Math 100c Spring 2016 Homework 4

Due Friday 4/29/2016 by 3pm in HW box in basement of AP&M

Reading

Review Chapter 6 in preparation for the midterm on Monday May 2, which will cover the first four homeworks (including this one) and all of the material from Chapter 6 we covered. Then begin to read Chapter 8.

Assigned Problems from the text (write up full solutions):

Section 6.5: #2, 4, 9, 10

Section 6.6 #3, 5, 6

Addtional problems not from the text (write up full solutions):

A. How many irreducible polynomials of degree 16 over $\mathbb{Z}_2$ are there?

B. Let F be a finite field of characteristic p, and let $\mathbb{Z}_p \subseteq F$ be its prime subfield. Suppose that $u \in F$. Show that $[\mathbb{Z}_p(u) : \mathbb{Z}_p]$ is equal to the smallest positive integer n such that $u^{p^n} = u$, and that it divides every other such positive integer.

C. (This is 6.5 #11 with hints).
Let p be prime, and consider the polynomial $f(x) = x^p - x + a \in \mathbb{Z}_p[x]$, where $0 \neq a \in \mathbb{Z}_p$.

(a). Let $\mathbb{Z}_p \subseteq F$ be a field extension such that $f(x)$ has a root $u \in F$. Show that $u + b$ is also a root of f, for all $b \in \mathbb{Z}_p$, and conclude that f splits in $F[x]$ as

$$f(x) = (x - u)(x - u - 1) \dots (x - u - p + 1).$$

(b). Show that f is irreducible over $\mathbb{Z}_p$. (let $g(x)$ be a nonconstant factor of $f(x)$ in $\mathbb{Z}_p[x]$. In $F[x]$, $g(x)$ is a product of some of the factors $(x - u - i)$. Writing $g(x) = b_0 + \dots + b_{m-1}x^{m-1} + x^m$, show that b_{m-1} cannot belong to $\mathbb{Z}_p$ unless $g(x) = f(x)$.)