DUE DATE: MAR. 24, 2016

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

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.

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.

REMARK. In other arguments (e.g., in class, or **H7** Q1) we have shown that given an irreducible polynomial $q(x) \in K[x]$, with roots in a Galois extension L/K, that the Galois group $G = \mathrm{Gal}(L/K)$ acts transitively on the set of roots of $q(x)$. Thus, the set of roots of $q(x)$ is a single orbit under G. Reversing this, we conclude that given an element $\beta \in L$, the minimal polynomial of β must be the polynomial whose roots are the orbit of β. In other words, arguments we have already made lead to the conclusion of Q3. On the other hand, the arguments in Q3 also imply that G acts transitively on the roots of $q(x)$, i.e., imply the arguments we have already made (and without using the lifting lemma!). Probably it is best to absorb these as a single fact.