A crash course in Galois theory

First version 0.1 — 14. september 2013 klokken 14:50

In these notes K denotes a field.

Embeddings

Assume that Ω is a field and that $\sigma\colon K \to \Omega$ and embedding. If $K \subseteq L$ is an extension, we say that the embedding $\tau\colon L \to \Omega$ *extends* σ if $\tau|_K = \sigma$. In the special case when $K \subseteq \Omega$, and σ is the inclusion of K, such an embedding τ is said to be *an embedding over K*.

A fact that makes life easy working with fields, is that ring homomorphism between fields always are injective. And if in addition the two fields are of the same finite dimension over some ground field K and the homomorphism is an embedding over K (that is, it is K-linear), the homomorphism is also surjective.

We introduce the notation $\mathrm{Emb}_\sigma(L, \Omega)$ for the set of embeddings $\tau\colon L \to \Omega$ extending σ. In case σ is the inclusion of K in Ω, we write $\mathrm{Emb}_K(L, \Omega)$ for the set of embeddings over K. That is, we have

- $\mathrm{Emb}_\sigma(L, \omega) = \{$ embeddings $\tau\colon L \to \omega$ such that $\sigma|_K = \sigma\}$
- $\mathrm{Emb}_K(L, \Omega) = \{$ embeddings $\tau\colon L \to \Omega$ such that $\sigma(x) = x$ for $x \in K\}$

THE GALOIS GROUP An important special case is when $\Omega = L$, and L is a finite extension of K. Then $\mathrm{Emb}_K(L, L)$ is a group. Indeed the composition of two embeddings over K is an embedding and this gives $\mathrm{Emb}_K(L, L)$ a monoid structure. Since L is of finite dimension over K, every embedding over K is invertible, So $\mathrm{Emb}_K(L, L)$ is a group. This group is the famous *Galois group* of L over K. We denote it by $\mathrm{Gal}(L/K)$.

In the more general case when L not necessarily is a finite extension, $\mathrm{Emb}_K(L, L)$ is not always a group, but the subset of invertible embeddings is a group. And in this case, this is the Galois group.

PROBLEM 1. Let $n \geq 2$ be an integer and p a prime (for simplicity). Show that $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}) = 1$ if n is odd and $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{p})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ if n is even. ✸

PROBLEM 2. Let K be any field and let $a \in K$ be an element. Let $n \geq 2$ be an integer and let $f(x) = x^n - a$ and $L = E_f$ the stem field. When is $f(x)$ irreducible? What are the possible Galois groups $\mathrm{Gal}(L/K)$? ✸

PROBLEM 3. The set up is the standard one: Two extensions $K \subseteq L$ and $K \subseteq \Omega$. Show that the two Galois groups $\mathrm{Gal}(K/L)$ and $\mathrm{Gal}(\Omega/K)$ both act on $\mathrm{Emb}_K(L, \Omega)$, respectively from the left and from the right. ✸

The stem field

In this paragraph $f(x) \in K[x]$ will be an *irreducible* polynomial whose degree we denote by n. The polynomial being irreducible the quotient ring $E_f = K[x](f(x))$ is a field, and we call it the *stem field* of f. It is an extension of K. The residue class of x, say α, is by definition a root of $f(x)$ in E_f. So E_f comes equipped with a *preferred root* of $f(x)$.

The degree of E_f over K equals the degree n of f, and the powers $1, x, \dots, x^{n-1}$ form a K-basis for E_f.

If $K \subseteq \Omega$ is a field extension, any root ω that $f(x)$ might have in Ω, gives rise to an embedding of E_f in Ω. Indeed, sending x to ω induces a homomorphism $K[x] \to \Omega$ which factors through $E_f = K[x]/(f(x))$ since it maps $f(x)$ to $f(\omega) = 0$. Hence we get a map $E_f \to \Omega$, which automatically is an embedding over K. Conversely, if $\tau\colon E_f \to \Omega$ is an embedding, the image of $\tau(\alpha)$ under τ is a root of f in Ω. Altogether, there is a (canonical) identification:

□ $\mathrm{Emb}_K(E_f, \Omega) \simeq \{$ roots of f in Ω $\}$.

