3 + (b + d + ac + 24)x^2 + (ad + bc)x + (bd - 4).[1]$$

If this is zero then (by inspecting the coefficient of x^3) we must have $c = -a$ [1]. After substituting for c and inspecting the coefficients of x^2, x and 1 we get

$$b + d + 24 = a^2 \qquad \text{(A)}$$

$$a(d - b) = 0 \qquad \text{(B)}$$

$$bd = 4.[1] \qquad \text{(C)}$$

From (B) we see that either $a = 0$ or $b = d$ [1]. Now suppose that a, b, c and d are integers. From (C) we see that $b, d \in \{\pm 1, \pm 2, \pm 4\}$ so $b + d + 24 \geq 16$. By comparing this with (A) we see that a cannot be zero. Using (B) we therefore see that $b = d$, so (C) gives $b = d = \pm 2$. Equation (A) now gives $a^2 = 24 \pm 4 \in \{20, 28\}$ which is impossible for integer a. Thus, there can be no factorisation of this type. [3]

(c) **Similar to examples in the notes and problem sheets.** A lemma of Gauss says that if $g(x)$ is a monic polynomial with integer coefficients that is irreducible over $\mathbb{Z}$, then it is also irreducible over $\mathbb{Q}$ [2]. We saw in (a) that $f(x)$ has no integer roots, so it cannot factor over $\mathbb{Z}$ as a linear polynomial times a cubic polynomial. We also saw in (b) that $f(x)$ cannot factor over $\mathbb{Z}$ as a product of two quadratic polynomials. It follows that $f(x)$ is irreducible over $\mathbb{Z}$, and thus also over $\mathbb{Q}$ [3].

(d) **Similar to examples in the notes and problem sheets.** As α is a root of $f(x)$ we have $\alpha^4 = 24\alpha^2 - 4$ [1]. Using this repeatedly we get

$$\begin{aligned}
\beta^2 &= (\tfrac{1}{2}\alpha^2 - 6)^2 = \tfrac{1}{4}\alpha^4 - 6\alpha^2 + 36 \\
&= 6\alpha^2 - 1 - 6\alpha^2 + 36 = 35[2] \\
\gamma^2 &= \tfrac{1}{16}\alpha^2(\alpha^2 - 22)^2 = \tfrac{1}{16}\alpha^2(\alpha^4 - 44\alpha^2 + 484) \\
&= \tfrac{1}{16}\alpha^2(480 - 20\alpha^2) = 30\alpha^2 - \tfrac{5}{4}\alpha^4 \\
&= 30\alpha^2 - \tfrac{5}{4}(24\alpha^2 - 4) = 5.[3]
\end{aligned}$$

(e) **Unseen.** Using the approximation $\alpha \simeq 4.882$ we also see that $\beta, \gamma > 0$ so $\beta = \sqrt{35}$ and $\gamma = \sqrt{5}$ [1]. This means that $\mathbb{Q}(\alpha)$ contains both $\gamma = \sqrt{5}$ and $\beta/\gamma = \sqrt{7}$, so it contains the field $K' = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ [1]. However, both K and K' have degree 4 over $\mathbb{Q}$, so we must have $K = K'$ [1].

(10)

(a) Give a detailed statement, without proof, of the Galois correspondence. You should include information about orders of subgroups, degrees and Galois groups of intermediate field extensions, conjugacy and containment between subgroups, and normality of field extensions. **(11 marks)**

(b) Suppose we have fields $K \subseteq L$ such that L is normal over K and $G(L/K)$ is cyclic of order 2^r.

(i) How many fields M are there with $K \subseteq M \subseteq L$? **(3 marks)**

(ii) Prove that every such field M is normal over K. **(3 marks)**

(c) Suppose instead that we have fields $K \subseteq L$ such that L is normal over K and $G(L/K)$ is isomorphic to Σ_5. What elements of order 5 are there in Σ_5? Prove that there are precisely six intermediate fields $M_1, \dots, M_6$ for which $[L : M_i] = 5$, and that none of these is normal over K. **(8 marks)**

Solution: Part (a) is pure bookwork. Parts (b) and (c) have some similarity with examples in the notes and exercises, but will still require original thought. The students will have been reminded of the subgroup structure of cyclic groups.

