UNIVERSITY OF ST ANDREWS
MT5826 Finite Fields
Tutorial Sheet: Chapter 2

1. Prove that the prime subfield of a field F is a prime field.

2. Give an example of an element which is algebraic over $\mathbb{R}$ but not over $\mathbb{Q}$.

3. Verify that, given $\alpha \in F$ which is algebraic over some subfield K of F, the set

$$J = \{f \in K[x] : f(\alpha) = 0\}$$

is a (non-zero) ideal of $F[x]$.

4. Give the minimal polynomial and degree of

(a) $\sqrt{2}$ over $\mathbb{Q}$;

(b) $\sqrt{2}$ over $\mathbb{R}$;

(c) $i + 1$ over $\mathbb{R}$;

(d) $a + b\sqrt{2}$ over $\mathbb{Q}$, for arbitrary $a, b \in \mathbb{Q}$.

5. Prove that if $\{u_1, \ldots, u_m\}$ spans E over F and if u_m is a linear combination of $u_1, \ldots, u_{m-1}$, then $\{u_1, \ldots, u_{m-1}\}$ spans E over F.

6. Show that the sets

(a) $\{1, i, \sqrt{3}, i\sqrt{3}\}$;

(b) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}\}$

are linearly independent over $\mathbb{Q}$.

7. Let K be a field. In the notes, Theorem 5.7 says that every finite extension of K is algebraic over K. Define the *algebraic numbers* $\mathbb{A}$ to be the set of all those complex numbers which are algebraic over $\mathbb{Q}$.
Show that the converse of Theorem 5.7 is false, by proving that $\mathbb{A}/\mathbb{Q}$ is an algebraic extension which is not finite.

8. Let $\alpha = \sqrt[5]{7} \in \mathbb{R}$. Let $K = \mathbb{Q}(\alpha)$.

(a) What is $[K : \mathbb{Q}]$?

(b) Give a basis for K over $\mathbb{Q}$.

(c) Describe the elements of K.

9. Consider the polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$.

(a) List the elements of $L = \mathbb{F}_2(\theta)$, where θ is a root of f.

(b) Write out the multiplication table for L.

(c) Determine the three linear factors of $x^3 + x + 1$ in $L[x]$.

(d) Have you already met the field L, on Tutorial Sheet 1? If so, where did it appear?

10. Give the splitting field over $\mathbb{Q}$, and its degree over $\mathbb{Q}$, for the following polynomials:

(a) $x^2 + 6 \in \mathbb{Q}[x]$;

(b) $x^3 - 5 \in \mathbb{Q}[x]$.

11. Let $f(x) = x^2 + 1, g(x) = x^2 + x - 1 \in \mathbb{F}_3[x]$.

(a) Show that f and g are irreducible over $\mathbb{F}_3$.

(b) Let $L = \mathbb{F}_3[x]/(f)$. Show that L is the splitting field for f over $\mathbb{F}_3$.

(c) Let $\alpha \in L$ be a root of f. By considering $\alpha + 1$ (or otherwise), show that L is also a splitting field for g over $\mathbb{F}_3$.