Algebra Lecture Notes -Galois Theory

Siddhartha Sahi

February 10, 2007

1 Galois extensions

Let F be a field. The set of all automorphisms of F is a group $Aut(F)$. Write $\mathcal{A}$ ={subgroups of $Aut(F)$} and $\mathcal{F} = \{$subfields of $F\}$. Then we have two order reversing maps $\phi : \mathcal{A} \to \mathcal{F}$ and $\gamma : \mathcal{F} \to \mathcal{A}$ defined by

1. $\phi(G) = F^G$ (fixed field of G)
2. $\gamma(K) = Aut_K(F) = Gal(F/K)$ (Galois group of F/K)

It is easy to see that $\phi\gamma(K) \supset K$ and $\gamma\phi(G) \supset G$. Since ϕ, γ are order-reversing it even follows that $\gamma\phi\gamma(K) = \gamma(K)$ and $\phi\gamma\phi(G) = \phi(G)$. Nevertheless the two maps are not quite inverses (examples!). The first result of Galois Theory is as follows:

Theorem 1 *$\gamma\phi(G) = G$ for any* finite *subgroup of A.*

The main idea is the following numerical result, where we write $ind(K) = [F : K] = \dim_K(F)$:

Proposition 2 *For any $G < A$, either $|G| = ind\left(F^G\right)$ or both numbers are infinite.*

Proof of the Theorem. Let $H = \gamma\phi(G)$ then we need to prove $H = G$. Note that we have

$$F^H = \phi(H) = \phi\gamma\phi(G) = \phi(G) = F^G.$$

If $|G|$ is finite then applying the proposition twice we conclude that

$$|G| = ind\left(F^G\right) = ind\left(F^H\right) = |H|.$$

Since we have $H \supset G$ (why?), it follows that $H = G$. ■

The proof of the proposition (following Dedekind and Artin) involves two lemmas. If S is a set, we write $Map(S, F)$ for the set of all maps from S to F; this is naturally an F vector space.

Lemma 3 *$Aut(F)$ is a linearly independent subset of $Map(F,F)$.*

Proof. If not, choose a minimal nontrivial dependence relation; i.e. choose $\sigma_i \in Aut(F)$ and $b_i \in F^\times$ such that

$$b_1\sigma_1(\alpha) + b_2\sigma_2(\alpha) + \cdots + b_m\sigma_m(\alpha) = 0 \text{ for all } \alpha \text{ in } F.$$

and m is minimal. We will arrive at a contradiction by showing it is possible to reduce m further.

We may assume $m \geq 2$ and $\sigma_1 \neq \sigma_m$ (why?). So pick β in F such that $\sigma_1(\beta) \neq \sigma_m(\beta)$. Modify the above equation in two ways – first replace α by $\beta\alpha$ and second simply multiply by $\sigma_1(\beta)$. Since $\sigma_i(\beta\alpha) = \sigma_i(\beta)\sigma_i(\alpha)$ subtracting the two expressions gives the new relation

$$c_1\sigma_1(\alpha) + c_2\sigma_2(\alpha) + \cdots + c_m\sigma_m(\alpha) = 0 \text{ for all } \alpha \text{ in } F.$$

where $c_i = b_i[\sigma_i(\beta) - \sigma_1(\beta)]$. Now we have $c_1 = 0$, but $c_m \neq 0$; therefore this is a smaller non-trivial dependence relation. ■

For a subgroup G of $Aut(F)$, consider the *evaluation* map $e : F \to Map(G,F)$

$$e(a)(\sigma) = \sigma(a)$$

this is easily seen to be F^G-linear.

Lemma 4 *The map e takes F^G-independent sets to F-independent sets.*

Proof. If not, choose a minimal nontrivial dependence relation. i.e. choose K-independent α_i in F, and coefficients b_i in $F^\times$ such that

$$b_1\sigma(\alpha_1) + b_2\sigma(\alpha_2) + \cdots + b_n\sigma(\alpha_n) = 0 \text{ for all } \sigma \text{ in } G.$$

and n is minimal. We will arrive at a contradiction by showing it is possible to reduce n further.

