UNIVERSITY OF ST ANDREWS
MT5826 Finite Fields
Tutorial Sheet: Chapter 5

1. Using any method you choose, find a primitive element of $\mathbb{F}_9$. Demonstrate, by direct verification, that each of its conjugates with respect to $\mathbb{F}_3$ is also a primitive element.

2. The set of automorphisms of $\mathbb{C}$ over $\mathbb{R}$ (i.e. the automorphisms of $\mathbb{C}$ which fix $\mathbb{R}$ pointwise) forms a group. Describe this group.
Hint: begin by considering the effect of such an automorphism on $i \in \mathbb{C}$.

3. Let $K = \mathbb{F}_q$ and let F be a finite extension of K. Let $\alpha = \beta^q - \beta$ for some $\beta \in F$.
Prove that

$$\alpha = \gamma^q - \gamma \text{ with } \gamma \in F \Leftrightarrow \beta - \gamma \in K.$$

4. Let $K = \mathbb{F}_q$ and let $F = \mathbb{F}_{q^m}$ be a finite extension of K.
Prove that: for $\alpha \in F$,

$$\mathrm{N}_{F/K}(\alpha) = 1 \Leftrightarrow \alpha = \beta^{q-1} \text{ for some } \beta \in F^*.$$

5. Prove that, if the order of basis elements is taken into account, then the number of different bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ is

$$(q^m - 1)(q^m - q)(q^m - q^2) \cdots (q^m - q^{m-1}).$$