Universität Regensburg

Infinite Galois Theory

Schneider Alexander

May 10, 2021

Contents

1 Classic Galois Theory

In this chapter we are going to review some basic Galois Theory, while omitting the proofs.

Definition 1.1
Let K be a field and L/K an extension of fields. We call $\alpha \in$L algebraic, if there exists a polynomial p(T)$\in$K[T], such that p(α)=0. Otherwise we say, that α is transcendental. We say that L/K is algebraic, if every $\alpha \in$L is algebraic.

Remark 1.2
For every $\alpha \in$L there exists a homomorphism ev: K[T]$\longrightarrow$L, p(T)$\longmapsto$p(α).
If α is algebraic, then there exists exactly one polynomial m(T)$\in$ker(ev), such that:

- ker(ev)=(m(T)) [=the ideal generated by m(T)]
- If n=deg(m(T)), then a_n, the coefficient of T^n in m(T), is 1
- m(T) has minimal degree, e.g. for every g(T)$\in$K[T]$\setminus$0 with deg(g(T))<deg(m(T)) $\Rightarrow$ g(α)$\neq$0.

We call m(T) the minimal polynomial of α.
We will denote the minimal polynomial of α over K by $\text{Mipo}_K(\alpha)$.

Definition 1.3
A field K is algebraically closed, if every non-constant polynomial p(T)$\in$K[T] has a zero in K.
An algebraic closure of a field L is an algebraic extension $\overline{L}$, which is algebraically closed.

Proposition 1.4
Let K be a field.

1. An algebraic closure $\overline{K}$ of K exists, and it is unique up to isomorphism.
2. For any algebraic extension L of K there exists an K-algebrahomomorphism ϕ:L$\longrightarrow\overline{K}$
3. Taking an algebraic closure $\overline{L}$ of L, the embedding ϕ from 2) yields an Isomorphism from $\overline{L}$ to $\overline{K}$:

$$\begin{array}{ccc} L & \xrightarrow{\phi} & \bar{K} \\ & \searrow & \uparrow \simeq \\ & & \bar{L} \end{array}$$

Remarks 1.5

- Any finite extension L/K is algebraic
- We call [L:K] = $\dim_K$(L) the degree of the extension L/K.
- If L=k(α) for some $\alpha \in$L, then [L:K]=deg($\text{Mipo}_K(\alpha)$)
- For a nested extension M/L/K we find the formula: [M:K]=[M:L]$\cdot$[L:K]

Definition 1.6
A polynomial $f \in K[T]$ is called separable, if all roots of f over some algebraic closure $\overline{K}$ have multiplicity 1.
An element $\alpha \in L$ of an algebraic extension L/K is called separable, if $\mathrm{Mipo}_K(\alpha)$ is separable.
We say that the extension L/K is separable, if every element of L is separable over K.

Remark 1.7
If F is a field with characteristic 0, then every extension T/F is separable.

Proposition 1.8
Let L/M/K be a nested field-extension, with every single extension being finite, then the extension L/K is separable if and only if L/M and M/K are.

Remark 1.9
Let K be a field, consider an algebraic closure $\overline{K}$. In general the extension $\overline{K}$/K will not be separable. Hence we can consider the set of all separable elements $K_s \subset \overline{K}$. Equivalently K_s is the compositum of all finite separable subextensions of $\overline{K}$ [=The smallest field, which contains all finite separable ...]. Thus K_s again forms a field, the so called separable closure of K.
We call a field perfect, if every finite extension is separable. In this case the algebraic closure and the separable closure are the same.

Definition 1.10
An algebraic field extension L/K is called normal, if every over K irreducible polynomial has no root in L or splits into linear factors in L.
We call L/K Galois, if it is normal and separable.

Remark 1.11
Let L/K be a finite field extension, let $\mathrm{Aut}(L/K)=\mathrm{Hom}_K(L,L)$, then the following are equivalent:

1. L/K is Galois
2. $|\mathrm{Aut}(L/K)|=[L:K]$

Definition 1.12
We call Gal(L/K)=Aut(L/K) the Galois group of the finite extension L/K, with group operation composition of maps.

