1. Denote $f := X^3 - aX + a$, by Gauss' lemma, we have that f is irreducible in $\mathbb{Q}[X]$ if and only if it is reducible in $\mathbb{Z}[X]$. Note that since f is monic, if it can be written as a product of polynomials g and h of smaller degrees, then taking $\overline{f_p} := f \mod p$, we have that $\overline{f_p} = \overline{gh}$ is reducible. Thus it suffices to show f is irreducible when taken in $\mathbf{F}_2$. Since the parity of k^2 is equal to the parity of k, $a \equiv 7 \mod 2$ is odd. It follows that $\overline{f_2} = X^3 - X + 1$. Since $\overline{f_2}$ is a cubic, it is reducible if and only if it finds a root, but $\overline{f_2}(0) = 1$, and $\overline{f_2}(1) = 1$ so that $\overline{f_2}$ is irreducible, implying that f is irreducible.

To examine the Galois group, we simply take the discriminant of f,

$$\begin{aligned} D(f) &= -(4(-a)^3 + 27a^2) = -a^2(27 - 4a) = -a^2(27 - 4(k^2 + k + 7)) \\ &= -a^2(-1 - 4k^2 - 4k) = a^2(4k^2 + 4k + 1) = a^2(2k+1)^2 \in \mathbb{Z}^2 \end{aligned}$$

Since f is irreducible with square discriminant its Galois group is A_3.

2. To see that $f := T^3 - T - 1$ is irreducible , we apply Gauss' lemma, so that it suffices to check for irreducibility in $\mathbb{Z}$. Furthermore, by the same argument as in problem one, to show that f is irreducible we may show that $\overline{f_3}$ is irreducible. $\overline{f_3}$ is irreducible over $\mathbf{F_3}$ since it is an Artin-Schreier polynomial. Alternatively; every element of $\mathbf{F_3}$ satisfies $x^3 - x = 0$, so that $\overline{f_3}(a) = -1$ for any $a \in \mathbf{F_3}$, and since $\overline{f_3}$ is a cubic finding no roots, it is irreducible. Thus implying irreducibility of f. Now to describe the Galois group, it will suffice to determine the discriminant of f,

$$D(f) = -(4(-1)^3 + 27(-1)^2) = -23 \notin \mathbb{Q}^2$$

And hence $\mathrm{Gal}_f = S_3$

3. We can identify f as the 5-th cyclotomic polynomial $\Phi_5(X)$, we have shownn that the p-th cyclotomic polynomial is irreducible for p prime. Furthermore, we have shown that

$$\mathrm{Gal}_{\Phi_n} \simeq (\mathbb{Z}/(n))^\times \implies \mathrm{Gal}_{\Phi_5} \simeq (\mathbb{Z}/(5))^\times$$

Which is cyclic and generated by 2, hence

$$\mathrm{Gal}_{\Phi_5} \simeq (\mathbb{Z}/(5))^\times \simeq C_4$$

4. To show that $x \notin \varphi^{-1}(F)$, assume for the sake of contradiction that $\varphi(\frac{f}{g}) = x$ where $(f, g) = 1$, then

$$\begin{aligned} x = \varphi(\frac{f}{g}) &= \frac{f^p}{g^p} - \frac{f}{g} = \frac{f^p - fg^{p-1}}{g^p} \\ \implies f^p &= fg^{p-1} + xg^p \end{aligned}$$

So that $g|f^p$, it follows by Euclid's lemma for Euclidean domains (in this case polynomial rings) that any irreducible factor q of g is such that $q|f$. This contradicts $(f, g) = 1$.

Now denote $t := \varphi^{-1}(x)$, t satisfies the polynomial $c(T) := T^p - T - x \in F[T]$, to show that $[F(t) : F] = p$, it will suffice to show that $T^p - T - x$ is irreducible which implies that $c(T) = \min(t; F)$. First note that $\min(t; F)|c(T)$, where $c(T)$ has roots $t + a$, for each $a \in \mathbf{F_p}$. To see this, let $a \in \mathbf{F_p}$, then

$$c(T + a) = T^p + a^p - T - a - x = T^p + a - T - a - x = T^p - t - x = c(T)$$

so that $c(T)$ is seperable, and thus so is $\min(t; F)$, implying that $F(t)$ is a seperable extension. Now to show that $c(T)$ is indeed irreducible, write

$$c(T) = h_1(T), \dots, h_k(T)$$

as its irreducible factor decomposition. It follows, by the uniqueness of this decomposition, that the map $T \overset{\sigma}{\mapsto} T + 1$ acts by permuting these factors. It may only fix a factor if for each monic factor $(t+a)|h_i$, we also have $(t+a+1)|h_i$, but continuing this inductively, the action only fixes a factor h_i if $(t+a)|h_i$, $\forall a \in \mathbf{F_p}$, implying that $h_i(T) = c(T)$. Hence we have that σ acts on the k factors of $c(T)$ via permutation for $k < p$ (we get this inequality since $c(T)$ cannot split linearly since $t \notin F$). Then we have that $\sigma \in S_k$, and $\sigma^p = 1$, by Lagranges theorem we have $o(\sigma)|k!$, so that in particular $o(\sigma)|(p, k!) = 1$ since p is a prime greater than k. This implies that σ acts via the identity so in particular σ fixes h_1, which as described earler implies that $h_1(T) = c(T)$. This suffices to show that $c(t)$ is irreducible, since $h_1(T) = c(T)$ was taken to be irreducible.

