Galois theory - Problem Set 4

To be solved on Monday 20.03

Problem 1. (Exercise 17.1.1 in the book.) Let $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$ be an extension field of $\mathbb{Q}$, where $\omega^3 = 1$, $\omega \neq 1$. For each of the following subgroups S_i of the group $G(E/\mathbb{Q})$ find E_{S_i}.

(a) $S_1 = \{1, \sigma_2\}$, where σ_2 is defined by $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$ and $\sigma_2(\omega) = \omega^2$.

(b) $S_2 = \{1, \sigma_3\}$, where σ_3 is defined by $\sigma_3(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ and $\sigma_3(\omega) = \omega^2$.

(c) $S_3 = \{1, \sigma_4\}$, where σ_4 is defined by $\sigma_4(\sqrt[3]{2}) = \sqrt[3]{2}$ and $\sigma_4(\omega) = \omega^2$.

(d) $S_4 = \{1, \sigma_5, \sigma_6\}$ where σ_5 is defined by $\sigma_5(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ and $\sigma_5(\omega) = \omega$ and σ_6 is defined by $\sigma_6(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$ and $\sigma_6(\omega) = \omega$.

Problem 2. (Exercise 17.2.1 in the book.) Find the Galois groups $G(K/\mathbb{Q})$ of the following extensions K of $\mathbb{Q}$:

(a) $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

(b) $K = \mathbb{Q}(\alpha)$, where $\alpha = \cos 2\pi/3 + i \sin 2\pi/3$.

(c) K is the splitting field of $x^4 - 3x^2 + 4 \in \mathbb{Q}[x]$.

Problem 3. (Exercise 17.2.3 in the book.) Let $u \in \mathbb{R}$ and let $\mathbb{Q}(u)$ be a normal extension of $\mathbb{Q}$ such that $[\mathbb{Q}(u) : \mathbb{Q}] = 2^m$, where $m \geq 0$. Show that there exist intermediate fields K_i such that

$$K_0 = \mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = \mathbb{Q}(u),$$

where $[K_i : K_{i-1}] = 2$. (Hint: Sylow's first theorem.)

Problem 4. (Exam May 2017, Problem 3(c)-(e).) Let E be the splitting field of $f(x) = x^{17} - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$, that is $E = \mathbb{Q}(\omega, \sqrt[17]{2})$ where $\omega = e^{\frac{2\pi i}{17}}$. (see Problem 7 in Problem Set 3).

(a) Let $G = \mathrm{Gal}(E/\mathbb{Q})$ be the Galois group of E over $\mathbb{Q}$. Show that there exists an intermediate field L, $\mathbb{Q} \subseteq L \subseteq E$, such that L corresponds by the Galois correspondence to a normal subgroup H of G of order 17. Explain your argument.

(b) Show that there exists an intermediate field M, $\mathbb{Q} \subseteq M \subseteq E$, such that $[M : \mathbb{Q}] = 34$. [*Hint*: Use Sylov's Theorem.]

(c) Show that G is non-abelian. [*Hint*: G abelian implies that all subgroups are normal.]

Solution.

(a) Let $L = \mathbb{Q}(\omega)$. Then ω is a root of $x^{17} - 1 = (x-1)\Phi_{17}(x)$. Moreover, the roots of $\Phi_{17}(x)$ are ω^i for $1 \leq 16$. Hence $\mathbb{Q}(\omega)$ is the splitting field of $\Phi_{17}(x) \in \mathbb{Q}[x]$. Therefore the field extension $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ is normal. By FTGT(5) we conclude $H := \mathrm{Gal}(E/L)$ is a normal subgroup of $\mathrm{Gal}(E/\mathbb{Q})$. On the other hand, we have that the minimal polynomial of ω over $\mathbb{Q}$ is $\Phi_{17}(x)$ by Example 3.11(2). Therefore

$$[L : \mathbb{Q}] = [\mathbb{Q}(\omega) : \mathbb{Q}] = \deg(\Phi_{17}(x)) = 16.$$

By Problem 7 in Problem Set 3 we have that $[E : \mathbb{Q}] = 17 \cdot 16$. Hence

$$17 \cdot 16 = [E : \mathbb{Q}] = [E : L][L : \mathbb{Q}] = [E : L] \cdot 16$$

implies that $[E : L] = 17$. Then we obtain by FTGT(3) that

$$|\mathrm{Gal}(E/L)| = [E : L] = 17,$$

as required.

