MINIMAL GALOIS THEORY

TERUYOSHI YOSHIDA

1. Galois Theory

Definition 1.1. Let K be a field.

(i) An **extension** F_τ/K is defined as a pair (F, τ) of a field F and a ring homomorphism $\tau : K \to F$. By a **subextension** L_τ/K of F_τ/K, we mean a field L satsifying $F \supset L \supset \tau(K)$. We often omit τ from the notation.
(ii) A **morphism** $f : F_\tau \to F'_{\tau'}$ of extensions is a morphism of K-algebras, i.e. a ring homomorphism $f : F \to F'$ such that $\tau' = f \circ \tau$. It is injective and $f(F)$ is a subextension of F'/K. We denote the set of all morphisms from F to F' by $\mathrm{Hom}_K(F, F')$, and the set of all automorphisms of F by $\mathrm{Aut}_K(F)$.
(iii) An extension F is a K-vector space by the action via τ. We write $[F : K] := \dim_K F$. We say F/K is **finite** if $[F : K] < \infty$. Morphisms are K-linear.

We have $[F : K] = 1 \Leftrightarrow \tau(K) = F$. If F/K is finite, then $[F : K] = [F' : K]$ implies $\forall f \in \mathrm{Hom}_K(F, F')$ are isomorphisms. In particular $\mathrm{Hom}_K(F, F) = \mathrm{Aut}_K(F)$, and:

Lemma 1.2. *Let $F/K, F'/K$ be extensions with F/K finite. If $\mathrm{Hom}_K(F, F')$ and $\mathrm{Hom}_K(F', F)$ are both non-empty, then $F \cong F'$ as extensions of K.*

Definition 1.3. For a subgroup H of $\mathrm{Aut}_K(F)$, its **fixed field** $F^H := \{x \in F \mid \forall \sigma \in H \ \ \sigma(x) = x\}$ is a subextension of F/K. A finite F/K is **Galois** if $|\mathrm{Aut}_K(F)| = [F : K]$.

Lemma 1.4. *Let $F_\tau/L, L_{\tau'}/K$ be extensions and consider $F_{\tau\tau'}/K$.*

(i) *$[F : K] = [F : L][L : K]$. In particular, if $F/L, L/K$ are finite then so is F/K.*
(ii) *If E/K is another extension, then $\mathrm{Hom}_K(F, E) = \coprod_{\rho \in \mathrm{Hom}_K(L,E)} \mathrm{Hom}_L(F, E_\rho)$.*

Proof. (i): If $\{a_i\}, \{b_j\}$ are bases of F over L and L over K respectively, then $\{a_i\tau(b_j)\}$ gives a basis of F over K. (ii): If $\sigma \in \mathrm{Hom}_K(F, E)$ then $\rho := \sigma|_L \in \mathrm{Hom}_K(L, E)$, and $\sigma \in \mathrm{Hom}_L(F, E_\rho)$. Conversely $\mathrm{Hom}_L(F, E_\rho) \subset \mathrm{Hom}_K(F, E)$ for $\forall \rho \in \mathrm{Hom}_K(L, E)$. □

Proposition 1.5. (Dedekind) *Let F/K, E/K be two extensions. Then $\mathrm{Hom}_K(F, E)$ is linearly independent over E in the E-vector space $\mathrm{Hom}_{K\text{-v.s.}}(F, E)$. In particular, if F/K is finite then $|\mathrm{Hom}_K(F, E)| \leq [F : K]$.*

Proof. Assume otherwise and take the minimal k such that $\{\sigma_1, \ldots, \sigma_k\}$ is linearly dependent, i.e. there exist $c_j \in E$ with $\sum_{j=1}^k c_j\sigma_j = 0$ and $c_k \neq 0$. As $\sigma_k \neq 0$, there is

Date: November 26, 2010.

