Notes on Galois Theory III

5 The main theorem of Galois theory

Let E be a finite extension of F. Then we have defined the Galois group $\mathrm{Gal}(E/F)$ (although it could be very small). If H is a subgroup of $\mathrm{Gal}(E/F)$, we have defined the *fixed field*

$$E^H = \{\alpha \in E : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Clearly $F \leq E^H \leq E$.

On the other hand, given an intermediate field K between F and E, i.e. a subfield of E containing F, so that $F \leq K \leq E$, we can define $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(E/K)$ is clearly a **subgroup** of $\mathrm{Gal}(E/F)$, since if $\sigma(a) = a$ for all $a \in K$, then $\sigma(a) = a$ for all $a \in F$. Thus we have two constructions: one associates an intermediate field to a subgroup of $\mathrm{Gal}(E/F)$, and the other associates a subgroup of $\mathrm{Gal}(E/F)$ to an intermediate field. In general, there is not much that we can say about these two constructions. But if E is a **Galois** extension of F, they turn out to set up a one-to-one correspondence between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields K between F and E, i.e. fields K with $F \leq K \leq E$.

Theorem 5.1 (Main Theorem of Galois Theory)**.** *Let E be a **Galois** extension of a field F. Then:*

(i) *There is a one-to-one correspondence between subgroups of $\mathrm{Gal}(E/F)$ and intermediate fields K between F and E, given as follows: To a subgroup H of $\mathrm{Gal}(E/F)$, we associate the fixed field E^H, and to an intermediate field K between F and E we associate the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$. These constructions are inverses, in other words*

$$\mathrm{Gal}(E/E^H) = H;$$
$$E^{\mathrm{Gal}(E/K)} = K.$$

In particular, the fixed field of the full Galois group $\mathrm{Gal}(E/F)$ *is* F *and the fixed field of the identity subgroup is* E*:*

$$E^{\mathrm{Gal}(E/F)} = F \qquad \textit{and} \qquad E^{\{\mathrm{Id}\}} = E.$$

Finally, since there are only finitely many subgroups of $\mathrm{Gal}(E/F)$*, there are only finitely many intermediate fields* K *between* F *and* E*.*

(ii) *The above correspondence is order reversing with respect to inclusion.*

(iii) *For every subgroup* H *of* $\mathrm{Gal}(E/F)$*,* $[E : E^H] = \#(H)$*, and hence* $[E^H : F] = (\mathrm{Gal}(E/F) : H)$*. Likewise, for every intermediate field* K *between* F *and* E*,* $\#(\mathrm{Gal}(E/K)) = [E : K]$*.*

(iv) *For every intermediate field* K *between* F *and* E*, the field is a* ***normal*** *extension of* F *if and only if* $\mathrm{Gal}(E/K)$ *is a* ***normal*** *subgroup of* $\mathrm{Gal}(E/F)$*. In this case,* K *is a Galois extension of* F*, and*

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)\Big/\mathrm{Gal}(E/K).$$

Example 5.2. 1) Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We keep the notation of 4) of Example 1.11. If $G = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, then $G = \{1, \sigma_1, \sigma_2, \sigma_3\}$. The subgroups of G are the trivial subgroups $\{1\}$ and G and the subgroups $\langle\sigma_i\rangle$ of order 2, hence of index 2. As always, $E^{\{1\}} = E$ and $E^G = F = \mathbb{Q}$. Clearly $\sigma_1(\sqrt{3}) = \sqrt{3}$. Thus $\mathbb{Q}(\sqrt{3}) \leq E^{\langle\sigma_1\rangle}$. But since $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 = (G : \langle\sigma_1\rangle)$, in fact $\mathbb{Q}(\sqrt{3}) = E^{\langle\sigma_1\rangle}$. Similarly $\mathbb{Q}(\sqrt{2}) = E^{\langle\sigma_2\rangle}$. As for $E^{\langle\sigma_3\rangle}$, since $\sigma_3(\sqrt{2}) = -\sqrt{2}$ and $\sigma_3(\sqrt{3}) = -\sqrt{3}$, it follows that $\sigma_3(\sqrt{6}) = \sqrt{6}$. Thus $\mathbb{Q}(\sqrt{6}) = E^{\langle\sigma_3\rangle}$.