(b) By FTGT(3) we have that

$$|\mathrm{Gal}(E/\mathbb{Q})| = [E : \mathbb{Q}] = 17 \cdot 16 = 272.$$

Since $8 = 2^3$ divides 272, it follows by Sylow's first theorem (Theorem 8.4.2 in the book) that there exists a subgroup $F < \mathrm{Gal}(E/\mathbb{Q})$ with $|F| = 8$. Let $M = E_F$ so that $\mathbb{Q} \subseteq M \subseteq E$. Then $F = \mathrm{Gal}(E/M)$ by FTGT(2). By FTGT(3) we obtain

$$[E : M] = |\mathrm{Gal}(E/M)| = |F| = 8.$$

But then

$$272 = [E : \mathbb{Q}] = [E : M][M : \mathbb{Q}] = 8 \cdot [M : \mathbb{Q}]$$

implies $[M : \mathbb{Q}] = 34$, as required.

(c) Consider the field extension

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[17]{2}) \subseteq E.$$

Then the polynomial $f(x) = x^{17} - 2$ is irreducible over $\mathbb{Q}$ (Eisenstein for $p = 2$) and has a root in $\mathbb{Q}(\sqrt[17]{2}$. However, it does not have all of its roots in $\mathbb{Q}(\sqrt[17]{2})$, since $\omega \notin \mathbb{Q}(\sqrt[17]{2})$. By Theorem 8.5 we conclude that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[17]{2})$ is not a normal extension. By FTGT(5) we conclude that $\mathrm{Gal}(E/\mathbb{Q}(\sqrt[17]{2}))$ is not a normal subgroup of $G = \mathrm{Gal}(E/\mathbb{Q})$. Using the hint we conclude that G is not an abelian group.

Problem 5. (Exam May 2017, Problem 5, Exam May 2013, Problem 6.) Let N be a Galois extension of K such that $G(N/K)$ is abelian. Let $\alpha \in N$ and let $p(x) \in K[x]$ be the minimal polynomial of α over K. Show that all roots of $p(x)$ lie in $K(\alpha)$.

Solution. By Theorem 8.5 it is enough to show that $K \subseteq K(\alpha)$ is a normal field extension. We have field extensions $K \subseteq K(\alpha) \subseteq N$ where $K \subseteq N$ is Galois by assumption. Let $G = \mathrm{Gal}(N/K)$ and $H = \mathrm{Gal}(N/K(\alpha))$. In particular, H is a subgroup of G. Since G is abelian by assumption, we conclude that H is a normal subgroup of G (since all subgroups of abelian groups are normal). By FTGT(5) we conclude that $K \subseteq K(\alpha)$, as required.

Problem 6. (Exam June 2015, Problem 5.) Let $E = F(\alpha_1, \alpha_2)$ be a Galois extension of a field F, and let $K_1 = F(\alpha_1)$ and $K_2 = F(\alpha_2)$. Consider the subgroups $H_1 = G(E/K_1)$ and $H_2 = G(E/K_2)$ of the Galois group $G(E/F)$.

(a) Show that $H_1 \cap H_2 = \{e\}$, that is, the intersection of H_1 with H_2 is the trivial subgroup of $G(E/F)$.

(b) Suppose that each element $g_1 \in H_1$ maps K_2 to K_2, and that each element $g_2 \in H_2$ maps K_1 to K_1. Show that $g_1 g_2 = g_2 g_1$ for all $g_1 \in H_1$, $g_2 \in H_2$.

Solution.

