Solution to additional problem B on HW #4

4/29/2016

Since I didn't give a clear proof of this exercise in the review class on Friday April 29th, here is one possible solution.

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.

Solution. First, note that if n is the degree of $f(x) = \text{minpoly}_{\mathbb{Z}_p}(u)$, then $n = [\mathbb{Z}_p(u) : \mathbb{Z}_p]$. Since this is also the number of elements in a basis of $\mathbb{Z}_p(u)$ as a vector space over $\mathbb{Z}_p$, we also have $|\mathbb{Z}_p(u)| = p^n$. Now suppose that $u^{p^r} = u$ for some positive integer r. Then u is a root of $x^{p^r} - x$. We must have that $f(x)$ divides $x^{p^r} - x$, since the minimal polynomial of u over $\mathbb{Z}_p$ divides every polynomial with $\mathbb{Z}_p$-coefficients which has u as a root. We also proved that $x^{p^r} - x$ is the product of all irreducible polynomials over $\mathbb{Z}_p$ of degree dividing r (Theorem 6.6.1 in the text). Since $f(x)$ is one of those irreducible factors, we must have $n|r$. Thus n divides every positive integer r such that $u^{p^r} = u$. Conversely, since $f(x)$ is irreducible of degree n, it must be a factor of $x^{p^n} - x$, by the same theorem. Thus u is a root of $x^{p^n} - x$, so $u^{p^n} = u$. We conclude that $u^{p^n} = u$ and that n divides every positive integer r such that $u^{p^r} = u$. In particular, n must be the smallest such r.