Infinite Galois theory

H.W. Lenstra, 8-2-2006, notes by Arjen Stolk

We begin with a brief review of finite Galois theory.

A field extension $K \subset L$ is called finite if $\dim_K L$ is finite. This number is called the degree of the field extension.

Algebraic extensions

An element α of L is called algebraic over K if the K-algebra morphism $K[X] \longrightarrow L$ sending X to α is not injective. The unique monic generator of the kernel is called the minimal polynomial of α over K and is denoted f_K^α. Note that it is irreducible since the kernel is a prime ideal. If the K-algebra map is injective then we call α transcendental.

We call the extension L/K algebraic if and only if every element of L is algebraic over K. Note that all finite extensions are automatically algebraic, as $K[X]$ has infinite dimension over K (and thus doesn't fit inside a finite dimensional vector space over K.)

To check whether an extension is algebraic, it suffices to look at a set of generators. That is, the extension L/K is algebraic if and only if there is a subset S of L such that $L = K(S)$ and every element of S is algebraic over K.

Also note that the subset of all elements of L that are algebraic over K is a subfield of L containing K. It is the intersection of L with an algebraic closure of K.

Separable extensions

Now let L/K be an algebraic extension. An element α of L is called separable if its minimal polynomial is separable, that is, the ideal $(f_K^\alpha, (f_K^\alpha)')$ is (1) in $K[X]$.

An algebraic extension L/K is called separable if and only if every element of L is separable over K. Again, it suffices to check this for a subset of generators. Also, the subset of all separable elements inside the subset of the algebraic elements in a field extension L/K is a subfield and it is the intersection of L with a separable closure of K.

An equivalent way of defining separable is as follows. Suppose that Ω is an algebraically closed field containing K. An element α of L is separable over K if and only if the set of K-algebra maps $K(\alpha) \longrightarrow \Omega$ has precisely $[K(\alpha) : K]$ elements.

Normal extensions

Again we let L/K be an algebraic extension. We call an element α normal in L/K if the minimal polynomial f_K^α splits into linear factors in $L[X]$.

Just as before we call the extension L/K normal if and only if every element of L is normal. It again suffices to check this for a set of generators. The subset of all normal elements inside the subset of all algebraic elements is again a subfield of any field extension.

An equivalent definition is the following. Let Ω be an algebraically closed field containing L. Then α in L is normal if and only if for all K-algebra maps $\sigma : K(\alpha) \longrightarrow \Omega$ we have $\sigma(\alpha) \in L$.

The main theorem of finite Galois theory

Definition. A field extension L/K is called finite Galois if there is a finite subgroup G of $\mathrm{Aut}(L)$ such that $K = L^G = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in G\}$.

Theorem. Let L/K be any field extension. Then the following are equivalent:

1. L is finite Galois over K;
2. $[L : K] < \infty$ and $\#\mathrm{Aut}_K(L) = [L : K]$;
3. L/K is finite (hence algebraic), separable and normal;
4. L is the splitting field of a separable monic polynomial f from $K[X]$, that is, f splits into linear factors in $L[X]$ and the roots of f generate L over K;
5. L/K is finite and the maps

$$\{E \text{ field} : L \supset E \supset K\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{H : H \text{ subgroup of } \mathrm{Aut}_K(L)\}$$

where $\phi(E) = \mathrm{Aut}_E(L)$ and $\psi(H) = L^H$, are eachothers inverse.

It is an interesting exercise to show that the requirement that L/K be finite may be omitted from the last statement.

Note that it follows from the theorem that the group G in the definition is equal to $\mathrm{Aut}_K(L)$.

The topology on the automorphisms

In order to describe the infinite variant of Galois theory, we must consider the topology on the automorphism groups. It is defined as follows. Let L be a field. For $\sigma \in \mathrm{Aut}(L)$ and F a finite subset of L we define $U(\sigma, F)$ to be the set

$$U(\sigma, F) = \left\{\tau \in \mathrm{Aut}(L) : \tau|_F = \sigma|_F\right\}.$$

We call a subset U of $\mathrm{Aut}(L)$ open if for every σ in U there is an F such that $U(\sigma, F)$ is contained in U.

We see at once that the empty set and $\mathrm{Aut}(L)$ are both open. The local nature of the definition implies at once that any union of opens is again open. For finite intersections it is enough to notice that $U(\sigma, F_1) \cap U(\sigma, F_2)$ is just $U(\sigma, F_1 \cup F_2)$. We conclude that the axioms for a topological space are indeed satisfied.