(a) Let $g \in H_1 \cap H_2$. Then $g \in \mathrm{Gal}(E/K_1)$ and so $g\big|_{K_1} = \mathrm{id}_{K_1}$. In particular, $g(\alpha_1) = \alpha_1$. Similarly, we have $g(\alpha_2) = \alpha_2$. Moreover, $g\big|_F = \mathrm{id}_F$ since $F \subseteq K_1$ and so $g(x) = x$ for every $x \in F$. Consider the field extensions

$$F \subseteq F(\alpha_1) \subseteq F(\alpha_1, \alpha_2).$$

Since $F \subseteq F(\alpha_1, \alpha_2)$ is a Galois extension, it is in particular a finite field extension. Hence a basis of $F(\alpha_1)$ over F is given by $\{1, \alpha_1, \dots, \alpha_1^d\}$ for some $d \geq 0$ and a basis of $F(\alpha_1, \alpha_2)$ over $F(\alpha_1)$ is given by $\{1, \alpha_2, \dots, \alpha_2^s\}$ for some $s \geq 0$. Hence a basis of $F(\alpha_1, \alpha_2)$ over F is given by

$$B = \{\alpha_1^i \alpha_2^j \mid 0 \leq i \leq d, 0 \leq j \leq s\}.$$

But $g(\alpha_1) = \alpha_1$ and $g(\alpha_2) = \alpha_2$ implies that $g\big|_B = \mathrm{id}_B$ since g is a ring homomorphism. It follows that $g : F(\alpha_1, \alpha_2) \to F(\alpha_1, \alpha_2)$ is the identity map. Since $g \in H_1 \cap H_2$ was arbitrary, we conclude that $H_1 \cap H_2 = \{\mathrm{id}_E\}$, as required.

(b) Let $\alpha \in E = F(\alpha_1, \alpha_2)$. It is enough to show that $g_1 g_2(\alpha) = g_2 g_1(\alpha)$ for any $\alpha \in E$. Since $g_1\big|_F = \mathrm{id}_F$ and $g_2\big|_F = \mathrm{id}_F$, for every $x \in E$ we have

$$g_1 g_2(x) = g_1 \mathrm{id}_F(x) = g_1(x) = \mathrm{id}_F(x) = x$$

and similarly $g_2 g_1(x) = x$. Hence $g_1 g_2(x) = g_2 g_1(x)$ for every $x \in F$. Moreover, since $g_1\big|_{F(\alpha_1)} = \mathrm{id}_{F(\alpha_1)}$, we have

$$g_2 g_1(\alpha_1) = g_2 \mathrm{id}_{F(\alpha_1)}(\alpha_1) = g_2(\alpha_1).$$

On the other hand, since $g_2(K_1) \subseteq K_1$, we have that $g_2(\alpha_1) \in K_1 = F(\alpha_1)$. Therefore

$$g_1 g_2(\alpha_1) = \mathrm{id}_{F(\alpha_1)} g_2(\alpha_1) = g_2(\alpha_1).$$

Hence we have shown that $g_2 g_1(\alpha_1) = g_1 g_2(\alpha_1)$. Similarly we have $g_2 g_1(\alpha_2) = g_1 g_2(\alpha_2)$. Therefore, and since $g_1 g_2$ and $g_2 g_1$ are ring homomorphisms, we see that $g_1 g_2\big|_B = g_2 g_1\big|_B$ where

$$B = \{\alpha_1^i \alpha_2^j \mid 0 \leq i \leq d, 0 \leq j \leq s\}.$$

is an F-basis of E as in part (a). Since $g_1 g_2$ and $g_2 g_1$ agree on both F and an F-basis of E, it readily follows that $g_1 g_2(\alpha) = g_2 g_1(\alpha)$ for every $\alpha \in E$, as required.

Problem 7. (Exam June 2015, Problem 6.) Let $F \subseteq E$ be a Galois extension of degree $[E : F]$.

(a) Is it possible that $[E : F] = 4$ and that there are precisely two proper intermediate fields between E and F?

(b) Suppose that $[E : F] = 6$ and that E is the splitting field of a polynomial of degree 3 (and a Galois extension of F.) How many proper intermediate fields are there between E and F?

Solution.

