MA 3419: Galois theory
Homework problems due October 17, 2017

Solutions to this are due by the end of the 11am class on Tuesday October 17. 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).

Below, for a prime power q, the notation $\mathbb{F}_q$ refers to the (unique up to isomorphism) finite field of q elements.

1. (**a**) Let $R = \mathbb{Z}/6\mathbb{Z}$. Give an example of a polynomial $x^2 + ax + b \in R[x]$ which has three distinct roots in R. (**b**) Let $R = \mathbb{Z}/4\mathbb{Z}$. Show that even though R is not a field, any polynomial $x^2 + ax + b \in R[x]$ has at most two distinct roots in R.

2. Show that the polynomial $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$, and explain how to use this to construct a field $\mathbb{F}_9$ of 9 elements as "complex numbers modulo three" multiplied by the familiar rule

$$(a + bi)(c + di) = ac - bd + (ad + bc)i.$$

(**a**) We know from class that the multiplicative group $(\mathbb{F}_9)^\times$ is cyclic. List all of the elements $a + bi \in \mathbb{F}_9$ that can be chosen as a generator of that group.

3. (**a**) List all irreducible polynomials with coefficients in $\mathbb{F}_2$ of degree at most 4. (Justify your answer.) (**b**) Explain how to construct a field of 8 elements and a field of 16 elements.

4. (**a**) Show that $x^3 + x + 1$ is irreducible in $\mathbb{Q}[x]$. Let a denote the image of x in $\mathbb{Q}[x]/(x^3 + x + 1)$; represent each of the elements (**b**) $1/a$, (**c**) $1/(1 + a)$, and (**d**) $1/(1 + a^2)$ as a polynomial in a.

5. (**a**) Show that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Determine the minimal polynomial of $\sqrt{2}+\sqrt{3}$ (**b**) over $\mathbb{Q}$; (**c**) over $\mathbb{Q}(\sqrt{2})$.

6. Show that if a and b are algebraic over $\mathbb{Q}$, then $a+b$ and ab are also algebraic over $\mathbb{Q}$.