21. Galois correspondence (continued)

21.1. **More on Galois correspondence.** Our first result provides yet another characterization of finite Galois extensions.

Proposition 21.1. *Let K/F be a finite extension. Then K/F is Galois $\iff$ $K^{\mathrm{Aut}(K/F)} = F$.*

Remark: The forward direction of Proposition 21.1 immediately yields the second half of the proof of the Fundamental Theorem of Galois Theory (FTGT). In fact, we could have (and should have) proved Proposition 21.1 before FTGT.

Proof. Let $G = \mathrm{Aut}(K/F)$. By Artin's Lemma K/K^G is Galois and $\mathrm{Aut}(K/K^G) = G$, so $[K : K^G] = |G|$ by Theorem 19.1.

Since $F \subseteq K^G$, the equality $K^G = F$ holds if and only if $[K : F] = |G|$. On the other hand, again by Theorem 19.1, $[K : F] = |G|$ if and only if K/F is Galois. □

Here is another result whose proof is of similar flavor.

Observation 21.2. *Let K/F be a finite Galois extension and $G = \mathrm{Aut}(K/F)$. Then for any subgroup H of G we have $[G : H] = [K^H : F]$.*

Proof. The same argument as in the proof of Proposition 21.1 shows that $[K : K^H] = |H|$. Therefore,

$$[K^H : F] = \frac{[K : F]}{[K : K^H]} = \frac{|G|}{|H|} = [G : H].$$

□

Let K/F be a Galois extension and $G = \mathrm{Aut}(K/F)$. By the Fundamental Theorem every subgroup of G has the form $\mathrm{Aut}(K/L)$ for unique subfield L of K/F. The next result tells us which subfields correspond to normal subgroups.

Proposition 21.3. *Let K/F be a finite Galois extension and L a subfield of K/F. The following hold:*

(i) *K/L is always Galois*

(ii) *L/F is always separable*

(iii) *L/F is normal (hence Galois) $\iff$ $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$. Furthermore, if this happens, then*

$$\mathrm{Aut}(L/F) \cong \mathrm{Aut}(K/F)/\mathrm{Aut}(K/L). \qquad (***)$$

Proof. (i) and (ii) are clear (in fact, we have already used both facts before), so we only need to prove (iii). We shall first prove the forward direction together with the "furthermore part" and then the backwards direction.

"$\Rightarrow$ + (***)" Assume that L/F is normal, and let $\sigma \in \mathrm{Aut}(K/F)$. Then $\sigma(L) = L$ by [HW8, Problem 4], and thus we get a natural restriction map

$$R : \mathrm{Aut}(K/F) \to \mathrm{Aut}(L/F) \text{ given by } \sigma \mapsto \sigma_{|L}.$$

It is clear that R is a group homomorphism and

$$\mathrm{Ker}\, R = \{\sigma \in \mathrm{Aut}(K/F) : \sigma_{|L} = id\} = \mathrm{Aut}(K/L).$$

In particular, $\mathrm{Aut}(K/L)$ is normal and $\mathrm{Im}R \cong \mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$. Isomorphism (***) would follow if we show that R is surjective, and the latter can be proved by a routine application of the Main Extension Lemma. Since we are assuming that K/F is finite, there is also a simple counting argument:

$$|\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)| = \frac{[K:F]}{[K:L]} = [L:F] = |\mathrm{Aut}(L/F)|,$$

which implies surjectivity of R.

"$\Leftarrow$" Suppose that $\mathrm{Aut}(K/L)$ is normal in $\mathrm{Aut}(K/F)$. Let $\sigma \in \mathrm{Aut}(K/F)$ and take any $\tau \in \mathrm{Aut}(K/L)$. Then $\sigma^{-1}\tau\sigma \in \mathrm{Aut}(K/L)$, so for any $l \in L$ we have $\sigma^{-1}\tau\sigma(l) = l$ and hence $\tau\sigma(l) = \sigma(l)$. Since this is true for any $\tau \in \mathrm{Aut}(K/L)$, we get $\sigma(l) \in K^{\mathrm{Aut}(K/L)}$ and $K^{\mathrm{Aut}(K/L)} = L$ by FTGT.

So, $\sigma(L) \subseteq L$, and similarly $\sigma^{-1}(L) \subseteq L$. Thus, $\sigma(L) = L$ for any $\sigma \in \mathrm{Aut}(K/F)$. This easily implies that L/F is normal by the Main Extension Lemma (fill in the details). $\square$

Isomorphism (***) in Proposition 21.3 can be thought of as an analogue of the double quotient isomorphism theorem. The next result is a similar analogue of the diamond isomorphism theorem.

Proposition 21.4. *Let K/F and L/F be field extensions, where K and L are subfields of the same field. Assume that L/F is finite and Galois. Then KL/K is also finite and Galois, and there is an isomorphism*

$$\mathrm{Aut}(KL/K) \cong \mathrm{Aut}(L/K \cap L).$$

In particular, $\mathrm{Aut}(KL/K)$ *is a subgroup of* $\mathrm{Aut}(L/F)$ *and hence*

$$[KL:K] \text{ divides } [L:F].$$

Proof. The extension KL/K is

(i) separable by Corollary 18.6: KL is generated by L over K, each element of L is separable over F, hence separable over F;

(ii) normal by Proposition 20.1: if L is a splitting field over F for a separable family $\Omega \subseteq F[x]$, then KL is a spitting field for Ω over K.

