1. For each of the following quartic polynomials f compute $\mathrm{Gal}(L/\mathbb{Q})$, where L is the splitting field of f. The resultant cubic $p(t)$ and discriminant $\Delta(f)$ for each f are included in the table. All of the polynomials are irreducible over $\mathbb{Q}$, a fact you may assume without having to prove.

	$f(x)$	$p(t)$	$\Delta(f)$
(a)	$x^4 - 2x^3 + 2x^2 + 2$	$t^3 - 2t^2 - 8t + 8$	3136
(b)	$x^4 + x^3 + 2x^2 + 2x + 1$	$t^3 - 2t^2 - 2t + 3$	117
(c)	$x^4 + 2x^3 + 2x^2 - 2x + 1$	$t^3 - 2t^2 - 8t$	2304
(d)	$x^4 + x^3 + x^2 + x + 1$	$t^3 - t^2 - 3t + 2$	125
(e)	$x^4 + 2x^3 + x^2 - 3x + 1$	$t^3 - t^2 - 10t - 9$	257

Solution. The algorithm for determining the Galois group of an irreducible quartic $f(x) = x^4 + bx^3 + cx^2 + dx + e \in K[x]$ is explained in the chart below.

$p(t)$	$\delta(f)$	$\sqrt{(b^2 - 4c + 4\beta)\Delta(f)}$ and $\sqrt{(\beta^2 - 4e)\Delta(f)}$	Group
irred. over K	$\notin K$		S_4
irred. over K	$\in K$		A_4
splits completely in K	$(\in K)$		V
one root $\beta \in K$	$(\notin K)$	one or both $\notin K$	D_4
one root $\beta \in K$	$(\notin K)$	both $\in K$	C_4

Here $p(t) = t^3 - ct^2 + (bd - 4e)t + (4ce - d^2 - b^2e)$ is the resolvent cubic, and the discriminant of $f(x)$ may be computed by computing the discriminant of $p(t)$. Applying the algorithm we see the following.

(a) The Galois group is A_4. We have $\Delta(f) = 2^6 \cdot 7^2$ is a square, so $\delta(f) = 2^3 \cdot 7 \in \mathbb{Q}$. On the other hand, $p(t) = t^3 - 2t^2 - 8t + 8$ is irreducible over $\mathbb{Q}$. One way to see that $p(t)$ is irreducible is to note that $p(t) \equiv t^3 + t^2 + t + 2 \pmod 3$, and that $t^3 + t^2 + t + 2$ has no root in $\mathbb{F}_3$. Therefore, by the chart, the Galois group is A_4.

(b) The Galois group is D_4. The resolvent cubic factors as $t^3 - 2t^2 - 2t + 3 = (t - 1) \cdot (t^2 - t - 3)$, and the quadratic factor is irreducible since its discriminant $(-1)^2 - 4 \cdot (-3)(1) = 13$ is not a square. Therefore the Galois group must be either V or D_4. The root of $p(t)$ in $\mathbb{Q}$ is $\beta = 1$, and $\Delta(f) = 117 = 3^2 \cdot 13$. Since $(b^2 - 4c + 4\beta) = (1^2 - 4 \cdot 2 + 4 \cdot 1) = -3$, and $(b^2 - 4c + 4\beta)\Delta(f) = -3 \cdot 117 = -351$ is not a square in $\mathbb{Q}$, we see that the Galois group must be D_4. (It's also true that $(\beta^2 - 4e)\Delta(f) = (1^2 - 4 \cdot 1) \cdot 117$, which is again -351, is not a square in $\mathbb{Q}$.)

(c) The Galois group is V. The resolvent cubic factors completely over $\mathbb{Q}$ as $t^3 - 2t^2 - 8t = t(t+2)(t-4)$, and V is the only possibility where the cubic factors completely.

(d) The Galois group is C_4. There are two ways to see this. The polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$ is the minimal polynomial of the primitive 5-th root of unity $\zeta = e^{2\pi i/5}$ (for example by **H3** Q1(a)). The Galois group after adding any p-th root of unity to $\mathbb{Q}$ is the same as the multiplicative group $\mathbb{F}_p^*$, which we know is cyclic of order $p-1$. (We did a computation like this for $p = 7$ in **H7** Q2.) Hence the Galois group is cyclic of order $5 - 1 = 4$.