We may assume $n \geq 2$, $b_1 = 1$, and then $b_n \notin F^G$ (why?). So pick τ in G such that $\tau(b_n) \neq b_n$. In the above equation, replace σ by $\tau^{-1}\sigma$ and apply τ. Since $\tau\left[b_i\tau^{-1}\sigma(\alpha_i)\right] = \tau(b_i)\sigma(\alpha_i)$, subtracting the new equation from the original gives the relation

$$c_1\sigma(\alpha_1) + c_2\sigma(\alpha_2) + \cdots + c_n\sigma(\alpha_n) = 0 \text{ for all } \sigma \text{ in } G.$$

where $c_i = b_i - \tau(b_i)$. Now we have $c_1 = 0$, but $c_n \neq 0$; therefore this is a smaller non-trivial dependence relation. ■

Proof of Proposition. For a finite subset $S = \{\sigma_1, \ldots, \sigma_m\} \subset G$ and a finite F^G independendent subset $T = \{\alpha_1, \ldots, \alpha_n\} \subset F$, we consider the $m \times n$ matrix $M_{S,T} = (\sigma_i(\alpha_j))$.

If $\text{ind}\left(F^G\right)$ is finite, choose T to be an F^G-basis of F. Then by the first lemma, the rows of $M_{S,T}$ are F-independent (verify!). Therefore we have $m \leq n = ind\left(F^G\right)$ and hence $|G| \leq ind\left(F^G\right)$. In particular, $|G|$ is also finite.

If $|G|$ is finite, then choose $S = G$. Now by the second lemma, the columns of $M_{S,T}$ are F-independent (verify!). Therefore we have $n \leq m = |G|$, and hence $ind\left(F^G\right) \leq |G|$. In particular $ind\left(F^G\right)$ is finite. ■

Definition 5 *F/K is said to be a Galois extension if $\phi\gamma(K) = K$.*

Then we have two characterization of Galois extensions

Corollary 6 *Let G be a finite group, TFAE*

1. *F/K is a finite Galois extension with $Aut_K(F) = G$*
2. *$K = F^G$.*

Proof. For $1 \Rightarrow 2$, we use $\phi(G) = \phi\gamma(K) = K$.
For $2 \Rightarrow 1$, we note that $\phi\gamma(K) = \phi\gamma\phi(G) = \phi(G) = K$, and $Aut_K(F) = \gamma\phi(G) = G$ by the theorem. ■

Corollary 7 *Let F/K be a finite extension. TFAE*

1. *F/K is Galois.*
2. *$[F : K] = |Aut_K(F)|$.*

Proof. Let $G = Aut_K(F)$, then clearly $F^G \supset K$, and by the proposition $[F : F^G] = |G|$. Therefore we have
$[F : K] = |G| \Longleftrightarrow K = F^G \Longleftrightarrow F/K$ is Galois. ■

Exercise 8 *Show that $\gamma(K)$ is a group, $\phi(G)$ is a field and γ, ϕ are order-reversing*

Exercise 9 *Show that $\phi\gamma(K) \supset K$ and $\gamma\phi(G) \supset G$, $\gamma\phi\gamma(K) = \gamma(K)$ and $\phi\gamma\phi(G) = \phi(G)$.*

Exercise 10 *Give examples such that $\phi\gamma(K) \neq K$ and $\gamma\phi(G) \neq G$.*

Exercise 11 *Explain the "whys" in the proof of the theorem.*

Exercise 12 *Prove the F^G-linearity of e.*

Exercise 13 *Justify the "we may assume ..." in the proofs of the two lemmas*

Exercise 14 *Verify the two F-independence assertions in the proof of the proposition.*

2 Imbeddings and splitting fields

If E is a finite (dimensional) extension of K and $\alpha \in E$, then the powers of α are linearly dependent over K. Therefore α is *algebraic over* K; i.e. it is the root of a K-polynomial p, which we may choose to be monic and of minimal degree. It follows then that p is irreducible (why?) and hence $K[x]/(p)$ is a field. Now since $x \mapsto \alpha$ defines a natural ring homomorphism $K[x]/(p) \to K[\alpha]$, it follows that (why?)

