HOMEWORK 3
SOLUTIONS

Problem 1 [13.2.18] Let k be a field and let $k(x)$ be the field of rational functions in x with coefficients from k. Let $t \in k(x)$ be the rational function $\frac{P(x)}{Q(x)}$ with relatively prime polynomials $P(x), Q(x) \in k[x]$, with $Q(x) \neq 0$.

(a) Show that the polynomial $P(X) - tQ(X)$ in the variable X and coefficients in $k(t)$ is irreducible over $k(t)$ and has x as a root.

(b) Show that the degree of $P(X) - tQ(X)$ as a polynomial in X with coefficients in $k(t)$ is the maximum of the degrees of $P(x)$ and $Q(x)$.

(c) Show that $[k(x) : k(t)] = \left[k(x) : k\left(\frac{P(x)}{Q(x)}\right)\right] = \max(\deg P(x), \deg Q(x))$.

Proof. (a) Since $k[t]$ is an UFD and $k(t)$ is its fields of fractions, Gauss' Lemma tells us that the polynomial $P(X) - tQ(X)$ is irreducible over $(k(t))[X]$ if and only if it is irreducible in $(k[t])[X]$. Now $(k[t])[X] = (k[X])[t]$, and $P(X) - tQ(X)$ is linear, and thus irreducible in $(k[X])[t]$. By the above, it is irreducible over $k(t)$. In addition, $P(x) - tQ(x) = P(x) - \frac{P(x)}{Q(x)}Q(x) = 0$, so x is a root.

(b) Let $n = \max(\deg P(x), \deg Q(x))$. Then $P(x) = a_n x^n +$ (lower degree terms) and $Q(x) = b_n x^n +$(lower degree terms), and at least one of a_n and b_n is not zero. Clearly, $\deg(P(X) - tQ(X)) \leq n$. Note that the coefficient of X^n in $P(X) - tQ(X)$ is $a_n - tb_n$. Since $t \in k(x)$, but $t \notin k$ (as P and Q are relatively prime) it follows that $a_n - tb_n \neq 0$, and thus $\deg(P(X) - tQ(X)) = n$.

(c) We know from (a) that $P(X) - tQ(X)$ is irreducible over $k(t)$ and has x as a root, so $P(X) - tQ(X)$ is the minimal polynomial of x over $k(t)$. By (b)

$$[k(x) : k(t)] = \deg(P(X) - tQ(X)) = \max(\deg(P(x)), \deg(Q(x))).$$

□

Problem 2 [13.5.7] Suppose K is a field of characteristic p which is not a perfect field: $K \neq K^p$. Prove there exist irreducible inseparable polynomials over K. Conclude that there exist inseparable finite extensions of K.

Proof. Since $K \neq K^p$ there exists an element $c \in K$ such that $c \notin K^p$. Consider $f(x) = x^p - c \in K[x]$, and let α be a root of f in an algebraic closure of K, i.e. $c = \alpha^p$. We obtain that $f(x) = x^p - c = x^p - \alpha^p = (x - \alpha)^p$ so α is the unique root (of multiplicity p) of f, showing that f is inseparable over K.

Now suppose that $g(x) \in K[x]$ is an irreducible factor of $f(x)$. By the above, it must be of the form $g(x) = (x - \alpha)^q$ for some $q \leq p$. By the binomial expansion $g(x) = (x - \alpha)^q = x^q - qx^{r-1}\alpha + \ldots + (-\alpha)^q \in K[x]$. In particular $q\alpha \in K$, and since $\alpha \notin K$ (for otherwise, $c = \alpha^p \in K^p$) we infer that $q = p$ and $g = f$. Therefore, $f(x)$ is an irreducible inseparable polynomial over K. In conclusion, $K(\alpha)$ is an inseparable finite extension of K.

□

Problem 3 [13.6.6] Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

Proof. Let $-\zeta_n$ be a root of $\Phi_n(-x)$, then $(-\zeta_n)^{2n} = (-1)^2 = 1$ and so $-\zeta_n$ is a root of $\Phi_{2n}(x)$.

