

Part II — Galois Theory

Theorems with proof

Based on lectures by C. Birkar

Notes taken by Dexter Chua

Michaelmas 2015

These notes are not endorsed by the lecturers, and I have modified them (often significantly) after lectures. They are nowhere near accurate representations of what was actually lectured, and in particular, all errors are almost surely mine.

Groups, Rings and Modules is essential

Field extensions, tower law, algebraic extensions; irreducible polynomials and relation with simple algebraic extensions. Finite multiplicative subgroups of a field are cyclic. Existence and uniqueness of splitting fields. [6]

Existence and uniqueness of algebraic closure. [1]

Separability. Theorem of primitive element. Trace and norm. [3]

Normal and Galois extensions, automorphic groups. Fundamental theorem of Galois theory. [3]

Galois theory of finite fields. Reduction mod p . [2]

Cyclotomic polynomials, Kummer theory, cyclic extensions. Symmetric functions. Galois theory of cubics and quartics. [4]

Solubility by radicals. Insolubility of general quintic equations and other classical problems. [3]

Artin's theorem on the subfield fixed by a finite group of automorphisms. Polynomial invariants of a finite group; examples. [2]

Contents

0	Introduction	3
1	Solving equations	4
2	Field extensions	5
2.1	Field extensions	5
2.2	Ruler and compass constructions	7
2.3	K -homomorphisms and the Galois Group	8
2.4	Splitting fields	8
2.5	Algebraic closures	10
2.6	Separable extensions	12
2.7	Normal extensions	18
2.8	The fundamental theorem of Galois theory	20
2.9	Finite fields	22
3	Solutions to polynomial equations	25
3.1	Cyclotomic extensions	25
3.2	Kummer extensions	27
3.3	Radical extensions	29
3.4	Solubility of groups, extensions and polynomials	31
3.5	Insolubility of general equations of degree 5 or more	33
4	Computational techniques	37
4.1	Reduction mod p	37
4.2	Trace, norm and discriminant	37

0 Introduction

1 Solving equations

2 Field extensions

2.1 Field extensions

Theorem (Tower Law). Let $F/L/K$ be field extensions. Then

$$[F : K] = [F : L][L : K]$$

Proof. Assume $[F : L]$ and $[L : K]$ are finite. Let $\{\alpha_1, \dots, \alpha_m\}$ be a basis for L over K , and $\{\beta_1, \dots, \beta_n\}$ be a basis for F over L . Pick $\gamma \in F$. Then we can write

$$\gamma = \sum_i b_i \beta_i, \quad b_i \in L.$$

For each b_i , we can write as

$$b_i = \sum_j a_{ij} \alpha_j, \quad a_{ij} \in K.$$

So we can write

$$\gamma = \sum_i \left(\sum_j a_{ij} \alpha_j \right) \beta_i = \sum_{i,j} a_{ij} \alpha_j \beta_i.$$

So $T = \{\alpha_j \beta_i\}_{i,j}$ spans F over K . To show that this is a basis, we have to show that they are linearly independent. Consider the case where $\gamma = 0$. Then we must have $b_i = 0$ since $\{\beta_i\}$ is a basis of F over L . Hence each $a_{ij} = 0$ since $\{\alpha_j\}$ is a basis of L over K .

This implies that T is a basis of F over K . So

$$[F : K] = |T| = nm = [F : L][L : K].$$

Finally, if $[F : L] = \infty$ or $[L : K] = \infty$, then clearly $[F : K] = \infty$ as well. So equality holds as well. \square

Lemma. Let L/K be a finite extension. Then L is algebraic over K .

Proof. Let $n = [L : K]$, and let $\alpha \in L$. Then $1, \alpha, \alpha^2, \dots, \alpha^n$ are linearly dependent over K (since there are $n + 1$ elements). So there exists some $a_i \in K$ (not all zero) such that

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0.$$

So we have a non-trivial polynomial that vanishes at α . So α is algebraic over K .

Since α was arbitrary, L itself is algebraic. \square

Proposition. Let L/K be a field extension, $\alpha \in L$ algebraic over K , and P_α the minimal polynomial. Then P_α is irreducible in $K[t]$.

Proof. Assume that $P_\alpha = QR$ in $K[t]$. So $0 = P_\alpha(\alpha) = Q(\alpha)R(\alpha)$. So $Q(\alpha) = 0$ or $R(\alpha) = 0$. Say $Q(\alpha) = 0$. So $Q \in I_\alpha$. So Q is a multiple of P_α . However, we also know that P_α is a multiple of Q_α . This is possible only if R is a unit in $K[t]$, i.e. $R \in K$. So P_α is irreducible. \square

Theorem. Let L/K a field extension, $\alpha \in L$ algebraic. Then

- (i) $K(\alpha)$ is the image of the (ring) homomorphism $\phi : K[t] \rightarrow L$ defined by $f \mapsto f(\alpha)$.
- (ii) $[K(\alpha) : K] = \deg P_\alpha$, where P_α is the minimal polynomial of α over K .

Proof.

- (i) Let F be the image of ϕ . The first step is to show that F is indeed a field. Since F is the image of a ring homomorphism, we know F is a subring of L . Given $\beta \in F$ non-zero, we have to find an inverse.

By definition, $\beta = f(\alpha)$ for some $f \in K[t]$. The idea is to use Bézout's identity. Since $\beta \neq 0$, $f(\alpha) \neq 0$. So $f \notin I_\alpha = \langle P_\alpha \rangle$. So $P_\alpha \nmid f$ in $K[t]$. Since P_α is irreducible, P_α and f are coprime. Then there exists some $g, h \in K[t]$ such that $fg + hP_\alpha = 1$. So $f(\alpha)g(\alpha) = f(\alpha)g(\alpha) + h(\alpha)P_\alpha(\alpha) = 1$. So $\beta g(\alpha) = 1$. So β has an inverse. So F is a field.

From the definition of F , we have $K \subseteq F$ and $\alpha \in F$, using the constant polynomials $f = c \in K$ and the identity $f = t$.

Now, if $K \subseteq G \subseteq L$ and $\alpha \in G$, then G contains all the polynomial expressions of α . Hence $F \subseteq G$. So $K(\alpha) = F$.

- (ii) Let $n = \deg P_\alpha$. We show that $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K .

First note that since $\deg P_\alpha = n$, we can write

$$\alpha^n = \sum_{i=0}^{n-1} a_i \alpha^i.$$

So any other higher powers are also linear combinations of the α^i 's (by induction). This means that $K(\alpha)$ is spanned by $1, \dots, \alpha^{n-1}$ as a K vector space.

It remains to show that $\{1, \dots, \alpha^{n-1}\}$ is linearly independent. Assume not. Then for some b_i , we have

$$\sum_{i=0}^{n-1} b_i \alpha^i = 0.$$

Let $f = \sum b_i t^i$. Then $f(\alpha) = 0$. So $f \in I_\alpha = \langle P_\alpha \rangle$. However, $\deg f < \deg P_\alpha$. So we must have $f = 0$. So all $b_i = 0$. So $\{1, \dots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K . So $[K(\alpha) : K] = n$. \square

Corollary. Let L/K be a field extension, $\alpha \in L$. Then α is algebraic over K if and only if $K(\alpha)/K$ is a finite extension.

Proof. If α is algebraic, then $[K(\alpha) : K] = \deg P_\alpha < \infty$ by above. So the extension is finite.

If $K \subseteq K(\alpha)$ is a finite extension, then by previous lemma, the entire $K(\alpha)$ is algebraic over K . So α is algebraic over K . \square

Theorem. Suppose that L/K is a field extension.

- (i) If $\alpha_1, \dots, \alpha_n \in L$ are algebraic over K , then $K(\alpha_1, \dots, \alpha_n)/K$ is a finite extension.
- (ii) If we have field extensions $L/F/K$ and F/K is a finite extension, then $F = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in L$.

Proof.

- (i) We prove this by induction. Since α_1 is algebraic over K , $K \subseteq K(\alpha_1)$ is a finite extension.
For $1 \leq i < n$, α_{i+1} is algebraic over K . So α_{i+1} is also algebraic over $K(\alpha_1, \dots, \alpha_i)$. So $K(\alpha_1, \dots, \alpha_i) \subseteq K(\alpha_1, \dots, \alpha_i)(\alpha_{i+1})$ is a finite extension. But $K(\alpha_1, \dots, \alpha_i)(\alpha_{i+1}) = K(\alpha_1, \dots, \alpha_{i+1})$. By the tower law, $K \subseteq K(\alpha_1, \dots, \alpha_{i+1})$ is a finite extension.
- (ii) Since F is a finite dimensional vector space over K , we can take a basis $\{\alpha_1, \dots, \alpha_n\}$ of F over K . Then it should be clear that $F = K(\alpha_1, \dots, \alpha_n)$. \square

Proposition (Eisenstein's criterion). Let $f = a_n t^n + \dots + a_1 t + a_0 \in \mathbb{Z}[t]$. Assume that there is some prime number p such that

- (i) $p \mid a_i$ for all $i < n$.
- (ii) $p \nmid a_n$
- (iii) $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[t]$.

2.2 Ruler and compass constructions

Theorem. Let $S \subseteq \mathbb{R}^2$ be finite. Then

- (i) If R is 1-step constructible from S , then $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$ or 2 .
- (ii) If $T \subseteq \mathbb{R}^2$ is finite, $S \subseteq T$, and the points in T are constructible from S , Then $[\mathbb{Q}(S \cup T) : \mathbb{Q}(S)] = 2^k$ for some k (where k can be 0).