1. The image is a field and hence equals $K(\alpha)$ (and $K[\alpha]$).
2. α and K uniquely determine p – *the minimal polynomial* of α over K.
3. $\deg(p) = [K(\alpha) : K]$ divides $[E : K]$.

Lemma 15 *Let E/K be a finite field extension. Given an imbedding $\sigma : K \to L$ there exists a finite field extension F/L and an imbedding $\tau : E \to F$ extending σ.*

$$\begin{array}{ccc} E & \xrightarrow{\tau} & F \\ \uparrow & \circlearrowright & \uparrow \\ K & \xrightarrow{\sigma} & L \end{array}$$

More generally, given $\sigma_i : K \to L$ for $i = 1, \ldots, n$ there exists a finite field extension F/L and imbeddings $\tau_i : E \to F$ extending σ_i.

Proof. Let $f \in K[x]$ be the minimum polynomial of some $\alpha \in E \setminus K$, and let $p \in L[x]$ be an irreducible factor of f^σ. Then we get an imbedding from $K(\alpha) \approx K[x]/(f)$ to $L[x]/(p)$ which extends σ, and the result follows by induction on $[E : K]$. For the general case, we extend the σ_i one at a time to succesively larger finite field extensions. ■

Definition 16 *If E is generated over K by the roots of a K-polynomial f, then we say that E is a splitting field of f.over K.*

Theorem 17 *Every $f \in K[x]$ of degree n admits a splitting field E with $[E : K] \leq n!$ Any two splitting fields are isomorphic.*

Proof. We proceed by induction on $n = \deg(f)$. If p is an irreducible factor of f, then $L = K[x]/(p)$ is a field with $[L : K] = \deg(p) \leq n$. Moreover $L = K(\xi)$ where $\xi := \overline{x}$ is a root of f (why?), hence in $L[z]$ we get

$$f(z) = (z - \xi)\, g(z)$$

By induction we can construct a splitting field E for g over L with $[E : L] \leq (n-1)!$. Then E is a splitting field for f over K with $[E : K] = [E : L][L : K] \leq n!$

If E' is another splitting field then we have an imbedding $\sigma : K \to E'$. This extends to an embedding $\tau : E \to F$ for some extension F of E'. But then $\tau(E) = E'$ since both are generated by the roots of f^τ in F, hence E and E'. ■

Example 18 *Let $F = K(t_1, \ldots, t_n)$ be the field of rational functions in n variables, and consider the "general" polynomial*

$$p(x) = (x - t_1) \ldots (x - t_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots \pm e_n$$

where the e_i are the elementary symmetric functions:

$$e_1 = \sum_i t_i,\ e_2 = \sum_{i<j} t_i t_j,\ \ldots,\ e_n = \prod_i t_i.$$

Then F is a splitting field of p over the subfield $E = K(e_1, e_2, \ldots, e_n)$. We claim that F/E is a Galois extension, with group S_n acting on F by permuting the t_i. Clearly $E \subset F^{S_n}$ and by the previous theorem $[F : E] \leq n! = \left[F : F^{S_n}\right]$. Therefore $E = F^{S_n}$.

2.1 Ruler and compass construction

Construction by ruler and compass means starting with $\mathbb{Q}^2 \subset \mathbb{R}^2$ and successively constructing new points by intersection of lines (passing through two previously contructed points) and circles (with previoulsy constructed centers and radii). A real number will be called constructible if it is a coordinate of a constructible point.