(a) Let L be a normal extension [1]of finite degree over a subfield K, with Galois group G. Let $\mathcal{H}$ be the set of subgroups of G, and let $\mathcal{M}$ be the set of fields M such that $K \subseteq M \subseteq L$ [1]. Then there is an order-reversing [1]bijection $\mathcal{H} \to \mathcal{M}$ given by $H \mapsto L^H$ [1], with inverse $M \mapsto G(L/M)$ [1]. Moreover, if H corresponds to M then

- $[L : M] = |H|$ [1]and $[M : K] = |G/H|$ [1].
- L is normal over M, with Galois group H [1].
- For any $\sigma \in G$, the subgroup $\sigma H \sigma^{-1}$ corresponds to the field $\sigma(M)$ [1].
- M is normal over K if and only if H is a normal subgroup of G [1], and if so, then the corresponding Galois group is G/H [1].

(b) Suppose we have fields $K \subseteq L$ such that L is normal over K and $G(L/K)$ is cyclic of order 2^r. Choose a generator σ for $G(L/K)$, so that $\sigma^{2^r} = 1$. For $0 \leq s \leq r$ let H_s be the subgroup generated by σ^{2^s}, which is cyclic of order 2^{r-s} [1]. We then have $\{1\} = H_r < H_{r-1} < \cdots < H_0 = G(L/K)$, and these are all the subgroups of $G(L/K)$ [1]. Put $M_s = L^{H_s}$, so that $L = M_r > M_{r-1} > \cdots > M_0 = K$, and these are the only intermediate fields [1]. There are thus $r+1$ such fields [1]. As $G(L/K)$ is abelian, we see that all subgroups are normal [1], and so all intermediate fields are normal over K [1].

(c) The intermediate fields M with $[L : M] = 5$ are the fields L^H, where $H \leq G(L/K) \simeq \Sigma_5$ and $|H| = 5$ [1]. Any group of order 5 is cyclic, generated by an element of order 5 [1]. An element of order 5 in Σ_5 is a 5-cycle [1]. Any 5-cycle can be written uniquely as $(1\ p\ q\ r\ s)$, where p, q, r and s are 2, 3, 4 and 5 in some order. It follows that there are $4! = 24$ different 5-cycles [1]. Any subgroup of order 5 consists of the identity together with 4 different generators. We can thus group the 5-cycles into 6 groups of 4 according to which subgroup they generate. This means that there are precisely six subgroups of order 5 [2]. As all 5-cycles are conjugate, we see that all subgroups of order 5 are conjugate to each other, so none of them is normal [1]. It follows that none of the corresponding intermediate fields is normal over K. [1]

(11) Put $f(x) = x^3 - 12x - 34$.

(a) State Eisenstein's criterion, and use it to prove that $f(x)$ is irreducible over $\mathbb{Q}$. **(4 marks)**

(b) Calculate $f(x)$ and $f'(x)$ for $x = -2$, $x = 2$ and $x = 5$. By considering the shape of the graph, show that $f(x)$ has precisely one real root, say α. **(5 marks)**

(c) Show that $\alpha = 2^{5/3} + 2^{1/3}$. **(4 marks)**

(d) Let the other two roots be β and γ, and put $K = \mathbb{Q}(\alpha, \beta, \gamma)$. Show that $G(K/\mathbb{Q})$ contains an element of order two, and deduce that $G(K/\mathbb{Q})$ is the full group of permutations of the set $\{\alpha, \beta, \gamma\}$. **(6 marks)**

(e) Calculate the numbers

$$\begin{aligned} s_1 &= \alpha + \beta + \gamma \\ s_2 &= \alpha\beta + \beta\gamma + \gamma\alpha \\ s_3 &= \alpha\beta\gamma. \end{aligned}$$

(3 marks)

(f) Calculate $\alpha^2+\beta^2+\gamma^2$ (by relating it to s_1, s_2 and s_3). **(3 marks)**

Solution:

(a) **(Standard)** Eisenstein's criterion: let $g(x)=x^n+\sum_{i=0}^{n-1}a_ix^i$ be a monic polynomial with coefficients $a_i\in\mathbb{Z}$. Let p be a prime number, and suppose that $a_0,\dots,a_{n-1}$ are divisible by p and that a_0 is not divisible by p^2. Then $g(x)$ is irreducible over $\mathbb{Q}$. [2]

Now consider the polynomial $f(x)=x^3+0x^2-12x-34$. If we take $p=2$, then the coefficients 0, -12 and -34 are all divisible by p and the constant term -34 is not divisible by p^2. Thus, Eisenstein's criterion applies, and we see that $f(x)$ is irreducible over $\mathbb{Q}$. [2]

(b) **(Similar problems have been seen.)** We have $f'(x)=3x^2-12=3(x-2)(x+2)$, which gives the following table:

x	$f(x)$	$f'(x)$
-2	-18	0
2	-50	0
5	31	63

[2]