a $t < k$ with $c_t \neq 0$. As $\sigma_t \neq \sigma_k$, choose $x \in F$ with $\sigma_t(x) \neq \sigma_k(x)$. For all $y \in F$ we have $\sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j(y) = \sum_{j=1}^{k} c_j\sigma_j(xy) = 0$, i.e. $\sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j = 0$. Hence

$$\textstyle\sum_{j=1}^{k-1} c_j\big(\sigma_j(x) - \sigma_k(x)\big)\sigma_j = \sum_{j=1}^{k} c_j\sigma_j(x)\sigma_j - \sigma_k(x)\sum_{j=1}^{k} c_j\sigma_j = 0,$$

which contradicts the minimality of k because $\sigma_t(x) - \sigma_k(x) \neq 0$. □

Corollary 1.6. *Let F_τ/L, $L_{\tau'}/K$ be finite such that $F_{\tau\tau'}/K$ is Galois. Then* $\mathrm{Aut}_K(F)$ *acts transitively on* $\mathrm{Hom}_K(L,F)$ *and* $|\mathrm{Hom}_K(L,F)| = [L:K]$. *For* $\forall\rho \in \mathrm{Hom}_K(L,F)$, *the extension F_ρ/L is Galois and* $\mathrm{Aut}_L(F_\rho)$ *is a subgroup of* $\mathrm{Aut}_K(F)$.

Proof. Proposition 1.5 and Lemma 1.4 shows $|\mathrm{Hom}_L(F,F_\rho)| = [F:L]$ for $\forall\rho$ and $|\mathrm{Hom}_K(L,F)| = [L:K]$. For $\rho,\rho' \in \mathrm{Hom}_K(L,F)$ we have $|\mathrm{Hom}_L(F_\rho,F_{\rho'})| = [F:L]$, as $f \in \mathrm{Hom}_L(F,F_\rho)$ gives $\mathrm{Hom}_L(F_\rho,F_{\rho'}) \cong \mathrm{Hom}_L(F,F_{\rho'})$ by $g \mapsto g\circ f$. Also F_ρ/L is Galois by setting $\rho = \rho'$, as $[F_\rho:L] = [F:K]/[L:K] = [F:L]$. □

Proposition 1.7. (Artin) *If H is a subgroup of* $\mathrm{Aut}_K(F)$, *then* $[F:F^H] \leq |H|$.

Proof. Assume otherwise, and let $H = \{\sigma_1,\dots,\sigma_m\}$ with $m < n = [F:F^H]$. Take a basis $\{x_1,\dots,x_n\}$ of F over F^H. Then the system of equations $\sum_{j=1}^{n} c_j\sigma_i(x_j) = 0$ $(1 \leq i \leq m)$ has a solution $c_j \in F$, not all zero. Take the minimal k such that there exist $c_j \in F$ with $\sum_{j=1}^{k} c_j\sigma_i(x_j) = 0$ with $c_k \neq 0$. We can assume $c_k = 1$ by dividing all c_j by c_k. As $x_1,\dots,x_k$ are linearly independent over F^H, there is a $t < k$ with $c_t \notin F^H$ (look at $\sigma_1 = \mathrm{id}$), so choose $\sigma \in H$ with $\sigma(c_t) \neq c_t$. As H is a group, applying σ to the system of equations gives $\sum_{j=1}^{k} \sigma(c_j)\sigma_i(x_j) = 0$ $(1 \leq i \leq m)$. As $\sigma(c_k) = 1 = c_k$,

$$\textstyle\sum_{j=1}^{k-1}\big(\sigma(c_j) - c_j\big)\sigma_i(x_j) = \sum_{j=1}^{k}\sigma(c_j)\sigma_i(x_j) - \sum_{j=1}^{k} c_j\sigma_i(x_j) = 0 \quad (1 \leq i \leq m),$$

which contradicts the minimality of k because $\sigma(c_t) - c_t \neq 0$. □

Theorem 1.8. (The fundamental theorem of Galois theory) *Let F/K be finite Galois, let A be the set of all subextensions of F/K, and B be the set of all subgroups of* $\mathrm{Aut}_K(F)$. *Then the following are inverse to each other:*

$$\Phi : A \ni L \longmapsto \Phi(L) = \mathrm{Aut}_L(F) \in B, \quad \Psi : B \ni H \longmapsto \Psi(H) = F^H \in A.$$