Exercise 19 *Let F be the subfield of $\mathbb{R}$ containing coordinates of all constructed numbers up to some stage. Show that numbers constructed by one further such intersection satisfy a quadratic or linear equation over F.*

Exercise 20 *Deduce that the new numbers lie in an extension field of degree 1 or 2 over F.*

Exercise 21 *Show that each constructible number lies in a field E such that $[E : \mathbb{Q}] = 2^n$ for some n.*

Exercise 22 *Show that constructible numbers cannot have a minimum polynomial of degee 3.*

Exercise 23 *Deduce that it is impossible to construct $2^{1/3}$ (duplicating a cube) and $\cos(20°)$ (trisecting $60°$).*

3 Normal extensions

Definition 24 *A finite field extension E/K is* normal *if every field extension F/K has at most one subextension isomorphic to E/K.*

Lemma 25 *For any finite field extension E/K TFAE*

1. *Every irreducible K-polynomial with a root in E, splits in E.*
2. *E is the splitting field of some K-polynomial.*
3. *E/K is normal.*

Proof. $1 \Rightarrow 2$ Choose a basis $\{\alpha_i\}$ for E/K; then the minimum polynomial p_i of each α_i splits in E, and E is the splitting field of Πp_i.

$2 \Rightarrow 3$ Suppose α_i are the roots of f and $E = K(\alpha_i)$ is the splitting field. Then the image of τ is $K(\beta_i)$ where $\beta_i = \tau(\alpha_i)$. But $(x - \beta_i)$ are the factors of $\sigma(f)$ Therefore the set $\{\beta_i\}$ is indep. of τ.

$3 \Rightarrow 1$ Suppose f is an irred. K-poly with root α in E, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be its roots in a splitting field L. Then for each i, $\alpha \mapsto \alpha_i$ defines an imbedding of $K(\alpha)$ into L which extends to $\tau_i : E \to F$ for some extension F of L. Now all have a common image E' which contains all α_i. Therefore f splits in E' and hence in E. ■

Suppose E/K is a finite extension with generators $a_1, \ldots, a_n$, and F is the splitting field of $p_1 \ldots p_n$ where p_i is the minimum polynomial of a_i. Then F/K is normal and is moreover contained in any normal extension containing E/K. Therefore F is independent of the choice of the generators, and is called the *normal closure* of E/K.

Note that if E/K is a normal subextension of F/K, then for any $g \in Aut_K(F)$, $g(E)$ being isomorphic to E must equal E. Hence E must be $Aut_K(F)$-invariant. Invariant subextensions of a *Galois* extension can be characterized in terms of normal subgroups as follows:

Lemma 26 *Suppose F/K is a finite Galois extension with group G and E/K is a subextension. TFAE*

1. *E is G-invariant.*
2. *$E = F^H$ for a normal subgroup H*

   Moreover in this case E/K is Galois with group G/H.

Proof. $2 \Rightarrow 1$ is easy. For $1 \Rightarrow 2$, note that by restriction we get a morphism $G \to Aut_K(E)$, whose kernel is a normal subgroup H of G. Clearly F^H contains E, and it is enough to prove $[F : F^H] = [F : E]$. Since $[F : F^H] = |H|$ and $[F : K] = |G|$ it suffices to prove that $[E : K] = |G| / |H| = |G/H|$. But we have an injection $G/H \to Aut_K(E)$ with $E^{G/H} = E^G = K$ and so the result follows.

The argument just given also proves E/K is Galois with group G/H. ■

4 Separable extensions

A polynomial is said to be separable if it has distinct roots in its splitting field. We have

Lemma 27 *Suppose $f \in K[x]$ TFAE*

1. *f is separable.*
2. *f and its derivative f' have no common roots in E.*
3. *f and f' are relatively prime in $K[x]$.*

Corollary 28 *Suppose $f \in K[x]$ is irreducible with degree ≥ 2.*

1. *f is separable iff $f' \neq 0$.*
2. *If $char(K) = 0$ then f is separable.*
3. *If $char(K) = p$ then f is separable unless it is a polynomial in x^p.*

We leave the proofs as easy exercises.

If E/K is a field extension an element in E is said to be separable if its minimum polynomial is separable; if every element is separable we say that E/K is separable.

Lemma 29 *Suppose E/K, F/L are extensions with E/K finite and $\sigma : K \to L$ is an imbedding*

$$\#\{\tau : E \to F \mid \tau|K = \rho\} \leq [E : K].$$

If F/L is normal, then equality holds iff E/K is separable.