From this we see that $f(x)$ increases from $-\infty$ to -2 on the interval $(-\infty,0)$, then decreases to -50 on $(-2,2)$, then increases on $(2,\infty)$, passing zero somewhere between 2 and 5. This means that there is precisely one real root. [3]

(c) **(Direct calculation)** Now put $\alpha=2^{5/3}+2^{1/3}=2\times 2^{2/3}+2^{1/3}$. We have

$$\begin{aligned}
\alpha^2 &= 4\times 2^{4/3}+4\times 2^{2/3}\times 2^{1/3}+2^{2/3}\\
&= 8\times 2^{1/3}+8+2^{2/3}[1]\\
\alpha^3 &= (2\times 2^{2/3}+2^{1/3})(8\times 2^{1/3}+8+2^{2/3})\\
&= 32+16\times 2^{2/3}+4\times 2^{1/3}+8\times 2^{2/3}+8\times 2^{1/3}+2\\
&= 34+12\times 2^{1/3}+24\times 2^{2/3}[2]\\
f(\alpha) &= \alpha^3-12\alpha-34\\
&= 34+12\times 2^{1/3}+24\times 2^{2/3}-24\times 2^{2/3}-12\times 2^{1/3}-34=0,
\end{aligned}$$

so α is a root of $f(x)$. It is clearly real, so it is the unique real root. [1]

(d) **(Similar ideas have been seen.)** Now let β be another root of $f(x)$, so the imaginary part of β must be nonzero. Put $\gamma=\overline{\beta}$, and note (by comparing real and imaginary parts) that α, β and γ are disinct. As the coefficients of $f(x)$ are real, we can conjugate the equation $f(\beta)=0$ to see that $f(\gamma)=f(\overline{\beta})=\overline{f(\beta)}=0$, so γ is the third complex root of $f(x)$ [3]. We put $R=\{\alpha,\beta,\gamma\}$, so $G(K/\mathbb{Q})$ can be identified with a transitive subgroup of Σ_R, which must either be the alternating group A_R or the full group Σ_R [1]. Note that the splitting field $K=\mathbb{Q}(\alpha,\beta,\gamma)$ is preserved by complex conjugation, so the map $z\mapsto\overline{z}$ gives an element of order 2 in $G(K/\mathbb{Q})$, corresponding to the transposition $(\beta\ \gamma)$ [1]. As A_R contains no permutations, we must have $G(K/\mathbb{Q})=\Sigma_R$ [1].

(e) **(Standard)** We now have

$$x^3-12x-34=f(x)=(x-\alpha)(x-\beta)(x-\gamma)=x^3-(\alpha+\beta+\gamma)x^2+(\alpha\beta+\alpha\gamma+\beta\gamma)x-\alpha\beta\gamma.$$

By comparing coefficients, we obtain

$$\begin{aligned}
s_1 &= \alpha+\beta+\gamma=0\\
s_2 &= \alpha\beta+\alpha\gamma+\beta\gamma=-12\\
s_3 &= \alpha\beta\gamma=34.[3]
\end{aligned}$$

(f) **(Similar problems have been seen.)** Note also that we always have

$$(\alpha+\beta+\gamma)^2 = \alpha^2+\beta^2+\gamma^2+2(\alpha\beta+\alpha\gamma+\beta\gamma), [2]$$

which in our case becomes $0 = \alpha^2+\beta^2+\gamma^2+2\times(-12)$, so

$$\alpha^2+\beta^2+\gamma^2 = 24.[1]$$

(12) Put $\zeta = e^{2\pi i/21}$ and $L = \mathbb{Q}(\zeta)$.

(a) State a general theorem about Galois groups of cyclotomic fields. Use it to show that there are automorphisms $\rho, \tau \in G(L/\mathbb{Q})$ such that $\rho^6 = \tau^2 = 1$ and

$$G(L/\mathbb{Q}) = \{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5, \tau, \rho\tau, \rho^2\tau, \rho^3\tau, \rho^4\tau, \rho^5\tau\}.$$

(8 marks)

(b) Give a formula for the cyclotomic polynomial $\varphi_{21}(x)$ in terms of polynomials of the form x^k-1. (You need not carry out the relevant divisions.) **(4 marks)**

(c) You may assume that

$$\sqrt{-3} = \zeta^7 - \zeta^{-7}$$
$$\sqrt{-7} = -(\zeta^3-\zeta^{-3})(\zeta^6-\zeta^{-6})(\zeta^9-\zeta^{-9}).$$