This construction of a topology is quite general. Let L and M be any two sets. We can put a topology on the set of maps from L to M by noting that it is equal to $\prod_{x \in L} M$. By putting the discrete topology on M we get a product topology on the set

of maps. This is the topology we have just described. Another way of characterising it is that it is the weakest topology in which all the projection maps are continuous. We have one projection map for every x in L and it sends a $\sigma : L \longrightarrow M$ to $\sigma(x)$.

This construction turns the group $\mathrm{Aut}(L)$ into a topological space. In fact, it even becomes a topological group. This means that the group operations are continuous. This follows at once from the fact that $U(\sigma, \rho F) \circ U(\rho, F) \subset U(\sigma\rho, F)$ and $U(\sigma, F)^{-1} = U(\sigma^{-1}, \sigma F)$.

Note also that the topological space $\mathrm{Aut}(L)$ is a Hausdorff space. Suppose σ and τ are two distinct elements in $\mathrm{Aut}(L)$. Then there is some x in L such that $\sigma(x) \neq \tau(x)$. It is now at once clear that $\sigma \in U(\sigma, \{x\})$ and $\tau \in U(\tau, \{x\})$ and that $U(\sigma, \{x\}) \cap U(\tau, \{x\})$ is empty.

If S is any subset of $\mathrm{Aut}(L)$ then its closure is seen to be equal to

$$\overline{S} = \left\{ \sigma \in \mathrm{Aut}(L) : \text{for each } F \subset L \text{ finite there is a } \tau \in S \text{ such that } \tau|_F = \sigma|_S \right\}.$$

For example, suppose K is a subfield of L. Then $\mathrm{Aut}_K(L)$ is a closed subgroup. Suppose $\sigma \in \overline{\mathrm{Aut}_K(L)}$. Let x be any element of K. From the characterisation of the closure we see that there is a τ in $\mathrm{Aut}_K(L)$ such that $\sigma(x) = \tau(x) = x$. We conclude that σ is the identity on K, so that $\sigma \in \mathrm{Aut}_K(L)$.

The main theorem of infinite Galois theory

Definition. A field extension L/K is called Galois if there is a compact subgroup G of $\mathrm{Aut}(L)$ such that $K = L^G$.

Theorem. Let L/K be any field extension. Then the following are equivalent:

1. L/K is Galois;
2. L is the union of all its subfields E that are finite Galois over K;
3. L/K is algebraic, separable and normal;
4. L is the splitting field of a set $\mathcal{F}$ of monic separable polynomials from $K[X]$;
5. L/K is algebraic and the maps

$$\{E \text{ field} : L \supset E \supset K\} \underset{\psi}{\overset{\phi}{\rightleftarrows}} \{H : H \text{ closed subgroup of } \mathrm{Aut}_K(L)\}$$

where $\phi(E) = \mathrm{Aut}_E(L)$ and $\psi(H) = L^H$, are eachothers inverse.

As before the theorem implies that the subgroup G from the definition is $\mathrm{Aut}_K(L)$.

Proof of the main theorem. We first show that points 2, 3 and 4 are equivalent, then we tackle the equivalence with the other two.

$4 \Rightarrow 2$. Let $f \in \mathcal{F}$. Then L contains a splitting field of f. Call it E_f. This field is finite Galois by the main theorem in the finite case. Now note that L is the union

over all finite subsets $F \subset \mathcal{F}$ of the composite field of the E_f with $f \in F$. These fields are all finite Galois.

$2 \Rightarrow 3$. This follows at once from the finite case.

$3 \Rightarrow 4$. We can take $\mathcal{F} = \{f_K^\alpha : \alpha \in L\}$.

$1 \Rightarrow 3$. Let $\alpha \in L$. Then the map $G \longrightarrow L$ that sends $\sigma \in G$ to $\sigma(\alpha)$ is continuous if we give L the discrete topology. Since G is compact, its image under this map is also compact, and therefore it is finite. This image is just the orbit $G\alpha$. Now we put $f = \prod_{\beta \in G\alpha}(X - \beta)$. The coefficients of this polynomial are left invariant by any σ in G, so they are in fact in K. We conclude that α is algebraic over K. Moreover, since all roots of f are distinct and in L, we see that α is also separable and normal. This is what we wanted to show. Note that in fact $f = f_K^\alpha$, since for every $\sigma \in G$ we have $0 = \sigma(f_K^\alpha(\alpha)) = f_K^\alpha(\sigma(\alpha))$, so every β in $G\alpha$ must be a root of f_K^α.