Proof. To prove the lemma, we may as well assume that F/L is normal.

First suppose $E = K(\alpha)$ for some α, and let p be the minimum polynomial of α. Since we have at least one imbedding $E \to F$, p^σ has a root in F (the image of α). Since F/L is normal p^σ splits as $\prod (x - \beta_i)$ say, and $\tau_i : \alpha \to \beta_i$ defines all possible extensions of σ. The number of such extensions is $\leq \deg(p) = [K(\alpha) : K]$ with equality iff the β_i are distinct, i.e. α is separable.

For the case of general E, we first extend σ to some $K(\alpha) \subset E$ and then argue by induction on $[E : K]$. ■

5 Main results of Galois Theory

We can now give a different characterization of Galois extensions:

Theorem 30 *A finite extension F/K is Galois iff it is normal and separable.*

Proof. Note that $Aut_K(F)$ consists precisely of the imbeddings $F \to F$ which extend the identity on K. Hence if F/K is normal and separable we get $|Aut_K(F)| = [F:K]$ whence F/K is Galois by an earlier Corollary.

Conversely, suppose F/K is Galois and $\tau : F/K \to E/L$ is an imbedding. Then $\{\tau\sigma : \sigma \in Aut_K(F)\}$ gives $|Aut_K(F)| = [F:K]$ different imbeddings. These must then be all possible imbeddings, and in particular they all have a fixed image. This implies both normality and separability of E/K. ■

Corollary 31 *If F/K is Galois and $F \supset E \supset K$, then F/E is Galois.*

Proof. For separability we note that for α in F, its minimum polynomial over E divides its minimum polynomial over K. Hence if the latter has distinct roots, so does the former. For normality, we note that by the theorem F is the spltting field of some f over K. Then it is also the splitting of f over E. ■

The following result is the "main theorem" of Galois theory:

Theorem 32 *Suppose F/K is a finite Galois extension with group G. Then the maps ϕ, γ are mutually inverse bijections between subgroups of G and intermediate subfields of F/K.*

Proof. Let $\mathcal{A}_G$ be the set of subgroups of G and let $\mathcal{F}_K$ be the set of fields between F and K. Clearly we have $\phi : \mathcal{A}_G \to \mathcal{F}_K$ and $\gamma : \mathcal{F}_K \to \mathcal{A}_G$, and by Theorem ... we have $\gamma\phi = 1$; therefore it suffices to prove that ϕ is surjective. However if $E \in \mathcal{F}_K$, by the previous corollary F/E is Galois and so by Corollary ... $E = F^H$ for some subgroup of G. ■

6 Cyclic extensions

Lemma 33 *A finite multiplicative subgroup of a field is cyclic.*

Proof. The group is finite, abelian, and hence a direct sum of finite cyclic groups $Z_{d_1} \oplus Z_{d_2} \oplus \cdots \oplus Z_{d_k}$ where we can arrange to have $d_i | d_{i+1}$. This means all orders divide d_k and so every element of the group satisfies $x^{d_k} = 1$. But this equation has at most d_k solutions in any field, hence the group must reduce to Z_{d_k}. ■

Thus in any field, the nth roots of 1 form a cyclic multiplicative group $W_n(K)$ of order $\leq n$.

Definition 34 *An extension F/K is called cyclic if it is Galois with $Aut_K(F)$ cyclic.*

We can give a characterization of cyclic extensions assuming that K contains all nth roots of 1.

Theorem 35 *Suppose $|W_n(K)| = n$. Then F/K is cyclic of degree n iff $F = K(\theta)$ with $\theta^n \in K$ but no smaller power.belongs to K.*

Proof. Suppose $F = K(\theta)$ as above, then we claim that the polynomial

$$f(x) = x^n - \theta^n = \prod_{w \in W_n} (x - \theta w)$$

is irreducible over K. (Else the constant term of a divisor of degree d would show $\theta^d \in K$ for $d < n$.). Therefore we have $F \approx K[x]/(f)$. Now W_n acts on F by $x \mapsto wx$ and $K = F^{W_n}$. Therefore the result follows from the Corollary.

