# Galois theory 2018–19: Example Sheet 4

1. Let $\zeta$ be a primitive $n$th root of unity, where $n \geq 3$, and write $\beta = \zeta + \frac{1}{\zeta}$.

   (a) Show that $\zeta$ satisfies a quadratic equation over $\mathbb{Q}(\beta)$ and deduce that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] \leq 2$.

   (b) Show that $\mathbb{Q}(\beta) \subset \mathbb{R}$, and deduce that $\zeta \notin \mathbb{Q}(\beta)$.

   (c) Deduce that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\beta)] = 2$ and hence calculate $[\mathbb{Q}(\beta) : \mathbb{Q}]$.

   (d) Prove by induction that for all $m$, $\zeta^m + \frac{1}{\zeta^m} \in \mathbb{Q}(\beta)$.

   (e) Express $\zeta^5 + \frac{1}{\zeta^5}$ as a polynomial in $\beta$.

   [*Hint for (d) and (e): if* $\zeta^m + \frac{1}{\zeta^m} = P_m(\beta)$, *show that* $\zeta^{m+1} + \frac{1}{\zeta^{m+1}} = P_1(\beta)P_m(\beta) - P_{m-1}(\beta)$.]

2. Let $\zeta$ be a primitive 5th root of unity, and let $\alpha$ denote the real 5th root of 2. You are given that $\mathbb{Q}(\zeta, \alpha)$ is the splitting field of $x^5 - 2$ over $\mathbb{Q}$ and that $[\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = 20$.

   (a) Specify the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q})$ by writing down how they act on $\zeta$ and on $\alpha$.

   (b) Show that there exist automorphisms $\phi$, $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q})$ such that $\phi$ has order 4, $\psi$ has order 5, and $\mathrm{Gal}(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}) = \langle \phi, \psi \rangle$.

   (c) Write $\phi\psi\phi^{-1}$ in the form $\phi^i\psi^j$.

   (d) Recall that if $\beta = \zeta + \frac{1}{\zeta}$, then $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{5})$. Under the Galois correspondence, what should be the order of the corresponding subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}(\beta))$?

   (e) Show that the group $\mathrm{Gal}(\mathbb{Q}(\zeta, \alpha)/\mathbb{Q}(\beta))$ is $\langle \phi^2, \psi \rangle$.

3. Let $L$ be the splitting field of $x^7 - 3$ over $\mathbb{Q}$. You know that $[L : \mathbb{Q}] = 42$. Calculate the elements of $\mathrm{Gal}(L/\mathbb{Q})$. Find $\psi$, $\phi \in \mathrm{Gal}(L/\mathbb{Q})$ which satisfy:

   (a) $\psi$ has order 7, $\phi$ has order 6

   (b) $\phi\psi\phi^{-1} = \psi^3$

   (c) $\mathrm{Gal}(L/\mathbb{Q}) = \langle \phi, \psi \rangle$

4. In Maple, you can compute Galois groups of polynomials as follows.

   Type `infolevel[galois]:=2;` and then compute the Galois groups of a polynomial $f$ (of degree up to 7), type `galois(`$f$`);` (you should replace $f$ here by `x^5-2` or `x^7-3`, for example). Try lots of different examples and write a paragraph or two describing how Maple's algorithm seems to work. Amongst others, you may like to compare what happens in the following examples:

   - $x^5 - 4x + 2$, $x^5 + 20x + 16$, $x^5 - 2$, $x^5 - 5x + 12$, $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$;
   - $x^4 + 8x + 12$, $x^4 + 8x - 12$, $x^4 - 10x^2 + 1$, $x^4 + 1$, $x^4 + x^3 + x^2 + x + 1$;
   - $x^3 + 3x + 1$, $x^3 - 3x + 1$.