Proof. We have $|\Phi(L)| = [F:L]$ by Corollary 1.6(ii). Therefore, as $H \subset \Phi(\Psi(H))$, we have $|H| \leq |\Phi(\Psi(H))| = [F:\Psi(H)]$. As $L \subset \Psi(\Phi(L))$, we have $[F:L] = |\Phi(L)| \leq [F:\Psi(\Phi(L))] \leq [F:L]$, thus $\Psi\circ\Phi = \mathrm{id}$. By Proposition 1.7, we have $|H| \leq |\Phi(\Psi(H))| = [F:\Psi(H)] \leq |H|$, thus $\Phi\circ\Psi = \mathrm{id}$. □

Corollary 1.9. *Let F_τ/L, $L_{\tau'}/K$ be finite such that $F_{\tau\tau'}/K$ is Galois, and let* $G := \mathrm{Aut}_K(F)$ *and* $H := \mathrm{Aut}_L(F)$. *Then $G \rhd H$ if and only if L/K is Galois. In this case,* $G/H \ni \overline{\sigma} \longmapsto \tau^{-1}\sigma\tau \in \mathrm{Aut}_K(L)$ *is an isomorphism.*

Proof. We have $\sigma H\sigma^{-1} = \mathrm{Aut}_L(F_{\sigma\tau})$ for $\sigma \in G$, and $\sigma H\sigma^{-1} = H$ if and only if $\sigma\tau(L) = \tau(L)$ by Theorem 1.8 ($\Psi\circ\Phi = \mathrm{id}$). But $\{\,\rho \in \mathrm{Hom}_K(L,F) \mid \rho(L) = \tau(L)\,\} \ni \rho \mapsto \tau^{-1}\rho \in \mathrm{Aut}_K(L)$ is a bijection with the inverse $\nu \mapsto \tau\nu$, thus $G \rhd H$ if and only if $|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L,F)| = [L:K]$ (Corollary 1.6). Then $G \ni \sigma \mapsto \tau^{-1}\sigma\tau \in \mathrm{Aut}_K(L)$ is a surjective homomorphism with kernel H. □

2. Splitting fields

Definition 2.1. If $P \in K[X] \setminus K$ is irreducible, then (P) is a maximal ideal of $K[X]$ and $K_P := K[X]/(P)$ is an extension of K. Then $\overline{X} := X \bmod P$ is a root of P in K_P. If $\deg P = n$, then $\{1, \overline{X}, \overline{X}^2, \dots, \overline{X}^{n-1}\}$ is a K-basis of K_P, thus $[K_P : K] = \deg P$.

Definition 2.2. For an extension F_τ/K, we extend τ to $K[X] \to F[X]$. For $P \in K[X] \setminus K$, we denote the set of roots of τP in F by $\mathrm{Root}_P(F_\tau) = \mathrm{Root}_{\tau P}(F)$. Any morphism $f \in \mathrm{Hom}_K(F, F')$ restricts to $\mathrm{Root}_P(F) \to \mathrm{Root}_P(F')$.

Definition 2.3. Let F_τ/K be finite. For $x \in F$, the morphism $f_x : K[X] \ni X \mapsto x \in F$ of K-algebras has $\mathrm{Ker}\, f_x \neq 0$ and $\mathrm{Im}\, f_x$ is a domain. Hence $\mathrm{Ker}\,(f_x) = (P)$ for a irreducible monic $P \in K[X] \setminus K$, called the **minimal polynomial** of x over K.

Then $x \in \mathrm{Root}_P(F_\tau)$, and we have $f_x \in \mathrm{Hom}_K(K_P, F_\tau)$ with $f_x(\overline{X}) = x$. Also $K(x) := \mathrm{Im}\, f_x$ is a subextension of F/K, isomorphic to K_P. Thus $[K(x) : K] = \deg P$.

