Liu's Solutions

1.

(a) Let $F = \mathbb{Q}(\xi)$, where $\xi = \mathrm{e}^{2\pi i/9}$. Notice that

$$x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1)$$

and we can check that the root of $x-1$ is 1, the roots of x^2+x+1 are ξ^3, ξ^6, so roots of x^6+x^3+1 are $\xi, \xi^8, \xi^2, \xi^7, \xi^4, \xi^5$.

In this case, x^6+x^3+1 has no roots in $\mathbb{Q}$, so if it is reducible, it would have rational factor of degree 2 or of degree 3. But if it had a rational factor of degree 2, the factor would have the form

$$(x-\xi^k)(x-\xi^{-k}) = x^2 - 2\cos 2k\pi/9x + 1$$

which is not rational. And if it had a rational factor of degree 3, it must have a real root, which contradicts to what we have known. Therefore, the polynomial x^6+x^3+1 is reducible and the extension $[F = \mathbb{Q}(\xi) : \mathbb{Q}] = 6$. Moreover, $F = \mathbb{Q}[\xi]$ is the splitting field of x^6+x^3+1 and $F/\mathbb{Q}$ is a Galois extension.

It is not hard for us to get that Galois Group $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_6$.

(b) Let $\alpha = \frac{\xi^2+1}{2\xi} = \cos\frac{2\pi}{9}$. Then the quadratic polynomial

$$(x-\xi)(x-\xi^{-1}) = x^2 - 2\alpha x + 1$$

is defined over $\mathbb{Q}(\alpha)$. The roots of it are non-real so $x^1 - 2\alpha x + 1$ is irreducible. Thus it is the minimal polynomial of ξ over $\mathbb{Q}(\alpha)$, and the extension $F/\mathbb{Q}(\alpha)$ has degree 2.

(c) Let β be the real root of $x^9 - 5$, which is obviously irreducible. So $[\mathbb{Q}(\beta) : \mathbb{Q}] = 9$. Suppose field K satisfies $\mathbb{Q} \subset K \subset \beta$, it must be of degree 3 because $[\mathbb{Q}(\beta) : K][K : \mathbb{Q}] = 3$. In this case, $k/\mathbb{Q}$ has degree 3, and hence we have $K = \mathbb{Q}(\beta^3)$.

(d) We know that $[F \cap L : \mathbb{Q}]$ must be 3 or 1, where $L = \mathbb{Q}(\beta)$ in (c). If $[F \cap L : \mathbb{Q}] = 3$, then by we know $F \cap L = K$. But by (b), we would have $\mathbb{Q}(\alpha) = (\beta^3)$, which leads to contradiction. Because $\mathbb{Q}(\alpha)$ contains all the roots of the minimal polynomial of β^3 while $\mathbb{Q}(\beta^3)$ dose not.

In this case, $F \cap L = \mathbb{Q}$. Now, we can clearly see $M = L(\xi) = \mathbb{Q}(\beta, \xi)$. Since x^6+x^3+1 is irreducible over L, it is the minimal polynomial of ξ. Therefore, $[M : L] = 6$ and then $[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = 54$.

(e) By (d), $[M : F] = 9$ and $x^9 - 5$ is irreducible over F. Then $M/\mathbb{Q}, F/\mathbb{Q}$ and M/F are Galois and hence $H = \mathrm{Gal}(M/F)$ is a normal subgroup of $\mathrm{Gal}(M/\mathbb{Q})$ of order 9, which is cyclic referring to the lecture.

Similarly, the extension M/L is Galois of degree 6 with $S = \mathrm{Gal}(M/L) \subset \mathrm{Gal}(M/\mathbb{Q})$ of order 6. Moreover G is clearly non-commutative or every subgroup of G would be normal, which is not true.

(f) E must be a fixed field of an index 2 subgroup N of $G = \mathrm{Gal}(M/\mathbb{Q})$. Since subgroups of index 2 are always normal, there must be a surjective homomorphism $G \to \mathbb{Z}_2$ with kernel N. In this case, $\varphi, \psi \in N$ and the subgroup of G generated by φ and ψ^2 has index 2 by (e). Therefore, $N = (\varphi, \psi^2)$.

So, E must be of degree 2 over $\mathbb{Q}$ and fixed by φ and ψ^2. Since $\xi^3 = \mathrm{e}^{2\pi i/3}$ fixed by φ and ψ^2 has minimal polynomial $x^2 + x = 1$, $E = \xi^{\nVdash}$. (g) The E that $\mathbb{Q} \subset E \subset M$ of degree 3 over $\mathbb{Q}$ must be the fixed field of an index normal subgroup N of G. Thus there must be a surjective homomorphism $G \to \mathbb{Z}_3$ with kernel N.

Under this homomorphism, ψ^3 must map to 0 and ψ can not(because the only degree 3 subfield of L is $\mathbb{Q}(\beta^3)$ which is not a Galois group). Therefore we could obtain that $N =< \varphi, \psi^3 >$.

Since $\varphi \in N$, the fixed field E of N is contained in the fixed field of φ, which is F. E is fixed by ψ^3, similarly. So we have $E \subset F \cap \mathbb{R} = \mathbb{Q}(\alpha)$, which implies that $E = \mathbb{Q}(\alpha)$.

2.

(a) We can easily obtain that $X^{p-1} - a$ is split in K, which roots together with 0 are roots of $X^p - aX$. In characteristic p, the map $X \mapsto X^p - aX$ is a homomorphism of $\mathbb{F}_p$-vector spaces, so its kernel is an $\mathbb{F}_p$-vector space of dimension one, which is a cyclic group of order p.

(b) By Kummer theory, this is cyclic of order dividing $p - 1$.

(c) gx is also a root of P and the difference of two roots of P is 0 or a root of $X^{p-1} - a$. We have

$$(gx_1 - x_1) - (gx_2 - x_2) = g(x_1 - x_2) - (x_1 - x_2)$$

where $g \in H$ and x_1, x_2 two roots of P. Notice that $x_1 - x_2 \in L$ and g is identity on L, so the above is zero.

(d) For $g \in H$, define $f(g) = gx - x$ for x a root of P, which is an injective group homomorphism $f : H \to \mathbb{Z}_p$. Since p is a prime, the image of f is either zero and $\mathbb{Z}_p$.

(e) The stem field of P over L is also its splitting field. If $H = \mathbb{Z}_p$ then the degree of the stem field of P over L is equal to the degree p of P, meaning that P is irreducible over L. If P was not irreducible over k, then the degree of K would have all its prime divisors less than p. However, it should be divisible by p since P is irreducible over L. Finally, if P is irreducible over k, we obtain that H has p elements by the same divisibility argument.

(f) $P(X) = X^p - TX - T$ and $X^{p-1} - T$ are irreducible over k, which implies that $[L : k] = p - 1$ and $[K : L] = p$, so the total degree is $p(p - 1)$ and the order of Galois group is the same.