It is also interesting to look at this example from the viewpoint of $\mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2}+\sqrt{3}$. Using the notation $\alpha = \beta_1 = \sqrt{2}+\sqrt{3}$, $\beta_2 = -\sqrt{2}+\sqrt{3}$, $\beta_3 = \sqrt{2} - \sqrt{3}$, and $\beta_4 = -\sqrt{2} - \sqrt{3}$ identifies σ_1 with $(12)(34)$, σ_2 with $(13)(24)$, and σ_3 with $(14)(23) \in S_4$. It is then clear that $\beta_1 + \beta_2$ is fixed by σ_1. (Of course, so is $\beta_3+\beta_4$, but it is easy to check that $\beta_3+\beta_4 = -(\beta_1+\beta_2)$.) Hence $\mathbb{Q}(\beta_1 + \beta_2) \leq E^{\langle\sigma_1\rangle}$. On the other hand, $\beta_1 + \beta_2 = 2\sqrt{3}$, and degree arguments as above show that

$$E^{\langle\sigma_1\rangle} = \mathbb{Q}(\beta_1 + \beta_2) = \mathbb{Q}(2\sqrt{3}) = \mathbb{Q}(\sqrt{3}).$$

Likewise using the element $\beta_1+\beta_3 = 2\sqrt{2}$ which is fixed by σ_2, corresponding to $(13)(24)$ gives $E^{\langle\sigma_2\rangle} = \mathbb{Q}(\sqrt{2})$. If we try to do the same thing with $\sigma_3 = (14)(23)$, however, we find that $\beta_1 + \beta_4 = 0$, since $\sigma_3(\beta_1) = -\beta_4$, and hence we obtain the useless information that $\mathbb{Q}(0) \leq E^{\langle \sigma_3 \rangle}$. To find a nonzero, in fact a nonrational element of E fixed by σ_3, note that as $\sigma_3(\beta_1) = -\beta_1$, $\sigma_3(\beta_1^2) = (-\beta_1)^2 = \beta_1^2$. Now $\beta_1^2 = (\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6}$, and $\mathbb{Q}(5 + 2\sqrt{6}) = \mathbb{Q}(\sqrt{6})$. Thus as before $\mathbb{Q}(\sqrt{6}) = E^{\langle \sigma_3 \rangle}$.

2) Take $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt[3]{2}, \omega)$. List the roots of $x^3 - 2$ as $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega \sqrt[3]{2}$, $\alpha_3 = \omega^2 \sqrt[3]{2}$. Let $G = \mathrm{Gal}(E/F) \cong S_3$. Now S_3 has the trivial subgroups S_3 and $\{1\}$, as well as $A_3 = \langle (123) \rangle$ and three subgroups of order 2, $\langle (12) \rangle$, $\langle (13) \rangle$, and $\langle (23) \rangle$. Clearly $\alpha_3 \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle}$. Since

$$[\mathbb{Q}(\alpha_3) : \mathbb{Q}] = 3 = (S_3 : \langle (12) \rangle),$$

$\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle} = \mathbb{Q}(\alpha_3)$. Similarly $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (13) \rangle} = \mathbb{Q}(\alpha_2)$ and $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (23) \rangle} = \mathbb{Q}(\alpha_1)$. The remaining fixed field is $\mathbb{Q}(\sqrt[3]{2}, \omega)^{A_3}$, which is a degree 2 extension of $\mathbb{Q}$. Since we already know a subfield of $\mathbb{Q}(\sqrt[3]{2}, \omega)$ which is a degree 2 extension of $\mathbb{Q}$, namely $\mathbb{Q}(\omega)$ it must be equal to $\mathbb{Q}(\sqrt[3]{2}, \omega)^{A_3}$ by the Main Theorem. However, let us check directly that $\omega \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{A_3}$. It suffices to check that the element φ of the Galois group corresponding to (123) satisfies $\varphi(\omega) = \omega$. Note that $\omega = \alpha_2/\alpha_1 = \alpha_3/\alpha_2$. Thus

$$\varphi(\omega) = \varphi(\alpha_2/\alpha_1) = \varphi(\alpha_2)/\varphi(\alpha_1) = \alpha_3/\alpha_2 = \omega,$$

as claimed.

