MA 362 — Homework 2 — Due Friday, Jan 25

1. Let $f(x) = 1 - x + x^2 - x^3 + x^4 \in \mathbb{Q}[x]$, which is an irreducible polynomial, and let $E = \mathbb{Q}[x]/(f(x))$ which is a field extension of $\mathbb{Q}$. Let α be the element $x + (f(x)) \in E$.

   a. What is the dimension of E as a vector space over $\mathbb{Q}$? Use the element α to write down a *basis* for E as a vector space over $\mathbb{Q}$.

   b. Write down a multiplication table for the elements of your basis from part (a.)

   c. Use this multiplication table to re-write the following elements of E as $\mathbb{Q}$-linear combinations of *basis* elements:

      i. α^5

      ii. $(\alpha^2 + \alpha^3)^5$

      iii. $(\alpha^3 + \alpha^4)(1 + \alpha^3)$

2. In class we proved that for any field extension $F \subseteq E$ and any algebraic element $\alpha \in E$, there is a *unique* monic irreducible polynomial $f(x) \in F[x]$ with the property that $f(\alpha) = 0$. It is called the *minimal polynomial* of α. Using the same field extension as in Question 1, find the *minimal polynomial* for each of the following elements of E.

   a. α^2

   b. $1 + \alpha^3$

   c. $\alpha + \alpha^2$

3. Consider the field $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is the smallest subfield of $\mathbb{R}$ that contains $\mathbb{Q}$ as well as $\sqrt{2}$ and $\sqrt{3}$.

   a. Find an element $\alpha \in E$ so that the simple extension $\mathbb{Q}(\alpha)$ is two dimensional as a $\mathbb{Q}$-vector space.

   b. Find an element $\beta \in E$ so that the simple extension $\mathbb{Q}(\beta)$ is four dimensional as a $\mathbb{Q}$-vector space.

   c. Prove that $E = \mathbb{Q}(\beta)$.

4. Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ and consider the field extension $L = \mathbb{Q}[x]/(f(x))$.

   a. Find an element $\beta \in L$ that satisfies $\beta^2 - 2 = 0$.

   b. Prove that the simple extension $E = \mathbb{Q}(\beta)$ is a *proper* subfield of L.

   c. Let $\alpha = x + (f(x)) \in L$. What is the minimal polynomial of α over $\mathbb{Q}$? (This is not a trick question)

   d. What is the minimal polynomial of α over E?

5. Let p be a prime number and let $F \subseteq E$ be a field extension of degree p. Prove that E is a *simple extension* of F.

Bonus. Finite Fields: We have seen already that the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a field with p elements. It is sometimes denoted $\mathbb{F}_p$.

a. Prove that if $f(x) \in \mathbb{F}_p$ is an irreducible polynomial of degree d, then the field extension $\mathbb{F}_p[x]/(f(x))$ has p^d elements.

b. Prove that for any $d \geqslant 2$, there exists an irreducible polynomial $f(x) \in \mathbb{F}_p$. This proves that for any power of a prime p^d there exists a finite field with that number of elements. It is sometimes denoted $\mathbb{F}_{p^d}$.

c. Prove that for any prime power p^d, any field with p^d elements is isomorphic to $\mathbb{F}_{p^d}$.

d. Prove that there are no other finite fields. If R is a ring with a finite number of elements and $|R|$ is not a power of a prime, then R is not a field.