Proof. By assumption, there are distinct lines or circles C, C' constructed from S using ruler and compass, such that $R \in C \cap C'$. By elementary geometry, C and C' can be given by the equations

$$\begin{aligned} C &: a(x^2 + y^2) + bx + cy + d = 0, \\ C' &: a'(x^2 + y^2) + b'x + c'y + d' = 0. \end{aligned}$$

where $a, b, c, d, a', b', c', d' \in \mathbb{Q}(S)$. In particular, if we have a line, then we can take $a = 0$.

Let $R = (r_1, r_2)$. If $a = a' = 0$ (i.e. C and C' are lines), then solving the two linear equations gives $r_1, r_2 \in \mathbb{Q}(S)$. So $[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 1$.

So we can now assume wlog that $a \neq 0$. We let

$$p = a'b - ab', \quad q = a'c - ac', \quad \ell = a'd - ad',$$

which are the coefficients when we perform $a' \times C - a \times C'$. Then by assumption, $p \neq 0$ or $q \neq 0$. Otherwise, c and c' would be the same curve. wlog $p \neq 0$. Then since (r_1, r_2) satisfy both equations of C and C' , they satisfy

$$px + qy + \ell = 0.$$

In other words, $pr_1 + qr_2 + \ell = 0$. This tells us that

$$r_1 = -\frac{qr_2 + \ell}{p}. \quad (*)$$

If we put r_1, r_2 into the equations of C and C' and use $(*)$, we get an equation of the form

$$\alpha r_2^2 + \beta r_2 + \gamma = 0,$$

where $\alpha, \beta, \gamma \in \mathbb{Q}(S)$. So we can find r_2 (and hence r_1 using linear relations) using only a single radical of degree 2. So

$$[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = [\mathbb{Q}(S)(r_2) : \mathbb{Q}(S)] = 1 \text{ or } 2,$$

since the minimal polynomial of r_2 over $\mathbb{Q}(S)$ has degree 1 or 2.

Then (ii) follows directly from induction, using the tower law. \square

Corollary. It is impossible to “double the cube”.

Proof. Consider the cube with unit side length, i.e. we are given the set $S = \{(0, 0), (1, 0)\}$. Then doubling the cube would correspond to constructing a side of length ℓ such that $\ell^3 = 2$, i.e. $\ell = \sqrt[3]{2}$. Thus we need to construct a point $R = (\sqrt[3]{2}, 0)$ from S .

If we can indeed construct this R , then we need

$$[\mathbb{Q}(S \cup \{R\}) : \mathbb{Q}(S)] = 2^k$$

for some k . But we know that $\mathbb{Q}(S) = \mathbb{Q}$ and $\mathbb{Q}(S \cup \{R\}) = \mathbb{Q}(\sqrt[3]{2})$, and that

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3.$$

This is a contradiction since 3 is not a power of 2. \square

2.3 K -homomorphisms and the Galois Group

2.4 Splitting fields

Lemma. Let L/K be a field extension, $f \in K[t]$ irreducible, $\deg f > 0$. Then there is a 1-to-1 correspondence

$$\text{Root}_f(L) \longleftrightarrow \text{Hom}_K(K[t]/\langle f \rangle, L).$$

Proof. Since f is irreducible, $\langle f \rangle$ is a maximal ideal. So $K[t]/\langle f \rangle$ is a field. Also, there is a natural inclusion $K \hookrightarrow K[t]/\langle f \rangle$. So it makes sense to talk about $\text{Hom}_K(K[t]/\langle f \rangle, L)$.

To any $\beta \in \text{Root}_f(L)$, we assign $\phi : K[t]/\langle f \rangle \rightarrow L$ where we map $\bar{t} \mapsto \beta$ (\bar{t} is the equivalence class of t). This is well defined since if $\bar{t} = \bar{g}$, then $g = t + hf$ for some $h \in K[t]$. So $\phi(\bar{g}) = \phi(\overline{t + hf}) = \beta + h(\beta)f(\beta) = \beta$.

Conversely, given any K -homomorphism $\phi : K[t]/\langle f \rangle \rightarrow L$, we assign $\beta = \phi(\bar{t})$. This is a root since $f(\beta) = f(\phi(\bar{t})) = \phi(f(\bar{t})) = \phi(0) = 0$.

This assignments are inverses to each other. So we get a one-to-one correspondence. \square

Corollary. Let L/K be a field extension, $f \in K[t]$ irreducible, $\deg f > 0$. Then

$$|\mathrm{Hom}_K(K[t]/\langle f \rangle, L)| \leq \deg f.$$

In particular, if $E = K[t]/\langle f \rangle$, then

$$|\mathrm{Aut}_K(E)| = |\mathrm{Root}_f(E)| \leq \deg f = [E : K].$$

So E/K is a Galois extension iff $|\mathrm{Root}_f(E)| = \deg f$.

Proof. This follows directly from the following three facts:

- $|\mathrm{Root}_f(L)| \leq \deg f$
- $\mathrm{Aut}_K(E) = \mathrm{Hom}_K(E, E)$
- $\deg f = [K(\alpha) : K] = [E : K]$. □

Theorem. Let K be a field, $f \in K[t]$. Then

- (i) There is a splitting field of f .
- (ii) The splitting field is unique (up to K -isomorphism).

Proof.

- (i) If $\deg f = 0$, then K is a splitting field of f . Otherwise, we add the roots of f one by one.

Pick $g \mid f$ in $K[t]$, where g is irreducible and $\deg g > 0$. We have the field extension $K \subseteq K[t]/\langle g \rangle$. Let $\alpha_1 = \bar{t}$. Then $g(\alpha_1) = 0$ which implies that $f(\alpha_1) = 0$. Hence we can write $f = (t - \alpha_1)h$ in $K(\alpha_1)[t]$. Note that $\deg h < \deg f$. So we can repeat the process on h iteratively to get a field extensions $K \subseteq K(\alpha_1, \dots, \alpha_n)$. This $K(\alpha_1, \dots, \alpha_n)$ is a splitting field of f .

- (ii) Assume L and L' are both splitting fields of f over K . We want to find a K -isomorphism from L to L' .

Pick largest F, F' such that $K \subseteq F \subseteq L$ and $K \subseteq F' \subseteq L'$ are field extensions and there is a K -isomorphism from $\psi : F \rightarrow F'$. By “largest”, we mean we want to maximize $[F : K]$.

We want to show that we must have $F = L$. Then we are done because this means that F' is a splitting field, and hence $F' = L'$.

So suppose $F \neq L$. We will try to produce a larger \tilde{F} with K -isomorphism $\tilde{F} \rightarrow \tilde{F}' \subseteq L'$.

Since $F \neq L$, we know that there is some $\alpha \in \mathrm{Root}_f(L)$ such that $\alpha \notin F$. Then there is some irreducible $g \in K[t]$ with $\deg g > 0$ such that $g(\alpha) = 0$ and $g \mid f$. Say $f = gh$.

Now we know there is an isomorphism $F[t]/\langle g \rangle \rightarrow F(\alpha)$ by $\bar{t} \mapsto \alpha$. The isomorphism $\psi : F \rightarrow F'$ extends to a isomorphism $\mu : F[t] \rightarrow F'[t]$. Then since the coefficients of f are in K , we have $f = \mu(f) = \mu(g)\mu(h)$. So $\mu(g) \mid f$ in $F'[t]$. Since g is irreducible in $F[t]$, $\mu(g)$ is irreducible in $F'[t]$. So there is some $\alpha' \in \mathrm{Root}_{\mu(g)}(L') \subseteq \mathrm{Root}_f(L')$ and isomorphism $F'[t]/\langle \mu(g) \rangle \rightarrow F'(\alpha')$.

Now μ induces a K -isomorphism $F[t]/\langle g \rangle \rightarrow F'[t]/\langle \mu(g) \rangle$, which in turn induces a K -isomorphism $F(\alpha) \rightarrow F'(\alpha')$. This contradicts the maximality of F . So we must have had $F = L$. □

2.5 Algebraic closures

Lemma. If R is a commutative ring, then it has a maximal ideal. In particular, if I is an ideal of R , then there is a maximal ideal that contains I .

Proof. Let

$$\mathcal{P} = \{I : I \text{ is an ideal of } R, I \neq R\}.$$

If $I_1 \subseteq I_2 \subseteq \dots$ is any chain of $I_i \in \mathcal{P}$, then $I = \bigcup I_i \in \mathcal{P}$. By Zorn's lemma, there is a maximal element of \mathcal{P} (containing I). So R has at least one maximal ideal (containing I). \square

Theorem (Existence of algebraic closure). Any field K has an algebraic closure.

Proof. Let

$$\mathcal{A} = \{\lambda = (f, j) : f \in K[t] \text{ irreducible monic}, 1 \leq j \leq \deg f\}.$$

We can think of j as labelling which root of f we want. For each $\lambda \in \mathcal{A}$, we assign a variable t_λ . We take

$$R = K[t_\lambda : \lambda \in \mathcal{A}]$$

to be the polynomial ring over K with variables t_λ . This R contains all the "roots" of the polynomials in K . However, we've got a bit too much. For example, (if $K = \mathbb{Q}$), in R , $\sqrt{3}$ and $\sqrt{3} + 1$ would be put down as separate, unrelated variables. So we want to quotient this R by something.

For every monic and irreducible $f \in K[t]$, we define

$$\tilde{f} = f - \prod_{j=1}^{\deg f} (t - t_{(f,j)}) \in R[t].$$

If we want the $t_{(f,j)}$ to be roots of f , then \tilde{f} should vanish for all f . Denote the coefficient of t^ℓ in \tilde{f} by $b_{(f,\ell)}$. Then we want $b_{(f,\ell)} = 0$ for all f, ℓ .

To do so, let $I \subseteq R$ be the ideal generated by all such coefficients. We now want to quotient R by I . We first have to check that $I \neq R$.