Alternatively, we can use algorithm. The resolvent cubic factors as $p(t) = t^3 - t^2 - 3t + 2 = (t-2)(t^2+t-1)$. The quadratic factor is irreducible over $\mathbb{Q}$ since its discriminant is $1^2 - 4(1)(-1) = 5$, which is not a square in $\mathbb{Q}$. Therefore the Galois group must be C_4 or D_4. The root of $p(t)$ in $\mathbb{Q}$ is $\beta = 2$, and $\Delta(f) = 125 = 5^3$. Since $(b^2 - 4c + 4\beta) \cdot \Delta(f) = (1^2 - 4(1) + 4(2)) \cdot 125 = 5 \cdot 125 = 5^4$ is a square in $\mathbb{Q}$, and since $(\beta^2 - 4e)\Delta(f) = (2^2 - 4(1))\Delta(f) = 0$ is a square in $\mathbb{Q}$, we see that the Galois group must be C_4.

(e) The Galois group is S_4. We have $\Delta(f) = 257$ is prime, so $\Delta(f)$ is not a square in $\mathbb{Q}$. The resolvent cubic $p(t) = t^3 - t^2 - 10t - 9$ and is irreducible over $\mathbb{Q}$. One way to see that $p(t)$ is irreducible over $\mathbb{Q}$ is to note that $p(t) \equiv t^3 + t^2 + 1 \pmod 2$, and that $t^3 + t^2 + 1$ has no root over $\mathbb{F}_2$. Therefore (by the chart), the Galois group is S_4.

2. In class we skipped over almost all of the details of the algorithm for detecting the difference between C_4 and D_4 when computing the Galois group of an irreducible quartic polynomial. In this problem we will check some of the claims for the polynomial $g_1(t)$.

Let K be a field of characteristic zero, and let $f = x^4 + bx^3 + cx^2 + dx + e \in K[x]$ be an irreducible quartic with splitting field L. We suppose that the resultant cubic $p(t)$ has a single root $\beta \in K$, $\beta = \gamma_{13|24}$. Recall that this means that the Galois group G is contained in $\langle (1\,2\,3\,4), (1\,3) \rangle = D_4$, and is either D_4 or $C_4 = \langle (1\,2\,3\,4) \rangle$. We set

$$g_1(t) = (t-(\alpha_1+\alpha_3))(t-(\alpha_2+\alpha_4)) = t^2-(\alpha_1+\alpha_2+\alpha_3+\alpha_4)t+(\alpha_1+\alpha_3)(\alpha_2+\alpha_4) = t^2+bt+(c-\beta).$$

The importance of the last equality is that it shows that $g_1(t) \in K[t]$.

(a) Explain what $\sigma = (1\,2\,3\,4)$ does to each of the roots α_1, α_2, α_3, and α_4. (This question is to asking if you understand the isomorphism $\mathrm{Perm}(S) \cong S_4$ we have been using.)

(b) Show that $\{\alpha_1 + \alpha_3, \alpha_2 + \alpha_4\}$ is a single orbit under C_4 and D_4.

(c) There is nothing to say that $\alpha_1+\alpha_3$ and $\alpha_2+\alpha_4$ couldn't be equal. (The set in (b) could consist of a single element, e.g. $\{z,z\}=\{z\}$.) Show that $\alpha_1+\alpha_3=\alpha_2+\alpha_4$ if and only if $\alpha_1+\alpha_3\in K$. (HINT : Your calculation in (b) is relevant.)

(d) Conclude that either $g_1(t)$ is irreducible over K or that $g_1(t)$ has a double root.

(e) Explain why either $\delta(g_1)\notin K$ or $\delta(g_1)=0$.

We now want to show that if $G=C_4$ then $\delta(g_1)\delta(f)\in K$. This is clear when $\delta(g_1)=0$, so for the rest of the problem we assume that $\delta(g_1)\neq 0$. We also assume that $G=C_4$.

(f) Explain why $\delta(f)\notin K$. (REMINDERS : What does $\delta(f)$ detect? What is G?)

(g) Explain why there is only one intermediate field $M\subset L$ of degree 2 over K.

(h) Explain why $K(\delta(g_1))$ and $K(\delta(f))$ are degree 2 extensions of K.

(i) By (g) and (h) there are $a_0, a_1\in K$ such that $\delta(g_1)=a_0+a_1\delta(f)$. Since $\delta(g_1)\notin K$, $\delta(g_1)$ is not fixed by G, and hence there is some $\tau\in G$ so that $\tau\cdot\delta(g_1)=-\delta(g_1)$. Applying τ to the equation above, explain why this means that $a_0=0$.

(j) Explain why $\delta(g_1)\delta(f)\in K$.