Remark 1.13

1. A separable closure K_s of a field K is always a Galois extension.
   We call $\mathrm{Gal}(K_s/K)$ the absolute Galois group of K.
2. A finite separable extension can be generated by a single element.

Proposition 1.14
Let K be a field, K_s a separable closure and $K \subset L \subset K_s$ be a subfield, then the follwoing statements are equivalent:

1. L/K is a Galois-extension

2. for all $\alpha \in$L:Mipo$_K(\alpha)$ splits into linear factors in L.

3. for all $\sigma \in$Gal(K$_s$/K) we have: σ(L)$\subset$L

Definition 1.15
Let L be a field, and G$\subset$Aut(L). The subfield L^G={a$\in$L | σ(a)=a for all $\sigma \in$G} is called the fixed field over G.

Remarks 1.16

- Let L be a field and G$\subset$Aut(L) a finite subset. Let K=L^G, then the extension L/K is Galois, [L:K]=|G| and G=Gal(L/K).

- Let L/K be a finite Galois-extension with Galoisgroup G=Gal(L/K), then L^G=K.

Theorem 1.17 (Main Theorem of Galois theory for finite extensions)
Let L/K be a finite Galois-extension with Galoisgroup G=Gal(L/K), then there exist two Isomorphisms ϕ and ψ, who are inverse to each other:

$$\{Subgroups\ of\ G\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{Subfields\ of\ L/K\}$$

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

Remark 1.18
A subgroup H$\subset$G is normal if and only if the field extension L^H/K is normal.
In this case we get an isomorphism of groups:

$$G/H \xrightarrow{\simeq} Gal(L^H/K)$$
$$\overline{\sigma} \longmapsto \sigma\ |_{L^H}$$

2 infinite Galois Theory

For this section let L/K be a possibly infinite Galois extension.

Lemma 2.1
Each finite subextension of L/K can be embedded in a Galois subextension.
proof:
Each finite Subextension has the form k(α) for some $\alpha \in$ L (by *Remark 1.13.2*). We now embed k(α) into the splitting field of Mipo$_K(\alpha)$, which is a Galois extension of k. ■

This means, that L is the union of finite Galois extensions of K, since for every $\alpha \in$ L we have the finite subextension k(α).

Definition 2.2
A filtered inverse system of groups (G$_\alpha$;$\phi_{\alpha,\beta}$) with index set Λ consits of:

- a partially ordered set (Λ, $\leq$), such that for all (α,β)$\in \Lambda^2$ there is a $\gamma \in \Lambda$, such that $\alpha \leq \gamma \wedge \beta \leq \gamma$
- for every $\alpha \in \Lambda$ we have a group G$_\alpha$
- for each $\alpha \leq \beta$ we have a homomorphism of groups $\phi_{\alpha,\beta}$: G$_\beta \rightarrow$ G$_\alpha$, such that for $\alpha \leq \beta \leq \gamma$ we get $\phi_{\alpha,\gamma} = \phi_{\alpha,\beta} \circ \phi_{\beta,\gamma}$

The inverse limit of (G$_\alpha$;$\phi_{\alpha,\beta}$), which we will denote by lim$_\leftarrow$ G$_\alpha$, is defined as the subgroup of the direct product $\prod_{\alpha\in\Lambda} G_\alpha$ consisting of sequences (g$_\alpha$) satisfying $\phi_{\alpha,\beta}(g_\beta) = g_\alpha$ for all $\alpha \leq \beta$.

Definition 2.3
A profinite group is an inverse limit of a system of finite groups.

Proposition 2.4
Gal(L/K) is a profinite group.
proof:
Let $\Lambda = \{Fields\ M \mid K \subset M \subset L\ is\ a\ finite\ Galois\ extension\ \}$

- partially ordered by $M \leq N := M \subset N$
- directed: for every M,N$\in \Lambda$ we have the compositum of M and N
- for all M $\in \Lambda$ we have the group G$_M$=Gal(M/K)
- If M$\subset$N we get the surjection $\phi_{M,N} : Gal(N/K) \longrightarrow Gal(M/K), \sigma \longmapsto \sigma \mid_M$
- finally if $\alpha \leq \beta \leq \gamma \in \Lambda$, we obviously obtain $\phi_{\alpha,\gamma} = \phi_{\alpha,\beta} \circ \phi_{\beta,\gamma}$, since these maps are all restrictions.