In case K is not contained in Ω, but there is given an embedding $\sigma\colon K \to \Omega$, there is a similar identification. If $f(x) = \sum_i a_i x^i$, we let $f_\sigma = \sum_i \sigma(a_i) x^i$, which is a polynomial with coefficients in $\sigma(K)$. We then have:

□ $\mathrm{Emb}_\sigma(E_f, \omega) \simeq \{$ roots of f_σ in Ω $\}$.

If $\omega \in L$ is a root of $f(x)$, then the corresponding embedding gives an isomorphism $E_f \simeq L(\omega)$ which is an isomorphism over K, in the sense that it is K-linear. Hence if ω and ω' are two roots of f in L, the two extension fields $K(\omega)$ and $K(\omega')$ are isomorphic over K. The isomorphism sends a polynomial expression $p(\omega)$ to the polynomial expression $p(\omega')$.

EXAMPLE 1. A basic example is $K = \mathbb{R}$ and $f(x) = x^2 + 1$. Then one has $\mathbb{C} = E_f$ (this might be taken as a definition!). The residue class of x is normally denoted by i, and of course $i^2 = -1$. The polynomial $x^2 + 1$ has another root in E_f, namely $-i$. This shows that f might have several roots in E_f, but one of them, the residue class of x, is singled out as *the* root. ❄

PROBLEM 4. Let p be a prime and let $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = (x^p - 1)/(x - 1)$. This is called the p-th *cyclotomic polynomial*.

a) Show that Φ_p is irreducible HINT: Apply Eisenstein's criterion to a twist of $\Phi_p(x)$.

b) Show that $\Phi_p(x)$ has p roots in the stem field E_f.

c) Show by an example, that Φ_n is not irreducible if n is not prime.

✸

PROBLEM 5. The setup is as in the previous exercise. Assume $p > 2$. Check that α^2 is a root of $\Phi_p(x)$, and let ϕ be the corresponding isomorphism of E_f to E_f sending α

to α^2. What is the matrix of ϕ in the basis formed by the powers $1, \ldots, x^{p-1}$? Do the same with α^2 replaced by α^q. ✸

EXISTENCE OF SPLITTING FIELDS We draw some easy consequences. It is interesting to note that what today is merely an observation once was a serious issue in mathematics involving the most prominent mathematicians at that time. In fact in proving that $\mathbb{C}$ is algebraically closed, Lagrange used that any polynomial has a root somewhere, but he was very vague about where somewhere was, and Gauss criticizes this severely—he did not like mysterious roots in the cloud. Anyhow, we have:

Proposition 1 *Given a field K and a polynomial $f(t) \in K[t]$. There exists a field extension $K \subseteq E$ in which f has a root.*

A slightly more complicated statement is the following. Recall that *a splitting field* for a polynomial $f(t) \in K[t]$ is field extension E of K over which f splits as a product of linear factors, and such that E is generated over K by the roots of f.

Proposition 2 *Every polynomial $f(t) \in K[t]$ has a splitting field E. If $n = \deg f(t)$, then $[E : K] < n!$*

PROOF: Induction on $\deg f$. Let F be a field where f has the root α, and let $g(t) = f(t)/(t-\alpha)$. Then a splitting field for $g(t)$ over $K(\alpha) \subseteq F$ is a splitting for $f(t)$. Furthermore $\deg g = n-1$, and therefore we get by induction that $[E : K] = [E : K(\alpha)][K(\alpha) : K] \leq (n-1)!n = n!$ ❏

EMBEDDINGS OF THE STEM FIELD The number of roots of f is bounded by the degree n of f, and f has n *distinct* roots in Ω if and only if f splits a product of n distinct linear factors in $\Omega[x]$. In that case we say that f *splits simply* in Ω. The following proposition, which finally is merely an observation, is one of the pillars of the foundational Galois theory. Combined with an induction procedure, involving towers of fields, it leads more or less directly to half of the fundamental theorem of Galois theory, the other half hinging on a result similar to Artin's theorem on characters.

Proposition 3 *Assume $\sigma \colon K \to \Omega$ is an embedding. Then*

- *The number of embeddings of E_f in Ω extending σ is bounded by $\deg f$. That is*

$$\#\mathrm{Emb}_\sigma(E_f, \Omega) \leq [E_f : K]$$

- *Equality holds if and only if f_σ splits simply in Ω.*

Climbing towers

The property of the stem field described in the previous proposition generalizes to any field extension. The technic of proof is, as indicated above, induction on the degree $[L : K]$ applied to intermediate fields $K \subseteq E \subseteq L$—that is three-story towers—combined with the stem field case.