Use this to find $\rho(\sqrt{-3})$, $\tau(\sqrt{-3})$, $\rho(\sqrt{-7})$ and $\tau(\sqrt{-7})$. **(6 marks)**

(d) Use the Galois correspondence to show that there is a unique field K with $\mathbb{Q} < K < L$ and $[K:\mathbb{Q}] = 4$. Give generators for that subfield. **(7 marks)**

Solution:

(a) **Bookwork.** For any integer k coprime to n, there is a unique automorphism σ_k of $\mathbb{Q}(\mu_n)$ such that $\sigma_k(\omega) = \omega^k$ for all $\omega \in \mu_n$. [2] This gives all the elements of $G(\mathbb{Q}(\mu_n)/\mathbb{Q})$, and we have $\sigma_j = \sigma_k$ iff $j \equiv k \pmod{n}$. Moreover, we have $\sigma_j\sigma_k = \sigma_{jk}$ for all j and k. Thus, $G(\mathbb{Q}(\mu_n)/\mathbb{Q})$ is isomorphic to the group of invertible elements in the ring $\mathbb{Z}/n\mathbb{Z}$ [2].

Unseen. We now specialise to the case $n = 21$ to see that

$$G(L/\mathbb{Q}) \simeq (\mathbb{Z}/21)^\times = \{1, 2, 4, 5, 8, 10, -1, -2, -4, -5, -8, -10\}.[1]$$

Note that the powers of 2 modulo 21 are

$$2^0 = 1 \qquad 2^1 = 2 \qquad 2^2 = 4 \qquad 2^3 = 8 \qquad 2^4 = -5 \qquad 2^5 = -10 \qquad 2^6 = 1.$$

Using this we see that every element of $(\mathbb{Z}/21)^\times$ can be written as 2^k or -2^k for some k with $0 \le k < 6$. We can thus take $\rho = \sigma_2$ and $\tau = \sigma_{-1}$. [3]

(b) **Slight adjustment of a standard problem.** Recall that $x^n - 1 = \prod_{d|n} \varphi_d(x)$ [1]. This gives

$$\varphi_1(x) = x - 1 \qquad (A)$$
$$\varphi_1(x)\varphi_3(x) = x^3 - 1 \qquad (B)$$
$$\varphi_1(x)\varphi_7(x) = x^7 - 1 \qquad (C)$$
$$\varphi_1(x)\varphi_3(x)\varphi_7(x)\varphi_{21}(x) = x^{21} - 1[1] \qquad (D)$$

We can multiply equations (A) and (D) and divide by (B) and (C) to get

$$\varphi_{21}(x) = \frac{(x^{21}-1)(x-1)}{(x^7-1)(x^3-1)}[2].$$

(c) **Similar to examples in the notes and problem sheets.** Recall that $\rho = \sigma_2$ is a homomorphism with $\rho(\zeta) = \zeta^2$. It follows that $\rho(\zeta^7) = \zeta^{14}$ but $\zeta^{21} = 1$ so $\zeta^{14} = \zeta^{-7}$ and similarly $\zeta^{-14} = \zeta^7$. This gives

$$\begin{aligned}\rho(\sqrt{-3}) &= \rho(\zeta^7 - \zeta^{-7}) = \zeta^{14} - \zeta^{-14} = \zeta^{-7} - \zeta^7 \\ &= -\sqrt{-3}[2].\end{aligned}$$

Similarly, we have

$$\begin{aligned}\rho(\zeta^3) &= \zeta^6 \\ \rho(\zeta^6) &= \zeta^{12} = \zeta^{-9} \\ \rho(\zeta^9) &= \zeta^{18} = \zeta^{-3}\end{aligned}$$

so

$$\begin{aligned}\rho(\sqrt{-7}) &= \rho\left(-(\zeta^3 - \zeta^{-3})(\zeta^6 - \zeta^{-6})(\zeta^9 - \zeta^{-9})\right) \\ &= -(\zeta^6 - \zeta^{-6})(\zeta^{-9} - \zeta^9)(\zeta^{-3} - \zeta^3) \\ &= -(\zeta^3 - \zeta^{-3})(\zeta^6 - \zeta^{-6})(\zeta^9 - \zeta^{-9}) \\ &= \sqrt{-7}[2].\end{aligned}$$