(a) Assume $[E : F] = 4$. Since $E \subseteq F$ is Galois, the Galois group $G(E/F)$ has order 4. Hence either $G(E/F) \cong \mathbb{Z}_4$ or $G(E/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. The group $\mathbb{Z}_4$ has precisely one proper subgroup, namely $\{0, 2\}$. The group $\mathbb{Z}_2 \times \mathbb{Z}_2$ has precisely three proper subgroups, namely $\{(0,0),(0,1)\}$, $\{(0,0),(1,0)\}$ and $\{(0,0),(1,1)\}$. By the FTGT it follows that there are either one or three proper intermediate fields between E and F and so the answer is no.

(b) Let $f(x) \in F[x]$ be the polynomial of degree 3 for which E is a splitting field. By the FTGT we have that $G(E/F)$ has order $[E : F] = 6$. Let $\alpha \in E$ be a root of $f(x)$. We claim that $\alpha \notin F$. Indeed, if $\alpha \in F$, then $f(x) = (x - \alpha)p(x)$ where $p(x) \in F[x]$ has degree 2. In particular, E is the splitting field of $p(x)$. Then let β, γ be the roots of $p(x)$ in E. Then $p(x)$ is divided by $x - \beta$ in $F(\beta)$, implying that $\gamma \in F(\beta)$. Hence $E = F(\beta, \gamma) = F(\beta)$ and so

$$6 = [E : F] = [F(\beta) : F] \leq \deg(p) = 2,$$

a contradiction.

Hence no root of $f(x)$ is in F. Let $\alpha_1, \alpha_2, \alpha_3 \in E$ be the roots of $f(x)$. Then $F \subseteq F(\alpha_i)$ is a proper field extension for each $i \in \{1, 2, 3\}$. We claim that $F(\alpha_i) \subseteq E$ is also a proper field extension for each $i \in \{1, 2, 3\}$. Indeed, we have

$$[F(\alpha_i) : F] \leq \deg(f(x)) = 3 < 6 = [E : F],$$

and so $E = F(\alpha_i)$ is impossible. We conclude that $F(\alpha_1)$, $F(\alpha_2)$ and $F(\alpha_3)$ are three proper intermediate fields between E and F. Since $[G(E/F)] = 6$, we have by the FTGT that $G(E/F) = S_3$ or $G(E/F) = \mathbb{Z}_6$. Since $\mathbb{Z}_6$ has only 2 proper subgroups, we conclude that $G(E/F) = S_3$. It remains to find how many proper subgroups S_3 has. Since S_3 has order 6, any nontrivial proper subgroup of S_3 has order 2 or 3 and so its cyclic. Hence if $S_3 = \{\text{id}, (12), (13), (23), (123), (132)\}$, then the subgroups are $\{\text{id}, (12)\}$, $\{\text{id}, (13)\}$, $\{\text{id}, (23)\}$ and $\{\text{id}, (123), (132)\}$. Since there are four proper nontrivial subgroups of S_3, by the FTGT it follows that there are three proper intermediate fields between F and E.

Problem 8. (Exam June 2015, Problem 7.) Let $f(x) = x^5 - x - 1 \in \mathbb{Z}_5[x]$ and $E = \mathbb{Z}_5(\beta)$, where β is a root of $f(x)$.

(a) Show that $\beta + 1$, $\beta + 2$, $\beta + 3$, $\beta + 4$ are also roots of $f(x)$. Deduce that $\beta \notin \mathbb{Z}_5$.

(b) Define $\sigma \in G(E/\mathbb{Z}_5)$ by $\sigma(\beta) = \beta + 1$. Find the order of σ in $G(E/\mathbb{Z}_5)$, and describe the action of σ on the roots of $f(x)$.

(c) Use the above and the FTGT to deduce that $f(x)$ is irreducible, and that $[E : \mathbb{Z}_5] = 5$.

Solution.