$5 \Rightarrow 1$. From 5 we see that $K = L^{\mathrm{Aut}_K(L)}$, so all we have to show is that $\mathrm{Aut}_K(L)$ is compact. We have already seen that it is closed. Note that we have $\mathrm{Aut}_K(L) \subset L^L$ by sending σ to $(\sigma(\alpha))_{\alpha \in L}$. In fact, it lands inside a much smaller subgroup, since for every α in L the image $\sigma(\alpha)$ is a root of f_K^α. So we have an inclusion $\mathrm{Aut}_K(L) \subset \prod_{\alpha \in L}\{$ roots of f_K^α $\}$. The latter is compact by Tychonoff's theorem and therefore the former, being a closed subset of a compact set is also compact.

$2, 3 \Rightarrow 5$. First we prove that $\psi\phi = \mathrm{Id}$, that is for every intermediate field E we have $E = L^{\mathrm{Aut}_E(L)}$. It is clear that $E \subset L^{\mathrm{Aut}_E(L)}$. Now let $\alpha \in L$, $\alpha \notin E$. Since L/K is Galois, α is algebraic over K, separable and normal in L/K. It is easy to see that α is therefore also algebraic over E, separable and normal in L/E. We conclude that there is a $\beta \in L$ such that $\alpha \neq \beta$ and $f_E^\alpha(\beta) = 0$. Therefore there is a field isomorphism $\sigma E(\alpha) \longrightarrow E(\beta)$ which is the identity on E and sends α to β. Let $\overline{L}$ be an algebraic closure of L. Note that it is an algebraic closure of both $E(\alpha)$ and $E(\beta)$. From field theory we know that σ can be extended to an isomorphism $\overline{L} \longrightarrow \overline{L}$. Since any element of L must be sent by σ to another root of its minimal polynomial over K and since all these roots are in L as L is normal, we see that σ maps L to L. So we get σ in $\mathrm{Aut}_E(L)$ with $\sigma(\alpha) \neq \alpha$, therefore $\alpha \notin L^{\mathrm{Aut}_E(L)}$.

What remains to be proved is that $\phi \circ \psi$ is the identity on the set $\{H : H \subset G\text{closed subgroup}\}$. So let H be a closed subgroup of $\mathrm{Aut}_K(L)$. We must show that $\mathrm{Aut}_{L^H}(L)$ is contained in H (the other inclusion is trivial) or equivalently, in the closure of H. Let $\sigma \in \mathrm{Aut}_{L^H}(L)$. Our aim is to prove that

$$\sigma \in \overline{H} = \left\{\tau \in \mathrm{Aut}_K(L) : \forall F \subset L \text{ finite } \exists \rho \in H : \tau|_F = \rho|_F\right\}$$

holds. Let F be a finite subset of L. We must exhibit a ρ in H such that $\sigma|_F$ is equal to $\rho|_F$. Let E be a finite subfield of L that is Galois and contains F. This can be done by (2). Now consider $H_E = \left\{\rho|_E : \rho \in H\right\}$. This is a subgroup of $\mathrm{Gal}(E/K)$. We observe that $E^{H_E} = E \cap L^H$ is the set of those elements in E fixed by H. Since $\sigma|_{L^H}$ is the identity, we have $\sigma \in \mathrm{Aut}_{E^{H_E}}(E)$, which is just H_E by finite Galois theory.

Some elementary results on Galois groups

We now include a couple of simple facts from topological algebra and derive from them several consequences in the context of Galois theory.

Theorem. Let G be a topological group and H a subgroup. Then

1. if H is open it is also closed;
2. if H is closed and of finite index, it is open;
3. if G is compact then H is open if and only if it is closed and of finite index.

Proof. Let $\tau \in G$. Then the map $G \longrightarrow G$ sending σ to $\tau\sigma$ is a homeomorphism. It is continuous since it is the composition of the inclusion $G \longrightarrow G \times G$ sending σ to (τ, σ) and the multiplication map. Its inverse is the same map with τ^{-1} in the place of τ, which is therefore also continuous.