On the other hand, we have $\tau(\zeta) = \zeta^{-1}$. This implies that τ is just the complex conjugation map, from which it is clear that $\tau(\sqrt{-3}) = -\sqrt{-3}$ and $\tau(\sqrt{-7}) = -\sqrt{-7}$ [2]. Alternatively, we can use the same method as above:

$$\begin{aligned}\tau(\sqrt{-3}) &= \tau(\zeta^7 - \zeta^{-7}) = \zeta^{-7} - \zeta^7 = -\sqrt{-3} \\ \tau(\sqrt{-7}) &= \tau\left(-(\zeta^3 - \zeta^{-3})(\zeta^6 - \zeta^{-6})(\zeta^9 - \zeta^{-9})\right) \\ &= -(\zeta^{-3} - \zeta^3)(\zeta^{-6} - \zeta^6)(\zeta^{-9} - \zeta^9) \\ &= (\zeta^3 - \zeta^{-3})(\zeta^6 - \zeta^{-6})(\zeta^9 - \zeta^{-9}) = -\sqrt{-7}.\end{aligned}$$

(d) **Unseen.** The Galois correspondence tells us that every intermediate field K with $[K : \mathbb{Q}] = 4$ has the form $K = L^H$ for some subgroup $H \leq G(L/\mathbb{Q})$ with $|H| = [L : K] = [L : \mathbb{Q}]/[K : \mathbb{Q}] = 12/4 = 3$ [2]. One can check that the only elements of $(\mathbb{Z}/21)^\times$ of order 3 are $4 = 2^2$ and $-5 = 4^2 = 2^4$. This means that there is only one subgroup of order 3 in $(\mathbb{Z}/12)^\times$, namely $\{1, 2^2, 2^4\}$. It follows that there is only one subgroup of order 3 in $G(L/\mathbb{Q})$, namely $H = \{1, \rho^2, \rho^4\}$ [2]. Thus, there is only one field $K = L^H$ of the relevant type. The field $\mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ is clearly contained in L and has degree 4 over $\mathbb{Q}$, so this must be K [3].

(13) Consider a cubic

$$f(x) = x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma)$$

with $a, b, c \in \mathbb{Q}$ and $\alpha, \beta, \gamma \in \mathbb{C}$. Suppose that $f(x)$ is irreducible, and put $K = \mathbb{Q}(\alpha, \beta, \gamma)$. You may assume that

$$(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2.$$

(a) Prove that α, β and γ are distinct and nonzero. If you use any general result about repeated roots, you should prove it. **(8 marks)**

(b) Prove that if $c = 1$ then $\alpha^{-1} + \beta^{-1} + \gamma^{-1} = -b$. **(4 marks)**

(c) Explain the two possibilities for the Galois group $G(K/\mathbb{Q})$. **(2 marks)**

(d) Now take $f(x) = x^3 + x^2 - 4x + 1$. What is the Galois group in this case? **(4 marks)**

(e) Put $u = (3\sqrt{-3} - 5)/(2\sqrt{13})$, let v be any cube root of u, and put $w = \sqrt{13}(v + v^{-1})/3$.

(i) Show that $u\overline{u} = 1$ and $u + u^{-1} = u + \overline{u} = -5/\sqrt{13}$.

(ii) Expand out $f(x-1/3)$.

(iii) Deduce that $w-1/3$ is one of the roots of $f(x)$. **(7 marks)**

Solution: Parts (a) and (c) are bookwork. The students have seen things similar to (b), but only involving positive powers. Part (d) is a standard problem. The discussion of cubics in the notes starts with an example similar to (e), but with the numbers working out more simply.

(a) First let $u(x)$ be the greatest common divisor of $f(x)$ and $f'(x)$ [1]. Then $u(x)$ is a monic divisor of the irreducible monic polynomial $f(x)$, so we must have $u(x)=1$ or $u(x)=f(x)$ [1]. However, $u(x)$ divides $f'(x)$, but $f(x)$ has larger degree than $f'(x)$ and so does not divide $f'(x)$; so we cannot have $u(x)=f(x)$ [1]. It follows that $u(x)=1$, so there exist polynomials $a(x)$ and $b(x)$ such that $a(x)f(x)+b(x)f'(x)=1$ [1].

Now suppose that two of the roots coincide, say $\alpha=\beta$, so that $f(x)=(x-\alpha)^2(x-\gamma)$. We find that $f'(x)=2(x-\alpha)(x-\gamma)+(x-\alpha)^2$, and so $f'(\alpha)=f(\alpha)=0$ [1]. We can thus put $x=\alpha$ in the relation $a(x)f(x)+b(x)f'(x)=1$ to get $0=1$, which is false. It follows that the roots cannot coincide, after all [1].

Now suppose that one of the roots is zero. This means that $c=f(0)=0$, so $f(x)=x^3+ax^2+bx=(x^2+ax+b)x$, which is visibly reducible, contrary to assumption. Thus, all the roots are nonzero, as claimed [2].