Proposition 4 *Given en embedding $\sigma\colon K \to \Omega$. Assume that $K \subseteq L$ is a finite field extension. Then the number of extensions of σ to L is bounded by the degree $[L : K]$, that is:*

$$\#\mathrm{Emb}_\sigma(L, \Omega) \leq [L : K]$$

PROOF: Induction on $[L : K]$. The proposition is true for stem fields. Let $x \in L$ and $x \notin K$. The embedding σ can by the stem field case be extended to $K(x)$ in at most $[K(x) : K]$ ways, and each of these extensions can by induction be further extended in at most $[L : K(x)]$ ways. Hence the proposition, since $[L : K(x)][K(x) : K] = [L : K]$. ❑

The "moral" content of this argument is that the two sides of the inequality both to a certain extent behave multiplicatively with respect to towers of field. That is, the right side is multiplicative in towers, but the left side is only submultiplicative. Hence to get conditions on L that guaranteed equality, we need conditions that make the number of embeddings behave well. And it turns out, as the second statement about the stem fields indicates, that the good condition is that any polynomial in $K[t]$ having a root in L splits simply in Ω. We have

Proposition 5 *Let $\sigma\colon K \to \Omega$ be an embedding and $K \subseteq L$ a field extensions. Then the two following conditions are equivalent:*

① $\#\mathrm{Emb}_\sigma(L, \Omega) = [L : K]$

② *Every polynomial $f(t) \in K[t]$ having a root in Ω splits simply in Ω*

PROOF: Assuming the condition 2, we use induction on $[L : K]$ to prove 1. We start by proving a lemma:

Lemma 1 *Let E be an intermediate field between K and L. Assume that the extension $K \subseteq L$ over K satisfies condition 2. Then the extension $E \subseteq L$ satisfies condition 2 as well.*

Indeed, pick an element $x \in L$ and let f_K and f_E be the minimal polynomials of x over respectively K and E. Then f_E is a factor in f_K. Indeed, $f_K \in E[t]$ and $f_K(x) = 0$. Therefore f_E has only simple roots since f_K only has simple roots, and it splits in linear factors in Ω as f_K does. This proves the lemma.

By induction it follows that, at least if $E \subsetneq L$, any embedding of E in Ω extends in exactly $[L : E]$ ways to L.

If now $E = K(x)$ for some $x \in L$, the minimal polynomial f_K splits simply in Ω, and hence by the stem field case, any embedding of K in ω extends to $K(x)$ in exactly $[K(x) : K]$ ways. This gives all together $[L : E][K(x) : K] = [L : K]$ extensions of σ to L, and we are through.

The other way around: If condition 2 does not hold, there is by the stem field case an element $x \in L$ with $\#\mathrm{Emb}_\sigma(K(x), \Omega) < [K(x) : K]$, and since each of these can be extended to L in at most $[L : K(x)]$ ways, it follows that $\#\mathrm{Emb}_\sigma(L, \Omega) < [L : K(x)][K(x) : K] = [L : K]$ ❑

PROBLEM 6. Use induction on $[L : K]$ combined with the stem field case, to show that any embedding of K into an *algebraically closed* field Ω can be extended along any finite extension $K \subseteq L$. Use Zorns's lemma to show that the result still holds true when L is merely algebraic over K (*i.e.,* not necessarily finite, but all elements algebraic over K). ✸

SPLITTING FIELDS Recall that if $f(x) \in K[x]$ is a polynomial, a *splitting field* for f over K is a field extension L of K with the following two properties. Firstly, f should split as a product of linear factors in L, that is, all its roots should be in L. Secondly, the field L should be generated over K by the roots of f. The splitting fields play a very special role in the theory of equations, and the following is a central result:

Proposition 6 *Assume that $f(x) \in K[x]$ is a polynomial and that L is a splitting field for f. If the roots of f are all distinct, then for any embedding σ of K in L, one has $\#\mathrm{Emb}_\sigma(L, L) = [L : K]$. In particular $\#\,\mathrm{Gal}(L/K) = [L : K]$.*