Lemma 2.4. *If F/K is finite and $P \in K[X]\setminus K$ is irreducible, then the map $\mathrm{Root}_P(F_\tau) \ni x \mapsto f_x \in \mathrm{Hom}_K(K_P, F_\tau)$ is a bijection with the inverse $f \mapsto f(\overline{X})$.*

Definition 2.5. We say $P \in K[X] \setminus K$ **splits** in an extension $F = F_\tau/K$ if τP is a product of linear factors in $F[X]$. If P splits in F'/K if and only if $\mathrm{Hom}_K(F, F') \neq \emptyset$, then we call F/K a **splitting field** of P over K.

If $Q \mid P$ in $K[X]$ and P splits in F/K then so does Q. If P splits in F/K and $f \in \mathrm{Hom}_K(F, F')$, then P splits in F'/K and f restricts to a bijection $\mathrm{Root}_P(F) \cong \mathrm{Root}_P(F')$. Any extension isomorphic to a splitting field of P is a splitting field of P.

Proposition 2.6. *For every $P \in K[X] \setminus K$, its splitting field over K exists and is unique up to isomorphism. It is a finite extension of K.*

Proof. We prove the existence by induction on $\deg P$. Let Q be an irreducible factor of P, and let $\alpha \in K_Q$ its root, so that $P = (X - \alpha)R$ in $K_Q[X]$. If F is a splitting field of R over K_Q (by induction hypothesis), then F/K is finite by Lemma 1.4(i). If P splits in F', then there exists $\tau \in \mathrm{Hom}_K(K_Q, F')$ by Lemma 2.4 because $\mathrm{Root}_Q(F') \neq \emptyset$, and $\mathrm{Hom}_{K_Q}(F, F'_\tau) \neq \emptyset$ as R splits in F'. Thus $\mathrm{Hom}_K(F, F') \neq \emptyset$ by Lemma 1.4(ii). If F''/K is also a splitting field of P, then $F \cong F''$ as extensions of K by Lemma 1.2. □

Definition 2.7. For a finite F/K and $x_1, \dots, x_n \in F$, we inductively define the subextensions $K(x_1, \dots, x_n) := K(x_1, \dots, x_{n-1})(x_n)$ of F/K. It is the intersection of all subextensions of F/K that contains $x_1, \dots, x_n$, hence is independent of the ordering of x_i. By Lemma 1.4(i) or taking a K-basis, there exist x_i with $F = K(x_1, \dots, x_n)$.

Proposition 2.8. *If P splits in F/K, then F/K has a unique subextension which is a splitting field of P, namely $K(x_1, \dots, x_n)/K$ where $\mathrm{Root}_P(F) = \{x_1, \dots, x_n\}$.*

Proof. Let F_0 be a splitting field of P. As P splits in $F' := K(x_1, \dots, x_n)$, there is $\tau \in \mathrm{Hom}_K(F_0, F')$, which restricts to $\mathrm{Root}_P(F_0) \cong \mathrm{Root}_P(F')$, hence is surjective and gives $\tau : F_0 \cong F'$. If F_0 a subextension of F/K, then $\mathrm{Root}_P(F_0) = \mathrm{Root}_P(F)$, thus $F' \subset F_0$ and $F' = F_0$. □

3. Separable extensions

Lemma 3.1. *If F/K is finite and E/K is arbitrary, then the following are equivalent:*

(i) $|\mathrm{Hom}_K(F,E)| = [F:K]$.
(ii) *If L, L' are subextensions of F/K with $L \subset L'$, then $|\mathrm{Hom}_L(L', E_\tau)| = [L':L]$ for all $\tau \in \mathrm{Hom}_K(L,E)$.*
(iii) *For $\forall x \in F$, its minimal polynomial P over K satisfies $|\mathrm{Root}_P(E)| = \deg P$.*
(iv) *There exist $x_1, \dots, x_n$ with $F = K(x_1, \dots, x_n)$ such that all x_i satisfy (iii).*