Suppose not. So there are $b_{(f_1,\ell_1)}, \dots, b_{(f_r,\ell_r)}$ with $g_1, \dots, g_r \in R$ such that

$$g_1 b_{(f_1,\ell_1)} + \dots + g_r b_{(f_r,\ell_r)} = 1. \quad (*)$$

We will attempt to reach a contradiction by constructing a homomorphism ϕ that sends each $b_{(f_i,\ell_i)}$ to 0.

Let E be a splitting field of $f_1 f_2 \dots f_r$. So in $E[t]$, for each i , we can write

$$f_i = \prod_{j=1}^{\deg f_i} (t - \alpha_{i,j}).$$

Then we define a homomorphism $\phi : R \rightarrow E$ by

$$\begin{cases} \phi(t_{(f_i,j)}) = \alpha_{i,j} \\ \phi(t_\lambda) = 0 \end{cases} \quad \text{otherwise}$$

This induces a homomorphism $\tilde{\phi} : R[t] \rightarrow E[t]$.

Now apply

$$\begin{aligned}\tilde{\phi}(\tilde{f}_i) &= \tilde{\phi}(f_i) - \prod_{j=1}^{\deg f_i} \tilde{\phi}(t - t_{(f_i,j)}) \\ &= f_i - \prod_{j=1}^{\deg f_i} (t - \alpha_{i,j}) \\ &= 0\end{aligned}$$

So $\phi(b_{(f_i,\ell_i)}) = 0$ as $b_{(f_i,\ell_i)}$ is a coefficient of f_i .

Now we apply ϕ to (*) to obtain

$$\phi(g_1 b_{(f_1,\ell_1)} + \cdots + g_r b_{(f_r,\ell_r)}) = \phi(1).$$

But this is a contradiction since the left hand side is 0 while the right is 1. Hence we must have $I \neq R$.

We would like to quotient by I , but we have to be a bit more careful, since the quotient need not be a field. Instead, pick a maximal ideal M containing I , and consider $L = R/M$. Then L is a field. Moreover, since we couldn't have quotiented out anything in K (any ideal containing anything in K would automatically contain all of R), this is a field extension L/K . We want to show that L is an algebraic closure.

Now we show that L is algebraic over K . This should all work out smoothly, since that's how we constructed L . First we pick $\alpha \in L$. Since $L = R/M$ and R is generated by the terms t_λ , there is some $(f_1, j_1), \dots, (f_r, j_r)$ such that

$$\alpha \in K(\bar{t}_{(f_1,j_1)}, \dots, \bar{t}_{(f_r,j_r)}).$$

So α is algebraic over K if each $\bar{t}_{(f_i,j_i)}$ is algebraic over K . To show this, note that $\tilde{f}_i = 0$, since we've quotiented out each of its coefficients. So by definition,

$$0 = f_i(t) - \prod_{j=1}^{\deg f_i} (t - \bar{t}_{(f_i,j)}).$$

So $f_i(\bar{t}_{(f_i,j_i)}) = 0$. So done.

Finally, we have to show that L is algebraically closed. Suppose $L \subseteq E$ is a finite (and hence algebraic) extension. We want to show that $L = E$.

Consider arbitrary $\beta \in E$. Then β is algebraic over L , say a root of $f \in L[t]$. Since every coefficient of f can be found in some finite extension $K(\bar{t}_{(f_1,j_1)}, \dots, \bar{t}_{(f_r,j_r)})$, there is a finite extension F of K that contains all coefficients of f . Since $F(\beta)$ is a finite extension of F , we know $F(\beta)$ is a finite and hence algebraic extension of K . In particular, β is algebraic in K .

Let P_β be the minimal polynomial of β over K . Since all polynomials in K split over L by construction ($f(t) = \prod (t - \bar{t}_{(f,j)})$), its roots must be in L . In particular, $\beta \in L$. So $L = E$. \square

Theorem (Uniqueness of algebraic closure). Any field K has a unique algebraic closure up to K -isomorphism.

Proof. (sketch) Suppose L, L' are both algebraic closures of K . Let

$$\mathcal{H} = \{(F, \psi) : K \subseteq F \subseteq L, \psi \in \text{Hom}_K(F, L')\}.$$

We define a partial order on \mathcal{H} by $(F_1, \psi_1) \leq (F_2, \psi_2)$ if $F_1 \subseteq F_2$ and $\psi_1 = \psi_2|_{F_1}$.

We have to show that chains have upper bounds. Given a chain $\{(F_\alpha, \psi_\alpha)\}$, we define

$$F = \bigcup F_\alpha, \quad \psi(x) = \psi_\alpha(x) \text{ for } x \in F_\alpha.$$

Then $(F, \psi) \in \mathcal{H}$. Then applying Zorn's lemma, there is a maximal element of \mathcal{H} , say (F, ψ) .

Finally, we have to prove that $F = L$, and that $\psi(L) = L'$. Suppose $F \neq L$. Then we attempt to produce a larger \tilde{F} and a K -isomorphism $\tilde{F} \rightarrow \tilde{F}' \subseteq L'$. Since $F \neq L$, there is some $\alpha \in L \setminus F$. Since L is an algebraic extension of K , there is some irreducible $g \in K[t]$ such that $\deg g > 0$ and $g(\alpha) = 0$.

Now there is an isomorphism $F[t]/\langle g \rangle \rightarrow F(\alpha)$ defined by $\bar{t} \mapsto \alpha$. The isomorphism $\psi : F \rightarrow F'$ then extends to an isomorphism $\mu : F[t] \rightarrow F'[t]$ and thus to $\mathbb{F}[t]/\langle g \rangle \rightarrow F'[t]/\langle \mu(g) \rangle$. Then if α' is a root of $\mu(g)$, then we have $F'[t]/\langle \mu(g) \rangle \cong F'(\alpha')$. So this gives an isomorphism $F(\alpha) \rightarrow F(\alpha')$. This contradicts the maximality of ϕ .

By doing the argument the other way round, we must have $\psi(L) = L'$. So done. \square

2.6 Separable extensions

Lemma. Let K be a field, $f, g \in K[t]$. Then

- (i) $(f + g)' = f' + g'$, $(fg)' = fg' + f'g$.
- (ii) Assume $f \neq 0$ and L is a splitting field of f . Then f has a repeated root in L if and only if f and f' have a common (non-constant) irreducible factor in $K[t]$ (if and only if f and f' have a common root in L).

Proof.

- (i) $(f + g)' = f' + g'$ is true by linearity.

To show that $(fg)' = fg' + f'g$, we use linearity to reduce to the case where $f = t^n, g = t^m$. Then both sides are $(n + m)t^{n+m-1}$. So this holds.

- (ii) First assume that f has a repeated root. So let $f = (t - \alpha)^2 h \in L[t]$ where $\alpha \in L$. Then $f' = 2(t - \alpha)h + (t - \alpha)^2 h' = (t - \alpha)(2h + (t - \alpha)h')$. So $f(\alpha) = f'(\alpha) = 0$. So f and f' have common roots. However, we want a common irreducible factor in $K[t]$, not $L[t]$. So we let P_α be the minimal polynomial of α over K . Then $P_\alpha \mid f$ and $P_\alpha \mid f'$. So done.

Conversely, suppose e is a common irreducible factor of f and f' in $K[t]$, with $\deg e > 0$. Pick $\alpha \in \text{Root}_e(L)$. Then $\alpha \in \text{Root}_f(L) \cap \text{Root}_{f'}(L)$.

Since α is a root of f , we can write $f = (t - \alpha)q \in L[t]$ for some q . Then

$$f' = (t - \alpha)q' + q.$$

Since $(t - \alpha) \mid f'$, we must have $(t - \alpha) \mid q$. So $(t - \alpha)^2 \mid f$. \square

Corollary. Let K be a field, $f \in K[t]$ non-zero irreducible. Then

- (i) If $\text{char } K = 0$, then f is separable.
- (ii) If $\text{char } K = p > 0$, then f is not separable iff $\deg f > 0$ and $f \in K[t^p]$. For example, $t^{2p} + 3t^p + 1$ is not separable.

Proof. By definition, for irreducible f , f is not separable iff f has a repeated root. So by our previous lemma, f is not separable if and only if f and f' have a common irreducible factor of positive degree in $K[t]$. However, since f is irreducible, its only factors are 1 and itself. So this can happen if and only if $f' = 0$.

To make it more explicit, we can write

$$f = a_n t^n + \cdots + a_1 t + a_0.$$

Then we can write

$$f' = n a_n t^{n-1} + \cdots + a_1.$$

Now $f' = 0$ if and only if all coefficients $i a_i = 0$ for all i .

- (i) Suppose $\text{char } K = 0$, then if $\deg f = 0$, then f is trivially separable. If $\deg f > 0$, then f is not separable iff $f' = 0$ iff $i a_i = 0$ for all i iff $a_i = 0$ for $i \geq 1$. But we cannot have a polynomial of positive degree with all its coefficients zero (apart from the constant term). So f must be separable.
- (ii) If $\deg f = 0$, then f is trivially separable. So assume $\deg f > 0$.

Then f is not separable $\Leftrightarrow f' = 0 \Leftrightarrow i a_i = 0$ for $i \geq 0 \Leftrightarrow a_i = 0$ for all $i \geq 1$ not multiples of $p \Leftrightarrow f \in K[t^p]$. \square

Lemma. Let $L/F/K$ be finite extensions, and E/K be a field extension. Then for all $\alpha \in L$, we have

$$|\text{Hom}_K(F(\alpha), E)| \leq [F(\alpha) : F] |\text{Hom}_K(F, E)|.$$

Proof. We show that for each $\psi \in \text{Hom}_K(F, E)$, there are at most $[F(\alpha) : F]$ K -isomorphisms in $\text{Hom}_K(F(\alpha), E)$ that restrict to ψ in F . Since each K -isomorphism in $\text{Hom}_K(F(\alpha), E)$ has to restrict to something, it follows that there are at most $[F(\alpha) : F] |\text{Hom}_K(F, E)|$ K -homomorphisms from $F(\alpha)$ to E .