Now we have shown that $F(t)$ is a seperable of extension of degree p, which is normal since it is the splitting field of $c(T) = \prod_{j=0}^{p-1}(T - (t+j))$ over F. This implies that the extension is Galois, and $\#\text{Gal}(F(t)/F) = [F(t) : F] = p$, so since this is a group of order p, it is cyclic.

5. We first show that $\min(a^{1/p} : \mathbb{Q}) = X^p - a$, proof being we can factor $X^p - a = \prod_{k=1}^{p}(X - a^{1/p}\zeta_p^k)$ in $\mathbb{C}[X]$. If this polynomial were reducible in $\mathbb{Q}$, then if g were a factor, the last coefficient of g must be of the form $\pm a^{k/p}$. This is impossible since $a^{k/p} \in \mathbb{Q}$, $k < p$, then by bezouts identity, there exist u, v such that $uk + vp = 1$, implying that $a^{1/p} = a^{uk/p}a^{vp/p} \in \mathbb{Q}$.

This gives the desired result for both L and F extensions, since by multiplicativity of degree,

$$p|[F(a^{1/p}) : \mathbb{Q}] \text{ and } [F : \mathbb{Q}] \leq p - 1$$
$$p|[L(a^{1/p}) : \mathbb{Q}] \text{ and } [L : \mathbb{Q}] \leq p - 1$$

implying that $p|[F(a^{1/p}) : F], \underline{[L(a^{1/p}) : L]}$. Then since $F \supset \cos(2\pi/p), -\sin^2(2\pi/p)$ (proven below), we get that $L = F(\sqrt{-\sin^2(2\pi/p)})$, i.e. $[L : F] = 2$, also note that $N = L(a^{1/p})$. So that $[L(a^{1/p}) : F] = [L(a^{1/p}) : L][L : F] = 2p$, implies $\#\text{Gal}(N/F) = 2p$. Finally, we have that $\text{Gal}(N/F) \supset \langle \tau, \sigma \rangle \simeq D_p$, where τ is complex conjugation and σ is a generator of the cyclic group $\text{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q})$. The isomorphism follows from $\sigma\tau = \tau\sigma^{-1}, \tau^2 = 1, \sigma^p = 1$, meaning the multiplication rules of D_p are satisfied. Then since $\#\text{Gal}(N/F) = 2p = \# \langle \tau, \sigma \rangle$ we have equality.

To show that $F \supset \cos(2\pi/p), \sin^2(2\pi/p)$, we have $\zeta_p, \zeta_p^{-1} \in F$, hence we have $\frac{1}{2}(\zeta_p + \zeta_p^{-1}) = \cos(2\pi/p) \in F$. This implies we also have $(\zeta_p - \cos(2\pi/p))^2 = -\sin^2(2\pi/p)$.

6. Since $[K : F] = n$, and $x^n - a$ is a degree n polynomial satisfied by α, we have that $\min(\alpha; F) = x^n - a$. Note that for each $0 \leq i < n$, we have that $a\zeta_n^i$ is also a root of $x^n - a$, so that in particular K is the splitting field of $x^n - a$, a seperable polynomial so that K/F is Galois with Galois group G permuting the n factors of $\min(\alpha; F)$.

We have that

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) = \sum_{i=0}^{n-1} \zeta_n^i \alpha$$

is the first elementary symmetric polynomial in the factors of $\min(\alpha; F)$, in particular it is equal to $-1c_{n-1}$, where c_{n-1} is the coefficient of x^{n-1} in $\min(\alpha; F)$ which is equal to 0. And hence $Tr_{K/F}(\alpha) = -c_{n-1} = 0$

Similarly, we have that

$$N_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{i=0}^{n-1} \zeta_n^i \alpha$$

Which is the n-th elementary symmetric polynomial in the factors of $\min(\alpha; F)$, in particular it is equal to $(-1)^n c_0$, where c_0 is the constant term in $\min(\alpha; F)$, in this case we have that $c_0 = -a$, implying that $N_{K/F}(\alpha) = (-1)^n c_n = (-1)^{n+1} a$