One can also try to describe $\mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle}$ as follows: Clearly $\alpha_1 + \alpha_2 \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle}$. But

$$\alpha_1 + \alpha_2 = \sqrt[3]{2} + \omega \sqrt[3]{2} = (1 + \omega)\sqrt[3]{2} = -\omega^2 \sqrt[3]{2},$$

since ω is a root of $x^3 - 1 = (x - 1)(x^2 + x + 1)$, and hence $\omega^2 + \omega + 1 = 0$. Thus $\omega^2 \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, \omega)^{\langle (12) \rangle}$, and both fields have degree 3 over $\mathbb{Q}$, hence they are equal.

Finally, we describe the more complicated example of $\mathrm{Gal}(\sqrt[4]{2}, i)/\mathbb{Q})$:

Elements of D_4: 1, (1234), $(1234)^2 = (13)(24)$, $(1234)^3 = (1432)$; (13), (24), (12)(34), (14)(23).

Subgroups of D_4: $\{1\}$ (order 1), D_4 (order 8). The three subgroups of order 4, all automatically normal:

$$\begin{aligned} H_1 &= \langle (1234) \rangle \\ H_2 &= \{1, (13)(24), (12)(34), (14)(23)\} \\ H_3 &= \{1, (13)(24), (13), (24)\}. \end{aligned}$$

The five subgroups of order 2: $\langle(13)(24)\rangle$, $\langle(13)\rangle$, $\langle(24)\rangle$, $\langle(12)(34)\rangle$, $\langle(14)(23)\rangle$. Of these, only $\langle(13)(24)\rangle$ is normal (it is the center of D_4).

The fixed fields: Label the roots of $x^4 - 2$ as

$$\alpha_1 = \sqrt[4]{2}; \qquad \alpha_2 = i\sqrt[4]{2}; \qquad \alpha_3 = -\sqrt[4]{2}; \qquad \alpha_4 = -i\sqrt[4]{2},$$

corresponding to the labeling of elements of D_4 above. Then the fixed field of $\{1\}$ is $E = \mathbb{Q}(\sqrt[4]{2}, i)$ and the fixed field of D_4 is $\mathbb{Q}$. As for the subgroups of order 2, they correspond to subfields K of E such that $[K : \mathbb{Q}] = 4$. For example, it is clear that $\sqrt[4]{2} \in E^{\langle(24)\rangle}$ and hence by counting degrees that

$$E^{\langle(24)\rangle} = \mathbb{Q}(\sqrt[4]{2}).$$

Likewise $E^{\langle(13)\rangle} = \mathbb{Q}(i\sqrt[4]{2})$. As for $E^{\langle(13)(24)\rangle}$, note that $\sqrt{2} = (\sqrt[4]{2})^2 = (-\sqrt[4]{2})^2$ is fixed by $(13)(24)$, and also i is fixed by $(13)(24)$ since if $\sigma(\sqrt[4]{2}) = -\sqrt[4]{2}$ and $\sigma(i\sqrt[4]{2}) = -i\sqrt[4]{2}$, then

$$\sigma(i) = \sigma(i\sqrt[4]{2}/\sqrt[4]{2}) = \sigma(i\sqrt[4]{2})/\sigma(\sqrt[4]{2}) = (-i\sqrt[4]{2})/(-\sqrt[4]{2}) = i.$$

Thus $\mathbb{Q}(\sqrt{2}, i) \subseteq E^{\langle(13)(24)\rangle}$, so again by counting degrees they are equal. As for $E^{\langle(12)(34)\rangle}$, note that $\sqrt[4]{2} + i\sqrt[4]{2} = \alpha_1 + \alpha_2 \in E^{\langle(12)(34)\rangle}$. In particular, this forces $\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) \neq F$. While it may not be obvious how to compute the degree $[\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) : \mathbb{Q}]$, note that