Now if H is open then so is τH for every $\tau \in G$. Pick a system of representatives R of G/H. Note that we have $G = \coprod_{\tau \in R} \tau H$ and therefore $G - H = \coprod_{\tau \in R, \tau \notin H} \tau H$. The latter is clearly open, so H is closed. This proves (1). It also proves (2) as the same argument works with open and closed reversed, when R is finite (i.e. H is of finite index.) For (3) observe that if H is open we have an open cover $G = \coprod_{\tau \in R} \tau H$, so it should have a finite subcover, which is to say that R is finite.

Theorem. Let L/K be a field extension which is Galois with group G. Let E be an intermediate field and H the corresponding closed subgroup. Then the following are equivalent

1. E/K is a finite extension;
2. H is open;
3. H is of finite index in G.

If these conditions are satisfied we have $[E : K] = (G : H)$.

Proof. Since G is compact, (2) and (3) are equivalent by the previous theorem. Suppose E/K is finite. By the primitive element theorem there now is an $\alpha \in E$ that generates E. Recall that we have $f_K^\alpha = \prod_{\beta \in G\alpha}(X - \beta)$. Comparing degrees we see that $[K(\alpha) : K] = \#G\alpha$. The number of elements in an orbit is equal to the index of the stabilizer, which is H since $K(\alpha) = E$, so we have $[E : K] = (G : G_\alpha) = (G : H)$. So (1) implies all other claims in the theorem.

It remains to show that (3) implies (1). So suppose that H has finite index in G. We know that E is the union of its finite subfields. Let E' be such a subfield and H' the subgroup corresponding to it. Since H' contains H, the index $(G : H')$ is bounded by $(G : H)$. Moreover, since E' satisfies (1) we have $[E' : K] = (G : H')$. This means that the field degree $[E' : K]$ is bounded above by $(G : H)$. So we can pick E' finite such that $[E' : K]$ is maximal. Let β be any element of E. Now $E'(\beta)$ is a finite extension of K containing E. This means $[E'(\beta) : K] \geq [E' : K]$, but the maximality

of E' gives that $[E'(\beta) : K] \leq [E' : K]$. We conclude that β is in E', so that $E = E'$ is a finite extension of K.

Theorem. Let G_1 and G_2 be two topological groups with G_1 compact and G_2 Hausdorff and let $f : G_1 \longrightarrow G_2$ be a continuous group homomorphism. Then f induces an isomorphism of compact Hausdorff topological groups

$$\begin{array}{ccc} G_1/\ker f & \xrightarrow{\sim} & f[G_1] \\ \uparrow\!\!\uparrow & & \cap \\ G_1 & \xrightarrow[f]{} & G_2 \end{array}$$

Proof. The map $f : G_1 \longrightarrow f[G_1]$ is continuous and surjective. Since $f(g_1) = f(g_2)$ holds if and only if $g_1 g_2^{-1}$ is in the kernel we get a continuous bijection $\bar{f} : G_1/\ker f \longrightarrow f[G_1]$. It remains to be proved that $\bar{f}$ is close.d Now if C is a closed subset of $G_1/\ker f$, then it compact (since $G_1/\ker f$ is) and therefore, its image is also compact. Being inside a Hausdorff space it follows that $\bar{f}[C]$ is closed. So $\bar{f}$ is a homeomorphism and therefore $G_1/\ker f$ is also Hausdorff and $f[G_1]$ is also compact. This finishes the proof.

Theorem. Let L/K be a Galois extension and E an intermediate field, corresponding to the closed subgroup H of the Galois group $G = \mathrm{Aut}_K(L)$. Then

1. L/E is a Galois extension with group H.
2. For all σ in G we have $\mathrm{Aut}_{\sigma E} L = \sigma H \sigma^{-1}$.
3. E/K is Galois if and only if H is a normal subgroup. In this case the map from G/H to $\mathrm{Gal}(E/K)$ sending σH to $\sigma|_E$ is an isomorphism of topological groups.

Proof.
(1) We only have to show L/E is Galois, since H is the only candidate for the Galois group. If L is algebraic, separable and normal over K then it is clearly also algebraic, separable and normal over E.