<u>claim:</u> $Gal(L/K) \simeq$ lim$_\leftarrow$ G$_\alpha$
Let $\Psi : Gal(L/K) \longrightarrow \prod_{M\in\Lambda} Gal(M/K)$, defined by sending an automorphism σ to the product of the restrictions $\sigma \mid_M$ for $M \in \Lambda$.
Remark:
This is well-defined, because for $L \in \Lambda$ we have $\sigma(L) \subset L$

- Ψ is injective:
  Let $\tau \in ker(\Psi)$, which means $\Psi(\tau) = (Id, Id, Id, ...)$. Let $\alpha \in L$, we then obtain $K \subset K(\alpha) \subset P \subset L$, where P is the finite Galois subextension from lemma 2.1. We know that $\tau(\alpha) = \alpha$, because $\tau \mid_P = id_P$, and $\alpha \in P$. Since α was arbitrary, we obtain $\tau = id_L$.
  $\Rightarrow$ injectivity

- $Im(\Psi) = \lim_{\leftarrow}$ G_α:
  $Im(\Psi) \subset \lim_{\leftarrow}$ G_α, because take $\sigma \in$Gal(L/K), let $\alpha \leq \beta$ be arbitrary. We thus get the map $\phi_{\alpha,\beta} : Gal(\beta, k) \longrightarrow Gal(\alpha, k)$ and $\phi_{\alpha,\beta}(\sigma \mid_\beta) = (\sigma \mid_\beta) \mid_\alpha = \sigma \mid_\alpha$. And thus per definition of the inverse limit we get the desired subset relation.
  If $(\sigma \mid_\beta)_{L\in\Lambda} \in \lim_{\leftarrow}$ G_α, then define a k-automorphism σ by $\sigma(\alpha) = \sigma_P(\alpha)$ for some finite Galois subextension P containing $K(\alpha)$. This is well-defined, because if H is another one, we can view the compositum of P and H, let´s name it C, by definition we have: $(\sigma_C) \mid_P = \phi_{P,C}(\sigma_C) = \sigma_P$ and $(\sigma_C) \mid_H = \phi_{H,C}(\sigma_C) = \sigma_H$, thus: $\sigma_P(\alpha) = \sigma_H(\alpha)$. By construction we have: $\Psi(\sigma) = (\sigma_L)_{L\in\Lambda}$ ■

Remark 2.5
Profinite groups have a natural topology:
Let G be the inverse limit of a system of finite froups (G_α;$\phi_{\alpha,\beta}$). For every $\alpha \in \Lambda$ let G_α have the discrete topology, then we can use the product topology on $\prod_{\alpha\in\Lambda} G_\alpha$. Finally we endow $G \subset \prod_{\alpha\in\Lambda} G_\alpha$ with the subspace topology. Observe that with this topology the natural projections $G \longrightarrow G_\alpha$ are continuous.

Lemma 2.6
Let (G_α,$\phi_{\alpha,\beta}$) be an inverse system of groups equipped with the discrete topology, then the inverse limit $\lim_{\leftarrow}$ G_α is a closed topological subgroup of the product $\prod_{\alpha\in\Lambda} G_\alpha$.
proof:
Let g=(g_α)$\in \prod_{\alpha\in\Lambda} G_\alpha$ $\lim_{\leftarrow} G_\alpha$. We need to find an open neighbourhood of g, which does not intersect with $\lim_{\leftarrow} G_\alpha$. By assumption there exist α, β such that $\phi_{\alpha,\beta}(g_\beta) \neq g_\alpha$. Let $H = \{(p) \in \prod_{\alpha\in\Lambda} G_\alpha \mid p_\alpha = g_\alpha \wedge p_\beta = g_\beta\} \subset \prod_{\alpha\in\Lambda} G_\alpha$. Let $pr_\alpha : \prod_{\alpha\in\Lambda} G_\alpha \longrightarrow G_\alpha$ be the natural projection for every $\alpha \in \Lambda$, we then have: $H = (pr_\alpha)^{-1}(g_\alpha) \cap (pr_\beta)^{-1}(g_\beta)$. Since every G_α has the discrete topology, the sets $\{g_\alpha\}$ and $\{g_\beta\}$ are open, and from Remark 2.5 we know that the natural projections are continuous. Thus H is an open subset, such that $g \in H \wedge H \cap \lim_{\leftarrow} G_\alpha = \varnothing$. ■

