$x^n - 2$

Thomas Browning

October 12, 2018

1 Introduction

Lemma 1. *For integers* $n \geq 1$, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Proof. The polynomial $f(x) = x^n - 2$ is irreducible by Eisteinstein. Then $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = \deg f = n$. $\square$

Lemma 2. *For integers* $n \geq 1$, *the subfields of* $\mathbb{Q}(\sqrt[n]{2})$ *are given by* $\mathbb{Q}(\sqrt[d]{2})$ *for each* $d \mid n$.

Proof. Let $L = \mathbb{Q}(\sqrt[n]{2})$, let K be a field with $\mathbb{Q} \subseteq K \subseteq L$, and let $d = [K : \mathbb{Q}]$. Lemma 1 shows that $n = d[L : K]$. Now note that $N_{L/K}(\sqrt[n]{2})$ is a product of $[L : K]$ conjugates of $\sqrt[n]{2}$. In particular,

$$N_{L/K}(\sqrt[n]{2}) = \zeta_n^k \sqrt[n]{2}^{[L:K]} = \zeta_n^k \sqrt[d]{2}$$

for some integer k. However, $N_{L/K}(\sqrt[n]{2}) \in K \subseteq L \subseteq \mathbb{R}$ so $\sqrt[d]{2} = \pm N_{L/K}(\sqrt[n]{2}) \in K$. Lemma 1 shows that $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[d]{2}) : \mathbb{Q}]$. Then $K = \mathbb{Q}(\sqrt[d]{2})$ where $d \mid n$. $\square$

Lemma 3. *For integers* $n \geq 1$, $\mathbb{Q}(\sqrt[n]{2}) \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\sqrt{2})$.

Proof. Lemma 2 shows that $\mathbb{Q}(\sqrt[n]{2}) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt[d]{2})$ for some $d \mid n$. However, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian so $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt[d]{2}))$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then $\mathbb{Q}(\sqrt[d]{2})$ is Galois over $\mathbb{Q}$ by the Galois correspondence. As a consequence, $d \leq 2$. $\square$

Lemma 4. *If* $\sqrt{2} \in \mathbb{Q}(\zeta_n)$ *then* $8 \mid n$.

Proof. If $\sqrt{2} \in \mathbb{Q}(\zeta_n)$ then $\sqrt{2} \in \mathbb{Q}(\zeta_8) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{\gcd(8,n)})$. However, $\sqrt{2} \notin \mathbb{Q}(i)$ so $\gcd(8, n) = 8$. $\square$

Lemma 5. *For integers* $n \geq 1$,

$$\mathbb{Q}(\sqrt[n]{2}) \cap \mathbb{Q}(\zeta_n) = \begin{cases} \mathbb{Q} & 8 \nmid n \\ \mathbb{Q}(\sqrt{2}) & 8 \mid n \end{cases}.$$

Proof. If $8 \mid n$ then $\sqrt{2} = \sqrt[n]{2}^{n/2} = \zeta_n^{n/8} + \zeta_n^{-n/8}$ so $\sqrt{2} \in \mathbb{Q}(\sqrt[n]{2}) \cap \mathbb{Q}(\zeta_n)$. By Lemma 4, $\sqrt{2} \in \mathbb{Q}(\sqrt[n]{2}) \cap \mathbb{Q}(\zeta_n)$ if and only if $8 \mid n$. Then the result follows from Lemma 3. $\square$

Theorem 1. *For integers* $n \geq 1$, *if* $8 \nmid n$ *then* $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2}, \zeta_n)/\mathbb{Q})$ *is isomorphic to the holomorph of* $\mathbb{Z}/n\mathbb{Z}$. *If* $8 \mid n$ *then* $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2}, \zeta_n)/\mathbb{Q})$ *is isomorphic to an index 2 subgroup of the holomorph of* $\mathbb{Z}/n\mathbb{Z}$.

Proof. First note that $\mathbb{Q}(\sqrt[n]{2}, \zeta_n)$ is the splitting field of $f(x) = x^n - 2$ over $\mathbb{Q}$. By Lemmas 1 and 5,

$$[\mathbb{Q}(\sqrt[n]{2}, \zeta_n) : \mathbb{Q}] = \frac{[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[n]{2}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]} = \begin{cases} n\varphi(n) & 8 \nmid n \\ n\varphi(n)/2 & 8 \mid n \end{cases}.$$

Every element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2},\zeta_n)/\mathbb{Q})$ is given by $\sqrt[n]{2} \mapsto \zeta_n^j \sqrt[n]{2}$ for some $j \in \mathbb{Z}/n\mathbb{Z}$ and $\zeta_n \mapsto \zeta_n^k$ for some $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2},\zeta_n)/\mathbb{Q})$ is isomorphic to a subgroup of

$$\{(j,k)\colon j \in \mathbb{Z}/n\mathbb{Z},\ k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$$

with multiplication given by

$$(j_1,k_1)\cdot(j_2,k_2) = (k_2 j_1 + j_2, k_1 k_2).$$

If $8 \mid n$ then the relation $\sqrt[n]{2}^{n/2} = \zeta_n^{n/8} + \zeta_n^{-n/8}$ forces $j \equiv 0 \pmod 2$ if and only if $k \equiv \pm 1 \pmod 8$. Comparing cardinalities shows that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{2},\zeta_n)/\mathbb{Q}) \cong \begin{cases} \{(j,k)\colon j \in \mathbb{Z}/n\mathbb{Z},\ k \in (\mathbb{Z}/n\mathbb{Z})^\times\} & 8 \nmid n \\ \{(j,k)\colon j \in \mathbb{Z}/n\mathbb{Z},\ k \in (\mathbb{Z}/n\mathbb{Z})^\times,\ j \equiv 0 \pmod 2 \iff k \equiv \pm 1 \pmod 8\} & 8 \mid n \end{cases}$$

where the group $\{(j,k)\colon j \in \mathbb{Z}/n\mathbb{Z},\ k \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ is isomorphic to the holomorph of $\mathbb{Z}/n\mathbb{Z}$. $\square$