HOMEWORK #7
SOLUTIONS TO SELECTED PROBLEMS

Problem 7.1 – Separability of towers. We prove the following:

Proposition 1. *Let L/K be a finite extension and let $K \subseteq F \subseteq L$ be an intermediate field. Then L/K is separable if and only if L/F and F/K are separable.*

Proof. First, assume that L/K is separable. Then any $\alpha \in L$ is separable over K. In particular, this it true for any $\alpha \in F$, so that F/K is separable. Let $\alpha \in L$. Then the minimal polynomial of α over F divides the minimal polynomial of α over K, which is separable. It follows that α is separable also over F and that L/F is separable.

Now assume that L/F and F/K are separable. We use the following fact about separability for finite extensions:

Fact: L/K is separable if and only if $[L : K] = [L : K]_s$.

Now $[L : K] = [L : F][F : K]$ and $[L : K]_s = [L : F]_s[F : K]_s$. Using the fact above we see that $[L : F] = [L : F]_s$ and $[F : K] = [F : K]_s$ hence $[L : K] = [L : K]_s$ so that L/K is separable. □

Problem 7.2 – Separability of the composite; maximal separable extension.

Lemma 1. *Let α be algebraic over K. Then $K(\alpha)/K$ is separable if and only if α is separable over K.*

I will not prove the lemma, but will show how it follows from the fact. Just note that if $f \in K[t]$ is the minimal polynomial of α over K, then $[K(\alpha) : K]$ is the degree of f, and $[K(\alpha) : K]_s$ is the number of distinct roots of f in an algebraic closure $\bar{K}$. These two numbers coincide if and only if f is separable.

Lemma 2. *Let $\alpha_1, \ldots, \alpha_n$ be algebraic over K. Then $K(\alpha_1, \ldots, \alpha_n)/K$ is separable if and only if $\alpha_1, \ldots, \alpha_n$ are separable over K.*

Proof. We assume $\alpha_1, \ldots, \alpha_n$ are separable over K (the other direction is trivial). The proof is by induction on n, the case $n = 1$ treated in lemma 1 We consider the tower

$$K \subseteq K(\alpha_1, \ldots, \alpha_{n-1}) \subseteq K(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$$

Then $K(\alpha_1, \ldots, \alpha_{n-1})/K$ is separable by the induction hypothesis. Now α_n is separable over K, hence also over the larger field $K(\alpha_1, \ldots, \alpha_{n-1})$ (the minimal polynomial over the larger field divides the minimal polynomial over K). By lemma 1 we see that $K(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)/K(\alpha_1, \ldots, \alpha_{n-1})$ is separable, and by proposition 1 we conclude that $K(\alpha_1, \ldots, \alpha_n)/K$ is separable. □

Corollary. *Let α, β be separable over K. Then $\alpha+\beta, \alpha\beta$ are also separable over K.*

Proof. By the previous lemma, the extension $K(\alpha, \beta)/K$ is separable. In particular, $\alpha+\beta, \alpha\beta \in K(\alpha, \beta)$ are separable over K. □

Proposition 2. *Let $K \subseteq E, F \subseteq L$ be extensions. The the composite EF/K is separable if and only if E/K and F/K are separable.*

Proof. If EF/K is separable, then each of E/K, F/K is separable being a subfield of EF. Conversely, write $E = K(\alpha_1, \dots, \alpha_n)$. Then $EF = F(\alpha_1, \dots, \alpha_n)$.

By lemma 2, each of $\alpha_1, \dots, \alpha_n$ is separable over K, and hence over F. By the same lemma, $EF/F = F(\alpha_1, \dots, \alpha_n)/F$ is separable, so by proposition 1 for the tower $K \subseteq F \subseteq EF$ we see that EF/K is separable. □

Proposition 3. *Let L/K be a finite extension and let*

$$L_s = \{\alpha \in L : \alpha \text{ is separable over } K\}$$

Then L_s is a subfield of L, the extension L_s/K is separable and the extension L/L_s is totally inseparable. In particular, $[L_s : K] = [L : K]_s$.

Proof. The fact that L_s is a field follows from the corollary after lemma 2. Since L_s consists of separable elements over K, the extension L_s/K is separable, so that $[L_s : K] = [L_s : K]_s$. Now by $[L : K]_s = [L : L_s]_s[L_s : K]_s = [L : L_s]_s[L_s : K]$ we see that $[L_s : K] = [L : K]_s$ is equivalent to $[L : L_s]_s = 1$.