Now let P_α be the minimal polynomial for α in F , and let $\psi \in \text{Hom}_K(F, E)$. To extend ψ to a morphism $F(\alpha) \rightarrow E$, we need to decide where to send α . So there should be some sort of correspondence

$$\text{Root}_{P_\alpha}(E) \longleftrightarrow \{\phi \in \text{Hom}_K(F(\alpha), E) : \phi|_F = \psi\}.$$

Except that the previous sentence makes no sense, since $P_\alpha \in F[t]$ but we are not told that F is a subfield of E . So we use our ψ to “move” our things to E .

We let $M = \psi(F) \subseteq E$, and $q \in M[t]$ be the image of P_α under the homomorphism $F[t] \rightarrow M[t]$ induced by ψ . As we have previously shown, there is a one-to-one correspondence

$$\text{Root}_q(E) \longleftrightarrow \text{Hom}_M(M[t]/\langle q \rangle, E).$$

What we really want to show is the correspondence between $\text{Root}_q(E)$ and the K -homomorphisms $F[t]/\langle P_\alpha \rangle \rightarrow E$ that restrict to ψ on F . Let's ignore the quotient for the moment and think: what does it mean for $\phi \in \text{Hom}_K(F[t], E)$ to

restrict to ψ on F ? We know that any $\phi \in \text{Hom}_L(F[t], E)$ is uniquely determined by the values it takes on F and t . Hence if $\phi|_F = \psi$, then our ϕ must send F to $\psi(F) = M$, and can send t to anything in E . This corresponds exactly to the M -homomorphisms $M[t] \rightarrow E$ that does nothing to M and sends t to that “anything” in E .

The situation does not change when we put back the quotient. Changing from $M[t] \rightarrow E$ to $M[t]/\langle q \rangle \rightarrow E$ just requires that the image of t must be a root of q . On the other hand, using $F[t]/\langle P_\alpha \rangle$ instead of $F[t]$ requires that $\phi(P_\alpha(t)) = 0$. But we know that $\phi(P_\alpha) = \psi(P_\alpha) = q$. So this just requires $q(t) = 0$ as well. So we get the one-to-one correspondence

$$\text{Hom}_M(M[t]/\langle q \rangle, E) \longleftrightarrow \{\phi \in \text{Hom}_K(F[t]/\langle P_\alpha \rangle, E) : \phi|_F = \psi\}.$$

Since $F[t]/\langle P_\alpha \rangle = F(\alpha)$, there is a one-to-one correspondence

$$\text{Root}_q(E) \longleftrightarrow \{\phi \in \text{Hom}_K(F(\alpha), E) : \phi|_F = \psi\}.$$

So done. □

Theorem. Let L/K and E/K be field extensions. Then

- (i) $|\text{Hom}_K(L, E)| \leq [L : K]$. In particular, $|\text{Aut}_K(L)| \leq [L : K]$.
- (ii) If equality holds in (i), then for any intermediate field $K \subseteq F \subseteq L$:
 - (a) We also have $|\text{Hom}_K(F, E)| = [F : K]$.
 - (b) The map $\text{Hom}_K(L, E) \rightarrow \text{Hom}_K(F, E)$ by restriction is surjective.

Proof.

- (i) We have previously shown we can find a sequence of field extensions

$$K = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = L$$

such that for each i , there is some α_i such that $F_i = F_{i-1}(\alpha_i)$. Then by our previous lemma, we have

$$\begin{aligned} |\text{Hom}_K(L, E)| &\leq [F_n : F_{n-1}] |\text{Hom}_K(F_{n-1}, E)| \\ &\leq [F_n : F_{n-1}] [F_{n-1} : F_{n-2}] |\text{Hom}_K(F_{n-2}, E)| \\ &\quad \vdots \\ &\leq [F_n : F_{n-1}] [F_{n-1} : F_{n-2}] \cdots [F_1 : F_0] |\text{Hom}_K(F_0, E)| \\ &= [F_n : F_0] \\ &= [L : K] \end{aligned}$$

- (ii) (a) If equality holds in (i), then every inequality in the proof above has to an equality. Instead of directly decomposing $K \subseteq L$ as a chain above, we can first decompose $K \subseteq F$, then $F \subseteq L$, then join them together. Then we can assume that $F = F_i$ for some i . Then we get

$$|\text{Hom}_K(L, E)| = [L : F] |\text{Hom}_K(F, E)| = [L : K].$$

Then the tower law says

$$|\text{Hom}_K(F, E)| = [F : K].$$

(b) By the proof of the lemma, for each $\psi \in \text{Hom}_K(F, E)$, we know that

$$\{\phi : \text{Hom}_K(L, E) : \phi|_F = \psi\} \leq [L : F]. \quad (*)$$

As we know that

$$|\text{Hom}_K(F, E)| = [F : K], \quad |\text{Hom}_K(L, E)| = [L : K]$$

we must have had equality in (*), or else we won't have enough elements. So in particular $\{\phi : \text{Hom}_K(L, E) : \phi|_F = \psi\} \geq 1$. So the map is surjective. \square

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

- (i) There is some extension E of K such that $|\text{Hom}_K(L, E)| = [L : K]$.
- (ii) L/K is separable.
- (iii) $L = K(\alpha_1, \dots, \alpha_n)$ such that P_{α_i} , the minimal polynomial of α_i over K , is separable for all i .
- (iv) $L = K(\alpha_1, \dots, \alpha_n)$ such that R_{α_i} , the minimal polynomial of α_i over $K(\alpha_1, \dots, \alpha_{i-1})$ is separable for all i .

Proof.

- (i) \Rightarrow (ii): For all $\alpha \in L$, if P_α is the minimal polynomial of α over K , then since $K(\alpha)$ is a subfield of L , by our previous theorem, we have

$$|\text{Hom}_K(K(\alpha), E)| = [K(\alpha) : K].$$

We also know that $|\text{Root}_{P_\alpha}(E)| = |\text{Hom}_K(K(\alpha), E)|$, and that $[K(\alpha) : K] = \deg P_\alpha$. So we know that P_α has no repeated roots in any splitting field. So P_α is a separable. So L/K is a separable extension.

- (ii) \Rightarrow (iii): Obvious from definition
- (iii) \Rightarrow (iv): Since R_{α_i} is a minimal polynomial in $K(\alpha_1, \dots, \alpha_{i-1})$, we know that $R_{\alpha_i} \mid P_{\alpha_i}$. So R_{α_i} is separable as P_{α_i} is separable.
- (iv) \Rightarrow (i): Let E be the splitting field of $P_{\alpha_1}, \dots, P_{\alpha_n}$. We do induction on n to show that this satisfies the properties we want. If $n = 1$, then $L = K(\alpha_1)$. Then we have

$$|\text{Hom}_K(L, E)| = |\text{Root}_{P_{\alpha_1}}(E)| = \deg P_{\alpha_1} = [K(\alpha_1) : K] = [L : K].$$

We now induct on n . So we can assume that (iv) \Rightarrow (i) holds for smaller number of generators. For convenience, we write $K_i = K(\alpha_1, \dots, \alpha_i)$. Then we have

$$|\text{Hom}_K(K_{n-1}, E)| = [K_{n-1} : K].$$

We also know that

$$|\text{Hom}_K(K_n, E)| \leq [K_n : K_{n-1}] |\text{Hom}_K(K_{n-1}, E)|.$$

What we actually want is equality. We now re-do (parts of) the proof of this result, and see that separability guarantees that equality holds. If

we pick $\psi \in \text{Hom}_K(K_{n-1}, E)$, then there is a one-to-one correspondence between $\{\phi \in \text{Hom}_K(K_n, E) : \phi|_{K_{n-1}} = \psi\}$ and $\text{Root}_q(E)$, where $q \in M[t]$ is defined as the image of R_{α_n} under $K_{n-1}[t] \rightarrow M[t]$, and M is the image of ψ .

Since $P_{\alpha_n} \in K[t]$ and $R_{\alpha_n} \mid P_{\alpha_n}$, then $q \mid P_{\alpha_n}$. So q splits over E . By separability assumption, we get that

$$|\text{Root}_q(E)| = \deg q = \deg R_{\alpha_n} = [K_n : K_{n-1}].$$

Hence we know that

$$\begin{aligned} |\text{Hom}_K(L, E)| &= [K_n : K_{n-1}] |\text{Hom}_K(K_{n-1}, E)| \\ &= [K_n : K_{n-1}] [K_{n-1} : K] \\ &= [K_n : K]. \end{aligned}$$

So done. \square

Lemma. Let L be a field, $L^* = L \setminus \{0\}$ be the multiplicative group of L . If G is a finite subgroup of L^* , then G is cyclic.

Proof. Since L^* is abelian, G is also abelian. Then by the structure theorem on finite abelian groups,

$$G \cong \frac{\mathbb{Z}}{\langle n_1 \rangle} \times \cdots \times \frac{\mathbb{Z}}{\langle n_r \rangle},$$

for some $n_i \in \mathbb{N}$. Let m be the least common multiple of n_1, \dots, n_r , and let $f = t^m - 1$.

