MA 3419: Galois theory
Homework problems due December 7, 2015

This homework is not compulsory, however, you may submit solutions to it, and if your mark is higher than one of the marks for assignment 1–4, the mark for this assignment will replace the lowest of those. In other words, your final mark will be

$$\frac{1}{4}\left(m_1+m_2+m_3+m_4-\min(m_1,m_2,m_3,m_4)+\max(\min(m_1,m_2,m_3,m_4),m_5)\right),$$

where $m_i$ is the mark for assignment $i$.

Solutions to this are due by the end of the class on Thursday December 7. Please attach a cover sheet with a declaration `http://tcd-ie.libguides.com/plagiarism/declaration` confirming that you know and understand College rules on plagiarism.

Please put your name and student number on each of the sheets you are handing in. (Or, ideally, staple them together).

**1.** Find a normal basis for the field extensions $\mathbb{F}_2 \subset \mathbb{F}_{2^k}$ for $k = 2, 3, 4$.

**2.** Find a normal basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, and a normal basis of the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

**3.** Show that the Galois group of the splitting field of $x^5 - x - 1$ over $\mathbb{Q}$ is $S_5$.

**4.** For which values of $n < 16$ do the primitive $n$-th roots of unity form a normal basis of the splitting field of $x^n - 1$ over $\mathbb{Q}$?

In the following problem, you may use without proof the following results:

- If $n = p_1^{a_1} \cdots p_k^{a_k}$ where $p_i$ are distinct primes, we have
$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$
- If $p$ is an odd prime, we have $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$.
- We have $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $k \geqslant 3$.

**5.** Show that there exist some complex numbers roots of unity $\xi_1, \ldots, \xi_s$, and some rational numbers $a_1, \ldots, a_s$, so that the number $\alpha = a_1\xi_1 + \cdots + a_s\xi_s$ satisfies $\mathrm{Gal}(\mathbb{Q}(\alpha)\colon \mathbb{Q}) \cong \mathbb{Z}/720\mathbb{Z}$.