(a) Since $\text{char}(E) = 5$, we have that $(a + b)^5 = a^5 + b^5$ for all $a, b \in E$. Moreover, by Fermat's little theorem we have $k^5 = k$ for all $k \in \mathbb{Z}_5$. Hence for $k \in \{1, 2, 3, 4\}$ we have

$$f(\beta + k) = (\beta + k)^5 - (\beta + k) - 1 = \beta^5 + k^5 - \beta - k - 1 = (\beta^5 - \beta - 1) + k^5 - k = f(\beta) = 0.$$

We conclude that $\beta + k$ is a root of f for $k \in \{1, 2, 3, 4\}$. Assume to a contradiction that $\beta \in \mathbb{Z}_5$. Since $f(0) = -1 \neq 0$, we conclude that $\beta \in \{1, 2, 3, 4\}$. But then $\beta + k$ is a root of $f(x)$ for all $k \in \{1, 2, 3, 4\}$ and since $\beta + k = 0$ for some $k \in \{1, 2, 3, 4\}$ we obtain a contradiction (again, because 0 is not a root of $f(x)$.)

(b) We have $\sigma(k) = k$ for all $k \in \mathbb{Z}_5$, since $\sigma \in G(E/\mathbb{Z}_5)$. Since σ is a ring homomorphism, we have $\sigma(\beta + k) = \sigma(\beta) + \sigma(k) = \beta + k$ for all $k \in \{1, 2, 3, 4\}$. Then

$$\beta \xmapsto{\sigma} \beta + 1 \xmapsto{\sigma} \beta + 2 \xmapsto{\sigma} \beta + 3 \xmapsto{\sigma} \beta + 4 \xmapsto{\sigma} \beta + 5 = \beta$$

and so the order of σ is 5.

If $\beta \in \mathbb{Z}_5$, then either $\beta = 0$ or $\beta \in \{1, 2, 3, 4\}$.

(c) The extension $\mathbb{Z}_5 \subseteq E = \mathbb{Z}_5(\beta)$ is finite since β is algebraic over $\mathbb{Z}_5$, is separable since $\mathbb{Z}_5$ is a finite field and is normal since it is the splitting field of $f(x)$ over $\mathbb{Z}_5$. Hence $\mathbb{Z}_5 \subseteq E$ is a Galois extension. Since $f(\beta) = 0$, we conclude that $[E : \mathbb{Z}_5] \leq 5$. On the other hand, since $\sigma \in G(E/\mathbb{Z}_5)$ has order 5, we conclude that $5 \leq |G(E/\mathbb{Z}_5)|$. By FTGT(3) we have that $|G(E/\mathbb{Z}_5)| = [E : \mathbb{Z}_5]$. Hence we have

$$5 \leq |G(E/\mathbb{Z}_5)| = [E : \mathbb{Z}_5] \leq 5,$$

from which we conclude that $[E : \mathbb{Z}_5] = 5$. We claim that $f(x)$ is the minimal polynomial of β over $\mathbb{Z}_5$. Indeed, if that is not the case, and since $f(\beta) = 0$ and $f(x)$ is monic, we conclude that there exists an irreducible polynomial $g(x)$ with $\deg(g) < 5$ and $g(\beta) = 0$. But then

$$5 = [E : \mathbb{Z}_5] = [\mathbb{Z}_5(\beta) : \mathbb{Z}_5] = \deg(g) = 4,$$

and we obtain a contradiction.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 9. Let F be a field and $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$. Let E be the splitting field of $f(x)$. Show that $[E : F]$ divides $n!$.

Solution. We use induction on $n \geq 1$. If $n = 1$ then $f(x) = a + bx$ for some $a, b \in F$ and so $E = F$. Then $[E : F] = 1$ divides $n! = 1! = 1$.

Suppose now that the claim is true for any polynomial of degree strictly less than n and we show that it holds for $f(x) \in F[x]$ of degree n. We consider the cases where $f(x)$ is reducible and $f(x)$ is irreducible separately.

