Problem Set #2 (Solutions)

(1) Show that an algebraically closed field must be infinite.

Suppose $|F| < \infty$, consider the polynomial

$$f(x) := 1 + \prod_{a \in F} (x - a).$$

Since $f(z) = 1$ for all $z \in F$, $f(x)$ has no root in F, hence not algebraically closed. □

(2) Suppose that $K(\alpha)/K$ is a simple extension and that α is transcendental over K. Show that $K(\alpha)$ is not algebraically closed.

Since α is transcendental, $K(\alpha)$ is isomorphic to the rational field $K(x)$, we claim that $x^2 - \alpha$ has no roots in $K(\alpha)$. Suppose not, then we have $f^2(x)/g^2(x) - x = 0$ for some $f(x), g(x) \in K[x]$, i.e., $f^2(x) = xg^2(x)$. However, $\deg f^2 - \deg g^2 = 2(\deg f - \deg g)$ is even, which leads to a contradiction. □

(3) Let $f(x)$ be irreducible in $F[x]$, F of characteristic p. Show that $f(x)$ can be written as $g(x^{p^e})$ where $g(x)$ is irreducible and separable. Use this to show that every root of $f(x)$ has the same multiplicity p^e (in splitting field).

Let $f \in F[x]$ and e be maximal such that $f(x) \in F[x^{p^e}]$. Such e exists because $f \in F[x^{p^0}]$ and f lies in $F[x^{p^r}]$ for only finitely may r for that any non-constant polynomial in $F[x^{p^r}]$ has degree at least p^r. Say $f(x) = g(x^{p^e})$, then $g(x) \notin F[x^p]$ by maximality of e. Further, $g(x)$ is irreducible over F, since if $g(x) = h(x)k(x)$, then $f(x) = h(x^{p^e})k(x^{p^e})$ is reducible over F.

Since $g(x)$ is irreducible, $\gcd(g, g')$ could only be 1 or g. Note that $g(x) \notin F[x^p]$ iff $g'(x) \neq 0$ iff $g | g'$ iff $\gcd(g, g') = g$, which shows g is separable over F.

Then $f(x) = \prod (X - a_i)^{n_i} = g(x^{p^e}) = \prod (x^{p^e} - b_i)$. Therefore we get $a_i^{p^e} - b_i = 0$ and hence $g(x^{p^e}) = \prod (x - a_i)^{p^e}$. □

4. The case $e = 0$ is obvious, and the case $e = 1$ follows from the lemma on page 232 since a is not a pth power. Suppose $e > 1$.

Suppose we had a factorization $x^{p^e} - a = g(x)h(x)$. Let E be a splitting field and let b be a root of the polynomial. Then $b^{p^e} = a$ and we have $(x - b)^{p^e} = g(x)h(x)$. If the degree of g is k, then we must have $g = (x - b)^k$ and $b^k \in F$. If k is coprime to p^e, or equivalently coprime to p, then by the argument on page 232 using the Bezout relation we see that $b \in F$. Since $b^{p^e} = a$ is also in F, and by hypothesis a is not a pth power of an element in F, $b^{p^{e-1}}$ is not in F. If $b \in F$, this is a contradiction, so k cannot be coprime to p and must be a multiple of p. If the power of p in this multiple is less than e, then applying the gcd trick again shows that some power of p less than e is in F, which is again a contradiction (by taking pth powers) as $b^{p^{e-1}}$ in not in F. So the polynomial is irreducible.

5. By Fermat's little theorem, every nonzero element of $\mathbb{Z}_p$ is a root of $x^{p-1} - 1$. There are $p - 1$ such elements, and the polynomial is of degree $p - 1$, so those are all of the roots, and the polynomial factors as $\prod_{k=1}^{p-1}(x - k)$. Equating the constant term in the factorization with the constant term of the original polynomial shows $(p - 1)! = -1 \bmod p$.

