QUIZ 3 CORRECTIONS – MATH 392
March 6, 2018

ALEX THIES
athies@uoregon.edu

Problem 1. Construct a field of order 9. Carefully cite all theorems used.

Solution. As I said on the original quiz, we want to make use of the fact that for $[E : K] = n$, and $|K| = q$, we have $|K(c)| = q^n$ for c a root of the minimal polynomial of degree n.[1] The field $\mathbb{Z}_3$ is a great candidate for our base field since it has order 3, and with the benefit of hindsight, we'll use an irreducible polynomial of degree 2, as $3^2 = 9$.

Consider the polynomial $p(x) = x^2 + 1$, since $\mathbb{Z}_3 = \{0, 1, 2\}$ we can check irreducibility by the long, but reliable way:

$$\begin{aligned} p(0) &= 1, \\ p(1) &= 2, \\ p(2) &= 4 \equiv 1 \pmod 3). \end{aligned}$$

Hence, $p(x)$ is irreducible over $\mathbb{Z}_3$, notice that it is also monic, thus minimal. Let c be a root of $\mathbb{Z}_3$ over some extension $\mathbb{Z}_3(c)$, it remains to create all of the basis elements of $\mathbb{Z}_3(c)$. It follows that we have $\mathbb{Z}_3(c) = \{0, 1, 2, 0 + c, 1 + c, 2 + c, 0 + 2c, 1 + 2c, 2 + 2c\}$. Notice that $|\mathbb{Z}_3(c)| = 9$ as desired. ☐

Problem 3. Let E be a finite extension of K. Let $c \in E$ be algebraic over K, with minimum polynomial $p(x)$. Prove that $\deg(p(x)) = [E : K]$ if and only if $E = K(c)$. Carefully cite all theorems used. (Hint: one direction should be immediate.)

Proof. Let E, K, c, $p(x)$ be as above.

$\Rightarrow$) Assume $\deg(p(x)) = [E : K]$, we will show that $E = K(c)$. Since E is a finite extension of K, and by Theorem 9.5 we know that $K(c) \subseteq E$, we can invoke Theorem 9.22 and write $[E : K] = [E : K(c)][K(c) : K]$. By Theorem 9.20, we have that $\deg(p(x)) = [K(c) : K]$, and by our hypothesis we assume that $\deg(p(x)) = [E : K]$. Pair these facts, and we have that $[E : K(c)] = 1$, which implies $E = K(x)$ as we aimed to show. It remains to prove the converse.

$\Leftarrow$) Assume that $E = K(c)$, we will show that $\deg(p(x)) = [E : K]$. By Theorem 9.20 we have that $\deg(p(x)) = [K(c) : K]$; moreover, since $E = K(c)$ we know they have identical bases, and we can write $[E : K] = [K(c) : K]$, which we just said is equal to $\deg(p(x))$. Thus, $\deg(p(x)) = [E : K]$, as desired. ☐

[1] This is a result of Theorem 9.20, and explained more thoroughly in the remarks following the proof of this Theorem on page 251 of the text.