Corollary 2.7
A profinite group is compact and totally disconnected (the only connected subsets are one-element subsets). Moreover: the open subgroups are precisely the closed subgroups of finite index.
proof:
By *Tychonoff´s Theorem* we have:
The product of any collection of compact topological spaces is compact with respect to the product topology.
Since finite discrete groups are compact, we get that $\prod_{\alpha\in\Lambda} G_\alpha$ is compact. Hence $\lim_{\leftarrow} G_\alpha$ is compact by *Lemma 2.6*
Observe that each open subgroup U is closed, since its complement is a disjoint union of sets of the form gU with $g \in \lim_{\leftarrow} G_\alpha$ U and the gU are open, because $U \longrightarrow gU$ is a

homeomorphism. By compactness of $\lim_{\leftarrow} G_\alpha$ there is only a finite number of the gU, and thus it has finite index.
If U is now a closed subgroup of finite index, then U is open, because it is the complement of the finite disjoint union of the gU´s, which are closed subsets. ∎

Krull´s Theorem
Let M be a subextension of the Galois extension L/K, then Gal(L/M) is a closed subgroup of Gal(L/K). Moreover the maps $M \longmapsto H := Gal(L/M)$ and $H \longmapsto M := L^H$ yield an inclusion-reversing bijection between subfields $k \subset M \subset L$ and closed subgroups $H \subset G$.
A subextension M/K is Galois over K if and only if Gal(L/M) is normal in Gal(L/K). In this case there is a natural isomorphism $Gal(M/K) \simeq Gal(L/K)/_{Gal(L/M)}$
proof:
Let $K \subset P \subset L$ be a finite, separable extension. We get a finite Galois extension R: $K \subset P \subset R \subset L$.
Then Gal(R/K) is a finite quotient of Gal(L/K), which contains Gal(R/P) as a subgroup.
Let $\pi : Gal(L/K) \longrightarrow Gal(R/K)$ be the projection, and let $U_L = \pi^{-1}(Gal(R/P))$. U_L is an open subset, because π is continuous and Gal(R/K) is endowed with the discrete topology.
We have $U_L \subset Gal(L/P)$, because each $\phi \in U_L$ fixes the field P. Moreover we have $\pi(Gal(L/P) \subset Gal(R/P)$, thus $U_L = Gal(L/P)$.
Now let $K \subset M \subset L$ be an arbitrary subextension. We can write M an a union of finite galois subextensions L_α K. We get that each Gal(L/L_α) is an open subgroup of Gal(L/K) and by *Corollary 2.7* they are also closed. Since M is the union of the L_α´s, the intersection of the Galois groups Gal(L/L_α) is exactly Gal(L/M). Hence Gal(L/M) is a closed subgroup of Gal(L/K).
Recall:
If $U \subset V \subset W$ are field extensions, then: W/U is Galois ⇒ W/V is Galois.
Thus L/M is a Galois extension, and hence the fixed field $L^{Gal(L/M)}$ is precisely M.
Now let $H \subset Gal(L/K)$ be a closed subgroup. We get a subextension $K \subset M \subset L$ and thus $H \subset Gal(L/M)$. Let $\sigma \in Gal(L/M)$, pick an open neighbourhood U_P of the identity, which corresponds to a Galois extension P/M. Looking at $\pi\mid_H$: $Gal(L/M) \supset H \longrightarrow Gal(P/M)$ we find that it is surjective, because otherwise the image would induce a field $M \subset F \subset P$, with $M \neq F$ by the main Theorem of finite Galois theory. However this contradicts our assumption, that every element of P\M is moved by some automorphism in H.
Especially we must have elements in H, which map to $\pi(\sigma)$. Thus H must contain an element of σU_P and since we chose U_P arbitrary, we obtain that σ must be in the closure of H in Gal(L/M). Since H is closed, we have: $H = \overline{H} \Rightarrow \sigma \in H$.
The other statements are proved similar to the finite case. ∎