Selected Solutions to Assignment 3

Question 3

We first want to show that $f(x)$ is separable, we take its derivative which is simply $f'(x) = -1$ (we note that the field has characteristic p). Then we have that $gcd(f, f') = 1$ implying that f is separable (lemma 7.2.2 in Goren's notes). This thus implies that K/F is Galois.

We now look at $GL_2(F_p)$, and note that $|GL_2(F_p)| = p(p-1)^2(p+1)$. We intend to show that $Gal(K/F) \subseteq GL_2(F_p)$. The crucial remark is that the set R of roots of $f(x)$ is not just a set, but is also equipped with a structure of a vector space over F_p, namely, it is closed under addition as well as multiplication by scalars in F_p. (This unusual feature of R arises from the fact that $f(x)$ is a *linear polynomial*, i.e., an F- linear combination of monomials of the form x^{p^j}.) Furthermore, the Galois automorphisms of K over $F = F_p(t)$ act on R not just as permutations on this set of p^2 elements (which would merely imply that the Galois group is contained in the symmetric group S_{p^2} on p^2 elements) but actually operates on R as F_p-linear transformations. All of this implies that

$$Gal(K/F) < GL_2(F_p),$$

implying that $Gal(K/F) \subseteq GL_2(F_p)$ and one concludes that $[K : F] | p(p-1)^2(p+1)$.

Question 4

We know that the Galois group in question here is $(\mathbb{Z}/7\mathbb{Z})^\times = (\mathbb{Z}/6\mathbb{Z})$. The subgroups are isomorphic to $(\mathbb{Z}/2\mathbb{Z})$, $(\mathbb{Z}/3\mathbb{Z})$, and the identity. Each subgroup corresponds to a subfield. We'll look at $(\mathbb{Z}/3\mathbb{Z})$ here. We take its elements as id, σ_2, σ_4, then an element that fixes the field is $a := \zeta + \zeta^2 + \zeta^4$, whose Galois conjugate is $b := \zeta^6 + \zeta^5 + \zeta^3$. Thus we get that one of the subfields is $\mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. An easy calculation shows that $a + b = -1$ and $ab = 2$ – the fact that these expressions are rational was expected, given that they are preserved under the full group of symmetries of $Q(\zeta)$. It follows that a and b satisfy the polynomial $x^2 + x + 2$, therefore

$$a, b = \frac{-1 \pm \sqrt{-7}}{2}.$$

It is rather interesting that the field of seventh roots of unity contains a square root of -7.

Question 5

Let E be the splitting field of $f(x)$ over F. By assumption, $Gal(E/F)$ acts as the full permutation group S_n on the roots of $f(x)$, and hence $Gal(E/K)$ acts as S_{n-1} on the $n-1$ roots of $g(x) \in K[x]$. Since this action is transitive, it follows that $g(x)$ is irreducible in $K[x]$.

Question 6

We want to show that $F(\alpha^2) \subseteq F(\alpha)$ and $F(\alpha) \subseteq F(\alpha^2)$. The first assertion is obvious, since obviously $\alpha \cdot \alpha = \alpha^2$. The other way a little trickier but not too hard. We note that α solves $x^2 - \alpha^2$, and hence we know that

$$[F(\alpha) : F(\alpha^2)] \leq 2$$

So then we get that

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$$

But then since F satisfies an irreducible polynomial of odd degree over F, we know that $[F(\alpha) : F(\alpha^2)]$ is odd, implying that $[F(\alpha) : F(\alpha^2)]$ is also odd. Since then $[F(\alpha) : F(\alpha^2)] \leq 2$, and it must be odd, we know now that $[F(\alpha) : F(\alpha^2)] =$, implying that $F(\alpha) \subseteq F(\alpha^2)$, and we are done.

Question 9

Let us view σ as an F-linear transformation acting on K. Since $\sigma^p = 1$ its eigenvalues consist of p-th roots of unity. Since these roots of unity are contained in F, it follows that σ is diagonalisable. Furthermore, $\sigma \neq 1$, hence there is a non-trivial p-th root of unity, ζ, which is an eigenvalue for σ. Let $b \in K$ be an associated eigenvector. Since $\sigma(b) = \zeta b \neq b$, it generates a non-trivial extension of F, hence it generates all of K since K is of prime degree over F. Furthermore, $a = b^p$ is fixed by σ, since $\sigma(b^p) = \sigma(b)^p = (\zeta b)^p = b^p$. It follows that $K = F(b) = F(a^{1/p})$.

Question 10a)

Noting that the polynomials are irreducible (Einstein Criterion), we start by doing

$$F(u^{1/p}, v^{1/p}) \cong (\frac{F[x]}{(x^p - u)})[y]/(y^p - v)$$

Then we have that

$$[F(u^{1/p}, v^{1/p}) : F] = [F(u^{1/p}, v^{1/p}) : F(v^{1/p}][F(v^{1/p} : F] = deg(x^p - u)deg(y^p - v) = p^2.$$

Question 10b)

Let $\sigma \in Aut(K/F)$. Since $x^p - u = (x - u^{1/p})^p$ is the minimal polynomial of $u^{1/p}$ over F, the automoprhism σ must send $u^{1/p}$ to another root of the same polynomial, but there is only one such root, hence σ fixes $u^{1/p}$. By the same reasoning it also fixes $v^{1/p}$ and it follows that $\sigma = 1$. Hence $Aut(K/F) = \{1\}$. This means that K is not Galois over F.

Question 10c)

With $\alpha \in F$, define a new field

$$F_\alpha = \left\{a + +b(u^{1/p} + \alpha v^{1/p}) | a, b \in F\right\}$$

We clearly have that $F \subseteq F_\alpha \subseteq K$. We know further that

$$p^2 = [K : F] = [K : F_\alpha][F_\alpha : F]$$

implying that $[F_\alpha : F] \in \left\{1, p, p^2\right\}$. Since $(a + bu^{1/p} + \alpha bv^{1/p})^p = a^p + b^p u + \alpha b^p v \in F$ (this holds due to the field having characteristic p), which then implies that $[F_\alpha : F] \neq p^2$. But then clearly $F_\alpha \neq F$, then we must have $[F_\alpha : F] = p$. Thus for different values of $\alpha \in F$, we get different fields F_α that have degree p over F, and there are an infinite number of them since F is infinite.