6. a. We know from a result in the book that the Frobenius homomorphism is injective. Suppose it is not the case that the Frobenius homomorphism $\phi : a \to a^p$ is an automorphism. Then we can find $a \in F$ not in the image of ϕ. By the lemma on page 232, $x^p - a$ is irreducible. Since its derivative is zero, it is not separable, and the field is not perfect. So in any perfect field, the Frobenius homomorphism is an automorphism.

Conversely, let F be a field where the Frobenius homomorphism is an automorphism. Let f be an inseparable irreducible polynomial, so that $(f, f') \neq 1$. By remarks in the book, this implies that $f(x) = g(x^p)$ for some polynomial g, so

$$f(x) = a_0 + a_1 x^p + \cdots + a_n x^{pn}.$$

One of these a_i cannot be in the image of the Frobenius homomorphism. Otherwise, if $a_i = b_i^p$ for some set of b_i, then

$$f(x) = (b_0 + b_1 x \cdots b_n x^n)^p$$

and f is reducible, a contradiction.

b. Recall totally inseparable means that the minimal polynomial of every element has multiple roots in its splitting field. Let m be the minimal polynomial over K for some element $a \in L$. This has multiple roots, so by the remarks at the bottom of page 231, $m(x) = g(x^p)$ for some irreducible polynomial g. Then a^p is a root of g, so g is the minimal polynomial for a^p, and we may repeat this process until g has degree 1. Unwinding, we find $m(x)$ is of the form $x^{p^n} - \alpha$ for some $\alpha \in K$.

(7) Suppose that L/K is algebraic. Show that there is a greatest intermediate field $M(\subset L)$ such that M/K is normal.

Let $M_\lambda, \lambda \in \Lambda$ be all the intermediate subfield of L/K which is normal over K. The indexing set Λ is non-empty since K itself is normal. Now let M be the intersection of those subfields of L which contains all of M_λ. we claim M is normal over K. To see this, for any $\lambda \in \Lambda$, let $\mathcal{S}_\lambda \subset K[x]$ be a collection of polynomials for which M_λ is the splitting field and let N be the splitting field of $\mathcal{S} = \bigcup_{\lambda \in \Lambda} \mathcal{S}_\lambda$. Clearly N contains all of M_λ, thus N also contains M by minimality. On the other hand, the polynomials in $\mathcal{S}$ split over M, then $N \subset M$ and hence $M = N$, which is normal over K. □

(8) Suppose that L/K is finite, with normal closure L^c/L. Show that L/K is separable iff there are exactly $[L : K]$ embeddings of L into L^c fixing K.

($\Rightarrow$) We shall prove by induction on $n = [L : K]$. For $n = 1$, $L = K$ and the statement is trivial.

Now let us suppose $[L : K] = n$ and the statement holds for field extensions of degree $n-1$. Let $\alpha \in L \backslash K$ and m_α is the minimal polynomial of α in $K[x]$ with degree $k > 1$. As m_α is separable and L^c/L is normal, m_α splits over L^c and has k distinct roots: $r_1, \ldots, r_k$. Next we assume $s = [L : K(\alpha)] < n$ and by our induction assumption, there are exactly s distinct embeddings $\rho_1, \ldots, \rho_s : L \to L^c$ fixing $K(\alpha)$. Then there are k distinct automorphisms $\theta_1, \ldots, \theta_k$ of L^c fixing K such that $\theta_j(\alpha) = r_j$. Therefore the maps $\theta_j \circ \rho_i : L \to L^c$ give $s \cdot k = n$ distinct embeddings fixing K.

To see there is no more, suppose $\phi : L \to L^c$ is such an embedding, then $\phi(\alpha)$ is a root of m_α and hence $\phi(\alpha) = r_i$ for some i. It is easy to check $\theta_j^{-1} \circ \phi$ is an embedding fixing $K(\alpha)$ and $\phi = \theta_j \circ \theta_j^{-1} \circ \phi$ which has the form of $\theta_j \circ \rho_i$, which completes the proof.

($\Leftarrow$) It is easy from the argument above. □