REMARKS. (1) The same argument, with $\alpha_1\alpha_3$ and $\alpha_2\alpha_4$ replacing $\alpha_1+\alpha_3$ and $\alpha_2+\alpha_4$, shows that if $G=C_4$ then $\delta(g_2)\delta(f)\in K$. (2) A separate (shorter) computation shows that both of these cannot happen if $G=D_4$, which leads to the criterion for the test.

Solution.

(a) The isomorphism of $\mathrm{Perm}(S)$ and S_4 is obtained by matching the root α_i with the integer i. Since σ sends 1 to 2, 2 to 3, 3 to 4, and 4 to 1, we have $\sigma(\alpha_1)=\alpha_2$, $\sigma(\alpha_2)=\alpha_3$, $\sigma(\alpha_3)=\alpha_4$, and $\sigma(\alpha_4)=\alpha_1$.

(b) From the formulae above we have $\sigma(\alpha_1+\alpha_3)=\sigma(\alpha_1)+\sigma(\alpha_3)=\alpha_2+\alpha_4$, and $\sigma(\alpha_2+\alpha_4)=\sigma(\alpha_2)+\sigma(\alpha_4)=\alpha_1+\alpha_3$. Since σ swaps $\alpha_1+\alpha_3$ and $\alpha_2+\alpha_4$, the set $\{\alpha_1+\alpha_3,\,\alpha_2+\alpha_4\}$ is a single orbit of $C_4=\langle\sigma\rangle$. The group D_4, which contains C_4, might have a larger orbit since other elements of D_4 might send $\alpha_1+\alpha_2$ and $\alpha_2+\alpha_4$ to different elements of L. However $\tau=(1\,3)$ fixes each of $\alpha_1+\alpha_3$ and $\alpha_2+\alpha_4$ (i.e, $\tau(\alpha_1+\alpha_3)=\alpha_1+\alpha_3$, and $\tau(\alpha_2+\alpha_4)=\alpha_2+\alpha_4$). Therefore the orbit of $D_4=\langle\sigma,\tau\rangle$ is again the set $\{\alpha_1+\alpha_3,\,\alpha_2+\alpha_4\}$.

(c) If $\alpha_1+\alpha_3$ is in K then it is fixed by all elements of the Galois group. In particular $\sigma(\alpha_1+\alpha_3)=\alpha_1+\alpha_3$. Above we have calculated that $\sigma(\alpha_1+\alpha_3)=\alpha_2+\alpha_4$, and combining these we conclude that $\alpha_1+\alpha_3=\alpha_2+\alpha_4$. Conversely, if $\alpha_1+\alpha_3=\alpha_2+\alpha_4$ then by (b) the set $\{\alpha_1+\alpha_3,\alpha_2+\alpha_4\}=\{\alpha_1+\alpha_3\}$ is fixed by G, and so $\alpha_1+\alpha_3$ is in $L^G=K$.

(d) If $g_1(t)$ is reducible then both of its roots, namely $\alpha_1 + \alpha_3$ and $\alpha_2 + \alpha_4$ are in K. Then by (c) $\alpha_1 + \alpha_3 = \alpha_2 + \alpha_4$, so that $g_1(t)$ has a double root. Conversely, if $g_1(t)$ has a double root then $\alpha_1 + \alpha_3 = \alpha_2 + \alpha_4$ so again by (c) both are in K and $g_1(t)$ factors over K.

(e) The quadratic formula tells us that a degree two polynomial $g(t) \in K[t]$ factors over K if and only if its discriminant $\Delta(g)$ is a square in K. By (d) we either have $g_1(t)$ is irreducible (and so $\delta(g_1) \notin K$) or $g_1(t)$ has a double root (so $\delta(g_1) = 0$).

(f) First note that $\delta(f) \neq 0$: since f is an irreducible polynomial over a field of characteristic zero it has no repeated roots. The action of the Galois group on $\delta(f)$ detects whether or not G is contained in the alternating group. The element $\sigma = (1\,2\,3\,4) \in C_4$ is not in A_4 and so $\sigma(\delta(f)) = -\delta(f)$, showing that $\delta(f) \notin K$.

(g) By the Galois correspondence, an intermediate field $K \subset M \subset L$ of degree 2 over K corresponds to a subgroup H of index 2 in $G = C_4$. Since C_4 is a cyclic group, it has only one subgroup of degree e for any e dividing 4. In particular, it has only one subgroup of index 2, and so there is only one intermediate field of degree 2 over K.