Conversely suppose F/K is cyclic of order n. Then $K = F^G$ where $G = Aut_K(F)$ is cyclic of order n. We fix an isomorphism $\varepsilon : G \to W_n \subset K^\times$ and consider the linear combination $\sum_{g \in G} \varepsilon(g)^{-1} g$. By the F-independence of $G \subset Map(F, F)$ (Lemma 3), we can choose α in F such that

$$0 \neq \sum_{g \in G} \varepsilon(g)^{-1} g(\alpha) = \theta \text{ say.}$$

Then for all $g \in G$ we get

$$g(\theta) = \sum_{h \in G} \varepsilon(h)^{-1} gh(\alpha) = \varepsilon(g) \left(\sum_{h \in G} \varepsilon(gh)^{-1} gh(\alpha) \right) = \varepsilon(g)\theta$$

It follows that θ^n is G-fixed but no smaller power is G-fixed. Since F/K is Galois we have $K = F^G$, so θ^n belongs to K but no smaller power does. ■

The necessity of the condition $|W_n(K)| = n$ is seen in the following exercise:

Exercise 36 *Let $\omega = e^{2\pi i/5}$ be the primitive root 5th of 1 in $\mathbb{C}$. ω is a root of the irreducible polynomial $x^4 + x^3 + x^2 + x + 1$. Show that $\mathbb{Q}(\omega)/\mathbb{Q}$ is cyclic of order 4, but is not generated by the 4th root of a rational number.*

7 Constructible extensions

Definition 37 *A finite extension E/K is called a radical extension if $E = K(\alpha)$ with $\alpha^n \in K$ for some n.*

Definition 38 *A finite extension E/K is said to be constructible (by radicals) if it possesses a radical filtration $K = E_0 \subset \cdots \subset E_m = E$ where each E_{i+1}/E_i is a radical extension.*

We need the following result in characteristic 0:

Lemma 39 *In characteristic 0 the normal closure of a constructible extension is constructible.*

Proof. Let E/K be a finite extension and F/K its normal closure. Since separability is automatic in characteristic 0, F/K is Galois. Let F_1 be the subfield generated by $g(E)$ for $g \in G$. Then F_1 is G-invariant, therefore F_1/K is Galois and it follows that $F = F_1$.

Now suppose E/K is constructible with E_i as in the definition, and $E_{i+1} = E_i(\theta_i)$ with $\theta_i^{n_i} \in E_i$. Then by the previous discussion, F is generated by $\{g_j(\theta_i) : g_j \in G, 1 \leq i \leq m\}$, i.e. we have

$$F = K(g_1(\theta_1), \ldots, g_1(\theta_m), g_2(\theta_1), \ldots, g_2(\theta_m), \ldots,)$$

Since $g_j(\theta_i)^{n_i} = g_j(\theta_i^{n_i}) \in g(E_i)$, we see that F possesses a radical filtration. ■

In any characteristic, constructible *Galois* extensions F/K can be characterized as follows:

Theorem 40 *Suppose F/K is Galois of degree dividing n and $|W_n(K)| = n$. Then F/K is constructible iff $Aut_K(F)$ is solvable.*

Proof. If F/K is constructible, the first filtration step gives a radical extension $K(\theta)$ whose degree divides n. Then $\theta^n \in K$, and so for any g in $G = Aut_K(F)$ we have

$$\left(g(\theta)\theta^{-1}\right)^n = g(\theta^n)\theta^{-n} = \theta^n\theta^{-n} = 1$$

So $g(\theta)\theta^{-1}$ belongs to $W_n(K) \subset K$. Therefore $g(\theta)$ belongs to $E = K(\theta)$ and hence E is G-invariant. Therefore $E = F^H$ for some normal subgroup H. Now H is the Galois group of the constructible extension F/E and hence solvable by induction on degree. Also G/H is the Galois group of $K(\theta)/K$ and hence cyclic since K contains a primitive kth root. Therefore G is solvable.