If $\alpha \in G$, then $\alpha^m = 1$. So $f(\alpha) = 0$ for all $\alpha \in G$. Therefore

$$|G| = n_1 \cdots n_r \leq |\text{Root}_f(L)| \leq \deg f = m.$$

Since m is the least common multiple of n_1, \dots, n_r , we must have $m = n_1 \cdots n_r$ and thus $(n_i, n_j) = 1$ for all $i \neq j$. Then by the Chinese remainder theorem, we have

$$G \cong \frac{\mathbb{Z}}{\langle n_1 \rangle} \times \cdots \times \frac{\mathbb{Z}}{\langle n_r \rangle} = \frac{\mathbb{Z}}{\langle n_1 \cdots n_r \rangle}.$$

So G is cyclic. \square

Theorem (Primitive element theorem). Assume L/K is a finite and separable extension. Then L/K is simple, i.e. there is some $\alpha \in L$ such that $L = K(\alpha)$.

Proof. At some point in our proof, we will require that L is infinite. So we first do the finite case first. If K is finite, then L is also finite, which in turn implies L^* is finite too. So by the lemma, L^* is a cyclic group (since it is a finite subgroup of itself). So there is some $\alpha \in L^*$ such that every element in L^* is a power of α . So $L = K(\alpha)$.

So focus on the case where K is infinite. Also, assume $K \neq L$. Then since L/K is a finite extension, there is some intermediate field $K \subseteq F \subsetneq L$ such that $L = F(\beta)$ for some β . Now L/K is separable. So F/K is also separable, and $[F : K] < [L : K]$. Then by induction on degree of extension, we can assume F/K is simple. In other words, there is some $\lambda \in F$ such that $F = K(\lambda)$. Now $L = K(\lambda, \beta)$. In the rest of the proof, we will try to replace the two generators λ, β with just a single generator.

Unsurprisingly, the generator of L will be chosen to be a linear combination of β and λ . We set

$$\alpha = \beta + a\lambda$$

for some $a \in K$ to be chosen later. We will show that $K(\alpha) = L$. Actually, almost any choice of a will do, but at the end of the proof, we will see which ones are the bad ones.

Let P_β and P_λ be the minimal polynomial of β and λ over K respectively. Consider the polynomial $f = P_\beta(\alpha - at) \in K(\alpha)[t]$. Then we have

$$f(\lambda) = P_\beta(\alpha - a\lambda) = P_\beta(\beta) = 0.$$

On the other hand, $P_\lambda(\lambda) = 0$. So λ is a common root of P_λ and f .

We now want to pick an a such that λ is the *only* common root of f and P_λ (in E). If so, then the gcd of f and P_λ in $K(\alpha)$ must only have λ as a root. But since P_λ is separable, it has no double roots. So the gcd must be $t - \lambda$. In particular, we must have $\lambda \in K(\alpha)$. Since $\alpha = \beta + a\lambda$, it follows that $\beta \in K(\alpha)$ as well, and so $K(\alpha) = L$.

Thus, it remains to choose an a such that there are no other common roots. We work in a splitting field of $P_\beta P_\lambda$, and write

$$\begin{aligned} P_\beta &= (t - \beta_1) \cdots (t - \beta_m) \\ P_\lambda &= (t - \lambda_1) \cdots (t - \lambda_n). \end{aligned}$$

We wlog $\beta_1 = \beta$ and $\lambda_1 = \lambda$.

Now suppose θ is a common root of f and P_λ . Then

$$\begin{cases} f(\theta) = 0 \\ P_\lambda(\theta) = 0 \end{cases} \Rightarrow \begin{cases} P_\beta(\alpha - a\theta) = 0 \\ P_\lambda(\theta) = 0 \end{cases} \Rightarrow \begin{cases} \alpha - a\theta = \beta_i \\ \theta = \lambda_j \end{cases}$$

for some i, j . Then we know that

$$\alpha = \beta_i + a\lambda_j.$$

However, by definition, we also know that

$$\alpha = \beta + a\lambda$$

Now we see how we need to choose a . We need to choose a such that the elements

$$\beta + a\lambda \neq \beta_i + a\lambda_j$$

for all i, j . But if they were equal, then we have

$$a = \frac{\lambda - \lambda_j}{\beta_i - \beta},$$

and there are only finitely many elements of this form. So we just have to pick an a *not* in this list. \square

Corollary. Any finite extension L/K of field of characteristic 0 is simple, i.e. $L = K(\alpha)$ for some $\alpha \in L$.

Proof. This follows from the fact that all extensions of fields of characteristic zero are separable. \square

Proposition. Let L/K be an extension of finite fields. Then the extension is separable.

Proof. Let the characteristic of the fields be p . Suppose the extension were not separable. Then there is some non-separable element $\alpha \in L$. Then its minimal polynomial must be of the form $P_\alpha = \sum a_i t^{pi}$.

Now note that the map $K \rightarrow K$ given by $x \mapsto x^p$ is injective, hence surjective. So we can write $a_i = b_i^p$ for all i . Then we have

$$P_\alpha = \sum a_i t^{pi} = \left(\sum b_i t^i \right)^p,$$

and so P_α is not irreducible, which is a contradiction. \square

2.7 Normal extensions

Lemma. Let $L/F/K$ be finite extensions, and \bar{K} is the algebraic closure of K . Then any $\psi \in \text{Hom}_K(F, \bar{K})$ extends to some $\phi \in \text{Hom}_K(L, \bar{K})$.

Proof. Let $\psi \in \text{Hom}_K(F, \bar{K})$. If $F = L$, then the statement is trivial. So assume $L \neq F$.

Pick $\alpha \in L \setminus F$. Let $q_\alpha \in F[t]$ be the minimal polynomial of α over F . Consider $\psi(q_\alpha) \in \bar{K}[t]$. Let β be any root of q_α , which exists since \bar{K} is algebraically closed. Then as before, we can extend ψ to $F(\alpha)$ by sending α to β . More explicitly, we send

$$\sum_{i=0}^N a_i \alpha^i \mapsto \sum \psi(a_i) \beta^i,$$

which is well-defined since any polynomial relation satisfied by α in F is also satisfied by β .

Repeat this process finitely many times to get some element in $\text{Hom}_K(L, \bar{K})$. \square

Theorem. Let L/K be a finite extension. Then L/K is a normal extension if and only if L is the splitting field of some $f \in K[t]$.

Proof. Suppose L/K is normal. Since L is finite, let $L = K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_i \in L$. Let P_{α_i} be the minimal polynomial of α_i over K . Take $f = P_{\alpha_1} \cdots P_{\alpha_n}$. Since L/K is normal, each P_{α_i} splits over L . So f splits over L , and L is a splitting field of f .

For the other direction, suppose that L is the splitting field of some $f \in K[t]$. First we wlog assume $L \subseteq \bar{K}$. This is possible since the natural injection $K \hookrightarrow \bar{K}$ extends to some $\phi : L \rightarrow \bar{K}$ by our previous lemma, and we can replace L with $\phi(L)$.

Now suppose $\beta \in L$, and let P_β be its minimal polynomial. Let β' be another root. We want to show it lives in L .

Now consider $K(\beta)$. By the proof of the lemma, we can produce an embedding $\iota : K(\beta) \rightarrow \bar{K}$ that sends β to β' . By the lemma again, this extends to an

embedding of L into \bar{K} . But any such embedding must send a root of f to a root of f . So it must send L to L . In particular, $\iota(\beta) = \beta' \in L$. So P_β splits over L . \square

Theorem. Let L/K be a finite extension. Then the following are equivalent:

- (i) L/K is a Galois extension.
- (ii) L/K is separable and normal.
- (iii) $L = K(\alpha_1, \dots, \alpha_n)$ and P_{α_i} , the minimal polynomial of α_i over K , is separable and splits over L for all i .

Proof.

- (i) \Rightarrow (ii): Suppose L/K is a Galois extension. Then by definition, this means

$$|\mathrm{Hom}_K(L, L)| = |\mathrm{Aut}_K(L)| = [L : K].$$

To show that L/K is separable, recall that we proved that an extension is separable if and only if there is some E such that $|\mathrm{Hom}_K(L, E)| = [L : K]$. In this case, just pick $E = L$. Then we know that the extension is separable.

To check normality, let $\alpha \in L$, and let P_α be its minimal polynomial over K . We know that

$$|\mathrm{Root}_{P_\alpha}(L)| = |\mathrm{Hom}_K(K[t]/\langle P_\alpha \rangle, L)| = |\mathrm{Hom}_K(K(\alpha), L)|.$$

But since $|\mathrm{Hom}_K(L, L)| = [L : K]$ and $K(\alpha)$ is a subfield of L , this implies

$$|\mathrm{Hom}_K(K(\alpha), L)| = [K(\alpha) : K] = \deg P_\alpha.$$

Hence we know that

$$|\mathrm{Root}_{P_\alpha}(L)| = \deg P_\alpha.$$

So P_α splits over L .

- (ii) \Rightarrow (iii): Just pick $\alpha_1, \dots, \alpha_n$ such that $L = K(\alpha_1, \dots, \alpha_n)$. Then these polynomials are separable since the extension is separable, and they split since L/K is normal. In fact, by the primitive element theorem, we can pick these such that $n = 1$.
- (iii) \Rightarrow (i): Since $L = K(\alpha_1, \dots, \alpha_n)$ and the minimal polynomials P_{α_i} over K are separable, by a previous theorem, there are some extension E of K such that

$$|\mathrm{Hom}_K(L, E)| = [L : K].$$

To simplify notation, we first replace L with its image inside E under some K -homomorphism $L \rightarrow E$, which exists since $|\mathrm{Hom}_K(L, E)| = [L : K] > 0$. So we can assume $L \subseteq E$.

We now claim that the inclusion

$$\mathrm{Hom}_K(L, L) \rightarrow \mathrm{Hom}_K(L, E)$$

is a surjection, hence a bijection. Indeed, if $\phi : L \rightarrow E$, then ϕ takes α_i to $\phi(\alpha_i)$, which is a root of P_{α_i} . Since P_{α_i} splits over L , we know $\phi(\alpha_i) \in L$ for all i . Since L is generated by these α_i , it follows that $\phi(L) \subseteq L$.

