Assignment 1

Q1: Consider the field extension $F = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \cdots)$. Clearly, $F/\mathbb{Q}$ is an algebraic extension and $F \subsetneq \overline{\mathbb{Q}}$ since i is not in F. Given any positive integer n, we see that $\mathbb{Q}(\sqrt[n+1]{2}) \subset F$. The minimal polynomial of $\sqrt[n+1]{2}$ is $x^{n+1} - 2 \in \mathbb{Q}[x]$ — the irreducibility is given by Eisenstein's Criterion taking prime $p = 2$. Hence

$$[F : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n+1]{2}) : \mathbb{Q}] = n + 1 > n.$$

Therefore, F is infinite dimensional over $\mathbb{Q}$.

Q2: Suppose that $F(\alpha) \neq F(\alpha^3)$. Clearly, $F(\alpha)/F(\alpha^3)$ is a finite extension. We see that α is a root of the polynomial $x^3 - \alpha^3 \in F(\alpha^3)[x]$, then the minimal polynomial of α over $F(\alpha^3)$ divides $x^3 - \alpha^3$. But α is not in $F(\alpha^3)$, so the minimal polynomial of α have degree 2 or 3 and hence $[F(\alpha) : F(\alpha^3)] = 2$ or 3. But then,

$$\begin{aligned}[K : F] &= [K : F(\alpha)][F(\alpha) : F(\alpha^3)][F(\alpha^3) : F] \\ &= 2[K : F(\alpha)][F(\alpha^3) : F] \text{ or } 3[K : F(\alpha)][F(\alpha^3) : F].\end{aligned}$$

But this contradicts to the assumption $[K : F]$ is relatively prime to 6. Hence we must have $F(\alpha) = F(\alpha^3)$.

Q3: Consider $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt{2}), L = \mathbb{Q}(\sqrt[4]{2})$. We insist real roots so they are subfields of $\mathbb{R}$. We claim that L/K and K/F are normal but L/F is not.

The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is clearly $x^2 - 2 \in \mathbb{Q}[x]$, whose roots are $\pm\sqrt{2}$. But K contains both $\pm\sqrt{2}$ and so is the splitting field of $x^2 - 2$. Therefore, K/F is normal. Similarly, the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $x^2 - \sqrt{2}$, whose roots are $\pm\sqrt[4]{2}$ both lying in $\mathbb{Q}(\sqrt[4]{2})$. Hence L is the splitting field $x^2 - \sqrt{2}$ and so L/K is normal.

On the other hand, the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$ is $x^4 - 2$ — the irreducible is checked by Eisenstein's Criterion with prime $p = 2$. But the roots are then

$$\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}.$$

But $i\sqrt[4]{2}$ is not in E, then $x^4 - 2$ cannot fact completely in $\mathbb{Q}(\sqrt[4]{2})[x]$. So L/F is not normal.

Q4: Let F be perfect and E/F an algebraic extension. Let $f(x) \in E[x]$ be an irreducible polynomial. Assume α is a root of f in an algebraic closure $\overline{F}$ — note that $\overline{F}$ is also an algebraic closure of E hence we definitely can find such a root in $\overline{F}$. Let $f'(x) \in F[x]$ be the minimal polynomial of α over F. Since F is perfect, f' has no repeated root. Regarding f' as a polynomial in $E[x]$, we see f divides f' and hence has no repeat root as well. Therefore, f is separable and E is perfect.

As an counter example, the function field $\mathbb{F}_2(t)$ is not perfect — $\mathbb{F}_2(t^{1/2})/\mathbb{F}_2(t)$ is not a separable extension. The main difference is that we cannot find a root of a polynomial, say $X^2 - t \in \mathbb{F}_2(t)[X]$, in $\overline{\mathbb{F}_2}$.

Q5: Assume $[\overline{F} : F]$ is finite. Then $\overline{F}$ is also finite and has $|F|^{[\overline{F}:F]}$ elements. Consider the polynomial

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

This is a well define polynomial since it is a product of finitely many terms. But $f(\alpha) = 1$ for every element $\alpha \in \overline{F}$, in other words, f has no root over $\overline{F}$. This contradicts to the definition of $\overline{F}$.

Q6: Take any element $\alpha \in E$. The minimal polynomial f_K of α over K is purely inseparable, namely, has one root only. But the minimal polynomial f_F of α over F divides f_K (by treating f_K as a polynomial in $F[x]$) and hence has one root only as well. In other words, f_F is purely inseparable and so E/F is purely inseparable.

Q7: I happen to have a copy of Hungerford's algebra in my hand. The problem is indeed on page 256. I will follow the hint.

We want to show $K^{\mathrm{Aut}(K(x)/K)} = K$, where x is an indeterminate and K is an infinite field, by breaking it into several small claims.

Let $t \in K(x)$ be in the lowest form $\frac{p(x)}{q(x)}$ with $q(x) \neq 0$ and $p(x), q(x) \in K[x]$.

Claim 1: $p(X) - tq(X) \in K(t)[X]$ (X is another indeterminate not x) is irreducible and has x as a root.

Proof of Claim 1: Since $K[t]$ is a PID and has $K(t)$ as its fraction field, Gauss's Lemma says $p(X) - tq(X)$ is irreducible in $K(t)[X]$ if and only if it is irreducible in $K[t][X]$. But $(K[t])[X] = (K[X])[t]$ and $p(X) - tq(X)$ is linear in $(K[X])[t]$ and thus irreducible. Therefore, $p(X) - tq(X)$ is irreducible over $K(t)$. Moreover, $p(x) - tq(x) = p(x) - \frac{p(x)}{q(x)}q(x) = 0$, so x is a root.