(b) We now expand out the relation $x^3+ax^2+bx+c=(x-\alpha)(x-\beta)(x-\gamma)$ to get

$$\begin{aligned} a &= -(\alpha+\beta+\gamma) \\ b &= \alpha\beta+\beta\gamma+\gamma\alpha \\ c &= -\alpha\beta\gamma[2]. \end{aligned}$$

As α, β and γ are nonzero, we can divide the last two equations to get

$$\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}=\frac{\beta\gamma+\gamma\alpha+\alpha\beta}{\alpha\beta\gamma}=-\frac{b}{c}[1].$$

If $c=1$, this reduces to $\alpha^{-1}+\beta^{-1}+\gamma^{-1}=-b$ [1].

(c) The Galois group is either the group Σ_R of all permutations of the set $R=\{\alpha,\beta,\gamma\}$, or the subgroup A_R of even permutations [2].

(d) Consider the element

$$\Delta=(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2=a^2b^2-4a^3c-4b^3+18abc-27c^2\in\mathbb{Q}.[1]$$

The Galois group is A_R if Δ is the square of some element of $\mathbb{Q}$, and Σ_R otherwise [1]. In the case $f(x)=x^3+x^2-4x+1$, we have $a=c=1$ and $b=-4$, so

$$\Delta=(-4)^2-4-4.(-4)^3+18.(-4)-27=16-4+256-72-27=169=13^2,[1]$$

so the Galois group is A_R [1].

(e) Now put $u=(3\sqrt{-3}-5)/(2\sqrt{13})$, let v be a cube root of u, and put $w=\sqrt{13}(u^{1/3}+\overline{u}^{1/3})/3$. We then have

$$u\overline{u}=\left(\frac{3\sqrt{-3}-5}{2\sqrt{13}}\right)\left(\frac{-3\sqrt{-3}-5}{2\sqrt{13}}\right)=-\frac{(3\sqrt{-3})^2-5^2}{4\times 13}=\frac{27+25}{52}=1,$$

or in other words $\overline{u}=1/u$ [2]. It is also clear that $u+\overline{u}=-5/\sqrt{13}$. Now

$$\begin{aligned} f(x-1/3) &= (x-1/3)^3+(x-1/3)^2-4(x-1/3)+1 \\ &= x^3-x^2+x/3-1/27+x^2-2x/3+1/9-4x+4/3+1 \\ &= x^3-13x/3+65/27,[1] \end{aligned}$$

and

$$\begin{aligned} w &= \frac{13^{1/2}}{3}(v+v^{-1}) \\ w^3 &= \frac{13^{3/2}}{27}(v^3+3v+3v^{-1}+v^{-3}) \\ &= \frac{13^{3/2}}{27}(u+3v+3v^{-1}+u^{-1})[2] \end{aligned}$$

so

$$\begin{aligned} f(w-1/3) &= w^3 - \frac{13}{3}w + \frac{65}{27}[1] \\ &= \frac{13^{3/2}}{27}(u+3v+3v^{-1}+u^{-1}) - \frac{13}{3}\frac{13^{1/2}}{3}(v+v^{-1}) + \frac{65}{27} \\ &= \frac{13^{3/2}}{27}(u+\overline{u}) + \frac{65}{27} = \frac{13^{3/2}}{27}.\frac{-5}{\sqrt{13}} + \frac{65}{27}[1] \\ &= 0. \end{aligned}$$

(14)

(a) Give a detailed statement, without proof, of the Galois correspondence. You should include information about orders of subgroups, degrees and Galois groups of intermediate field extensions, conjugacy and containment between subgroups, and normality of field extensions. **(11 marks)**

(b) Suppose we have a normal extension L/K such that $G(L/K)$ is cyclic of order 30. Prove that for each positive integer d that divides 30, there is a unique field M_d with $K \subseteq M_d \subseteq L$ and $[M_d : K] = d$. Prove also that M_d is normal over K. **(9 marks)**

(c) Suppose we have a normal extension L/K with $|G(L/K)| = 105$ and subgroups $A, B \leq G(L/K)$ with $|A| = 21$ and $|B| = 35$. Prove that $L^A \cap L^B = K$. **(5 marks)**

Solution:

(a) **(Bookwork)** Let L be a normal extension [1]of finite degree over a subfield K, with Galois group G. Let $\mathcal{H}$ be the set of subgroups of G, and let $\mathcal{M}$ be the set of fields M such that $K \subseteq M \subseteq L$ [1]. Then there is an order-reversing [1]bijection $\mathcal{H} \to \mathcal{M}$ given by $H \mapsto L^H$ [1], with inverse $M \mapsto G(L/M)$ [1]. Moreover, if H corresponds to M then

- $[L : M] = |H|$ [1]and $[M : K] = |G/H|$ [1].
- L is normal over M, with Galois group H [1].
- For any $\sigma \in G$, the subgroup $\sigma H \sigma^{-1}$ corresponds to the field $\sigma(M)$ [1].
- M is normal over K if and only if H is a normal subgroup of G [1], and if so, then the corresponding Galois group is G/H [1].