Conversely if G is solvable then there is a chain of subgroups $G = G_0 > G_1 > \cdots > G_m = 1$ such that each G_i is normal in G_{i-1} and G_{i-1}/G_i is cyclic. Writing $F_i = F^{G_i}$ we get a chain of intermediate fields $K = F_0 < F_1 < \ldots < F_m = F$ such that F_{i-1}/F_i is a cyclic extension with group G_{i-1}/G_i. Then each F_{i-1}/F_i is radical and F/K is constructible. ■

8 Solvability by radicals

In this section we assume that all fields under discussion have characteristic 0. Then the splitting field for F any polynomial $f \in K[x]$ is automatically a Galois extension of K, and we call $Aut_K(F)$ the Galois group of f.

We need a brief discussion of roots of unity

Definition 41 *The splitting field of $x^n - 1 \in K[x]$ is called the* cyclotomic *extension $C_n = C_n(K)$ of order n over K.*

Note that since $x^n - 1$ and its derivative nx^{n-1} are relatively prime, $x^n - 1$ has n distinct roots in C_n and therefore $|W_n(C_n)| = n$. Any generator ω of $W_n(C_n)$ is called a primitive nth root of 1.

Lemma 42 *For $char(K) = 0$, C_n/K is a radical Galois extension with abelian Galois group.*

Proof. Clearly $C_n = K(\omega)$ where ω is primitive root, hence it is radical. Also since C_n/K is normal (splitting field) and separable (char. 0) it is Galois. Moreover $Aut_K(C)$ is completely determined by its action on ω, which must be of the form $\omega \mapsto \omega^d$ for some d relatively prime to n. Therefore $Aut_K(C)$ is isomorphic to a subgroup of the group of units of the ring Z/n, and hence is abelian. ■

We also need to discuss how the Galois group of a spltting field changes under base extension.

Lemma 43 *SupposeK'/K is an extension and F, F' are splitting fields for f over K, K'. Then $Aut_{K'}(F')$ is a subgroup of $Aut_K(F)$.*

Proof. F, F' are generated over K, K' by the roots of f, and the Galois groups are determined by their action on these roots. Therefore we get a restriction map from $Aut_{K'}(F')$ to $Aut_K(F)$ which is easily seen to be an injection. ■

We say that f is solvable by radicals if F can be imbedded in a constructible extension of K. Galois' big achievement is the following result:

Theorem 44 *f is solvable by radicals iff its Galois group is a solvable group.*

Proof. Let F/K be the splitting field of f. Then F/K is a Galois extension.

First suppose that $G = Aut_K(F)$ is solvable, unless K contains enough roots of 1 we cannot deduce that F/K is constructible. However let $n = [F : K]$ and let $C_n(K)$ and $C_n(F)$ be the cyclotomic extensions then $C_n(K)/C_n(F)$ is constructible because its Galois group is a subgroup of G and hence solvable. Thus the filtration $K \subset C_n(K) \subset C_n(F)$ can be refined to a radical filtration of $C_n(F)/K$. Since F/K imbeds in $C_n(F)/K$, f is solvable.

Conversely suppose F/K can be imbedded in a constructible extension E/K. By the previous lemma we can assume E/K to be Galois but again unless K contains enough roots of 1 we cannot deduce that $Aut_K(E)$ is solvable. However if we pass further to the extension $C_n(E)/K$ where $n = [E : K]$, then we can deduce that $C_n(E)/C_n(K)$ is a Galois extension with solvable Galois group. Also note that $C_n(E)/K$ is still Galois (it splits $(x^n - 1)g(x)$ if E splits $g(x)$); moreover we have a filtration $K \subset C_n(K) \subset C_n(E)$. Since $C_n(K)/K$ is normal with abelian Galois group, we deduce that $C_n(E)/K$ has solvable Galois group. Since F/K is normal in $C_n(E)/K$ $Aut_K(F)$ is a quotient of $Aut_K(C_n(E))$, hence solvable since the latter is solvable. ■

Theorem 45 *The general polynomial of degree n is not solvable by radicals for $n \geq 5$.*

Proof. It suffices to show that S_n is not solvable for $n \geq 5$, but this contains A_5, which is simple. ■