Claim 2: The degree of $p(X) - tq(X) \in K(t)[X]$ as a polynomial in X with coefficients in $K(t)$ is the maximum of the degrees of $p(x)$ and $q(x)$. And so $[K(x) : K(t)] = \max\{\deg(p), \deg(q)\}$.

Proof of Claim 2: Let $n = \max\{\deg(p), \deg(q)\}$. 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, b_n is nonzero. Clearly, $\deg(p(X) - tq(X)) \leq n$ and the coefficient of X^n is then $a_n - tb_n$. Since $t \in K(x)$ but $t \notin K$, it follows that $a_n - tb_n \neq 0$ and so $\deg(p(X) - tq(X)) = n$. Note $p(X) - tq(X)$ is the minimal polynomial of x over $K(t)$ and hence $[K(x) : K(t)] = \deg(p(X) - tq(X)) = \max\{\deg(p), \deg(q)\}$.

Claim 3: If $E \neq K$ is an indeterminate field, then $[K(x) : E]$ is finite.

Proof of Claim 3: Since $E \neq K$, we can find a rational function $t = \frac{p}{q} \in (K(x) \cap E) \setminus K$. But then $K(t) \subset E$ and $[K(x) : K(t)] = \max\{\deg(p), \deg(q)\}$. Thus $[K(t) : E]$ is a finite extension.

Now we define a map $\phi : K(x) \to K(x), f(x) \mapsto f(\frac{ax+b}{cx+d})$, where $a, b, c, d \in K$. If $ad - bc = 0$, then $\frac{ax+b}{cx+d} = \alpha \in K$ and ϕ is an evaluation map at α not well defined on $K(x)$ since α can be a singular point of $f(x)$. We want to exclude this case.

Claim 4: ϕ is a K-map when $ab - bc \neq 0$. Moreover, $K(x) = K(\frac{ax+b}{cx+d})$ and ϕ is indeed an automorphism.

Proof if Claim 4: It is straightforward to check the ϕ is a K-map. Let $f, g \in K(x)$, then

$$\phi((f+g)(x)) = (f+g)(\frac{ax+b}{cx+d}) = f(\frac{ax+b}{cx+d}) + g(\frac{ax+b}{cx+d}) = \phi(f(x)) + \phi(g(x)),$$
$$\phi((fg)(x)) = (fg)(\frac{ax+b}{cx+d}) = f(\frac{ax+b}{cx+d})g(\frac{ax+b}{cx+d}) = \phi(f(x))\phi(g(x)).$$

And it is trivial to see that ϕ fixes K, which are constant functions in $K(x)$. From Claim 2, we see that $[K(x) : K(\frac{ax+b}{cx+d})] = \max\{\deg(ax-b), \deg(cx-d)\} = 1$ since $ad - bc \neq 0$. Hence $K(x) = K(\frac{ax+b}{cx+d})$ and the surjectivity from the equality $\mathrm{im}(\phi) = K(\frac{ax+b}{cx+d})$ implies ϕ is an automorphism indeed.

Claim 5: If $\phi \in \mathrm{Aut}(K(x)/K)$, then ϕ has the from as in Claim 4.

Proof of Claim 5: Let $f(x) \in K(x)$ be in the lowest form $f(x) = \frac{\sum_{i=0}^{n} a_i x^i}{\sum_{j=0}^{m} b_j x^j}$. Note that

$$\phi(f(x)) == \frac{\phi(\sum_{i=0}^{n} a_i x^i)}{\phi(\sum_{j=0}^{m} b_j x^j)} = \frac{\sum_{i=0}^{n} a_i \phi(x^i)}{\sum_{j=0}^{m} b_j \phi(x^j)} = f(h(x)),$$

where $h(x) = \phi(x) = \frac{p(x)}{q(x)} \in K(x)$ is the lowest form where $p(x), q(x) \in K[x]$. But then

$$1 = [K(x) : K(h(x))] = \max\{\deg(p), \deg(q)\}.$$

Hence p, q have degree less or equal to 1 and so ϕ has the form in Claim 4. But if $ad - bc = 0$, then $h(x) = \frac{ax+b}{cx+d}$ is a constant and hence ϕ is an evaluation map but not an automorphism. So we have $ad - bc \neq 0$.

CLaim 6: $\mathrm{Aut}(K(x)/K) \cong \mathrm{PGL}_2(K)$.

Proof of Claim 6: We already have a map $\mathrm{GL}_2(K) \to \mathrm{Aut}(K(x)/K)$ base on Claim 4 & 5. What left is to determine the kernel. If ϕ is the identity map, then $\frac{ax+b}{cx+d} = x$ or $ax+b = cx^2+dx$ and the only possibility is $b = d = 0, a = c \neq 0$ by arguing about the degree. So the kernel is of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI$ where a can be any nonzero element in K hence $\mathrm{Aut}(K(x)/K) \cong \mathrm{PGL}_2(K)$.

Claim 7: $K^{\mathrm{Aut}(K(x)/K)} = K$.

Proof of Claim 7: Clearly, $K^{\mathrm{Aut}(K(x)/K)}$ is a field. Suppose $K^{\mathrm{Aut}(K(x)/K)} = E \neq K$. By Claim 3, $K^{\mathrm{Aut}(K(x)/K)}/E$ is a finite extension. And then $\mathrm{Aut}(K(x)/K)) = \mathrm{Aut}(K(x)/E)$. It follows that

$$|\mathrm{Aut}(K(x)/K)| = |\mathrm{Aut}(K(x)/E| \leq [K(x) : E].$$

However, K is an infinite field and so $\mathrm{PGL}_2(K) \cong \mathrm{Aut}(K(x)/K)$ is also infinite. We reach a contradiction.