Thus, KL/K is indeed Galois. We have a natural restriction homomorphism $R : \mathrm{Aut}(KL/K) \to \mathrm{Aut}(L/F)$ which is injective: if $\sigma \in \mathrm{Ker}\, R$, then σ acts trivially on both L and K hence also on KL.

Let $H = \mathrm{Im}R$ and $G = \mathrm{Aut}(L/K \cap L)$. To finish the proof we need to show that $H = G$, and by FTGT it is enough to show that $L^H = K \cap L$. The inclusion $K \cap L \subseteq L^H$ is clear since each element of H is a restriction of some element of $\mathrm{Aut}(KL/K)$.

Conversely, if $\alpha \in L^H$, then α (considered as an element of KL) is fixed by $\mathrm{Aut}(KL/K)$, so $\alpha \in (KL)^{\mathrm{Aut}(KL/K)} = K$. So $\alpha \in K \cap L$, and we have shown that $L^H \subseteq K \cap L$. □

21.2. **Computational applications.** A standard computational problem that can be solved using the Galois correspondence is determination of all subfields in a given finite Galois extension K/F. Indeed, by FTGT we just need to determine $G = \mathrm{Gal}(K/F)$, find all subgroups of G and for each subgroup H compute the fixed field K^H. Let us look at an example of such computations.

Example 21.1: Let K be the splitting field of $x^5 - 2$ over $\mathbb{Q}$.
From Midterm#2 we know that $K = \mathbb{Q}(\sqrt[5]{2}, \zeta)$ where $\zeta = e^{2\pi i/5}$ and that $[K : \mathbb{Q}] = 20$. Furthermore, the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is generated by the elements σ and τ given by

$$\sigma : \sqrt[5]{2} \mapsto \sqrt[5]{2}\zeta \qquad\qquad \tau : \sqrt[5]{2} \mapsto \sqrt[5]{2}$$
$$\zeta \mapsto \zeta \qquad\qquad \zeta \mapsto \zeta^2$$

Let us label the roots of $x^5 - 2$ as

$$\alpha_1 = \sqrt[5]{2},\ \alpha_2 = \sqrt[5]{2}\zeta,\ \alpha_3 = \sqrt[5]{2}\zeta^2,\ \alpha_4 = \sqrt[5]{2}\zeta^3,\ \alpha_5 = \sqrt[5]{2}\zeta^4.$$

By Lemma 19.3(b) this labeling determines an embedding of $\mathrm{Gal}(K/\mathbb{Q})$ in S_5, and it is clear that $\sigma = (12345)$ and $\tau = (2354)$. Let us compute fixed fields for three subgroups of G: $\langle\sigma\rangle$, $\langle\tau\rangle$ and $\langle\tau^2\rangle$.

Case 1: $H = \langle\sigma\rangle$. Since $|H| = 5$, we have $[K^H : \mathbb{Q}] = \frac{20}{5} = 4$ by Observation 21.2. On the other hand, σ fixes ζ and thus K^H contains $\mathbb{Q}(\zeta)$. Since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg_{\mathbb{Q}} \zeta = 4$, we conclude that $K^H = \mathbb{Q}(\zeta)$.

Case 2: $H = \langle\tau\rangle$ Using similar argument to Case 1 we conclude that $K^H = \mathbb{Q}(\sqrt[5]{2})$.

Case 3: $H = \langle\tau^2\rangle$. Since $\tau^2 = (25)(34)$, we have $|H| = 2$, and therefore $[K^H : \mathbb{Q}] = 10$. Since $K^{\langle\tau^2\rangle} \supseteq K^{\langle\tau\rangle}$, by Case 2 we have $K^H \supseteq \mathbb{Q}(\sqrt[5]{2})$. Moreover since $[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$, we have $K^H = \mathbb{Q}(\sqrt[5]{2}, \beta)$ for any $\beta \in K^H \setminus \mathbb{Q}(\sqrt[5]{2})$.

Note that $\tau^2 = (25)(34)$ fixes the elements α_1 and $\alpha_2 + \alpha_5$, hence also fixes $\beta := \frac{\alpha_2+\alpha_5}{\alpha_1} = \zeta + \zeta^4$. A direct computation shows that β is a root of $x^2 + x - 1 = 0$. This polynomial is irreducible over $\mathbb{Q}$ (since it has degree 2 and no roots in $\mathbb{Q}$), whence $\deg_{\mathbb{Q}} \beta = 2$. Since any element of $\mathbb{Q}(\sqrt[5]{2})$ has degree 1 or 5 over $\mathbb{Q}$, we conclude that $\zeta + \zeta^4 \in K^H \setminus \mathbb{Q}(\sqrt[5]{2})$, whence $K^H = \mathbb{Q}(\sqrt[5]{2}, \zeta + \zeta^4)$.