HW 11

1 a. $F = \mathbb{Z}/2\mathbb{Z}$ has elements $\{0, 1\}$.

once we adjoin a root α of x^2+x+1, we get a 2-dimensional vector space over F, with elements $\{0, 1, \alpha, \alpha+1\}$.

Elements of the Galois group are determined by their value on α: There are two:

the identity, and
$$\begin{aligned} 1 &\mapsto 1 \\ 0 &\mapsto 0 \\ \alpha &\mapsto \alpha+1 \\ \alpha+1 &\mapsto \alpha. \end{aligned}$$

So $G(K/F)$ is a cyclic group of order 2. It has composition series:

$$\langle id \rangle \trianglelefteq G(K/F)$$

the quotient here is cyclic of order 2, which is abelian.

So $G(K/F)$ is solvable.

b. Recall: $\alpha^2+\alpha+1 = 0$ (and in F, $-1 = 1$).

So $\alpha^2 = \alpha+1$ and
$$\begin{aligned} \alpha^3 = \alpha(\alpha+1) &= \alpha^2+\alpha \\ &= \alpha+1+\alpha \\ &= 1 \quad \left(\text{since } 1+1=0, \ \alpha+\alpha=0\right). \end{aligned}$$

so $\alpha^3 \in F$ and $K = F(\alpha)$. So K is an extension by radicals.

2. To solve $0 = ax^6 + bx^3 + c$, Let $T = x^3$.

Then $0 = aT^2 + bT + c$, which has roots

$$T = \frac{-b+\sqrt{b^2-4ac}}{2a}, \quad \frac{-b-\sqrt{b^2-4ac}}{2a}.$$

the ~~three~~ cube roots of ~~th~~ these roots are

$$\sqrt[3]{\frac{-b+\sqrt{b^2-4ac}}{2a}}, \quad \sqrt[3]{\frac{-b-\sqrt{b^2-4ac}}{2a}}$$

$$w \cdot \sqrt[3]{\frac{-b+\sqrt{b^2-4ac}}{2a}}, \quad w \cdot \sqrt[3]{\frac{-b-\sqrt{b^2-4ac}}{2a}}$$

$$w^2 \cdot \sqrt[3]{\frac{-b+\sqrt{b^2-4ac}}{2a}}, \quad w^2 \cdot \sqrt[3]{\frac{-b-\sqrt{b^2-4ac}}{2a}}$$

where $w = \frac{-1+i\sqrt{3}}{2}$, which satisfies $w^3 = 1$.

An explicit extension by radicals containing the roots of $ax^6 + bx^3 + c$ is therefore

$$\mathbb{Q}\left(\sqrt[3]{\frac{-b+\sqrt{b^2-4ac}}{2a}}, \sqrt[3]{\frac{-b-\sqrt{b^2-4ac}}{2a}}, w\right).$$

3. The subnormal series

$$\langle id \rangle \trianglelefteq K \trianglelefteq G$$

can be refined to a composition series:

(by Schreyer / Jordan-Hölder)

$$\langle id \rangle = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = K \trianglelefteq H_{m+1} \trianglelefteq \dots \trianglelefteq H_{n-1} \trianglelefteq H_n = G.$$

with abelian quotients since G is solvable

So $H_0 \trianglelefteq \dots \trianglelefteq H_m$ is a composition series for K with abelian quotients, and it follows that K is solvable (by defn).

In the series $K = H_m \trianglelefteq H_{m+1} \trianglelefteq \dots \trianglelefteq H_n = G$,

K is a normal subgroup of G, which means K is also a normal subgroup of any H_i in this series. By the 3^{rd} isomorphism theorem, each H_i/K is a normal subgroup of G/K, hence of any intermediate subgroup of G/K, letting us write

$$\langle id \rangle = K/K \trianglelefteq H_{m+1}/K \trianglelefteq \dots \trianglelefteq H_{n-1}/K \trianglelefteq G/K.$$

with quotients $\dfrac{H_{i+1}/K}{H_i/K} \cong H_{i+1}/H_i$ the simple abelian groups from the comp. series for G. So G/K is solvable.