Proof. (i)⇒(ii): Proposition 1.5, Lemma 1.4. (ii)⇒(iii): Take $L = K$, $L' = K(x)$, use $[K(x) : K] = \deg P$ and Lemma 2.4. (iii)⇒(iv): Clear. (iv)⇒(i): Let $L_i := K(x_1, \dots, x_i)$, and Q_i the minimal polynomial of x_i over L_{i-1}. Then $Q_i \mid P_i$ in $L_{i-1}[X]$, hence $\tau Q_i \mid P_i$ in $E[X]$ for all $\tau \in \mathrm{Hom}_K(L_{i-1}, E)$, thus $|\mathrm{Hom}_{L_{i-1}}(L_i, E_\tau)| = |\mathrm{Root}_{\tau Q_i}(E)| = \deg Q_i = [L_i : L_{i-1}]$ (Lemma 2.4). Now use Lemma 1.4. □

Definition 3.2. We say $P \in K[X] \backslash K$ is **separable** if $|\mathrm{Root}_P(E)| = \deg P$ for some E/K. A finite F/K is **separable** if $|\mathrm{Hom}_K(F,E)| = [F:K]$ for some E/K (we say E/K **splits** F/K). If E'/K splits F/K if and only if $\mathrm{Hom}_K(E, E') \neq \emptyset$, then we say E/K is a **splitting field** of F/K. If F/K is Galois, then $E = F$.

If P is separable, then $|\mathrm{Root}_P(E')| = \deg P$ whenever P splits in E', because $f \in \mathrm{Hom}_K(E, E')$ for a splitting field E/K of P gives $\mathrm{Root}_P(E) \cong \mathrm{Root}_P(E')$. Any extension isomorphic to a splitting field of F/K is a splitting field of F/K.

Lemma 3.3. *Let $F = K(x_1, \dots, x_n)$, and suppose the minimal polynomials P_i of x_i over K are separable. Then a splitting field E/K of $P = P_1 \cdots P_n$ gives a splitting field of F/K. It is finite, and hence is unique up to isomorphism (by Lemma 1.2).*

Proof. As P_i is separable and splits in E, by Lemma 3.1(iv)⇒(i) E splits F. If E' splits F, then P splits in E' by Lemma 3.1(i)⇒(iii), thus $\mathrm{Hom}_K(E, E') \neq \emptyset$. □

Proposition 3.4. *Let F/K be a finite extension, and denote by P_x the minimal polynomial of $x \in F$ over K. The following are equivalent:*

(i) *F/K is separable (resp. Galois).*
(ii) *P_x is separable (resp. $|\mathrm{Root}_{P_x}(F)| = \deg P_x$) for every $x \in F$.*
(iii) *There exist $x_1, \dots, x_n \in F$ with $F = K(x_1, \dots, x_n)$ such that all x_i satisfy (ii).*

Proof. Sep.: Lemmas 3.1(i)⇒(iii), 3.3. Gal.: Lemma 3.1(i)⇔(iii)⇔(iv) for $E = F$. □

Theorem 3.5. *Splitting field E/K of $P \in K[X]$ is Galois if all irreducible factors of P are separable. In particular, a splitting field (Lemma 3.3) of a separable F/K is Galois.*

Proof. If $\mathrm{Root}_P(E) = \{x_1, \dots, x_n\}$ then $E = K(x_1, \dots, x_n)$ (Proposition 2.8). The minimal polynomials of x_i over K divide P, hence are separable and split in E. Use Proposition 3.4(iii)⇒(i). (Thus splitting fields of F/K are called **Galois closures**.) □

Let $P \in K[X]$ be separable with $\deg P = n \geq 1$ and F/K its splitting field. Then $\mathrm{Aut}_K(F)$ acts on $\mathrm{Root}_P(F) = \{x_1, \dots, x_n\}$, and as $F = K(x_1, \dots, x_n)$ (Proposition 2.8), an element $\sigma \in \mathrm{Aut}_K(F)$ is determined by $\sigma(x_1), \dots, \sigma(x_n)$, thus $\mathrm{Aut}_K(F)$ injects to $\mathrm{Aut}(\mathrm{Root}_P(F)) \cong \mathrm{Aut}(\{1, \dots, n\}) =: S_n$ (the **symmetric group** in n letters).