(2) Let σ and τ be in G and x be in L. The we have $\tau\sigma(x) = \sigma(x)$ if and only if $\sigma^{-1}\tau\sigma(x) = x$. This means that τ is in $\mathrm{Aut}_{\sigma E}(L)$ if and only if $\sigma^{-1}\tau\sigma$ is in $\mathrm{Aut}_E(L)$. The result follows.

(3) Since E is a subextension of L, it is clearly algebraic and separable over K. So it is Galois if and only if it is normal, i.e. if σE is E for all σ in the Galois group. By the previous part this happens precisely when $\sigma H \sigma^{-1}$ is H for all σ, i.e., when H is a normal subgroup. Now consider the restriction map from G to $\mathrm{Gal}(E/K)$. It is easily seen to be onto and continuous. The kernel is H. Therefore, by the previous topological theorem, we get the desired result.

Theorem. Let K, L and F be subfields of some big field, such that L/K is Galois and F contains K. Then LF/F is also Galois and the restriction map from $\mathrm{Gal}(LF/F)$ to $\mathrm{Gal}(L/(L \cap F))$ is an isomorphism of topological groups.

Proof. We know that L is a splitting field for a collection of separable monic polynomials in $K[X]$. Now LF is the splitting field of the same set of polynomials, considered over F. We conclude that LF/F is Galois. The restriction map from $\mathrm{Gal}(LF/F)$ to $\mathrm{Gal}(L/K)$ is a continuous group homomorphism. It is injective, since any automorphism that is the identity on F and L is the identity on LF. It need not be surjective, however if we only consider the image of the restriction map, it will be an isomorphism of topological groups. Let H be that image. Note that H is closed, being a compact set inside a Hausdorff space. We see that $H = \mathrm{Gal}(L/E)$ for some intermediate field E. Since $H = \mathrm{Gal}(LF/F)|_L$ we see that

$$E = L^H = L \cap (LF)^{\mathrm{Gal}(LF/F)} = L \cap F.$$

Relation with profinite groups

We now briefly go into another description of the Galois group and its topology. Let L/K be a Galois extension. We have seen that the intermediate fields which are finite Galois correspond to the open normal subgroups of $\mathrm{Gal}(L/K)$. Note that $\mathrm{Gal}(L/K)$ maps onto $\mathrm{Gal}(E/K)$ for all such intermediate fields E. Moreover, these maps are compatible. We therefore get a map from $\mathrm{Gal}(L/K)$ to the projective limit $\lim_{\leftarrow E} \mathrm{Gal}(E/K)$. The later is a profinite group. Since all the projection maps are onto, the image of $\mathrm{Gal}(L/K)$ is dense. It is also compact (since $\mathrm{Gal}(L/E)$ is) and therefore closed, as profinite groups are Hausdorff. This means that the map is in fact onto. It is also clearly injective, since L is the union of all these subfields. This means the map is an isomorphism of groups. Using the topological theorem from before we see that it is in fact an isomorphism of topological groups. Often, one defines the topology on the Galois group via this isomorphism. We mention without proof the following.

Theorem. Let G be a topological group. Then the following are equivalent

1. G is the Galois group of some field extension.
2. G is profinite;
3. G is compact, Hausdorff and totally disconnected;

Up until this point we have always considered Galois groups for an extension L/K. There is an L that is in some sense the largest, that is, we find all Galois groups as quotients of the Galois group of that large extension. Let K be a field. Fix an algebraic closure $\overline{K}$ of K. Let K_s be the separable closure of K in $\overline{K}$. Note that it is also a normal extension, since the conjugates of a separable element are also separable. Note that any algebraic extension L of K can be embedded in $\overline{K}$. If it is separable, it will in fact land inside K_s. So if L/K is Galois, then its Galois group is a quotient of $\mathrm{Gal}(K_s/K)$. We write G_K for $\mathrm{Gal}(K_s/K)$ and call it the absolute Galois group of K. it will in fact sit inside K_s.

If F is an extension of the field K, then the restriction map from G_F to G_K is a continuous group homomorphism. Using the theorems from before we see that its kernel is $\mathrm{Gal}(K_sF/F_s)$ and its image is $\mathrm{Gal}(K_s/(K_s \cap F))$.

It now looks as though the association of G_K to K defines a contravariant functor from fields to profinite groups. However, this is not true. The problem is that the construction of G_K depends on a choice of an algebraic closure. Different choices give different G_K's and although these are isomorphic, there are, in general, many of such isomorphism. The problem lies in the fact that G_K may have non-trivial inner automorphisms.

