Homework 7

Aleck Zhao

March 29, 2017

1. Let R be a ring, and let σ be an automorphism of R. Show that $\{ a \in R \mid \sigma(a) = a \}$ is a subring of R, and a subfield if R is a field.

2. Let F be a finite field with p^n elements for p a prime. Show that each element $a \in F$ has a pth root in F, i.e. there exists $b \in F$ such that $b^p = a$. Is b unique? By contrast, for $K := F(x)$ the fraction field of the polynomial ring $F[x]$, show that x has no pth root in K.

Section 6.4: Finite Fields

8. Find $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$ where $m \mid n$.

18. (a) Show that a monic irreducible polynomial $f \in F[x]$ has no repeated root in any splitting field over F if and only if $f \not\cong 0$ in $F[x]$.
    (b) If $\operatorname{char} F = 0$, show that no irreducible polynomial has a repeated root in any splitting field over F.

19. If $\operatorname{char} F = p$, show that a monic irreducible polynomial $f \in F[x]$ has a repeated root in some splitting field if and only if $f = g(x^p$ for some $g \in F[x]$. (Hint: Ex 18)

21. Let p be a prime and write $f = x^p - x - 1$. Show that the splitting field of f over $\mathbb{F}_p$ is $\mathbb{F}_p(u)$, where u is any root of f. (Hint: Compute $f(u+a), a \in \mathbb{F}_p$) tin

22. (a) Let f be a monic irreducible polynomial of degree n in $\mathbb{F}_p[x]$. Show that f divides $x^{p^n} - x$ in $\mathbb{F}_p[x]$. (Hint: First work over $\mathbb{F}_p(u), f(u) = 0$. Use the uniqueness in Theorem 4 § 4.1.)
    (b) Show that the degree of each monic irreducible divisor f of $x^{p^n} - x$ is a divisor of n. (Hint: Theorem 5)
    (c) Factor $x^8 - x$ into irreducibles in $\mathbb{F}_2[x]$.

Section 4.5: Symmetric Polynomials

14. Given $\sigma \in S_n$, define $\theta_\sigma : R[x_1, \cdots, x_n] \to R[x_1, \cdots, x_n]$ by $\theta_\sigma\left[f(x_1, \cdots, x_n)\right] = f(x_{\sigma 1}, \cdots, x_{\sigma n})$.
    (a) Show that θ_σ is a ring automorphism of $R[x_1, \cdots, x_n]$.
    (b) Show that $\sigma \mapsto \theta_s$ is a group homomorphism $S_n \to \operatorname{aut} R[X_1, \cdots, x_n]$, which is injective.
    (c) If $G \subseteq \operatorname{aut} R[x_1, \cdots, x_n]$ is a subgroup, show that $S_G = \{ f \mid \theta(f) = f, \forall \theta \in G \}$ is a subring of $R[x_1, \cdots, x_n]$.