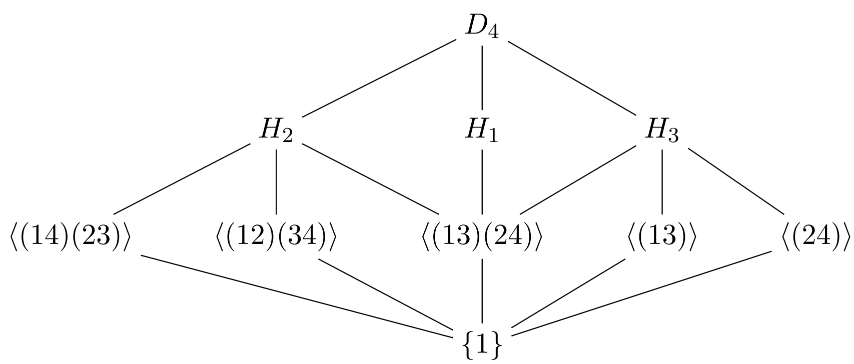
$$(\sqrt[4]{2} + i\sqrt[4]{2})^2 = (1+i)^2(\sqrt[4]{2})^2 = 2i\sqrt{2}.$$

Thus $[\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) : \mathbb{Q}(i\sqrt{2})] = 2$ since $\sqrt[4]{2} + i\sqrt[4]{2} \notin \mathbb{Q}(i\sqrt{2})$, and since $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$ since $i\sqrt{2} = \sqrt{-2}$, it follows that

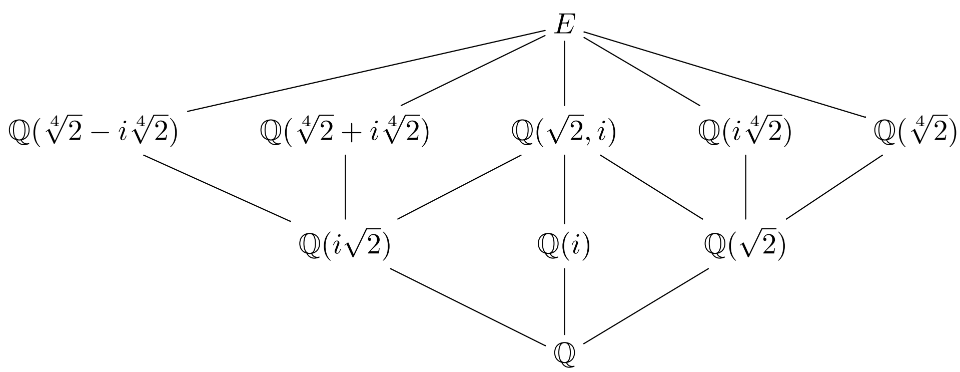
$$[\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}) : \mathbb{Q}(i\sqrt{2})][\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 4.$$

Hence, again by counting degrees, $E^{\langle(12)(34)\rangle} = \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2})$. Similarly, $E^{\langle(14)(23)\rangle} = \mathbb{Q}(\sqrt[4]{2} - i\sqrt[4]{2})$.
Finally, there are the 3 fields E^{H_1}, E^{H_2}, E^{H_3}. A computation shows that $i \in E^{H_1}$, hence $E^{H_1} = \mathbb{Q}(i)$. As for the others, clearly $E^{H_2} = E^{\langle(13)(24)\rangle} \cap E^{\langle(12)(34)\rangle}$. Since $E^{\langle(13)(24)\rangle} = \mathbb{Q}(\sqrt{2}, i)$ and $i\sqrt{2} \in E^{\langle(12)(34)\rangle}$, $i\sqrt{2} \in E^{H_2}$ and hence $E^{H_2} = \mathbb{Q}(i\sqrt{2})$. The other equality $E^{H_3} = \mathbb{Q}(\sqrt{2})$ is similar.

Picture of the subgroups of D_4:



Picture of the intermediate subfields between E and $\mathbb{Q}$:



6 Proofs

For simplicity, we shall always assume that F has characteristic zero, or more generally is perfect. In particular, every irreducible polynomial $f \in F[x]$ has only simple zeroes in any extension field of F, and every finite extension of F is automatically separable.