(h) We know that $\Delta(f) = \delta(f)^2$ and $\Delta(g_1) = \delta(g_1)^2$ are in K. Therefore the generators of $K(\delta(g_1))$ and $K(\delta(f))$ satisfy degree 2 equations over K. The generators $\delta(g_1)$ and $\delta(f)$ are also not in K themselves by our assumption and (f). Therefore the extensions are of degree 2 over K.

(i) Applying τ to $\delta(g_1) = a_0 + a_1\delta(f)$ we get

$$-\delta(g_1) = \tau(\delta(g_1)) = \tau(a_0 + a_1\delta(f)) = a_0 + a_1\tau(\delta(f)) = a_0 \pm a_1\delta(f).$$

(At the moment we don't' know whether $\tau(\delta(f)) = \delta(f)$ or $-\delta(f)$.) But we also know that $-\delta(g_1) = -(a_0 + a_1\delta(f)) = -a_0 - a_1\delta(f)$, and comparing these gives $-a_0 - a_1\delta(f) = a_0 \pm a_1\delta(f)$. Since 1 and $\delta(f)$ are a basis for $K(\delta(f))$ over K, this means that we have $-a_0 = a_0$ (and so $a_0 = 0$) and $\tau(\delta(f)) = -\delta(f)$ (which we don't need at the moment).

(j) Since $a_0 = 0$ this means that $\delta(g_1) = a_1\delta(f)$ with $a_1 \in K$, and so $\delta(g_1)\delta(f) = (a_1\delta(f))\delta(f) = a_1\delta(f)^2 = a_1\Delta(f) \in K$.

3. Let L/K be a Galois extension with Galois group G, and β an element of L. Let $S = \mathrm{Orb}_G(\beta)$ be the orbit of β under G, say $S = \{\beta = \beta_1, \beta_2, \ldots, \beta_s\}$, and finally set $q(x) = \prod_{j=1}^{s}(x - \beta_j)$.

In this problem we will show that $q(x)$ is the minimal polynomial of β over K.

(a) Explain why all the coefficients of $q(x)$ are in K, so that $q(x) \in K[x]$. (SUGGESTION : what does acting by G do to the elements of S?)

It is clear that $q(x)$ is a monic polynomial with β as a root. Therefore to show that $q(x)$ is the minimal polynomial of β, it is sufficient to show that $q(x)$ is irreducible over K.

(b) Suppose that $q(x)$ factors as $q(x) = q_1(x)q_2(x)$, with each of $q_1, q_2 \in K[x]$, and of degree at least one. By relabelling q_1 and q_2 if necessary, we may assume that $q_1(\beta) = 0$. Explain why, for every $\sigma \in G$, $\sigma(\beta)$ is a root of $q_1(x)$.

(c) Show that none of the roots of $q_2(x)$ are in the orbit of β.

(d) Explain why the result in (c) is a contradiction, and hence that $q(x)$ must be irreducible.

Solution.

(a) Since the set S is a single orbit of G, G acts on S by permuting its elements. The coefficients of $q(x)$ are, up to sign, the elementary symmetric polynomials in $\beta_1, \ldots, \beta_s$. Hence any permutation leaves them unchanged, in particular, action by G leaves them unchanged. Thus the coefficients are in $L^G = K$.

(b) We have seen this argument many times, first in the class "Automorphisms fixing a subfield" from January 20th. If $q_1(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ with the $a_i \in K$, then

$$\begin{aligned} 0 &= \sigma(0) = \sigma(q_1(\beta)) = \sigma(\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0) \\ &= \sigma(\beta)^n + a_{n-1}\sigma(\beta)^{n-1} + \cdots + a_1\sigma(\beta) + a_0 = q_1(\sigma(\beta)), \end{aligned}$$

so $\sigma(\beta)$ is a root of $q_1(x)$.

(c) The elements of the set S are distinct, so $q(x)$ has no repeated roots. This means that $q_1(x)$ and $q_2(x)$ have no roots in common. Part (b) shows that the orbit of β is contained in the subset of roots of $q_1(x)$, therefore no roots of $q_2(x)$ are in the orbit of β.

(d) Since $\deg q_2(x) \geqslant 1$, $q_2(x)$ must have at least one root. By construction the roots of $q(x)$ are the elements in the orbit of β, so all roots of $q_2(x)$ are a subset of the orbit. This contradicts (c), and shows that we could not have had the factorization $q(x) = q_1(x)q_2(x)$ over K with both $q_1(x)$ and $q_2(x)$ of degree $\geqslant 1$. Therefore $q(x)$ is irreducible over K.

REMARK. We have used the argument in part (a) before : see the proof of (3) $\Longrightarrow$ (2) on February 4th ("Galois Extensions").