Thus, we have

$$[L : K] = |\mathrm{Hom}_K(L, E)| = |\mathrm{Hom}_K(L, L)|,$$

and the extension is Galois. \square

Corollary. Let K be a field and $f \in K[t]$ be a separable polynomial. Then the splitting field of f is Galois.

2.8 The fundamental theorem of Galois theory

Lemma (Artin's lemma). Let L/K be a field extension and $H \leq \mathrm{Aut}_K(L)$ a finite subgroup. Then L/L^H is a Galois extension with $\mathrm{Aut}_{L^H}(L) = H$.

Proof. Pick any $\alpha \in L$. We set

$$\{\alpha_1, \dots, \alpha_n\} = \{\phi(\alpha) : \phi \in H\},$$

where α_i are distinct. Here we are allowing for the possibility that $\phi(\alpha) = \psi(\alpha)$ for some distinct $\phi, \psi \in H$.

By definition, we clearly have $n < |H|$. Let

$$f = \prod_1^n (t - \alpha_i) \in L[t].$$

We know that any $\phi \in H$ gives an homomorphism $L[t] \rightarrow L[t]$, and any such map fixes f because ϕ just permutes the α_i . Thus, the coefficients of f are in L^H , and thus $f \in L^H[t]$.

Since $\mathrm{id} \in H$, we know that $f(\alpha) = 0$. So α is algebraic over L^H . Moreover, if q_α is the minimal polynomial of α over L^H , then $q_\alpha \mid f$ in $L^H[t]$. Hence

$$[L^H(\alpha) : L^H] = \deg q_\alpha \leq \deg f \leq |H|.$$

Further, we know that f has distinct roots. So q_α is separable, and so α is separable. So it follows that L/L^H is a separable extension.

We next show that L/L^H is simple. This doesn't immediately follow from the primitive element theorem, because we don't know it is a finite extension yet, but we can still apply the theorem cleverly.

Pick $\alpha \in L$ such that $[L^H(\alpha) : L^H]$ is maximal. This is possible since $[L^H(\alpha) : L^H]$ is bounded by $|H|$. The claim is that $L = L^H(\alpha)$.

We pick an arbitrary $\beta \in L$, and will show that this is in $L^H(\alpha)$. By the above arguments, $L^H \subseteq L^H(\alpha, \beta)$ is a finite separable extension. So by the primitive element theorem, there is some $\lambda \in L$ such that $L^H(\alpha, \beta) = L^H(\lambda)$. Note that we must have

$$[L^H(\lambda) : L^H] \geq [L^H(\alpha) : L^H].$$

By maximality of $[L^H(\alpha) : L^H]$, we must have equality. So $L^H(\lambda) = L^H(\alpha)$. So $\beta \in L^H(\alpha)$. So $L = L^H(\alpha)$.

Finally, we show it is a Galois extension. Let $L = L^H(\alpha)$. Then

$$[L : L^H] = [L^H(\alpha) : L^H] \leq |H| \leq |\mathrm{Aut}_{L^H}(L)|$$

Recall that we have previously shown that for any extension L/L^H , we have $|\text{Aut}_{L^H}(L)| \leq [L : L^H]$. Hence we must have equality above. So

$$[L : L^H] = |\text{Aut}_{L^H}(L)|.$$

So the extension is Galois. Also, since we know that $H \subseteq \text{Aut}_{L^H}(L)$, we must have $H = \text{Aut}_{L^H}(L)$. \square

Theorem. Let L/K be a finite field extension. Then L/K is Galois if and only if $L^H = K$, where $H = \text{Aut}_K(L)$.

Proof. (\Rightarrow) Suppose L/K is a Galois extension. We want to show $L^H = K$. Using Artin's lemma (and the definition of H), we have

$$[L : K] = |\text{Aut}_K(L)| = |H| = |\text{Aut}_{L^H}(L)| = [L : L^H]$$

So $[L : K] = [L : L^H]$. So we must have $L^H = K$.

(\Leftarrow) By the lemma, $K = L^H \subseteq L$ is Galois. \square

Theorem (Fundamental theorem of Galois theory). Assume L/K is a (finite) Galois extension. Then

- (i) There is a one-to-one correspondence

$$H \leq \text{Aut}_K(L) \longleftrightarrow \text{intermediate fields } K \subseteq F \subseteq L.$$

This is given by the maps $H \mapsto L^H$ and $F \mapsto \text{Aut}_F(L)$ respectively. Moreover, $|\text{Aut}_K(L) : H| = [L^H : K]$.

- (ii) $H \leq \text{Aut}_K(L)$ is normal (as a subgroup) if and only if L^H/K is a normal extension if and only if L^H/K is a Galois extension.
- (iii) If $H \triangleleft \text{Aut}_K(L)$, then the map $\text{Aut}_K(L) \rightarrow \text{Aut}_K(L^H)$ by the restriction map is well-defined and surjective with kernel isomorphic to H , i.e.

$$\frac{\text{Aut}_K(L)}{H} = \text{Aut}_K(L^H).$$

Proof. Note that since L/K is a Galois extension, we know

$$|\text{Aut}_K(L)| = |\text{Hom}_K(L, L)| = [L : K],$$

By a previous theorem, for any intermediate field $K \subseteq F \subseteq L$, we know $|\text{Hom}_K(F, L)| = [F : K]$ and the restriction map $\text{Hom}_K(L, L) \rightarrow \text{Hom}_K(F, L)$ is surjective.

- (i) The maps are already well-defined, so we just have to show that the maps are inverses to each other. By Artin's lemma, we know that $H = \text{Aut}_{L^H}(L)$, and since L/F is a Galois extension, the previous theorem tells that $L^{\text{Aut}_F(L)} = F$. So they are indeed inverses. The formula relating the index and the degree follows from Artin's lemma.

- (ii) Note that for every $\phi \in \text{Aut}_K(L)$, we have that $L^{\phi H \phi^{-1}} = \phi L^H$, since $\alpha \in L^{\phi H \phi^{-1}}$ iff $\phi(\psi(\phi^{-1}(\alpha))) = \alpha$ for all $\psi \in H$ iff $\psi(\phi^{-1}(\alpha)) = \phi^{-1}(\alpha)$ for all $\psi \in H$ iff $\alpha \in \phi L^H$. Hence H is a normal subgroup if and only if

$$\phi(L^H) = L^H \text{ for all } \phi \in \text{Aut}_K(L). \quad (*)$$

Assume (*). We want to first show that $\text{Hom}_K(L^H, L^H) = \text{Hom}_K(L^H, L)$. Let $\psi \in \text{Hom}_K(L^H, L)$. Then by the surjectivity of the restriction map $\text{Hom}_K(L, L) \rightarrow \text{Hom}_K(L^H, L)$, ψ must be the restriction of some $\tilde{\psi} \in \text{Hom}_K(L, L)$. So $\tilde{\psi}$ fixes L^H by (*). So ψ sends L^H to L^H . So $\psi \in \text{Hom}_K(L^H, L^H)$. So we have

$$|\text{Aut}_K(L^H)| = |\text{Hom}_K(L^H, L^H)| = |\text{Hom}_K(L^H, L)| = [L^H : K].$$

So L^H/K is Galois, and hence normal.

Now suppose L^H/K is a normal extension. We want to show this implies (*). Pick any $\alpha \in L^H$ and $\phi \in \text{Aut}_K(L)$. Let P_α be the minimal polynomial of α over K . So $\phi(\alpha)$ is a root of P_α (since ϕ fixes $P_\alpha \in K$, and hence maps roots to roots). Since L^H/K is normal, P_α splits over L^H . This implies that $\phi(\alpha) \in L^H$. So $\phi(L^H) = L^H$.

Hence, H is a normal subgroup if and only if $\phi(L^H) = L^H$ if and only if L^H/K is a Galois extension.

- (iii) Suppose H is normal. We know that $\text{Aut}_K(L) = \text{Hom}_K(L, L)$ restricts to $\text{Hom}_K(L^H, L)$ surjectively. To show that we in fact have restriction to $\text{Aut}_K(L^H)$, by the proof above, we know that $\phi(L^H) = L^H$ for all $\phi \in \text{Aut}_K(L)$. So this does restrict to an automorphism of L^H . In other words, the map $\text{Aut}_K(L) \rightarrow \text{Aut}_K(L^H)$ is well-defined. It is easy to see this is a group homomorphism.

Finally, we have to calculate the kernel of this homomorphism. Let E be the kernel. Then by definition, $E \supseteq H$. So it suffices to show that $|E| = |H|$. By surjectivity of the map and the first isomorphism theorem of groups, we have

$$\frac{|\text{Aut}_K(L)|}{|E|} = |\text{Aut}_K(L^H)| = [L^H : K] = \frac{[L : K]}{[L : L^H]} = \frac{|\text{Aut}_K(L)|}{|H|},$$

noting that L^H/K and L/K are both Galois extensions, and $|H| = [L^H : K]$ by Artin's lemma. So $|E| = |H|$. So we must have $E = H$. \square

2.9 Finite fields

Lemma. Let K be a finite field with $q = |K|$ element. Then

- (i) $q = p^d$ for some $d \in \mathbb{N}$, where $p = \text{char } K > 0$.
- (ii) Let $f = t^q - t$. Then $f(\alpha) = 0$ for all $\alpha \in K$. Moreover, K is the splitting field of f over \mathbb{F}_p .

Proof.

