Assignment 6 Qual Problems

D. Zack Garza

November 7, 2019

Contents

1 Problem 1

1.1 Part (a)

Definition: A field extension L/F is said to be a *splitting field* of a polynomial $f(x)$ if L contains all roots of f and thus decomposes as

$$f(x) = \prod_{i=1}^{n} (x - \alpha_i)^{k_i} \in L[x]$$

where α_i are the distinct roots of f and k_i are the respective multiplicities.

1.2 Part (b)

Let F be a finite field with q elements, where $q = p^k$ is necessarily a prime power, so $F \cong \mathbb{F}_{p^k}$. Then any finite extension of E/F is an F-vector space, and contains $q^n = (p^k)^n = p^{kn}$ elements. Thus $E \cong \mathbb{F}_{p^{kn}}$ Then if $\alpha \in E$, we have $\alpha^{p^{kn}} = \alpha$, so we can define

$$f(x) \coloneqq x^{p^{kn}} - x \in F[x].$$

The roots of f are exactly the elements of E, so f splits in E.

1.3 Part (c)

The polynomial f is separable, since $f'(x) = p^{kn}x^{p^{kn}-1} - 1 = -1$ since $\text{char}(E) = p$. Since E is a finite extension, E is thus a separable extension. Then, since E is a separable splitting field, it is a Galois extension by definition.

2 Problem 2

We can write $I = \text{Ann}_\mu$ for some $\mu \in R$, so suppose $xy \in I$ so $xy\mu = 0$.

If $y\mu = 0$, then $y \in I$.

Otherwise, $y\mu \neq 0$ and $x \in \text{Ann}_{y\mu}$. But by maximality, $\text{Ann}_{y\mu} \subseteq I$, so $x \in I$.

3 Problem 3

Let $I \trianglelefteq R$, then since R is a PID we have $I = (b)$ for some $b \in R$. We can write $(b) = Rb$; if $a \in I$ is an irreducible element, we'd like to show that $Rb = Ra$.

Note that since $a \in (b)$, we have $(a) \subseteq (b)$ and thus $Ra \subseteq Rb$.

Since $a \in Rb$, we have $a = rb$ for some $r \in R$. Since a is irreducible, either r is a unit or b is a unit.

If r is a unit, then $a = rb \implies r^{-1}a = b$. But then $x \in Rb \implies x = r'b = r'r^{-1}a \in Ra$, so $Rb \subseteq Ra$ and thus $Ra = Rb = I$.

Otherwise, if b is a unit, $a = rb \implies Ra = R$. But any ideal containing a unit is the entire ring, so $Rb = (b) = R$ as well, so again $Ra = I$.