To fix this, we can 'divide out' all such inner automorphisms. If we let **Pfg**' be the category whose objects are the profinite groups and whose morphisms are the equivalence classes of homomorphisms under the following relation: two homomorphisms f and g from G to H are equivalent if and only if there is a ρ in H such that for all σ in G we have $g(\sigma) = \rho f(\sigma)\rho^{-1}$. From the discussion above we now see that $K \mapsto G_K$ is a functor from **Fld** to **Pfg**'.

Another way to fix the non-functoriality is by passing to the largest abelian quotient. Since abelian groups have no inner automorphism, the association

$$K \mapsto G_K^{ab} = G_K/\overline{[G_K, G_K]} = \mathrm{Gal}(K^{ab}/K)$$

is a contravariant functor from **Fld** to **Pfab**.

Inside K^{ab} there is a subfield $K(\mu)$, where $\mu = (K_s^\times)_{tor}$ consists of the roots of unity. Since the Galois group $\mathrm{Gal}(K(\mu)/K)$ is abelian, it has no inner automorphisms and we again get a contravariant functor from **Fld** to **Pfab**, sending K to $\mathrm{Gal}(K(\mu), K)$.

Traces and finite étale algebras

In the remainder of this text we will explain a different version of Galois theory, which was developed by Grothendieck. It is applicable in much greater generality than the 'traditional' Galois theory we've been studying up until now.

Let A be a commutative ring and P a finitely generated projective A-module. We want to define a A-linear homomorphism $\mathrm{Tr} : \mathrm{End}_A(P) \longrightarrow A$, the so-called trace map.

Fix and A-module M. Let P^* be the dual of P, that is, $P^* = \mathrm{Hom}_A(P, A)$. We consider the map

$$\begin{array}{rccc} f_P & : & P^* \otimes_A M & \longrightarrow & \mathrm{Hom}_A(P, M) \\ & & f \otimes x & \mapsto & [y \mapsto f(y)x]\,. \end{array}$$

We claim that the map f_P is an isomorphism for every finitely generated projective module P and every M. First note that this is clear if $P = A$. Also if f_P and f_Q are isomorphisms, so is $f_{P\oplus Q}$. So the claim holds for every A^n and now it easily follows that it holds for all finitely generated projective P.

To obtain the trace map we apply the above with $M = P$ and put

$$\begin{array}{rccccc} \mathrm{Tr} & : & \mathrm{End}_A(P) & \xrightarrow{f_P^{-1}} & P^* \otimes_A P & \longrightarrow & A \\ & & & & f \otimes x & \mapsto & f(x). \end{array}$$

Again, let A be a commutative ring and now let B be an A-algebra, that is, a ring homomorphism $A \longrightarrow B$ such that the image of A lies in the center of B. We also demand that B is finitely generated and projective as an A-module. In this context we define the trace of B over A to be the map

$$\begin{array}{rccccc} \mathrm{Tr}_{B/A} & : & B & \longrightarrow & \mathrm{End}_A(B) & \underset{\mathrm{Tr}}{\longrightarrow} & A \\ & & b & \mapsto & [x \mapsto bx]\,. & & \end{array}$$

Note that $\mathrm{Hom}_A(B, A)$ is a left-B-module, the B-action is defined by putting $bf(x) = f(bx)$ for all b, x in B and A-linear $f : B \longrightarrow A$. We can now make a B-linear map

$$\begin{array}{ccc} B & \xrightarrow{\#} & \mathrm{Hom}_A(B, A) \\ 1 & \mapsto & \mathrm{Tr}_{B/A} \\ b & \mapsto & [x \mapsto \mathrm{Tr}(bx)]\,. \end{array}$$

We call a commutative A-algebra B finite étale over A if it is finitely generated and projecive as an A-module and the map $\#$ defined above is an isomorphism.

For example, if $f \in A[x]$ is a monic polynomial and $B = A[x]/f$ then B is finite étale over A if and only if the discriminant $\Delta(f)$ is in $A^\times$.

