MODULE 3: EXERCISE SHEET 1

These problems are due Sunday, 12 June, 2016. They must be sent to nap@rnta.eu (copy to nickgill@cantab.net) by 10 pm Nepal time.

(1) Let p be an odd prime, and let ζ be a primitive pth root of 1 in $\mathbb{C}$. Let $E = \mathbb{Q}[\zeta]$ and let $G = \mathrm{Gal}(E, \mathbb{F}_q)$; thus $G = \mathbb{Z}/p\mathbb{Z}$. Let H be the subgroup of index 2 in G. Put $\alpha = \sum_{i \in H} \zeta^i$ and $\beta = \sum_{i \in G \setminus H} \zeta^i$. Show:
  (a) α and β are fixed by H;
  (b) if $\sigma \in G \setminus H$, then $\sigma\alpha = \beta$, $\sigma\beta = \alpha$.

  Thus α and β are roots of the polynomial $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$. Compute $\alpha\beta$ and show that the fixed field of H is $\mathbb{Q}[\sqrt{p}]$ when $p \equiv 1 \pmod 4$, and $\mathbb{Q}[\sqrt{-p}]$ when $p \equiv 3 \pmod 4$.

(2) (a) Prove that if g is a group for which $g^2 = 1$ for all $g \in G$, then G is abelian.
  (b) Prove that the only non-abelian groups of order 8 are the quaternion group, Q_8, and D_4.

(3) Let $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $E = M\left[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}\right]$.
  (a) Show that M is Galois over $\mathbb{Q}$ with Galois group the 4-group $C_2 \times C_2$.
  (b) Show that E is Galois over $\mathbb{Q}$ with Galois group Q_8.

(4) Let G be the Galois group of $f(X) = X^4 - 2$ over $\mathbb{Q}$. Thus if θ is the positive fourth root of 2, then G is the Galois group of $\mathbb{K} : \mathbb{Q}$ where $\mathbb{K} = \mathbb{Q}(\theta, i)$.
  (a) Describe all 8 automorphisms in G.
  (b) Show that G is isomorphic to the dihedral group D_4.
  (c) The group G has two normal subgroups N_1 and N_2 that are of order 4 and are not cyclic. Write down the elements of N_1 and N_2 and verify that the corresponding fixed fields, $\mathbb{K}^{N_1}$ and $\mathbb{K}^{N_2}$, are normal extensions of $\mathbb{Q}$.

(5) In this question we generalize Example 3.22 from the notes. Let $f = X^p - 2 \in \mathbb{Q}[x]$ (where p is a prime), and let E be the splitting field of f over $\mathbb{Q}$.
  (a) Prove that f is irreducible.
  (b) Prove that $[E : \mathbb{Q}] = p(p-1)$.
  (c) Prove that $\mathrm{Gal}(E, \mathbb{Q})$ has a normal subgroup N of order p, and calculate E^N.
  (d) Write down a subgroup $H \leq \mathrm{Gal}(E, \mathbb{Q})$ of order $p - 1$.
  (e) Prove that $\mathrm{Gal}(E, \mathbb{Q}) = N \rtimes H$, and describe the action of H on N.

(6) Describe the Galois groups of $f = X^6 - 1$ and $X^6 + 1$ over $\mathbb{Q}$. Write down the lattice of fields/ groups for each polynomial, identifying which inclusions are normal.

(7) The complex numbers $i\sqrt{3}$ and $1 + i\sqrt{3}$ are roots of the quartic $f = X^4 - 2X^3 + 7X^2 - 6X + 12$. Does there exist an automorphism σ of the splitting field extension for f over $\mathbb{Q}$ with $\sigma(i\sqrt{3}) = 1 + i\sqrt{3}$?

(8) Describe the transitive subgroups of S_3, S_4 and S_5.

(9) Find the Galois group of $X^4 - 2$ over (a) $\mathbb{F}_3$, (b), $\mathbb{F}_7$. (You calculated the Galois group of $X^4 - 2$ over $\mathbb{Q}$ in question (4).)

(10) Find the Galois group of $X^4 + 2$ over (a) $\mathbb{Q}$, (b) $\mathbb{F}_3$, (c), $\mathbb{F}_5$.

(11) **(Optional extra)** Suppose that $L : K$ is an extension with $[L : K] = 2$, that every element of L has a square root in L, that every polynomial of odd degree in $K[X]$ has a root in K and that $\mathrm{char} K \neq 2$. Let f be an irreducible polynomial in $K[X]$, let $M : L$ be a splitting field extension for f over L, Let $G = \mathrm{Gal}(M : K)$ and let $H = \mathrm{Gal}(M : L)$.
  (a) By considering the fixed field of a Sylow 2-subgroup of G, show that $|G| = 2^n$.
  (b) By considering a subgroup of index 2 in H, show that if $n > 1$ then there is an irreducible quadratic in $L[X]$.
  (c) Show that L is algebraically closed.
  (d) Show that the complex numbers are algebraically closed.

(12) **(Optional extra)** By considering the splitting field of all polynomials of odd degree over $\mathbb{F}_2$, show that the condition $\mathrm{char} K \neq 2$ cannot be dropped from the previous question.