We begin with a proof of the primitive element theorem:

Theorem 6.1. *Let F be a perfect field and let E be a finite extension of F. Then there exists $\alpha \in E$ such that $E = F(\alpha)$.*

Proof. If F is finite we have already proved this. So we may assume that F is infinite. We begin with the following:

Claim 6.2. *Let L be an extension field of the field K, and suppose that $p, q \in K[x]$. If the gcd of p and q in $L[x]$ is of the form $x - \xi$, then $\xi \in K$.*

Proof of the claim. We have seen that the gcd of p, q in $K[x]$ is a gcd of p, q in $L[x]$, and hence they are the same if they are both monic. It follows that $x - \xi$ is the gcd of p, q in $K[x]$ and in particular that $\xi \in K$. $\square$

Returning to the proof of the theorem, it is clearly enough by induction to prove that $F(\alpha, \beta) = F(\gamma)$ for some $\gamma \in F(\alpha, \beta)$. Let $f = \mathrm{irr}(\alpha, F)$ and let $g = \mathrm{irr}(\beta, F)$. There is an extension field L of $F(\alpha, \beta)$ such that f factors into distinct linear factors in L, say $f = (x - \alpha_1) \cdots (x - \alpha_n)$, with $\alpha = \alpha_1$, and likewise g factors into distinct linear factors in L, say $g = (x - \beta_1) \cdots (x - \beta_m)$, with $\beta = \beta_1$. Since F is infinite, we can choose a $c \in F$ such that, for all i, j with $j \neq 1$,

$$c \neq \frac{\alpha - \alpha_i}{\beta - \beta_j}.$$

(Notice that we need to take $j \neq 1$ so that the denominator is not zero.) In other words, for all i and j with $j \neq 1$, $\alpha - \alpha_i \neq c(\beta - \beta_j)$. Set $\gamma = \alpha - c\beta$. Then

$$\gamma = \alpha - c\beta \neq \alpha_i - c\beta_j$$

for all i and j with $j \neq 1$. Thus $\gamma + c\beta = \alpha = \alpha_1$, but for all $j \neq 1$, $\gamma + c\beta_j \neq \alpha_i$ for any i.

We are going to construct a polynomial $h \in F(\gamma)[x]$ such that $h(\beta) = 0$ but, for $j \neq 1$, $h(\beta_j) \neq 0$. Once we have done so, consider the gcd of g and h in L (which contains all of the roots $\beta = \beta_1, \ldots, \beta_m$ of g). The only irreducible factor of g which divides h is $x - \beta$, which divides g only to the first power. Thus the gcd of g and h in $L[x]$ is $x - \beta$. Since $h \in F(\gamma)[x]$ by construction and $g \in F[x] \leq F(\gamma)[x]$, both g and h are elements of $F(\gamma)[x]$. Then Claim 6.2 implies that $\beta \in F(\gamma)$. But then $\alpha = \gamma + c\beta \in F(\gamma)$ also (recall $c \in F$ by construction). So $\alpha, \beta \in F(\gamma)$, but clearly $\gamma \in F(\alpha, \beta)$. Hence $F(\alpha, \beta) = F(\gamma)$.

Finally we construct $h \in F(\gamma)[x]$. Take $h = f(\gamma + cx)$, where $f = \mathrm{irr}(\alpha, F)$. Clearly the coefficients of h lie in $F(\gamma)$. Note that $h(\beta) = f(\gamma + c\beta) = f(\alpha) = 0$, but for $j \neq 1$, $h(\beta_j) = f(\gamma + c\beta_j)$. By construction, for $j \neq 1$, $\gamma + c\beta_j \neq \alpha_i$ for any i, hence $\gamma + c\beta_j$ is not a root of f and so $h(\beta_j) \neq 0$. This completes the construction of h and the proof of the theorem. $\square$

Remark 6.3. For fields F which are not perfect, there can exist simple extensions of F which are not separable as well as finite extensions which are not simple. One can show that a finite extension E of a field F is a simple extension $\iff$ there are only finitely many fields K with $F \leq K \leq E$.

Next we turn to a proof of the Main Theorem of Galois Theory. Let E be a Galois extension of F. Recall that the correspondence given in the Main Theorem between intermediate fields K (i.e. $F \leq K \leq E$ and subgroups H of $\mathrm{Gal}(E/F)$ is as follows: given K, we associate to it the subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/F)$, and given $H \leq \mathrm{Gal}(E/F)$, we associate to it the fixed field $E^H \leq E$. Both of these constructions are clearly order-reversing with respect to inclusion, in other words

$$H_1 \leq H_2 \implies E^{H_2} \leq E^{H_1}$$

and

$$F \leq K_1 \leq K_2 \leq E \implies \mathrm{Gal}(E/K_2) \leq \mathrm{Gal}(E/K_1).$$

This is (ii) of the Main Theorem.