If K is of characteristic zero, that $L_s = L$ so that $[L_s : L]_s \leq [L_s : L] = 1$ and there is nothing to prove. So assume K is of characteristic p. Let $\alpha \in L$. By the corollary of the next lemma (see below), there exists $e \geq 0$ such that $a := \alpha^{p^e} \in L_s$. We see that α is a root of the polynomial $t^{p^e} - a \in L_s[t]$, hence any embedding of L/L_s to an algebraic closure must take α to a root. But the polynomial splits as $t^{p^e} - a = t^{p^e} - \alpha^{p^e} = (t-\alpha)^{p^e}$ so that the only root is α. Hence any embedding must take α to itself. As this was true for any $\alpha \in L$, we conclude that $[L : L_s]_s = 1$. □

Lemma 3. *Assume* $\operatorname{char} K = p$ *and let $f \in K[t]$ be an irreducible polynomial. Then there exist an integer $e \geq 0$ and an irreducible separable polynomial $h \in K[t]$ such that $f(t) = h(f^{p^e})$.*

Proof. If f is separable over K, take $e = 0$ and $h = f$. Otherwise, $(f, f') \neq 1$ and f is irreducible, so we must have $f' = 0$. Write $f(t) = \sum_i c_i t^i$. Then $f'(t) = \sum_i i c_i t^{i-1} = 0$. It follows that $c_i = 0$ for all i not divisible by p. In other words, $f(t) = c_0 + c_p t^p + c_{2p} t^{2p} + \cdots = g(t^p)$ where $g(s) = c_0 + c_p s + c_{2p} s^2 + \dots$. g is irreducible, because any factorization of g gives rise to a factorization of f by $f(t) = g(t^p)$.

If g is separable, take $e = 1$ and $h = g$. Otherwise, one may continue the process and at any stage extract an exponent of p from the polynomial. Since the degree is divided by p at each stage, the process must eventually stop. This means that we finally get an irreducible polynomial $h \in K[t]$ which is not of the form $h(t) = h_1(t^p)$, so h is separable. The number $e \geq 0$ is the number of steps needed to get h. □

Corollary. *Assume* $\operatorname{char} K = p$. *If* L/K *is a finite extension and* $\alpha \in L$, *there exists* $e \geq 0$ *such that* α^{p^e} *is separable over* K.

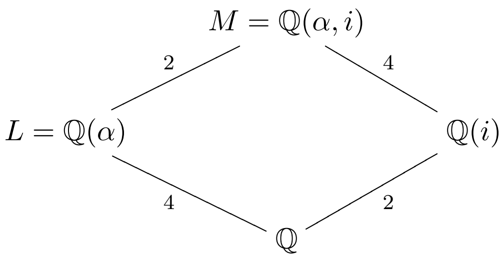
Proof. Let $f \in K[t]$ be the minimal polynomial of α, and write $f(t) = h(t^{p^e})$ for $e \geq 0$ and $h \in K[t]$ irreducible and separable. Then $0 = f(\alpha) = h(\alpha^{p^e})$, so that α^{p^e} is a root of the separable irreducible polynomial $h \in K[t]$ and therefore α^{p^e} is separable over K. □

Problem 7.3. ($\mathbf{P_2} \Rightarrow \mathbf{P_3}$) Let $\alpha \in L$ be totally inseparable. Then $\alpha^{p^n} \in K$ for some $n \geq 0$, so α is a root of the polynomial $t^{p^n} - a \in K[t]$ for $a = \alpha^{p^n}$. This polynomial factorizes (over $L[t]$) as $t^{p^n} - a = t^{p^n} - \alpha^{p^n} = (t-\alpha)^{p^n}$, so any irreducible factor of it (in $K[t]$) is of the form $(t-\alpha)^j$.

Write $j = p^i r$ where $(p, r) = 1$, and assume that $(t-\alpha)^{p^i r} \in K[t]$ is an irreducible factor. Then $(t-\alpha)^{p^i r} = (t^{p^i} - \alpha^{p^i})^r = t^{p^i r} - r\alpha^{p^i} t^{p^i(r-1)} + \cdots \in K[t]$. Since r is not divisible by p, it follows that $\alpha^{p^i} \in K$, so $(t-\alpha)^{p^i} = t^{p^i} - \alpha^{p^i} \in K[t]$, hence $r = 1$ and the minimal polynomial is of the form $t^{p^i} - b$ for some $b \in K$.

($\mathbf{P_3} \Rightarrow \mathbf{P_4}$) Trivial; just take any generators $\alpha_1, \ldots, \alpha_n$ such that $L = K(\alpha_1, \ldots, \alpha_n)$. By P_3, the minimal polynomial of each α_j is $t^{p^{n_j}} - a_j$ so α_j is totally inseparable over K.

Problem 7.4.



(a) The polynomial $t^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion with the prime 2. Hence, if α is a positive fourth root of 2 and $L = \mathbb{Q}(\alpha)$, $[L : \mathbb{Q}] = 4$.