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then $B = \mathcal{O}_K$ is a finitely generated projective $A = \mathbf{Z}$-module. However, we have an exact sequence

$$0 \longrightarrow \mathcal{O}_K \xrightarrow{\#} \mathrm{Hom}_{\mathbf{Z}}(\mathcal{O}_K, \mathbf{Z}) \longrightarrow \mathcal{O}_K/\mathcal{D}_{K/\mathbf{Q}} \longrightarrow 0,$$

where $\mathcal{D}_{K/\mathbf{Q}}$ is the *different* ideal of the number field K. The quotient $\mathcal{O}_K/\mathcal{D}_{K/\mathbf{Q}}$ is a finite group whose order is $|\Delta_{K/\mathbf{Q}}|$, so $\#$ is never onto if K is not $\mathbf{Q}$. We can fix this by considering the rings $A = \mathbf{Z}[\Delta_{K/\mathbf{Q}}^{-1}]$ and $B = \mathcal{O}_K[\Delta_{K/\mathbf{Q}}^{-1}]$. In that case B is a finite étale algebra over A.

The main theorem

We call a commutative ring A connected if the only idempotent elements are 0 and 1.

Theorem. Let A be a commutative ring that is connected. Then there is a profinite group π such that the category $\mathbf{FEt}_A$ of finite étale A-algebras and π-**sets** of finite sets with continuous π-action are anti-equivalent.

Theorem. Let K be a field, then the category $\mathbf{FEt}_K$ is anti-equivalent to G_K-**sets**, where G_K is the absolute Galois group of K.

We shall sketch a proof of this last theorem, leaving most routine verifications to the reader. An important ingredient is the following fact, which we shall prove later on.

Fact. If B is a commutative K-algebra then B is finite étale over K if and only if there is a non-negative integer t and there are finite separable field extensions $L_1, \ldots, L_t$ of K such that B is isomorphic to $L_1 \times \cdots \times L_t$ as a K-algebra.

Note that a finite separable extension of K can be embedded as a subfield of K_s and then corresponds to an open subgroup H of G_K. This process is not canonical; different embeddings give conjugated subfields. So we see that a finite separable extension of K is specified up to isomorphism by giving a conjugacy class of open subgroups H of G_K.

From the above we see that giving a finite étale algebra over K is the same as giving a finite set of conjugacy classes of open subgroups of G_K.

Now we look at the other side. Let X be a finite set with continuous G_K action. We can write X as a disjoint union of orbits. On each of the orbits, G_K acts transitively. Therefore such an orbit is as a G_K-set isomorphic to G/H, where H is the stabilizer of one of the elements of the orbit. This is in fact an open subgroup. If we choose a different element from the same orbit, the stabilizer we get is a conjugate of the original one. Thus we see that a transitive G_K-set is classified up to isomorphism by a conjugacy class of open subgroups.

We are now morally convinced that the objects on the same side are indeed represented by the same data, so it's time to write out the functors for the equivalence.

To a finite étale algebra B over K we can associate the set $\mathrm{Hom}_K(B, K_s)$. It is clearly finite, recall that B is isomorphic to a product of finite separable extensions of K and each of these can only be embedded in a finite number of ways. It also has a natural action of G_K. Thus we have a functor from finite étale algebras to G_K-sets.

To go in the other way we associate to a finite set X with G_K action the set ${}_{G_K}\mathrm{Map}(X, K_S)$ of G_K equivariant maps from X to K_s. Pointwise operations turn this set into a K-algebra, which one checks to be finite étale.

The remainder of the proof consists of straightforward verifications, reducing to finite separable extensions on the one side and transitive G_K-sets on the other. The reader should think of it as a nice exercise to complete the proof.

What remains is to sketch a proof of our fact concerning the structure of finite étale algebras over K. Let B be such an algebra. Since it has finite dimension over K, it is an Artinian ring. So we can write $B \cong B_1 \times \cdots \times B_t$ as a product of local Artinian rings that are K-algebras.

So we may assume that B is local and that $\mathfrak{m}_B^n = 0$ for some positive integer n. Note that by comparing K-dimensions the map

$$\begin{array}{ccc} B & \xrightarrow{\#} & \mathrm{Hom}_A(B, A) \\ b & \mapsto & [x \mapsto \mathrm{Tr}(bx)] \end{array}$$

is an isomorphism if and only if it is injective. But clearly, any nilpotent element goes to zero, so if B is finite étale, then in fact $\mathfrak{m}_B$ must be the zero ideal, that is, B is a field. Moreover, it will be finite étale if and only if the trace map doesn't vanish and by general field theory one knows this happens only if B is in fact a finite separable extension.