(b) **(Similar problems have been seen.)** Suppose we have fields $K \subseteq L$ such that L is normal over K and $G(L/K)$ is cyclic of order 30. Choose a generator $\phi \in G(L/K)$, so $G(L/K) = \{\phi^i \mid 0 \leq i < 30\}$. For each d dividing 30, let H_d be the subgroup generated by ϕ^d, so $|H_d| = 30/d$ [2]. Put $M_d = L^{H_d}$, so $[L : M_d] = |H_d| = 30/d$ [1]. On the other hand, as L/K is normal we have $[L : M_d][M_d : K] = [L : K] = |G(L/K)| = 30$, so $[M_d : K] = 30/[L : M_d] = d$ as required [1]. As $G(L/K)$ is abelian we also see that H_d is automatically a normal subgroup [1], so M_d is normal over $\mathbb{Q}$ (with Galois group $G(L/K)/H_d$) [1]. As $G(L/K)$ is cyclic, it is standard that the groups H_d are the only subgroups [1]. It follows by the Galois corresponding that the fields M_d are the only intermediate fields between K and L; in particular, M_d is the unique intermediate field with $[M_d : K] = d$ [1].

(c) **(Unseen)** Suppose we have a normal extension L/K with $|G(L/K)| = 105$ and subgroups $A, B \leq G(L/K)$ with $|A| = 21$ and $|B| = 35$. The Galois correspondence tells us that $[L^A : K] = |G(L/K)|/|A| = 105/21 = 5$ and similarly $[L^B : K] = 105/35 = 3$ [2]. Now put $M = L^A \cap L^B$. We have a chain of fields $K \leq M \leq L^A$, so $5 = [L^A : K] = [L^A : M][M : K]$, so $[M : K]$ divides 5. Similarly, using $K \leq M \leq L^B$ we see that $[M : K]$ divides 3 [3]. We must therefore have $[M : K] = 1$, so $M = K$ [1].

(15)

(a) Give a detailed statement, without proof, of the Galois correspondence. You should include information about orders of subgroups, degrees and Galois groups of intermediate field extensions, conjugacy and containment between subgroups, and normality of field extensions. **(10 marks)**

(b) List all the elements of the alternating group A_4 and their orders. **(3 marks)**

(c) List all the subgroups of A_4, and state which of them are normal. In particular, you should show that there is a unique subgroup of order 4. You may assume without proof that there are no subgroups of order 6. **(8 marks)**

(d) Let L be a normal extension of $\mathbb{Q}$ such that the Galois group $G(L/\mathbb{Q})$ is isomorphic to A_4. What can we deduce about the subfields of L? You should give as many details as possible, but you need not justify them. **(4 marks)**

Solution:

(a) **Bookwork.** Let L be a normal extension [1]of finite degree over a subfield K, with Galois group G. Let $\mathcal{H}$ be the set of subgroups of G, and let $\mathcal{M}$ be the set of fields M such that $K \subseteq M \subseteq L$ [1]. Then there is an order-reversing bijection $\mathcal{H} \to \mathcal{M}$ given by $H \mapsto L^H$ [1], with inverse $M \mapsto G(L/M)$ [1]. Moreover, if H corresponds to M then

- $[L : M] = |H|$ [1]and $[M : K] = |G/H|$ [1].
- L is normal over M, with Galois group H [1].
- For any $\sigma \in G$, the subgroup $\sigma H \sigma^{-1}$ corresponds to the field $\sigma(M)$ [1].
- M is normal over K if and only if H is a normal subgroup of G [1], and if so, then the corresponding Galois group is G/H [1].

(b) **The students will have seen a similar analysis for other groups such as Σ_3 and D_8 and $(\mathbb{Z}/n)^\times$ for various n. They will also have seen some facts about A_4 in connection with quartics.** The elements of A_4 are as follows:

(1) The identity permutation has order one.