4a $\langle (1) \rangle \trianglelefteq \langle (12)(13) \rangle \trianglelefteq \langle (12)(13), (13)(24) \rangle \trianglelefteq A_4 \trianglelefteq S_4.$

since A_4 is index 2 in S_4, S_4/A_4 is cyclic of order 2.

since $\langle (12)(13), (13)(24) \rangle = \{(1), (12)(34), (13)(24), (14)(23)\}$ is index 3 in A_4, the quotien $A_4 / \langle (12)(13), (13)(24) \rangle$ is cyclic of order 3.

$\langle (12)(13) \rangle$ is a cyclic gp of order 2, with index 2 as a subgroup of $\langle (12)(34), (13)(24) \rangle$. so the quotient $\langle (12)(34), (13)(24) \rangle / \langle (12)(34) \rangle$ is cyclic of order 2.

Finally, $\langle (12)(34) \rangle / \langle (1) \rangle$ is cyclic of order 2.

cyclic gps of prime order are simple + abelian, so this is a composition series for S_4 w/ abelian quotients. $\therefore$ S_4 is solvable.

4b if $f(x)$ has degree ≤ 4, then it has at most 4 roots.

any automorphism of K (the splitting field of $f(x)$ over F) is determined by its value on this set of ≤ 4 roots.

But automorphisms must send elements to their conjugates, so any automorphism is determined by a permutation of these ≤ 4 roots. So $G(K/F)$ can be identified with a subgroup of S_4.

Subgroups of solvable groups are solvable.

if G is solvable, ~~then~~ with comp. series

$\langle id \rangle \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq G$, then for any $H \leq G$ the series

$\langle id \rangle \trianglelefteq H \cap H_1 \trianglelefteq H \cap H_2 \trianglelefteq \cdots \trianglelefteq H \cap H_{n-1} \trianglelefteq H \cap G = H$

is a composition series for H (2^{nd} isom. thm).

5. Let τ be a transposition and σ a 5 cycle.

without loss of generality, we can assume $\tau = (12)$ and $\sigma = (1\ a\ b\ c\ d)$.

Note that any power of σ is still a 5-cycle, unless the power is 0 mod 5, the order of σ.

Note also that $\sigma(1) = a$, $\sigma^2(1) = b$, $\sigma^3(1) = c$, $\sigma^4(1) = d$. since one of a, b, c, d must be 2, we know one of these 5 cycles sends 1 to 2 so by replacing σ with its appropriate power, we can assume $\sigma = (1\,2\,a\,b\,c)$ and $\tau = (1\,2)$ [different a, b, c].

without loss of generality we can assume $a=3$, $b=4$, $c=5$.

So $\tau = (12)$, $\sigma = (1\,2\,3\,4\,5)$ are the two elements we can safely assume are in our subgroup $H \leq S_5$.

Now,
$$\sigma \tau \sigma^{-1} = (2\,3)$$
$$\sigma^2 \tau \sigma^{-2} = (3\,4)$$
$$\sigma^3 \tau \sigma^{-3} = (4\,5)$$

so the transpositions of "adjacent" elements are all in H.

Any transposition can be written as a product of these 4 adjacent transpositions.

$(12) = (12)$
$(23) = (23)$
$(34) = (34)$
$(45) = (45)$
$(13) = (12)(23)(12)$
$(24) = (23)(34)(23)$
$(35) = (34)(45)(34)$
$(14) = (12)(23)(34)(23)(12)$
$(25) = (23)(34)(45)(34)(23)$
$(15) = (12)(23)(34)(45)(34)(23)(12)$.

So H contains all transpositions. But any n-cycle can be written as a product of transpositions:

$$(a_1\ a_2\ \ldots\ a_n) = (a_1\ a_n)\cdots(a_1\ a_3)(a_1\ a_2)$$

So H contains all n-cycles, for $2 \leq n \leq 5$

there are 10 2-cycles, 20 3-cycles, 30 4-cycles, and 24 5 cycles. so $|H| \geqslant 84$, but must divide 120, so $|H| = 120$ and so $H = S_5$

(Equivalently, any permutation is a product of disjoint cycles).