MATH 340 Assignment 7, Fall 2017

Michael Monagan

This assignment is due Wednesday November 22nd at 11:20am in the drop off box.
Late penalty: -20% for up to 48 hours late. Zero after that.

Section 2.3: Vector Spaces

Let F be a field and $f \in F[x]$ with $n = \deg f > 0$. Let $R = F[x]/f$ and $[a], [b] \in R$ and $s \in F$. With $[a] +_R [b] = [a + b]$ and scalar multiplication $s \cdot [a] = [s \cdot a]$.

(i) Show that the ring R is a vector space wrt $+$ and $\cdot$. The axioms for a vector space are listed on page 95. Since R is a ring you don't need to prove all of them. You may also assume that polynomials of degree $< n$ form a vector space over F.

(ii) Show that $B = \{[1], [x], [x^2], \ldots, [x^{n-1}]\}$ is a basis for R.

(iii) Show that R is isomorphic to F^n.

Section 2.11: Subfield Structure of Finite Fields

Exercises 2, 4, 5.

Section 2.12: Minimal Polynomials

Exercises 3, 4, 8.

For exercise 8 use proof by contradiction.

Let $\alpha = \sqrt{2} + i \in \mathbb{C}$. Find the minimal polynomial $m(z) \in \mathbb{Q}[z]$ for α. Use both methods shown in examples 2.12.3 and 2.12.4. To save some work, assume the degree of $m(x)$ is 4.

Section 2.13: Isomorphisms Between (finite) Fields

Exercises 1, 3, 6(i), 10 and prove Lemma 2.13.1 part (ii).

For exercise 6(i) use proof by contradiction.

For exercise 10, Corollary 2.12.9 says α and β have the same minimal polynomial $m(x)$. Now in the proof of Corollary 2.12.10 we learn that $\deg m(x) = n$. This means $GF(p^n)$ is isomorphic to $\mathbb{Z}_p[x]/m(x)$. Now connect this information with exercise 6(i).