(2) The elements $\tau_1 = (2\ 3)(1\ 4)$, $\tau_2 = (1\ 3)(2\ 4)$ and $\tau_3 = (1\ 2)(3\ 4)$ are the only elements of order 2. [1]

(3) There are 8 elements of order 3:

$$\begin{aligned} \rho_1 &= (2\ 3\ 4) & \rho_1^{-1} &= (4\ 3\ 2) \\ \rho_2 &= (1\ 3\ 4) & \rho_2^{-1} &= (4\ 3\ 1) \\ \rho_3 &= (1\ 2\ 4) & \rho_3^{-1} &= (4\ 2\ 1) \\ \rho_4 &= (1\ 2\ 3) & \rho_4^{-1} &= (3\ 2\ 1). \end{aligned}$$ [2]

(c) The subgroups of A_4 are as follows:

(1) There is the trivial subgroup, denoted by 1.

(2) There are three subgroups of order 2, namely $P_i = \{1, \tau_i\}$ for $i = 0, 1, 2$. These are all conjugate to each other, so none of them are normal. [1]

(3) There are four subgroups of order 3, namely $Q_i = \{1, \rho_i, \rho_i^{-1}\}$ for $i = 0, 1, 2, 3$. These are all conjugate to each other, so none of them are normal. [2]

(4) Put $R = \{1, \tau_1, \tau_2, \tau_3\}$ [1], which is the set of all elements of order 1 or 2. One can check that $\tau_1\tau_2 = \tau_2\tau_1 = \tau_3$ and $\tau_2\tau_3 = \tau_3\tau_2 = \tau_1$ and $\tau_3\tau_1 = \tau_1\tau_3 = \tau_2$, so R is a subgroup of A_4 [1]. We claim that it is the only one. To see this, note that there are no elements of order 4 (because 4-cycles are odd permutations and so do not lie in A_4). Thus, any subgroup R' of order 4 must consist of elements of order one or two, so we must have $R' \subseteq R$, but $|R'| = |R| = 4$ so $R' = R$ [2].

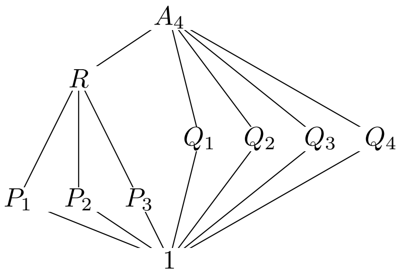
(5) It is given that there are no subgroups of order 6. For completeness we record a proof, which students are not expected to provide. Any subgroup T of order 6 would have to contain an element of order 2 (say τ_i) and an element of order 3 (say ρ_j). Put $k = \tau_i(j)$ and note that $k \neq j$. The permutation $\tau_i\rho_j\tau_i^{-1}$ sends k to itself, so must be different from ρ_j, which sends only j to itself. Thus τ_i and ρ_j do not commute, so the conjugate $\rho_j\tau_i\rho_j^{-1}$ is an element of order 2 different from τ_i, so it must be τ_m for some $m \neq i$. Now τ_i and τ_m generate R, so $R \leq T$, so $|T|$ is divisible by $|R| = 4$, which contradicts the assumption that $|T| = 6$.

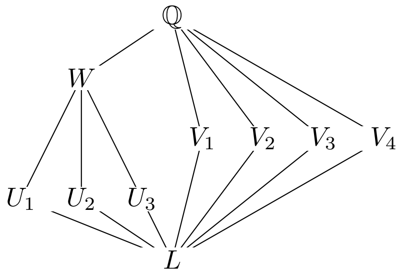
Alternatively, we can recall that any subgroup of index two is automatically normal. This means that T would have to be a disjoint union of conjugacy classes, and a straightforward check of cases shows that this is impossible.

(6) The full group A_4 is the unique subgroup of order 12.

(7) The order of any subgroup must be a divisor of $|A_4| = 12$, so we have now covered all possibilities. [1]

(d) We now see that the subgroup lattice is as shown on the left below, with the larger subgroups towards the top.





It follows that the lattice of subfields of L is as shown on the right, where $U_i = L^{P_i}$ and $V_i = L^{Q_i}$ and $W = L^R$. The larger subfields are towards the bottom, and the degrees are as follows:

$$\begin{array}{ccc} [L : U_i] = 2 & [U_i : W] = 2 & [W : \mathbb{Q}] = 3 \\ [L : V_i] = 3 & & [V_i : \mathbb{Q}] = 4. \end{array}$$

The field W is normal over $\mathbb{Q}$, with $G(W/\mathbb{Q}) = A_4/R \simeq C_3$, but the fields P_i and Q_i are not normal over $\mathbb{Q}$. [4]