- (i) Consider the set $\{m \cdot 1_K\}_{m \in \mathbb{Z}}$, where 1_K is the unit in K and $m \cdot$ represents repeated addition. We can identify this with \mathbb{F}_p . So we have the extension $\mathbb{F}_p \subseteq K$. Let $d = [K : \mathbb{F}_p]$. Then $q = |K| = p^d$.
- (ii) Note that $K^* = K \setminus \{0\}$ is a finite multiplicative group with order $q - 1$. Then by Lagrange's theorem, $\alpha^{q-1} = 1$ for all $\alpha \in K^*$. So $\alpha^q - \alpha = 0$ for all $\alpha \neq 0$. The $\alpha = 0$ case is trivial.

Now every element in K is a root of f . So we need to check that all roots of f are in K . Note that the derivative $f' = qt^{q-1} - 1 = -1$ (since q is a power of the characteristic). So $f'(\alpha) = -1 \neq 0$ for all $\alpha \in K$. So f and f' have no common roots. So f has no repeated roots. So K contains q distinct roots of f . So K is a splitting field. \square

Lemma. Let $q = p^d$, $q' = p^{d'}$, where $d, d' \in \mathbb{N}$. Then

- (i) There is a finite field K with exactly q elements, which is unique up to isomorphism. We write this as \mathbb{F}_q .
- (ii) We can embed $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ iff $d \mid d'$.

Proof.

- (i) Let $f = t^q - t$, and let K be a splitting field of f over \mathbb{F}_p . Let $L = \text{Root}_f(K)$. The objective is to show that $L = K$. Then we will have $|K| = |L| = |\text{Root}_f(K)| = \deg f = q$, because the proof of the previous lemma shows that f has no repeated roots.

To show that $L = K$, by definition, we have $L \subseteq K$. So we need to show every element in K is in L . We do so by showing that L itself is a field. Then since L contains all the roots of f and is a subfield of the splitting field K , we must have $K = L$.

It is straightforward to show that L is a field: if $\alpha, \beta \in L$, then

$$(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta.$$

So $\alpha + \beta \in L$. Similarly, we have

$$(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta.$$

So $\alpha\beta \in L$. Also, we have

$$(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}.$$

So $\alpha^{-1} \in L$. So L is in fact a field.

Since any field of size q is a splitting field of f , and splitting fields are unique to isomorphism, we know that K is unique.

- (ii) Suppose $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$. Then let $n = [\mathbb{F}_{q'} : \mathbb{F}_q]$. So $q' = q^n$. So $d' = nd$. So $d \mid d'$.

On the other hand, suppose $d \mid d'$. Let $d' = dn$. We let $f = t^{q'} - t$. Then for any $\alpha \in \mathbb{F}_q$, we have

$$f(\alpha) = \alpha^{q'} - \alpha = \alpha^{q^n} - \alpha = (\cdots((\alpha^q)^q)\cdots)^q - \alpha = \alpha - \alpha = 0.$$

Since $\mathbb{F}_{q'}$ is the splitting field of f , all roots of f are in $\mathbb{F}_{q'}$. So we know that $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$. \square

Theorem. Consider $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then Fr_q is an element of order n as an element of $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.

Proof. For all $\alpha \in \mathbb{F}_{q^n}$, we have $\text{Fr}_q^n(\alpha) = \alpha^{q^n} = \alpha$. So the order of Fr_q divides n .

If $m \mid n$, then the set

$$\{\alpha \in \mathbb{F}_{q^n} : \text{Fr}_q^m(\alpha) = \alpha\} = \{\alpha \in \mathbb{F}_{q^n} : \alpha^{q^m} = \alpha\} = \mathbb{F}_{q^m}.$$

So if m is the order of Fr_q , then $\mathbb{F}_{q^m} = \mathbb{F}_{q^n}$. So $m = n$. \square

Theorem. The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois with Galois group $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong \mathbb{Z}/n\mathbb{Z}$, generated by Fr_q .

Proof. The multiplicative group $\mathbb{F}_{q^n}^* = \mathbb{F}_{q^n} \setminus \{0\}$ is finite. We have previously seen that multiplicative groups of finite fields are cyclic. So let α be a generator of this group. Then $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$. Let P_α be the minimal polynomial of α over \mathbb{F}_q . Then since $\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ has an element of order n , we get

$$n \leq |\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})| = |\text{Hom}_{\mathbb{F}_q}(\mathbb{F}_q(\alpha), \mathbb{F}_{q^n})|.$$

Since $\mathbb{F}_q(\alpha)$ is generated by one element, we know

$$|\text{Hom}_{\mathbb{F}_q}(\mathbb{F}_q(\alpha), \mathbb{F}_{q^n})| = |\text{Root}_{P_\alpha}(\mathbb{F}_{q^n})|$$

So we have

$$n \leq |\text{Root}_{P_\alpha}(\mathbb{F}_{q^n})| \leq \deg P_\alpha = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

So we know that

$$|\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

So $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a Galois extension.

Since $|\text{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})|$, it has to be generated by Fr_q , since this has order n . In particular, this group is cyclic. \square

3 Solutions to polynomial equations

3.1 Cyclotomic extensions

Theorem. For each $d \in \mathbb{N}$, there exists a d th cyclotomic monic polynomial $\phi_d \in \mathbb{Z}[t]$ satisfying:

(i) For each $n \in \mathbb{N}$, we have

$$t^n - 1 = \prod_{d|n} \phi_d.$$

(ii) Assume $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Then

$$\text{Root}_{\phi_n}(L) = \{n\text{th primitive roots of unity}\}.$$

Note that here we have an abuse of notation, since ϕ_n is a polynomial in $\mathbb{Z}[t]$, not $K[t]$, but we can just use the canonical map $\mathbb{Z}[t] \rightarrow K[t]$ mapping 1 to 1 and t to t .

Proof. We do induction on n to construct ϕ_n . When $n = 1$, let $\phi_1 = t - 1$. Then (i) and (ii) hold in this case, trivially.

Assume now that (i) and (ii) hold for smaller values of n . Let

$$f = \prod_{d|n, d < n} \phi_d.$$

By induction, $f \in \mathbb{Z}[t]$. Moreover, if $d \mid n$ and $d < n$, then $\phi_d \mid (t^n - 1)$ because $(t^d - 1) \mid (t^n - 1)$. We would like to say that f also divides $t^n - 1$. However, we have to be careful, since to make this conclusion, we need to show that ϕ_d and $\phi_{d'}$ have no common roots for distinct $d, d' \mid n$ (and $d, d' < n$).

Indeed, by induction, ϕ_d and $\phi_{d'}$ have no common roots because

$$\begin{aligned} \text{Root}_{\phi_d}(L) &= \{d\text{th primitive roots of unity}\}, \\ \text{Root}_{\phi_{d'}}(L) &= \{d'\text{th primitive roots of unity}\}, \end{aligned}$$

and these two sets are disjoint (or else the roots would not be *primitive*). Therefore ϕ_d and $\phi_{d'}$ have no common irreducible factors. Hence $f \mid t^n - 1$. So we can write

$$t^n - 1 = f\phi_n,$$

where $\phi_n \in \mathbb{Q}[t]$. Since f is monic, ϕ_n has integer coefficients. So indeed $\phi_n \in \mathbb{Z}[t]$. So the first part is proven.

To prove the second part, note that by induction,

$$\text{Root}_f(L) = \{\text{non-primitive } n\text{th roots of unity}\},$$

since all n th roots of unity are d th primitive roots of unity for some smaller d .

Since $f\phi_n = t^n - 1$, ϕ_n contains the remaining, primitive n th roots of unity. Since $t^n - 1$ has no repeated roots, we know that ϕ_n does not contain any extra roots. So

$$\text{Root}_{\phi_n}(L) = \{n\text{th primitive roots of unity}\}. \quad \square$$

Theorem. Let K be a field with $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Let L be the n th cyclotomic extension of K . Then L/K is a Galois extension, and there is an injective homomorphism $\theta : \text{Gal}(L/K) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.

In addition, every irreducible factor of ϕ_n (in $K[t]$) has degree $[L : K]$.

Proof. Let μ be an n th primitive root of unity. Then

$$\text{Root}_{t^n-1}(L) = \{1, \mu, \mu^2, \dots, \mu^{n-1}\}$$

is a cyclic group of order n generated by μ . We first construct the homomorphism $\theta : \text{Aut}_K(L) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ as follows: for each $\phi \in \text{Aut}_K(L)$, ϕ is completely determined by the value of $\phi(\mu)$ since $L = K(\mu)$. Since ϕ is an automorphism, it must take an n th primitive root of unity to another n th primitive root of unity. So $\phi(\mu) = \mu^i$ for some i such that $(i, n) = 1$. Now let $\theta(\phi) = \bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Note that this is well-defined since if $\mu^i = \mu^j$, then $i - j$ has to be a multiple of n .

Now it is easy to see that if $\phi, \psi \in \text{Aut}_K(L)$ are given by $\phi(\mu) = \mu^i$, and $\psi(\mu) = \mu^j$, then $\phi \circ \psi(\mu) = \phi(\mu^j) = \mu^{ij}$. So $\theta(\phi\psi) = \bar{ij} = \theta(\phi)\theta(\psi)$. So θ is a group homomorphism.

Now we check that θ is injective. If $\theta(\phi) = \bar{1}$ (note that $(\mathbb{Z}/n\mathbb{Z})^\times$ is a multiplicative group with unit 1), then $\phi(\mu) = \mu$. So $\phi = \text{id}$.

Now we show that L/K is Galois. Recall that $L = K(\mu)$, and let P_μ be a minimal polynomial of μ over K . Since μ is a root of $t^n - 1$, we know that $P_\mu \mid t^n - 1$. Since $t^n - 1$ has no repeated roots, P_μ has no repeated roots. So P_μ is separable. Moreover, P_μ splits over L as $t^n - 1$ splits over L . So the extension is separable and normal, and hence Galois.