Next we prove (i) and (iii). First, suppose that K is an intermediate field. We will show that $E^{\mathrm{Gal}(E/K)} = K$. Clearly, $K \leq E^{\mathrm{Gal}(E/K)}$. It thus suffices to show that, if $\alpha \in E$ but $\alpha \notin K$, then there exists a $\sigma \in \mathrm{Gal}(E/K)$ such that $\sigma(\alpha) \neq \alpha$, i.e. $\alpha \notin E^{\mathrm{Gal}(E/K)}$. (This says that $E^{\mathrm{Gal}(E/K)} \leq K$ and hence $E^{\mathrm{Gal}(E/K)} = K$.) If $\alpha \notin K$, then $f = \mathrm{irr}(\alpha, K)$ is an irreducible polynomial in $K[x]$ of degree $k > 1$. Since E is a normal extension of F and hence of K and the root α of the irreducible polynomial $f \in K[x]$ lies in E, all roots $\alpha = \alpha_1, \dots, \alpha_k$ of f lie in E. Choose some $i > 1$. Then there is an injective homomorphism $\psi\colon K(\alpha) \to E$ such that $\psi|K = \mathrm{Id}$ but $\psi(\alpha) = \alpha_i \neq \alpha$. By the isomorphism extension theorem, there exists an extension L of E such that the homomorphism ψ extends to a homomorphism $\sigma\colon E \to L$. Since E is a normal extension of F and $\sigma|F = \mathrm{Id}$, $\sigma(E) = E$ and thus $\sigma \in \mathrm{Gal}(E/F)$. Since $\sigma|K = \psi|K = \mathrm{Id}$, in fact $\sigma \in \mathrm{Gal}(E/K)$. We have thus found the desired σ. Note further that, as E is a Galois extension of K, we must have $\#(\mathrm{Gal}(E/K)) = [E : K]$.

Now suppose that H is a subgroup of $\mathrm{Gal}(E/F)$. We claim that

$$\mathrm{Gal}(E/E^H) = H.$$

Clearly, $H \leq \mathrm{Gal}(E/E^H)$ by definition. Thus, $\#(H) \leq \#(\mathrm{Gal}(E/E^H))$. To prove that $\mathrm{Gal}(E/E^H) = H$, it thus suffices to show that $\#(\mathrm{Gal}(E/E^H)) \leq \#(H)$. This will follow from:

Claim 6.4. *For all $\alpha \in E$, $\deg_{E^H} \alpha \leq \#(H)$.*

First let us see that Claim 6.4 implies that $\#(\mathrm{Gal}(E/E^H)) \leq \#(H)$. By the Primitive Element Theorem, there exists an $\alpha \in E$ such that $E = E^H(\alpha)$, and hence $\deg_{E^H} \alpha = [E : E^H]$. For this α, Claim 6.4 implies that

$$\#(\mathrm{Gal}(E/E^H)) = [E : E^H] = \deg_{E^H} \alpha \leq \#(H).$$

Thus $\#(H) \geq \#(\mathrm{Gal}(E/E^H))$. But $H \leq \mathrm{Gal}(E/E^H)$ and hence $\#(H) \leq \#(\mathrm{Gal}(E/E^H))$. Clearly we must have $\mathrm{Gal}(E/E^H) = H$ and $\#(H) = \#(\mathrm{Gal}(E/E^H))$, proving the rest of (i) and (iii).

To prove Claim 6.4, given $\alpha \in E$ consider the polynomial

$$f = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

The number of linear factors of f is $\#(H)$, so that $f \in E[x]$ is a polynomial of degree $\#(H)$. We claim that in fact $f \in E^H[x]$, in other words that all coefficients of f lie in the fixed field E^H. It suffices to show that, for all $\psi \in H$, $\psi(f) = f$. Now, using the fact that ψ is an automorphism, it is easy to see that

$$\psi(f) = \prod_{\sigma \in H} (x - \psi\sigma(\alpha)).$$

As $\psi \in H$, the function $\sigma \in H \mapsto \psi\sigma$ is a permutation of the group H (cf. the proof of Cayley's theorem!) and so the product $\prod_{\sigma \in H}(x - \psi\sigma(\alpha))$ is the same as the product $\prod_{\sigma \in H}(x - \sigma(\alpha))$ (but with the order of the factors changed, if $\psi \neq \mathrm{Id}$). Hence $\psi(f) = f$ for all $\psi \in H$, so that $f \in E^H[x]$. It follows that $\mathrm{irr}(\alpha, E^H)$ divides f, and hence that $\deg_{E^H} \alpha \leq \deg f = \#(H)$.