4. Cyclotomic and Kummer extensions

Definition 4.1. A Galois F/K is called **abelian** (resp. **cyclic**) if $\mathrm{Aut}_K(F)$ is such.

Definition 4.2. Let $n \geq 1$ and $(\mathrm{char}\, K, n) = 1$. A splitting field of $X^n - 1$ is denoted by $K(\boldsymbol{\mu}_n)/K$, and is called a **cyclotomic extension** of K. Let $\boldsymbol{\mu}_n := \mathrm{Roots}_{X^n-1}(K(\boldsymbol{\mu}_n))$.

As $X^n - 1$ has no multiple roots (Exercise a.2(ii)), its factors are all separable and $K(\boldsymbol{\mu}_n)/K$ is Galois by Theorem 3.5. As $\boldsymbol{\mu}_n$ is a finite subgroup of $K(\boldsymbol{\mu}_n)^\times$, it is cyclic of order n. Its generator is called a **primitive n-th root of unity**. There are $\varphi(n)$ of them, and if we denote one of them by ζ, they are written as $\zeta^k,\ k \in (\mathbb{Z}/(n))^\times$.

Theorem 4.3. *Let ζ be a primitive n-th root of unity in $K(\boldsymbol{\mu}_n)$, and P_ζ its minimal polynomial over K. Then all the roots of P_ζ in $K(\zeta)$ are primitive n-th roots of unity. There is an injective homomorphism as follows, and in particular $K(\boldsymbol{\mu}_n)/K$ is abelian:*

$$\mathrm{Aut}_K(K(\boldsymbol{\mu}_n)) \ni (\zeta \mapsto \zeta^k) \longmapsto k \bmod n \in (\mathbb{Z}/(n))^\times.$$

Proof. By $P_\zeta \mid X^n - 1$, all roots of P_ζ are in $\boldsymbol{\mu}_n$. For $d < n$, as ζ is not a root of $X^d - 1$, the P_ζ and $X^d - 1$ are coprime, thus all roots of P_ζ have order n in $\boldsymbol{\mu}_n$. Lemma 2.4 gives a bijection $\mathrm{Aut}_K(K(\zeta)) \ni \sigma \mapsto \sigma(\zeta) \in \mathrm{Root}_{P_\zeta}(K(\zeta)) \subset \{\zeta^k \mid k \in (\mathbb{Z}/(n))^\times\}$, thus the desired injection. It does not depend on the choice of ζ, and as the composite of $\zeta \mapsto \zeta^k$ and $\zeta \mapsto \zeta^l$ is $\zeta \mapsto \zeta^{kl}$, it is a group homomorphism. □

Let $n \geq 1$, $(\mathrm{char}\, K, n) = 1$ and $K(\boldsymbol{\mu}_n) = K$, i.e. $X^n - 1$ splits in K. For $a \in K^\times$ such that $P(X) := X^n - a$ is irreducible in $K[X]$, consider $F = K_P$. Denoting one root in F by $x = \sqrt[n]{a}$, and fixing a primitive n-th root of unity $\zeta \in K$, we have $\mathrm{Root}_P(F) = \{\zeta^i x \in F \mid 0 \leq i \leq n-1\}$ as they are distinct. Thus $F = K(x)/K$ is Galois (Proposition 3.4(iii)⇒(i)), and is cyclic by the isomorphism (Lemma 2.4):

$$\mathrm{Aut}_K(K(\sqrt[n]{a})) \ni (\sqrt[n]{a} \mapsto \zeta^i \sqrt[n]{a}) \longmapsto i \bmod n \in \mathbb{Z}/n\mathbb{Z}.$$

Definition 4.4. For a field K with $(\mathrm{char}\, K, n) = 1$, $\boldsymbol{\mu}_n \subset K$, a cyclic extension of degree n of the form $F = K(\sqrt[n]{a}) \cong K[X]/(X^n - a)$ is called a **Kummer extension**.

