1

HOMEWORK #1

8.1 #1: $[GF(2^2):GF(2)] = 2$, so

Thm 8.1.8 $\Rightarrow Gal(GF(2^2)/GF(2)) = \mathbb{Z}_2$.

8.1 #4: $\theta_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) = a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$

So $\{x \in \mathbb{Q}(\sqrt{2}+\sqrt{3}) \mid \theta_2(x) = x\} = \{a+c\sqrt{3} \mid a, c \in \mathbb{Q}\}$.

$= \mathbb{Q}(\sqrt{3})$.

8.1 #5: Since $x^3-1 = (x-1)(x^2+x+1)$, and x^2+x+1 has distinct roots (by the quadratic formula), we can use Thm 8.1.6 to say

$$|Gal_{\mathbb{Q}}(x^2+x+1)| = [\text{Splitting field} : \mathbb{Q}]$$
$$= 2.$$

There's only one group of order 2.

8.1 #7: Let $\phi : E \xrightarrow{\sim} F$. Then we define

$$\mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(F/K)$$

$$\theta \longmapsto \phi \circ \theta \circ \phi^{-1}.$$

& Think of the square

$$\begin{tikzcd}
E \arrow[r, "\theta"] & E \arrow[d, "\phi"] \\
F \arrow[u, "\phi^{-1}"] \arrow[r, dashed, "\phi\circ\theta\circ\phi^{-1}"'] & F
\end{tikzcd}$$

Well defined: $\phi\circ\theta\circ\phi^{-1}$ is a composition of automorphisms, so it's an automorphism. It fixes K because ϕ and θ do.

Injective: Suppose $\phi\circ\theta\circ\phi^{-1}(x) = x \ \forall x \in F$.

$\Rightarrow \theta\circ\phi^{-1}(x) = \phi^{-1}(x) \ \forall x \in F$. Since ϕ^{-1} is surjective, $\theta(y) = y \ \forall y \in E \Rightarrow \theta = id_E$.

(3)

Surjective Suppose $\psi \in Gal(F/K)$.

Consider $\theta = \phi^{-1} \circ \psi \circ \phi \in Gal(E/K)$.

Then $\phi \circ \theta \circ \phi^{-1} = \phi \circ \phi^{-1} \circ \psi \circ \phi \circ \phi^{-1} = \psi$. //

8.2#1: Let F be the splitting field of $p(x)$ over K. Then $[F:K] = 4$, and the result follows from 8.1.8. (by Cor 6.2.2)

8.2#2: $x^4 - 2 = (x^2 + x - 1)(x^2 - x - 1)$, so its splitting field over $GF(3)$ is $GF(3^2)$.

Thm 8.1.8 $\Rightarrow$ Galois group is $\mathbb{Z}_2$.

8.2#3: $x^4 + 2 = (x+1)(x-1)(x^2+1)$, so its splitting field is $GF(3^2)$. Thm 8.1.8 $\Rightarrow$ Galois group is $\mathbb{Z}_2$.

8.2 #7 Claim $\mathbb{Q}(\sqrt[3]{2}+\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Only show "$\supseteq$":

Note $3 = (\sqrt[3]{2}+\omega)(\sqrt[3]{4} - \sqrt[3]{2}\omega + \omega^2)$

$$\Rightarrow (\sqrt[3]{4} - \sqrt[3]{2}\omega + \omega^2) \in \mathbb{Q}(\sqrt[3]{2}+\omega).$$

As $(\sqrt[3]{2}+\omega)^2 = \sqrt[3]{4} + 2\sqrt[3]{2}\omega + \omega^2$, we know

$$\boxed{\sqrt[3]{2}\omega \in \mathbb{Q}(\sqrt[3]{2}+\omega).}$$

So $(\sqrt[3]{4} + \sqrt[3]{2}\omega + \omega^2)(\sqrt[3]{4} - \sqrt[3]{2}\omega + \omega^2) \in \mathbb{Q}(\sqrt[3]{2}+\omega)$

$$= 2\sqrt[3]{2} + \sqrt[3]{4}\omega^2 - \sqrt[3]{4}\omega^2 + \omega$$

$$= 2\sqrt[3]{2} + \omega$$

Subtract $\cancel{\sqrt[3]{2}\omega}$ $\sqrt[3]{2}+\omega$ to see $\boxed{\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}+\omega).}$

Then $(\sqrt[3]{2}+\omega) - \cancel{\omega}\,\sqrt[3]{2} = \boxed{\omega \in \mathbb{Q}(\sqrt[3]{2}+\omega).}$

8.2 #8 Suppose $\left(\frac{f(x)}{g(x)}\right)^p = x$.

$\Rightarrow (f(x))^p = x(g(x))^p$.

But the highest power of x on LHS is a power of x^p, and the —— " —— RHS is of the form x^{p+1}. #.

8.2 #9. Let α be a root of $x^p - a$, so in $F[\alpha]$, $x^p - a = (x-\alpha)^p$. Thus we can write the minimal polynomial of α as $(x-\alpha)^k \in F[x]$.

The coeff. of the $(k-1)^{st}$ term is $-k\alpha$.

Since this is an element of F, either

① $\alpha \in F$, so $x^p - a$ is a p^{th} power; or

② $p \mid k \Rightarrow m_\alpha(x) = (x-\alpha)^p = x^p - a$ is irreducible.