Case $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$ with $\deg(g(x)) = l \geq 1$ and $\deg(h(x)) = m \geq 1$. Then $n = l + m$ and so $l, m < n$. Let K be the splitting field of $g(x)$ over F. Then $g(x)$ factors as a product of linear factors in $K[x]$ and

$$K = F(\{r \in K \mid g(r) = 0\}).$$

Moreover, we have that $[E : K]$ divides $l!$ by induction hypothesis. Notice that $h(x) \in K[x]$. Let L be the splitting field of $h(x)$ over K. Then $h(x)$ factors as a product of linear factors in $L[x]$ and

$$L = K(\{s \in L \mid h(s) = 0\}).$$

Again by induction hypothesis we have that $[L : K]$ divides $m!$. Now notice that $f(x)$ factors as a product of linear factors in $L[x]$ (since $g(x)$ and $h(x)$ do so) and that

$$L = K(\{s \in L \mid h(s) = 0\}) = F(\{s, r \in L \mid h(s) = 0, g(r) = 0\}) = F(\{t \in L \mid f(t) = 0\}).$$

Hence L is the splitting field of $f(x)$ over F and so $L \cong E$. Then

$$[E : F] = [L : F] = [L : K][K : F] \mid m!l! = m!(n-m)!.$$

But $m!(n-m)!$ divides $n!$ since $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ is an integer. Hence $[E : F]$ divides $n!$ as required.

Case $f(x)$ is irreducible. Let $\alpha \in E$ be a root of $f(x)$. Then $[F(\alpha) : F] = \deg(f(x)) = n$. Moreover, in $F(\alpha)$ we have $f(x) = (x - \alpha)g(x)$ where $\deg(g(x)) = n - 1$. Let L be the splitting field of $g(x)$ over $F(\alpha)$. Then $g(x)$ factors as a product of linear factors in $L[x]$ and

$$L = F(\alpha)(\{r \in L \mid g(r) = 0\}).$$

Moreover we have that $[L : F(\alpha)]$ divides $(n-1)!$ by induction hypothesis. Notice that $f(x)$ factors as a product of linear factors in $L[x]$ (since $g(x)$ does so) and that

$$L = F(\alpha)(\{r \in L \mid g(r) = 0\}) = F(\{r \in L \mid g(r) = 0\} \cup \{\alpha\}) = F(\{r \in L \mid f(r) = 0\}),$$

since $\alpha \in L$. Hence L is the splitting field of $f(x)$ over $K(\alpha)$ and so $L \cong E$. Then

$$[E : F] = [L : F] = [L : F(\alpha)][F(\alpha) : F] = [L : F(\alpha)] \cdot n.$$

Since $[L : F(\alpha)]$ divides $(n-1)!$, we conclude that $[E : F]$ divides $n!$ as required.

Problem 10. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 3. Let E be the splitting field of $f(x)$. What are the possible values of $[E : \mathbb{Q}]$? Provide an explicit example for each such possible value.

Solution. From Problem 9 we know that $[E : \mathbb{Q}]$ divides $3! = 6$. Hence $[E : \mathbb{Q}] \in \{1, 2, 3, 6\}$.

Case $[E : \mathbb{Q}] = 1$. In this case $f(x) = x - 1$ is an example, since the splitting field of $f(x)$ is $E = \mathbb{Q}$.

Case $[E : \mathbb{Q}] = 2$. We claim that this is impossible. Indeed, assume to a contradiction that $[E : \mathbb{Q}] = 2$. The there exists $\alpha \in E \backslash \mathbb{Q}$ which is a root of $f(x)$. Since $f(x)$ is irreducible, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f(x)) = 3$. But then $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq E$ gives

$$2 = [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)] \deg(f(x)) = [E : \mathbb{Q}(\alpha)] \cdot 3 \geq 3,$$

which is a contradiction.