(b) The roots of $t^4 - 2$ in $\mathbb{C}$ are $\alpha, i\alpha, -\alpha, -i\alpha$, and the splitting field M generated by them over $\mathbb{Q}$ is equal to $L(i)$; it is obviously contained in $L(i)$, the other inclusion follows from $i = (i\alpha)/\alpha \in M$.

(c) Since $L \subset \mathbb{R}$ (because $\alpha \in \mathbb{R}$) and $i \notin \mathbb{R}$, it follows that $L \neq L(i)$. On the other hand, i is a root of $t^2 + 1$ so that $[L(i) : L] \leq 2$. Therefore $[L(i) : L] = 2$, hence $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = 2 \cdot 4 = 8$. Now $8 = [M : \mathbb{Q}] = [M : \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}]$. Since $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, we have $[M : \mathbb{Q}(i)] = 4$. But $M = \mathbb{Q}(i, \alpha)$ so that $[M : \mathbb{Q}(i)] = 4$ is the degree of the minimal polynomial of α over $\mathbb{Q}(i)$. But α is a root of $t^4 - 2$. It follows that this is the minimal polynomial; in other words, $t^4 - 2$ stays irreducible over $\mathbb{Q}(i)$.

(d) Consider $M/\mathbb{Q}(i)$. This is a normal extension since $M/\mathbb{Q}$ is normal (as a splitting field). The elements $\alpha, i\alpha \in M$ are two roots of the irreducible polynomial $t^4 - 2 \in \mathbb{Q}(i)[t]$ (by (c)), hence there exists an automorphism $\sigma \in \operatorname{Gal}(M/\mathbb{Q}(i))$ taking α to $i\alpha$. In particular, $\sigma \in \operatorname{Gal}(M/\mathbb{Q})$ with $\sigma(i) = i$, $\sigma(\alpha) = i\alpha$.

(e) A simple calculation shows that $\sigma^r(\alpha) = i^r\alpha$ and $\sigma^r(i) = i$, hence σ is of order 4.

(f) Analogously to (d), M/L is normal and $i, -i$ are roots of the irreducible polynomial $t^2 + 1 \in L[t]$ (because $[L(i) : L] = 2$), so there exists $\tau \in \mathrm{Gal}(M/L)$ taking i to $-i$. Viewing $\tau \in \mathrm{Gal}(M/\mathbb{Q})$, we have $\tau(\alpha) = \alpha$, $\tau(i) = -i$.

(g) It is enough to consider the values of the automorphisms on i and α, as M is generated by these two elements. We calculate:

$$\tau\sigma(i) = \tau(i) = -i \qquad \sigma^3\tau(i) = \sigma^3(-i) = -i$$

$$\tau\sigma(\alpha) = \tau(i\alpha) = \tau(i)\tau(\alpha) = -i\alpha \qquad \sigma^3\tau(\alpha) = \sigma^3(\alpha) = -i\alpha$$

(h) Using the relation $\tau\sigma = \sigma^3\tau$ one can transform any word in σ, τ to the form $\sigma^i\tau^j$ (move σ to the left as σ^3). Since $\sigma^4 = 1, \tau^2 = 1$, one can assume $0 \le i < 4, 0 \le j < 2$, so the group generated by σ, τ and the relations is of size at most 8. One can verify that it is exactly 8, because if $\sigma^i\tau^j = \sigma^{i'}\tau^{j'}$ then $\sigma^{-i'+i} = \tau^{j'-j}$ hence $i = i'$ and $j = j'$. On the other hand, $\mathrm{Gal}(M/\mathbb{Q}) = [M : \mathbb{Q}] = 8$ and we see that the group generated by σ, τ exhausts the Galois group.

Problem 7.5. Let $\alpha \in \bar{K}$ be algebraic over K. If α is not separable, let f be its minimal polynomial over K. Then f is not separable, and as in the proof of lemma 3, we can write $f(t) = g(t^p)$ for irreducible $g \in K[t]$. In particular, $\deg f = p \deg g$. Now $0 = f(\alpha) = g(\alpha^p)$, and since f, g are irreducible we have $[K(\alpha) : K] = \deg f = p \deg g$ and $[K(\alpha^p) : K] = \deg g$, so $K(\alpha^p) \subsetneq K(\alpha)$.

Conversely, if $K(\alpha^p) \subsetneq K(\alpha)$, write $a := \alpha^p$ so that α is a root of $t^p - a \in K(\alpha^p)[t]$. But this polynomial is not separable, since it splits as $t^p - a = t^p - \alpha^p = (t - \alpha)^p$. It is irreducible, since any factor must be of the form $(t - \alpha)^r \in K(\alpha^p)[t]$, but the coefficient of t^{r-1} is $-r\alpha \in K(\alpha^p)$ so by $\alpha \notin K(\alpha^p)$ (by assumption) we must have $r = p$.

We see that α is not separable over $K(\alpha^p)$, *a fortiori* it is not separable over K.