Finally we must prove (iv) of the Main Theorem. Let $F \leq K \leq E$. The first statement of (iv) is the statement that K is a normal (hence Galois) extension of $F \iff \mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$. A slight variation of the proof of Theorem 3.5 shows that K is a normal extension of $F \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(K) = K$. More generally, for K an arbitrary intermediate field, given $\sigma \in \mathrm{Gal}(E/F)$, we can ask for a description of the image subfield $\sigma(K)$ of E. By Part (i) of the Main Theorem (already proved), it is equivalent to describe the corresponding subgroup $\mathrm{Gal}(E/\sigma(K))$ of $\mathrm{Gal}(E/F)$.

Claim 6.5. *In the above notation,* $\mathrm{Gal}(E/\sigma(K)) = \sigma \cdot \mathrm{Gal}(E/K) \cdot \sigma^{-1} = i_\sigma(\mathrm{Gal}(E/K))$*, where* i_σ *is the inner automorphism of* $\mathrm{Gal}(E/F)$ *given by conjugation by the element* σ*.*

Proof. If $\varphi \in \mathrm{Gal}(E/F)$, then $\varphi \in \mathrm{Gal}(E/\sigma(K)) \iff$ for all $\alpha \in K$, $\varphi(\sigma(\alpha)) = \sigma(\alpha) \iff$ for all $\alpha \in K$, $\sigma^{-1}\varphi\sigma(\alpha) = \alpha \iff \sigma^{-1}\varphi\sigma \in \mathrm{Gal}(E/K) \iff \varphi \in \sigma \cdot \mathrm{Gal}(E/K) \cdot \sigma^{-1}$. $\square$

Now apply the remarks above: K is a normal extension of $F \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\sigma(K) = K \iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\mathrm{Gal}(E/\sigma(K)) = \mathrm{Gal}(E/K)$ (by (i) of the Main Theorem) $\iff$ for all $\sigma \in \mathrm{Gal}(E/F)$, $\mathrm{Gal}(E/K) = \sigma \cdot \mathrm{Gal}(E/K) \cdot \sigma^{-1} \iff \mathrm{Gal}(E/K)$ is a normal subgroup of $\mathrm{Gal}(E/F)$. This proves the first statement of (iv). We must then show that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \Big/ \mathrm{Gal}(E/K)$. To see this, given $\sigma \in \mathrm{Gal}(E/F)$, we have seen that $\sigma(K) = K$, and hence that $\sigma \mapsto \sigma|K$ defines a function from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. Clearly, this is a homomorphism, and by definition its kernel is just the subgroup of $\sigma \in \mathrm{Gal}(E/F)$ such that $\sigma|K = \mathrm{Id}$, which by definition is $\mathrm{Gal}(E/K)$. To see that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \Big/ \mathrm{Gal}(E/K)$, by the fundamental homomorphism theorem, it suffices to show that the homomorphism $\sigma \mapsto \sigma|K$ is a surjective homomorphism from $\mathrm{Gal}(E/F)$ to $\mathrm{Gal}(K/F)$. This says that, given a $\psi\colon K \to K$ such that $\psi|F = \mathrm{Id}$, there exists an extension of ψ to a $\sigma \in \mathrm{Gal}(E/F)$. But it follows from the Isomorphism Extension Theorem that, given ψ, there exists an extension field L of E and an extension of ψ to a homomorphism $\sigma\colon E \to L$. Since E is a normal extension of F, $\sigma(E) = E$, and hence $\sigma \in \mathrm{Gal}(E/F)$ is such that $\sigma \mapsto \psi \in \mathrm{Gal}(K/F)$. It follows that restriction defines a surjective homomorphism $\mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ with kernel $\mathrm{Gal}(E/K)$, so that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F) \Big/ \mathrm{Gal}(E/K)$. This concludes the proof of the Main Theorem. $\square$