Case $[E:\mathbb{Q}]=3$. Our aim is to find a Galois field extension $\mathbb{Q}\subseteq L$ with $[L:\mathbb{Q}]=6$ and a normal subgroup H of $G:=\mathrm{Gal}(L/\mathbb{Q})$ such that H has order 2. Then by FTGT(2) we obtain $H=\mathrm{Gal}(L/L_H)$, by FTGT(3) we obtain $[L:L_H]=|H|=2$, by FTGT(5) we obtain that $\mathbb{Q}\subseteq L_H$ is normal and by FTGT(6) we obtain $[L_H:\mathbb{Q}]=\frac{\mathrm{Gal}(L/\mathbb{Q})}{\mathrm{Gal}(L/L_H)}=\frac{[L:\mathbb{Q}]}{[L:L_H]}=\frac{6}{2}=3$. Moreover, in this case there exist no intermediate fields strictly between $\mathbb{Q}$ and L_H. Indeed, if $\mathbb{Q}\subseteq F\subseteq L_H$, then

$$3=[E:\mathbb{Q}]=[E:L_H][L_H:\mathbb{Q}]$$

implies that either $[E:L_H]=1$ or $[L_H:\mathbb{Q}]=1$ and so either $L_H=E$ or $L_H=\mathbb{Q}$. By Theorem 11.4 we conclude in this case that $L_H=\mathbb{Q}(\alpha)$ for some $\alpha\in E$. In particular, since $[E:\mathbb{Q}]<\infty$, we have that α is algebraic over $\mathbb{Q}$ and hence the minimum polynomial $p_\alpha(x)\in\mathbb{Q}[x]$ exists. Now let $g\in\mathrm{Gal}(L_H/\mathbb{Q})$ have order three. Then $g:\mathbb{Q}(\alpha)\to\mathbb{Q}(\alpha)$ is an isomorphism with $g(\alpha)\neq\alpha$. Then

$$0=g(p_\alpha(\alpha))=p_\alpha(g(\alpha))$$

implies that $g(\alpha)\neq\alpha$ is also a root of $p_\alpha(x)$ and similarly $g^2(\alpha)$ is also a root of $p_\alpha(x)$. We conclude that in this case $\mathbb{Q}(\alpha)$ is the splitting field of $p_\alpha(x)$. Now we proceed with finding a concrete example. Recall by Example 12.13(1) that if $\zeta=e^{\frac{2\pi i}{7}}$, then $\mathbb{Q}(\zeta)$ is the splitting field of $\Phi_7(x)=1+x+x^2+x^3+x^4+x^5+x^6$. Moreover, in this case, the Galois group $G=\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})$ is isomorphic to $\mathbb{Z}_7^*$ and so $[\mathbb{Q}(\zeta):\mathbb{Q}]=6$. More precisely, we have that $G=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6\}$ where $\sigma_i(\zeta)=\zeta^i$. In particular, we have

$$\sigma_6^2(\zeta)=\sigma(\zeta^6)=\zeta^{36}=\zeta,$$

and so $H=\{\sigma_1,\sigma_6\}$ is a subgroup of G of order 2 (notice that $\sigma_1=\mathrm{id}_{\mathbb{Q}(\zeta)}$. Let us compute the fixed field $\mathbb{Q}(\zeta)_H$. A $\mathbb{Q}$-basis of L is given by $\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$. If $q=a+b\zeta+c\zeta^2+d\zeta^3+e\zeta^4+f\zeta^5\in\mathbb{Q}(\zeta)$, then $\sigma_6(q)=q$ if and only if

$$a+b\zeta^6+c\zeta^5+d\zeta^4+e\zeta^3+f\zeta^2=a+b\zeta+c\zeta^2+d\zeta^3+e\zeta^4+f\zeta^5,$$

which, using $\zeta^6=-1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5$ (which holds since ζ is a root of $\Phi_7(x)$), becomes equivalent to

$$(a-b)-b\zeta+(f-b)\zeta^2+(e-b)\zeta^3+(d-b)\zeta^4+(c-b)\zeta^5=a+b\zeta+c\zeta^2+d\zeta^3+e\zeta^4+f\zeta^5.$$

By equating the coefficients of the same elements (which we can do since $\{1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5\}$ is a linearly independent set), we obtain a linear system of equations with unknowns a,b,c,d,e,f. Solving this system we obtain $b=0$, $c=f$ and $d=e$. Hence

$$q=a+c\zeta^2+d\zeta^3+d\zeta^4+c\zeta^5=a+c(\zeta^2+\zeta^5)+d(\zeta^3+\zeta^4).$$