PROOF: We use induction on $[L : K]$ and apply a variant of the tower-climbing technic. Let α be one of the roots of f not in K, and let $E = K(\alpha)$. Then L is also a splitting field for f viewed as poly in $E[x]$. Now $E \neq K$, so $[L : E] < [L : K]$, and by induction

$$\#\mathrm{Emb}_\tau(L, L) = [L : E]$$

for any embedding τ of E in L. The minimal polynomial of α over K is a factor in f, hence splits completely in L as L is a splitting field for f, and its roots are distinct, since those of f are. From proposition 3 on page 3 it follows that for any embedding σ of K in L it holds true that

$$\#\mathrm{Emb}_\sigma(E, L) = [E : K].$$

The proposition then follows by multiplicativity in towers. ❑

EXAMPLE 2. The splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\xi, \sqrt[3]{2})$ where ξ is a primitive third root of unity. Indeed, the three roots $\sqrt[3]{2}$, $\xi\sqrt[3]{2}$ and $\bar{\xi}\sqrt[3]{2}$ all lie in $\mathbb{Q}(\xi, \sqrt[3]{2})$, and since $\xi = \xi\sqrt[3]{2}/\sqrt[3]{2}$, L is generated by the roots. ❄

PROBLEM 7. Show that the splitting field of $f(x) \in K[x]$ is unique up to isomorphism over K. ✸

PROBLEM 8. Let p be a prime and let ξ be a primitive p-th root of unity. Let $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. Show that the splitting field of f is equal to $\mathbb{Q}(\xi)$. ✸

PROBLEM 9. Let a and b be to different members of the field K neither being a square. Show that $L = K(\sqrt{a}, \sqrt{b})$ is the splitting field of $f(x) = x^4 - (a+b)x^2 + (a-b)^2$. What is thew Galois group $\mathrm{Gal}(E/K)$ and how does it act on L? Fields like $K(\sqrt{a}, \sqrt{b})$ are classically called *biquadratic fields*. ✸

PROBLEM 10. Let a be a rational number. Determine the splitting field of $x^4 - a$. ✸

GALOIS FIELDS The condition 2 is naturally split in two. The extension L is *separable* if the minimal polynomial of any $x \in L$ over K only has simple roots. And on may say that L is *normal towards* Ω if any polynomial in $K[t]$ having a root in K factors in a product of linear factors over Ω, or so to say, has all its roots in Ω. If $\Omega = L$, this last condition is what is called *normal*. Field extensions $K \subseteq L$ satisfying the condition 2 above with $\Omega = L$ are called *Galois fields*.

Recalling that $\mathrm{Emb}_K(L, L)$ is the Galois group $\mathrm{Gal}(L/L)$, we have

Proposition 7 *Let $K \subseteq L$ be a field extension. Then the order of the Galois group $\mathrm{Gal}(L/K)$ is equal to $[L : K]$ if and only if the extension is separable and normal.*

One has

Proposition 8 *The field extension $K \subseteq L$ is Galois if and only if L is the splitting field over K of some polynomial,*

PROOF: Any splitting field is Galois by proposition 6 on page 5. Assume that L is Galois over K. Take the minimal polynomial f of any element α in L. Since L is normal and separable, the roots $\alpha_1, \ldots, \alpha_s$ of f are all in L. Let $E = K(\alpha_1, \ldots, \alpha_s)$. Then L is Galois over E by lemma 1 and is by induction the splitting field of some g. Then L is the splitting field of fg. ❑

To a subgroup $H \subseteq \mathrm{Gal}(L/K)$ one associates the *fixed field* L^H of L consisting of elements untouched by any element in Galois group. That is

$$L^H = \{\, x \in L \mid \sigma(x) = x \text{ for all } \sigma \in \mathrm{Gal}(L/K) \,\}.$$

This is clearly a field, the σ's being ring homomorphisms.

Theorem 1 *Let G be a group of automorphisms of the field L and let $K = L^G$. Then $[L : K] \leq |G|$*

A theorem of Artin on automorphisms of fields.

Let L be a field and let G be a finite group of automorphism of L. The *fixed field* of G is the subfield

$$L^G = \{\, x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G \,\}.$$

The following theorem is closely related to Artin's result on characters, although it goes in a different direction.