Theorem 4.5. (Kummer theory) *Let $n \geq 1$. Let K be a field with $(\mathrm{char}\, K, n) = 1$ and $\boldsymbol{\mu}_n \subset K$. Then every cyclic extension of degree n is a Kummer extension.*

Proof. Let F/K be cyclic of degree n, and choose a generator σ of $\mathrm{Aut}_K(F)$ and a primitive n-th root of unity $\zeta \in K$. By Proposition 1.5, there exist $\alpha \in F$ with $x := \sum_{j=1}^n \zeta^{-j}\sigma^j(\alpha) \neq 0$. Then $\sigma(x) = \zeta x$ and $\sigma(x^n) = \sigma(x)^n = x^n =: a$ is in $F^{\mathrm{Aut}_K(F)} = K$ (Theorem 1.8). As $\sigma^i(x) = \zeta^i x$ are all distinct $n \leq |\mathrm{Hom}_K(K(x), F)| \leq [K(x) : K] \leq n$ (Proposition 1.5), hence $F = K(x)$ and the minimal polynomial of x is $X^n - a$. □

Lemma 4.6. *Let L/K be a subextension of finite F/K. If $K(x)/K$ is Galois for $x \in F$, then $L(x)/L$ is Galois and $\mathrm{Aut}_L(L(x)) \ni \sigma \longmapsto \sigma|_{K(x)} \in \mathrm{Aut}_K(K(x))$ is injective.*

Proof. As the minimal polynomial of x over L divides that of x over K, by Proposition 3.4(iii)⇒(i) $L(x)/L$ is Galois. Injectivity: $\sigma \in \mathrm{Aut}_L(L(x))$ is determined by $\sigma(x)$. □

5. Soluble and radical extensions

Definition 5.1. A pair (G, G') of a finite group G and its subgroup G' is called **soluble** if there is a sequence (G_i) of subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = G'$ with $G_{i-1} \rhd G_i$ and G_{i-1}/G_i cyclic for all $1 \leq i \leq n$. We say G is **soluble** if $(G, \{1\})$ is.

Lemma 5.2. (i) *If $G \rhd H \supset G'$, then (G, G') : soluble $\iff$ (H, G'), G/H : soluble.* (ii) *Finite abelian groups are soluble.*

Proof. (i): Let $p : G \to G/H$ be the canonical surjection. If (G_i) is a sequence for (G, G'), then $(H \cap G_i), (p(G_i))$ give sequences for (H, G') and G/H. If $(H_i), (G_i)$ are sequences for (H, G') and G/H, combine (H_i) and $(p^{-1}(G_i))$. (ii): If $G \ni \sigma \neq 1$ and $H = \langle \sigma \rangle$, then H is cyclic and $|G/H| < |G|$. Use (i)$\Leftarrow$ and induction on $|G|$. □

Definition 5.3. A Galois F/K is called **soluble** if $\mathrm{Aut}_K(F)$ is soluble, and **radical** if there is a finite E/F where E/K is a succession of cyclotomic and Kummer extensions. A finite separable F/K is called **soluble/radical** if its splitting field is such.

Theorem 5.4. *If* $\mathrm{char}\, K = 0$*, then F/K : radical $\iff$ F/K : soluble.*

Proof. We can replace F/K by its splitting field and assume F/K is Galois. $\Rightarrow$: Let $E/F/K$ with E/K a tower of cyclotomic/Kummer extensions, and let E'/K be a splitting field of E/K. If $G := \mathrm{Aut}_K(E')$, $H := \mathrm{Aut}_F(E')$ and $G' := \mathrm{Aut}_E(E')$ then (G, G') is soluble by Lemma 5.2, Theorem 1.8 and Corollary 1.9, as cyclotomic/Kummer extensions are abelian. Thus $G/H \cong \mathrm{Aut}_K(F)$ is soluble by Lemma 5.2(i)$\Rightarrow$. $\Leftarrow$: Let F/K be Galois and $G := \mathrm{Aut}_K(F)$ soluble. Take a sequence (G_i) for G and the corresponding subextensions $K = K_0 \subset \cdots \subset K_m = F$ (Theorem 1.8), both of which we subdivide (each step remains cyclic by Corollary 1.9) so that $K_i = K_{i-1}(x_i)$ for all i. Let $n_i := |G_{i-1}/G_i|$ and $n := n_1 \cdots n_m$. By Lemma 4.6 $K_i(\boldsymbol{\mu}_n)/K_{i-1}(\boldsymbol{\mu}_n)$ is Galois with its group injecting to $\mathrm{Aut}_{K_{i-1}}(K_i) \cong G_{i-1}/G_i$ (Corollary 1.9), hence cyclic of degree dividing n and Kummer (Theorem 4.5). Thus $F(\boldsymbol{\mu}_n) = K_m(\boldsymbol{\mu}_n)/K$ is radical. □

