

HW #2.

①

[1] Because $[\mathbb{F}_{3^{16}} : \mathbb{F}_{3^2}] = 8$, Theorem 8.1.8

says that $\text{Gal}(\mathbb{F}_{3^{16}}/\mathbb{F}_{3^2}) \cong \mathbb{Z}_8$, ~~is~~ generated

by ϕ^2 , where $\phi: \mathbb{F}_{3^6} \rightarrow \mathbb{F}_{3^6}$ by $x \mapsto x^3$.

[2] The subgroups of \mathbb{Z}_8 correspond to divisors

of 8: $\mathbb{Z}_8 = \langle \phi^2 \rangle$, $\mathbb{Z}_4 = \langle \phi^4 \rangle$, $\mathbb{Z}_2 = \langle \phi^8 \rangle$,

$\{e\} = \langle \phi^0 \rangle$.

[3] claim: The fixed field of $\langle \phi^n \rangle$ is \mathbb{F}_{3^n} .

for $n = 2, 4, 8, 16$

pf: $\phi^n(x) = x^{3^n}$, so every element of the fixed

field satisfies $x^{3^n} - x = 0$. But the roots of this

polynomial are precisely the elements of \mathbb{F}_{3^n} //

Subgroups

Fixed fields

$\{e\}$

$\mathbb{F}_{3^{16}}$

|

|

\mathbb{Z}_2

\mathbb{F}_{3^8}

|

|

\mathbb{Z}_4

\mathbb{F}_{3^4}

|

|

\mathbb{Z}_8

\mathbb{F}_{3^2}

[4] The roots of $x^3 - 2 = 0$ are $\sqrt[3]{2} \omega^i$,
 where $\omega^3 = 1$. So clearly

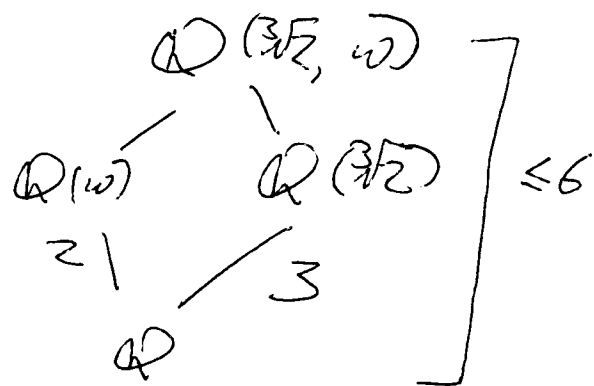
$$\mathbb{Q}(\sqrt[3]{2}, \omega) \supseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) \\ = \text{splitting field.}$$

We have the reverse inclusion because

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

[5] Looking at the (partial) field
 diagram tells us that

$$[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6.$$



Thus $G := \text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega) / \mathbb{Q})$ has order 6.

Define $\theta \in G$ by $\theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$
 $\theta(\omega) = \omega.$

$\phi \in G$ by $\phi(\sqrt[3]{2}) = \sqrt[3]{2}\omega$
 $\phi(\omega) = \omega^2$

Note $\theta^3 = \text{id}$, since $\theta^3(\sqrt[3]{2}) = \theta^2(\sqrt[3]{2}\omega) = \theta(\sqrt[3]{2}\omega^2) = \sqrt[3]{2}\omega^3 = \sqrt[3]{2}$
 $\theta^3(\omega) = \omega.$

and $\phi^2 = \text{id}$ since $\phi^2(\sqrt[3]{2}) = \sqrt[3]{2}$
 $\phi^2(\omega) = \phi(\omega^2) = \omega^4 = \omega.$

