Kris Harper
MATH 25900
Homework 4 May 7, 2010

Problem 1 (14.3.3)**.** *Prove that an algebraically closed field must be infinite.*

Proof. Let $F = \{a_1, \dots a_n\}$ be a finite field. Consider $p(x) = (x - a_1) \dots (x - a_n) + 1$. This clearly has no roots in F so F cannot be algebraically closed. $\square$

Problem 2 (14.3.5)**.** *Exhibit an explicit isomorphism between the splitting fields of $x^3 - x + 1$ and $x^3 - x - 1$ over $\mathbb{F}_3$.*

Proof. Let K and L be splitting fields for $x^3 - x + 1$ and $x^3 - x - 1$ respectively. Let α, β and γ be the roots of $x^3 - x + 1$ in K. Then note that $\alpha^3 - \alpha = -1$ so $(-\alpha)^3 + \alpha = 1$ and $-\alpha$ is a root for $x^3 - x - 1$ in L. Thus there is an isomorphism from K to L fixing $\mathbb{F}_3$ and taking α, β and γ to $-\alpha$, $-\beta$ and $-\gamma$. $\square$

Problem 3 (14.4.2)**.** *Find a primitive generator for $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$.*

Proof. Note that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ is generated by ρ, σ and τ where $\rho : \sqrt{2} \mapsto -\sqrt{2}$, $\sigma : \sqrt{3} \mapsto -\sqrt{3}$ and $\tau : \sqrt{5} \mapsto -\sqrt{5}$. But then none of ρ, σ or τ or their products will fix $\sqrt{2}+\sqrt{3}+\sqrt{5}$. Thus only the trivial automorphism fixes it so $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5})$. The other inclusion is obvious so $\sqrt{2}+\sqrt{3}+\sqrt{5}$ is a generator. $\square$

Problem 4 (14.4.6)**.** *Prove that $\mathbb{F}_p(x, y)/\mathbb{F}_p(x^p, y^p)$ is not a simple extension by explicitly exhibiting an infinite number of intermediate subfields.*

Proof. Let $F = \mathbb{F}_p(x^p, x^p)$ and consider the extensions $F(x + y^k)$ where $p \nmid k$. Clearly each of these contains F. Suppose $F(x + y^k) = F(x + y^j)$. Then we have the element $y^k - y^j$ in both of these fields. Note that if $k \neq j$, $F(y^k - y^j)$ is a degree p extension and it contains $F(y)$, also a degree p extension. Thus $F(x + y^k)$ contains the element y and therefore also x. Then $F(x + y^k) = F(x, y)$ which we know can't be true by degree considerations. Thus any two $F(x + y^k)$ and $F(x + y^j)$ are distinct. $\square$