Theorem 2 *The degree of L over the fixed field L^G is bounded by the order of G. That is $[L : L^G] \leq |G|$*

PROOF: Assume that $a_1, \ldots, \alpha_m$ are elements in L and that $m > |G|$. We have to show that they are linearly dependent over K. Now, as $m > |G|$, there is a non-trivial solution $(\xi_1, \ldots, \xi_m)$ in L of the system of equations where σ_i's are the elements in G

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_m)x_m &= 0 \\ &\cdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha_m)x_m &= 0, \end{aligned}$$

indeed, the number of equations being less than the number of unknowns.

Since $1 \in G$ is among the σ's, any solution $\xi = (\xi_1, \ldots, \xi_m)$ of the system gives the linear relation

$$\alpha_1\xi_1 + \cdots + \alpha_m\xi_m = 0$$

where the ξ_i's are in L. Our task is to find one solution with ξ_i's all in L^G.

The set of solutions of the system is invariant under the action of G. Applying any $\sigma \in G$ to the equations, and using that $\sigma\tau$ runs through G when σ does, we see that if $\xi = (\xi_1, \ldots, \xi_m)$ is any solution, $\sigma(\xi) = (\sigma(\xi_1), \ldots, \sigma(\xi_m))$ is also a solution.

Now, we pick a solution with the greatest number of ξ_i's different from zero. By renumbering and scaling we may assume that $\xi_1 \in K$. Assume that $\xi_k \notin L^G$, that is for one of the elements $\sigma \in G$ we have $\sigma(\xi_k) \neq \xi_k$. Then $\xi - \sigma(\xi) = (\xi - \sigma(\xi_1), \ldots, \xi_k - \sigma(\xi_k), \ldots) = (0, \ldots, \xi_k - \sigma(\xi_k), \ldots)$ is a non-trivial solution with fewer non-zero coordinates than ξ. Contradiction. ❏

Combining with xxx we get

Theorem 3 *Let G be a finite group acting on the field L. Then the extension L of L^G is Galois and $[L : L^G] = |G|$*

The following theorem, which on may call the first Main theorem in Galois Theorem follows from this combined with xxx.

Theorem 4 (The first main theorem) *Let $K \subseteq L$ be an extension. Then the following are equivalent*

- ☐ *K is the fixed field of the Galois group, that is $K = L^{\mathrm{Gal}(L/K)}$*
- ☐ *The order of the Galois group equals the degree, that is $|\mathrm{Gal}(L/K)| = [L : K]$*
- ☐ *The extension $K \subseteq L$ is separable and normal.*

The second main theorem of Galois theory

Of the more acclaimed theorems in algebra is the fundamental theorems of Galois theory. Their history is long and glorious going back to Galois, with its dramatic twists and non-mathematical ingredient: love stories, duels and early death. It is an very important and deep theorem, and touches the groundwater of mathematics. It illustrates very well the deep analogy between algebra and geometry uncovered by formalization and abstraction. The classification of covering spaces of a topological spaces by subgroups of the fundamental group, is strikingly similar—and indeed the two theorems are just different faces of the same principle.

The setting of The fundamental theorem is Galois extension $K \subseteq L$. It states that there is a one-one-correspondence between on the one hand subgroups of the Galois group $\mathrm{Gal}(L/K)$ and on the other hand intermediate fields E lying between K and L, that is a three-story tower $K \subseteq E \subseteq L$.

Given a subgroup $H \subseteq G$, the associated intermediate field is *the fixed field* of H. That is

$$L^H = \{\, x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H \,\}.$$

Given an intermediate field E, the corresponding subgroup of the Galois group is the Galois-group $\mathrm{Gal}(L/E)$ which obviously is contained in $\mathrm{Gal}(L/k)$. It consists of the elements of $\mathrm{Gal}(L/K)$ not moving any member of E, i n formula-lingo:

$$\mathrm{Gal}(L/E) = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = x \text{ for all } x \in E \,\}$$

Clearly, by definition, there are inclusions

$$E \subseteq L^{\mathrm{Gal}(L/E)}$$
$$H \subseteq \mathrm{Gal}(L/L^H)$$

and the content of the Fundamental Theorem is that these two inclusions are equalities:

Theorem 5 *Let $K \subseteq L$ be a Galois extension (i.e., separable and normal) then*

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

Thus the assignment $H \mapsto L^H$ and $E \mapsto \mathrm{Gal}(L/E)$ set up mutually inverse maps that one may depict as follows:

$$\{\text{ Subgroups of } \mathrm{Gal}(L/K) \} \longleftrightarrow \{\text{ Intermediate fields } E, \textit{ i.e., } \text{towers } K \subseteq E \subseteq L \}$$

PROOF: We first attack the inclusion $E \subseteq L^{\mathrm{Gal}(L/)E}$. By lemma 1 on page 4, the extension $E \subseteq L$ is normal and separable, and hence by proposition 5 on page 4 we have $[L : E] = \mathrm{Gal}(L/)E$. On the other hand, Artin's theorem gives us $[L : L^{\mathrm{Gal}(L/E)}] = |\mathrm{Gal}(L/K)|$, and therefore $[L : L^{\mathrm{Gal}(L/E)}] = [L : E]$, and the two fields E and $L^{\mathrm{Gal}(L/E)}$ are equal.

Now, the second equality $H \subseteq \mathrm{Gal}(L/L^H)$ is just theorem 4. ❑

INCLUSIONS ARE REVERSED The correspondence in the main theorem has several nice properties, it reverses inclusions and preserves indices. If H and H' are two subgroups of $\mathrm{Gal}(L/K)$ the it holds true that

- $H \subseteq H'$ is and only if $L^{H'} \subseteq L^H$.
- $[H' : H] = [L^H : L^{H'}]$.

CONJUGATE SUBGROUPS AND NORMAL SUBGROUPS Let $\sigma \in \mathrm{Gal}(L/K)$ be an element and let H be a subgroup. The conjugate subgroup $\sigma H \sigma^{-1}$ has as fixed field the image $\sigma(L^H)$ of the fixed field of H. Indeed, for any $\tau \in H$, if $\sigma\tau\sigma^{-1}(x) = x$, clearly $\tau\sigma^{-1}(x) = \sigma^{-1}(x)$. Hence

- $L^{\sigma H \sigma^{-1}} = \sigma L^H$

This observation leads the the following theorem, that we might consider as the third in the row of main theorems. It states that in the Galois correspondence normal subgroups correspond to sub fields normal and separable over K. Separability holds for every intermediate field, so the real content of this statement is that normal subgroups and normal field extensions correspond.

Theorem 6 *Assume that $K \subseteq L$ is a Galois extension and that $H \subseteq \mathrm{Gal}(L/K)$ is a subgroup. The fixed field L^H is Galois over K if and only if H is a normal subgroup. In that case the Galois group $\mathrm{Gal}(L^H/K)$ is naturally isomorphic to the quotient $\mathrm{Gal}(L/K)/H$.*

PROOF: Since $\mathrm{Gal}(L/L^{\sigma H \sigma^{-1}}) = \sigma H \sigma^{-1}$ and $\mathrm{Gal}(L/L^H) = H$ the subgroup H and its conjugate $\sigma H \sigma^{-1}$ are equal if (and only if) the corresponding fixed fields are. That is, if and only $\sigma(L^H) = L^H$. From this we conclude that H being a normal subgroup is equivalent to the fixed field L^H being invariant under the action of the *whole* Galois group $\mathrm{Gal}(L/K)$.

Assume that L^H is invariant. The subgroups H acts by definition trivially on L^H which implies that the quotient $\mathrm{Gal}(L/K)/H$ acts on L^H and since $\mathrm{Gal}(L/L^H) = H$, this action is faithful. It follows that $\mathrm{Gal}(L/K)/H$ is contained in $\mathrm{Gal}(L^H/K)$, but the two are of the same order, and therefore equal. Indeed

$$|\mathrm{Gal}(L^H/K)| \leq [L^H, K] = \frac{[L : K]}{[L : L^H]} = \frac{|\mathrm{Gal}(L/K)|}{|\mathrm{Gal}(L/L^H)|} = |\mathrm{Gal}(L/K)/H|.$$

This shows as well that L^H is galois over K, since $|\mathrm{Gal}(L^H/K)| = [L^H : L]$. ❏