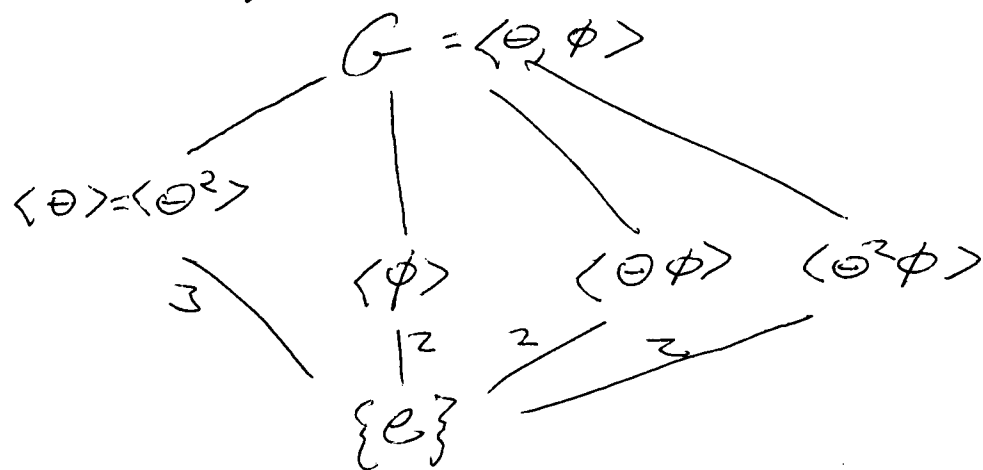
Hence $\langle \theta, \phi \rangle \leq G$ has order at least 6
 $\Rightarrow \langle \theta, \phi \rangle = G$.

Now $\phi \circ \theta(\sqrt[3]{2}) = \phi(\sqrt[3]{2}\omega) = \sqrt[3]{2}\omega^2$
 $\theta \circ \phi(\sqrt[3]{2}) = \theta(\sqrt[3]{2}) = \sqrt[3]{2}\omega$.

So $\phi \circ \theta \neq \theta \circ \phi$, so G is not abelian.

The only nonabelian group of order 6 is S_3 .

[6] Any nontrivial proper subgroup of G has order 2 or 3, and hence is cyclic. Thus, we can list all of G 's subgroups as follows:



Note: $\phi, \theta\phi, \theta^2\phi$ all have order 2. For example,

$$(\theta\phi)^2(\sqrt[3]{2}) = \theta\phi\theta(\sqrt[3]{2}) = \theta\phi(\sqrt[3]{2}\omega) = \theta(\sqrt[3]{2}\omega^2) = (\sqrt[3]{2}\omega)\omega^2 = \sqrt[3]{2}$$

$$(\theta\phi)^2(\omega) = \theta\phi\theta(\omega^2) = \theta\phi(\omega^2) = \theta(\omega^4) = \omega$$

(4)

Clearly $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle \theta \rangle} \subseteq \mathbb{Q}(\sqrt[3]{2}, \omega)$
↑
index $|\langle \theta \rangle| = 3$

Since $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)] = 3$, we know

$$\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle \theta \rangle}$$

Similarly, $\mathbb{Q}(\sqrt[3]{2}^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle \phi \rangle}$

For $\langle \theta \phi \rangle$, we compute $\theta \phi(\sqrt[3]{2}) = \theta(\sqrt[3]{2}) = \sqrt[3]{2} \omega$
 $\theta \phi(\omega) = \theta(\omega^2) = \omega^2$

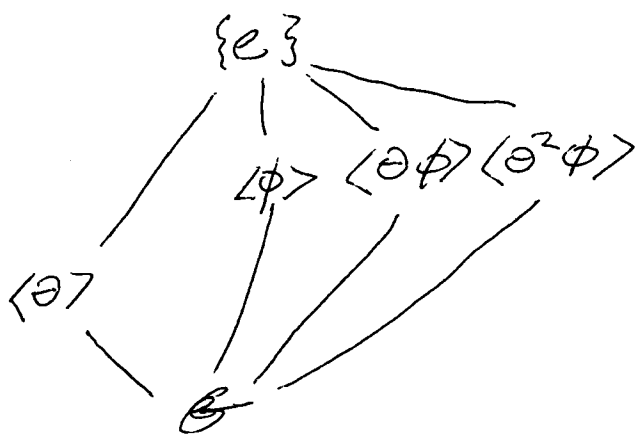
and we notice (or guess) that

$$\theta \phi(\sqrt[3]{2} \omega^2) = \theta(\sqrt[3]{2} \omega) = \sqrt[3]{2} \omega^2$$

so $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle \theta \phi \rangle} = \mathbb{Q}(\sqrt[3]{2} \omega^2)$

Similarly, $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle \theta^2 \phi \rangle} = \mathbb{Q}(\sqrt[3]{2} \omega)$

Subgroups



Fixed Fields

