1. (1) A ring homomorphism \( \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{3}) \) must map \( \mathbb{Q} \) identically to \( \mathbb{Q} \) and \( \sqrt{2} \) to a root of polynomial \( x^2 - 2 \) in \( \mathbb{Q}(\sqrt{3}) \). We need to show that the roots do not lie in \( \mathbb{Q}(\sqrt{3}) \). For example, by previous homework, \( \mathbb{Q}(\sqrt{2}, \sqrt{3}) \) has degree 4 over \( \mathbb{Q} \), hence \( \mathbb{Q}(\sqrt{3}) \not\subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \). Or we can check that no element \( a + b\sqrt{3}, a, b \in \mathbb{Q} \) is a root of \( x^2 - 2 \).

(2) The group is \( S_2 \times S_2 \), acting by permuting \( \sqrt{2} \leftrightarrow \sqrt{3} \) and \( \sqrt{3} \leftrightarrow -\sqrt{3} \).

2. (1) The polynomial \( x^5 - 2 \) has roots \( \sqrt[5]{2}, \sqrt[5]{2}, \sqrt[5]{2}, \sqrt[5]{2}, \sqrt[5]{2} \).

Thus clearly \( E = \mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}) \). We have a diagram of fields:

\[
\begin{array}{c}
E = \mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}) \\
\text{degree 5} \\
\end{array}
\]

\[
\begin{array}{c}
\mathbb{Q}(\sqrt[5]{2}) \\
\text{degree 5} \\
\end{array}
\] \[\begin{array}{c}
\mathbb{Q}(\sqrt[5]{2}) \\
\text{degree 5} \\
\end{array}
\]

It follows that \( \text{deg}(E/\mathbb{Q}) \) is divisible by 4 and 5.

The degree must be 20. (It cannot be more than 20)
(2). The Galois group has 20 elements.
First, there are 5 maps \( \sigma \):
\[
\begin{array}{ccc}
\mathbb{Q}(\sqrt[5]{2}) & \xrightarrow{\sigma} & E \\
\downarrow & & \downarrow \\
\mathbb{Q} & \xrightarrow{\sigma} & E
\end{array}
\]
where \( \sigma \) sends \( \sqrt[5]{2} \) to one of the 5 roots of \( x^5 - 2 \).
For each fixed \( \sigma \), we have 4 maps \( \sigma_i \):
\[
\begin{array}{ccc}
\mathbb{Q}(\sqrt[5]{2})(\sigma) & \xrightarrow{\sigma_i} & E \\
\downarrow & & \downarrow \\
\mathbb{Q}(\sqrt[5]{2}) & \xrightarrow{\sigma_i} & E
\end{array}
\]
where \( \sigma_i \) sends \( f \) to any of the 4 roots of \( x^4 + x^3 + x^2 + x + 1 \).
Note that this polynomial is irreducible over \( \mathbb{Q}(\sqrt[5]{2}) \) because
\( E \) has degree 4 over this field.
Let
\[
\sigma_{i,j} : \begin{cases} \\
\sqrt[5]{2} & \mapsto s^i \sqrt[5]{2} \\
f & \mapsto s^j f
\end{cases}
\]
\( i = 0, \ldots, 5 \)
\( j = 1, \ldots, 4 \).
These elements form \( \text{Gal}(E/\mathbb{Q}) \).
Now \( \sigma_{i,j} \circ \sigma_{k,e} \) maps
\[
\begin{array}{c}
\sqrt[5]{2} \xrightarrow{\sigma_{k,e}} s^k \sqrt[5]{2} \xrightarrow{\sigma_{i,j}} s^i (s^k \sqrt[5]{2}) \\
\downarrow \quad \downarrow \quad \downarrow \\
\sqrt[5]{2} \xrightarrow{\sigma_{k,e}} s^k \xrightarrow{\sigma_{i,j}} s^i s^j \end{array}
\]
Thus \( \sigma_{i,j} \circ \sigma_{k,e} = \sigma_{i+k,j} \), \( i, j \). (When we compute mod 5).
The subgroup \( \{ \sigma_{i,j} \}_{i=0}^{5} \) is normal and
the quotient is
\[
\text{Gal}(E/\mathbb{Q}) / C_5 = C_4.
\]
In fact, \( \text{Gal}(E/\mathbb{Q}) \) is a semidirect product \( C_5 \rtimes C_4 \).
3. (1) We can find $r_i(x), \ldots, r_n(x)$ as described, using division algorithm, $f(s^i) = r_i(s)$. Since $s^i$ depends on $i \mod n$, these $r_i, \ldots, r_n$ also work for large $i$:

$$f(s^i) = r_i \mod n(s)$$

If $f(s^i) = s(s)$, then $s$ is a root of $r_i - s$, which has degree less than $d$, hence $r_i - s = 0$.

(2) For any polynomial $g(x) \in \mathbb{F}_p[x]$ we have

$$[g(x)]^p = g(x^p).$$

Now apply division algorithm to $f(x^p)$ and $f(x)$:

$$f(x^p) = f(x) \cdot q(x) + r(x), \quad \deg r(x) < d.$$

We can reduce this mod $p$ to $\mathbb{F}_p[x]$:

$$\overline{f(x^p)} = \overline{f(x)} \cdot \overline{q(x)} + \overline{r(x)}.$$

where $\overline{\cdot}$ means reduce coefficients to $\mathbb{F}_p$. We know that $\overline{f(x)} = [f(x)]^p$, hence $f(x)$ divides $\overline{f(x^p)}$ and $\overline{r(x)} = 0$.

This implies $r(x) = p \cdot s(x)$ for some $s(x) \in \mathbb{F}_p[x]$. Since $f(s^i) = r_j(s)$ and also $f(s^i) = p \cdot s^i$, it follows that $r_j = p \cdot s^i$.

(3) Choose $p$ greater than all coefficients of $r_1(x), \ldots, r_n(x)$. Then some $r_j(x) = p \cdot s^i$ implies $r_j(x) = 0$, $f(s^i) = 0$.

(4) We can replace $s$ with $s^p$ to get $f(s^p) = 0$. (Note that $r_1, \ldots, r_n$ depend on $f(x)$, but not on the root $s$.)

Thus $s^p$ is a root of $f(x)$ for any $m > 0$ and prime $p$. Replacing $s$ with $s^p$ and taking a new prime $q$, we get $f(s^p) = 0$. Thus $f(s^m) = 0$ when $m$ is a product of large primes. Such $m$ (mod $n$) give all $i$ (mod $n$) that are relatively prime to $n$. 