Hence

$$\mathbb{Q}(\zeta)_H=\{a+c(\zeta^2+\zeta^5)+d(\zeta^3+\zeta^4)\mid a,c,d\in\mathbb{Q}\}=\mathbb{Q}(\zeta^2+\zeta^5,\zeta^3+\zeta^4).$$

As claimed in the general case, we have $[\mathbb{Q}(\zeta)_H,\mathbb{Q}]=3$ since $[\mathbb{Q}(\zeta):\mathbb{Q}(\zeta)_H]=|H|=2$ by FTGT(3) and $[\mathbb{Q}(\zeta):\mathbb{Q}]=6$ by construction. We claim that $\mathbb{Q}(\zeta^2+\zeta^5,\zeta^3+\zeta^4)=\mathbb{Q}(\zeta^2+\zeta^5)$. Indeed, since there exist no intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta^2+\zeta^5,\zeta^3+\zeta^4)$, it is enough to show that $\zeta^2+\zeta^5$ is not in $\mathbb{Q}$. To this end we compute the minimal polynomial of $\zeta^2+\zeta^5$ over $\mathbb{Q}$. Notice that since $[\mathbb{Q}(\zeta^2+\zeta^5,\zeta^3+\zeta^4):\mathbb{Q}]=3$, the minimal polynomial has degree at most 3. We set $\alpha=\zeta^2+\zeta^5$ and we compute

$$\alpha^2=2+\zeta^3+\zeta^4,$$

and $\alpha^3=\zeta+3\alpha+\zeta^6$. Now we investigate if there exist $k,l,m\in\mathbb{Q}$ such that

$$\alpha^3+k\alpha^2+l\alpha+m=0.$$

Replacing α^3 and α^2 and replacing $\zeta^6=-1-\zeta-\zeta^2-\zeta^3-\zeta^4-\zeta^5$, the above equation becomes

$$(m+2k-1)+(2+l)\zeta^2+(k-1)\zeta^3+(k-1)\zeta^4+(2+l)\zeta^5=0.$$

Again equating the coefficients gives $k = 1$, $l = -2$ and $m = -1$. Hence ζ is a root of $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. Notice that this polynomial has no roots in $\mathbb{Z}$ (since the only possible integer roots are divisors of the constant term 1, and neither 1 nor -1 is a root) and so it has no roots in $\mathbb{Q}$ by Theorem 3.7. Hence $\alpha \notin \mathbb{Q}$ and so $\mathbb{Q}(\zeta)_H = \mathbb{Q}(\alpha)$. Moreover, since $f(x)$ is of degree 3, it follows that it is irreducible over $\mathbb{Q}$. Now notice that if $K = \mathrm{Gal}(\mathbb{Q}(\zeta)_H/\mathbb{Q})$, then by FTGT(6) we have

$$K = \mathrm{Gal}(\mathbb{Q}(\zeta)_H/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q})/\,\mathrm{Gal}(\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)_H) = G/H$$

has order 3. Given an element of $g \in K$ of order 3, $g(\alpha)$ and $g(\alpha^2)$ are both roots of $f(x)$ different than α and inside $\mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha)$ is a splitting field of $f(x) = x^3 + x^2 - 2x - 1$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, as required. (For an explicit $g \in K$ we may pick σ_3, so that $\sigma_3(\zeta^2 + \zeta^5) = \zeta + \zeta^6$, $\sigma_3(\zeta + \zeta^6) = \zeta^3 + \zeta^4$ and $\sigma_3(\zeta^3 + \zeta^4) = \zeta^2 + \zeta^5$, showing that the roots of $f(x)$ are $\zeta^2 + \zeta^5, \zeta + \zeta^6$ and $\zeta^3 + \zeta^4$.

Case $[E : \mathbb{Q}] = 6$. For an example of this case let $f(x) = x^3 - 2$. Then if E is the splitting field of $f(x)$, we have $[E : \mathbb{Q}] = 6$ as we computed in Example 7.5(1).