Proposition 5.5. *Let $F = K(x_1, \ldots, x_n)$ be a field of rational functions of indeterminates $x_1, \ldots, x_n$. Let a_i be the i-th elementary symmetric polynomials of x_i, and let $L := K(a_1, \ldots, a_n)$ be the subfield of F consisting of all rational functions of a_i. If $P(X) = X^n + \sum_{i=1}^n (-1)^i a_i X^{n-i} \in L[X]$, then F/L is Galois with $\mathrm{Aut}_L(F) \cong S_n$.*

Proof. As $\mathrm{Root}_P(F) = \{x_1, \ldots, x_n\}$ and $F = L(x_1, \ldots, x_n)$, the F/L is a splitting field of P, thus Galois by Theorem 3.5, and $\mathrm{Aut}_L(F) \subset G := \mathrm{Aut}(\{x_1, \ldots, x_n\}) \cong S_n$. But G acts on F by permuting $x_1, \ldots, x_n$ and $L \subset F^G$, hence $G \subset \mathrm{Aut}_L(F)$. □

Theorem 5.6. *A general equation of degree $n \geq 5$ is not solvable by iterated radicals.*

Proof. As A_n is simple for $n \geq 5$, the group S_n is not soluble by Lemma 5.2(i)$\Rightarrow$. Now use Proposition 5.5 and Theorem 5.4$\Rightarrow$. □

Remark 5.7. A little more argument shows that a finite F/K is soluble as soon as there is a finite E/F where E/K is a succession of cyclotomic and Kummer extensions (essentially: $F'/F, F/K$ soluble implies F'/K soluble).

a. Appendix: Separability in characteristic zero

Definition a.1. The K-linear map $D : K[X] \to K[X]$ characterized by the following is called the **derivation** of $K[X]$: (i) $D(1) = 0$, (ii) $D(X^n) = nX^{n-1}$ $(n \in \mathbb{Z}_{>0})$.

Exercise a.2. (i) For $P, Q \in K[X]$, $D(PQ) = D(P)Q + D(Q)P$.
(ii) For $P \in K[X]$, $\alpha \in K$: a multiple root of $P \iff (X - \alpha) \mid P, D(P)$.

Lemma a.3. *Let $P \in K[X] \setminus K$. If P is irreducible, then P is separable if and only if $D(P) \neq 0$. In particular, if $\operatorname{char} K = 0$, every irreducible P is separable, hence every finite F/K is separable (Proposition 3.4(i)⇒(iii)).*

Proof. If $D(P) = 0$, all roots of P are multiple roots in any field. If $D(P) \neq 0$, as $\deg D(P) < \deg P$ and $D(P) \notin (P)$ in $K[X]$, $(P) + (D(P)) = K[X] \ni 1$ as (P) is a maximal ideal. If E is a splitting field of P, as $1 \in (P) + (D(P))$ remains true in $E[X]$, the linear factors of P cannot divide $D(P)$, i.e. there is no multiple root of P in E. □

Prerequisites: very basic linear algebra, groups/rings/fields, including: PID (non-zero prime ideals are maximal and generated by irreducibles), finite subgroups of multiplicative group of a field are cyclic, subgroups of cyclic groups, normal subgroups and quotient groups. A_n is simple.