Conversely, if ζ_{2n} is a root of $\Phi_{2n}(x)$ then $\zeta_{2n} = e^{2ki\pi/2n} = e^{ki\pi/n}$ for some positive integer k, which is relatively prime to $2n$. Hence $-(\zeta_{2n})^n = -e^{ki\pi} = 1$, showing that ζ_{2n} is a root if $\Phi_n(-x)$.

Consequently, the two polynomials $\Phi_{2n}(x)$ and $\Phi_n(-x)$ share the same roots. Moreover, both of them are monic, irreducible, and of the same degree (as $\phi(2n) = \phi(2)\phi(n) = \phi(n)$ for n-odd) meaning that they should in fact be equal.

□

Problem 4. Let α be a real number such that $\alpha^4 = 5$.

(a) Is $\mathbb{Q}(i\alpha^2)$ normal over $\mathbb{Q}$?

(b) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}(i\alpha^2)$?

(c) Is $\mathbb{Q}(\alpha + i\alpha)$ normal over $\mathbb{Q}$?

Solution. (a) The roots of the polynomial $x^2 + 5 \in \mathbb{Q}[x]$ are $\pm i\alpha^2$, so this polynomial splits completely in $\mathbb{Q}(i\alpha^2)$. Therefore $\mathbb{Q}(i\alpha^2)/\mathbb{Q}$ is normal.

(b) The roots of the polynomial $x^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)[x]$ are $\pm(\alpha + i\alpha)$, so this polynomial splits completely in $\mathbb{Q}(\alpha + i\alpha)$. Therefore $\mathbb{Q}(\alpha + i\alpha)/\mathbb{Q}(i\alpha^2)$ is normal.

(c) Since $\alpha + i\alpha$ satisfies the polynomial $f(x) = x^4 + 20$ we get that $F = \mathbb{Q}(\alpha + i\alpha)$ is an extension of degree at most 4 over $\mathbb{Q}$. Now if $F/\mathbb{Q}$ were normal, then this extension would contain all roots of f, so in particular $\alpha - i\alpha \in F$. But then α and i are in F, so $\mathbb{Q}(\alpha, i) \subset F$. However, it is not hard to see that $\mathbb{Q}(\alpha, i)$ is of degree 8 over $\mathbb{Q}$ which contradicts the above fact that $[F : \mathbb{Q}] \leq 4$. In conclusion, F is not normal over $\mathbb{Q}$.

Remark. *Notice that every degree 2 extension is normal. Indeed, if $[K : F] = 2$ then $K = F(\alpha)$, where α is a root of an irreducible (quadratic) polynomial f over F. But then $f(x) = (x - \alpha)g(x)$ with $\deg g = 1$. Therefore f splits in K, so K/F is normal.*

□

Problem 5. Let K be a field of characteristic p. If L is a finite extension of K such that $[L : K]$ is relatively prime to p, show that L is separable over K.

Proof. Since L/K is a finite extension we can write $L = K(\alpha_1, \dots \alpha_n)$. It is enough to show that each α_i is separable over F. Choose any α_i (call it α) and let $f(x)$ be its minimal polynomial over K. If $f(x)$ were not separable over K, then (by Proposition 33, Sec 13.5) $f(x)$ and $D_x(f(x))$ would not be relatively prime. By definition $f(x)$ is irreducible, so it must be the case that $f(x) \mid D_x(f(x))$. Since $|f(x)| > |D_x(f(x))|$ it follows that $D_x(f(x)) = 0$.

Now denote by $m = \deg(f(x))$, then clearly $m \mid [L : K]$. Since p is a prime not dividing $[L : K]$, we have that $p \nmid m$, and thus the derivative $D_x(f(x))$ is not identically 0, which is a contradiction. Therefore, $f(x)$ is separable over K.

$\square$