Applying the previous theorem, each irreducible factor g of ϕ_n is a minimal polynomial of some n th primitive root of unity, say λ . Then $L = K(\lambda)$. So

$$\deg g = \deg P_\lambda = [K(\lambda) : K] = [L : K]. \quad \square$$

Lemma. Under the notation and assumptions of the previous theorem, ϕ_n is irreducible in $K[t]$ if and only if θ is an isomorphism.

Proof. (\Rightarrow) Suppose ϕ_n is irreducible. Recall that $\text{Root}_{\phi_n}(L)$ is exactly the n th primitive roots of unity. So if μ is an n th primitive root of unity, then P_μ , the minimal polynomial of μ over K is ϕ_n . In particular, if λ is also an n th primitive root of unity, then $P_\mu = P_\lambda$. This implies that there is some $\phi_\lambda \in \text{Aut}_K(L)$ such that $\phi_\lambda(\mu) = \lambda$.

Now if $\bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then taking $\lambda = \mu^i$, this shows that we have $\phi_\lambda \in \text{Aut}_K(L)$ such that $\theta(\phi_\lambda) = \bar{i}$. So θ is surjective, and hence an isomorphism.

(\Leftarrow) Suppose that θ is an isomorphism. We will reverse the above argument and show that all roots have the same minimal polynomial. Let μ be a n th primitive root of unity, and pick $\bar{i} \in (\mathbb{Z}/n\mathbb{Z})^\times$, and let $\lambda = \mu^i$. Since θ is an isomorphism, there is some $\phi_\lambda \in \text{Aut}_K(L)$ such that $\theta(\phi_\lambda) = \bar{i}$, i.e. $\phi_\lambda(\mu) = \mu^i = \lambda$. Then we must have $P_\mu = P_\lambda$.

Since every n th primitive root of unity is of the form μ^i (with $(i, n) = 1$), this implies that all n th primitive roots have the same minimal polynomial. Since the roots of ϕ_n are all the n th primitive roots of unity, its irreducible factors are exactly the minimal polynomials of the primitive roots. Moreover, ϕ_n does not have repeated roots. So $\phi_n = P_\mu$. In particular, ϕ_n is irreducible. \square

Theorem. ϕ_n is irreducible in $\mathbb{Q}[t]$. In particular, it is also irreducible in $\mathbb{Z}[t]$.

Proof. As before, this can be achieved by showing that all n th primitive roots have the same minimal polynomial. Moreover, let μ be our favorite n th primitive root. Then all other primitive roots λ are of the form $\lambda = \mu^i$, where $(i, n) = 1$. By the fundamental theorem of arithmetic, we can write i as a product $i = q_1 \cdots q_r$. Hence it suffices to show that for all primes $q \nmid n$, we have $P_\mu = P_{\mu^q}$. Noting that μ^q is also an n th primitive root, this gives

$$P_\mu = P_{\mu^{q_1}} = P_{(\mu^{q_1})^{q_2}} = P_{\mu^{q_1 q_2}} = \cdots = P_{\mu^{q_1 \cdots q_r}} = P_{\mu^i}.$$

So we now let μ be an n th primitive root, P_μ be its minimal polynomial. Since μ is a root of ϕ_n , we can write $P_\mu \mid \phi_n$ inside $\mathbb{Q}[t]$. So we can write

$$\phi_n = P_\mu R,$$

Since ϕ_n and P_μ are monic, R is also monic. By Gauss' lemma, we must have $P_\mu, R \in \mathbb{Z}[t]$.

Note that showing $P_\mu = P_{\mu^q}$ is the same as showing μ^q is a root of P_μ , since $\deg P_\mu = \deg P_{\mu^q}$. So suppose it's not. Since μ^q is an n th primitive root of unity, it is a root of ϕ_n . So μ^q must be a root of R . Now let $S = R(t^q)$. Then μ is a root of S , and so $P_\mu \mid S$.

We now reduce mod q . For any polynomial $f \in \mathbb{Z}[t]$, we write the result of reducing the coefficients mod q as \bar{f} . Then we have $\bar{S} = \overline{R(t^q)} = \overline{R(t)}^q$. Since \bar{P}_μ divides \bar{S} (by Gauss' lemma), we know \bar{P}_μ and $\overline{R(t)}$ have common roots. But $\bar{\phi}_n = \bar{P}_\mu \bar{R}$, and so this implies $\bar{\phi}_n$ has repeated roots. This is impossible since $\bar{\phi}_n$ divides $t^n - 1$, and since $q \nmid n$, we know the derivative of $t^n - 1$ does not vanish at the roots. So we are done. \square

Corollary. Let $K = \mathbb{Q}$ and L be the n th cyclotomic extension of \mathbb{Q} . Then the injection $\theta : \text{Gal}(L/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism.

3.2 Kummer extensions

Theorem. Let K be a field, $\lambda \in K$ non-zero, $n \in \mathbb{N}$, $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Let L be the splitting field of $t^n - \lambda$. Then

- (i) L contains an n th primitive root of unity, say μ .
- (ii) $L/K(\mu)$ is a cyclic (and in particular Galois) extension with degree $[L : K(\mu)] \mid n$.
- (iii) $[L : K(\mu)] = n$ if and only if $t^n - \lambda$ is irreducible in $K(\mu)[t]$.

Proof.

- (i) Under our assumptions, $t^n - \lambda$ and $(t^n - \lambda)' = nt^{n-1}$ have no common roots in L . So $t^n - \lambda$ has distinct roots in L , say $\alpha_1, \dots, \alpha_n \in L$.

It then follows by direct computation that $\alpha_1 \alpha_1^{-1}, \alpha_2 \alpha_1^{-1}, \dots, \alpha_n \alpha_1^{-1}$ are distinct roots of unity, i.e. roots of $t^n - 1$. Then one of these, say μ must be an n th primitive root of unity.

- (ii) We know $L/K(\mu)$ is a Galois extension because it is the splitting field of the separable polynomial $t^n - \lambda$.

To understand the Galois group, we need to know how this field exactly looks like. We let α be any root of $t^n - \lambda$. Then the set of all roots can be written as

$$\{\alpha, \mu\alpha, \mu^2\alpha, \dots, \mu^{n-1}\alpha\}$$

Then

$$L = K(\alpha_1, \dots, \alpha_n) = K(\mu, \alpha) = K(\mu)(\alpha).$$

Thus, any element of $\text{Gal}(L/K(\mu))$ is uniquely determined by what it sends α to, and any homomorphism must send α to one of the other roots of $t^n - \lambda$, namely $\mu^i\alpha$ for some i .

Define a homomorphism $\sigma : \text{Gal}(L/K(\mu)) \rightarrow \mathbb{Z}/n\mathbb{Z}$ that sends ϕ to the corresponding i (as an element of $\mathbb{Z}/n\mathbb{Z}$, so that it is well-defined).

It is easy to see that σ is an injective group homomorphism. So we know $\text{Gal}(L/K(\mu))$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$. Since the subgroup of any cyclic group is cyclic, we know that $\text{Gal}(L/K(\mu))$ is cyclic, and its size is a factor of n by Lagrange's theorem. Since $|\text{Gal}(L/K(\mu))| = [L : K(\mu)]$ by definition of a Galois extension, it follows that $[L : K(\mu)]$ divides n .

- (iii) We know that $[L : K(\mu)] = [K(\mu, \alpha) : K(\mu)] = \deg q_\alpha$. So $[L : K(\mu)] = n$ if and only if $\deg q_\alpha = n$. Since q_α is a factor of $t^n - \lambda$, $\deg q_\alpha = n$ if and only if $q_\alpha = t^n - \lambda$. This is true if and only if $t^n - \lambda$ is irreducible $K(\mu)[t]$. So done. \square

Lemma. Assume L/K is a field extension. Then $\text{Hom}_K(L, L)$ is linearly independent. More concretely, let $\lambda_1, \dots, \lambda_n \in L$ and $\phi_1, \dots, \phi_n \in \text{Hom}_K(L, L)$ distinct. Suppose for all $\alpha \in L$, we have

$$\lambda_1\phi_1(\alpha) + \dots + \lambda_n\phi_n(\alpha) = 0.$$

Then $\lambda_i = 0$ for all i .

Proof. We perform induction on n .

Suppose we have some $\lambda_i \in L$ and $\phi_i \in \text{Hom}_K(L, L)$ such that

$$\lambda_1\phi_1(\alpha) + \dots + \lambda_n\phi_n(\alpha) = 0.$$

The $n = 1$ case is trivial, since $\lambda_1\phi_1 = 0$ implies $\lambda_1 = 0$ (the zero homomorphism does not fix K).

Otherwise, since the homomorphisms are distinct, pick $\beta \in L$ such that $\phi_1(\beta) \neq \phi_n(\beta)$. Then we know that

$$\lambda_1\phi_1(\alpha\beta) + \dots + \lambda_n\phi_n(\alpha\beta) = 0$$

for all $\alpha \in L$. Since ϕ_i are homomorphisms, we can write this as

$$\lambda_1\phi_1(\alpha)\phi_1(\beta) + \dots + \lambda_n\phi_n(\alpha)\phi_n(\beta) = 0.$$

On the other hand, by just multiplying the original equation by $\phi_n(\beta)$, we get

$$\lambda_1\phi_1(\alpha)\phi_n(\beta) + \dots + \lambda_n\phi_n(\alpha)\phi_n(\beta) = 0.$$

Subtracting the equations gives

$$\lambda_1\phi_1(\alpha)(\phi_1(\beta) - \phi_n(\beta)) + \dots + \lambda_{n-1}\phi_{n-1}(\alpha)(\phi_{n-1}(\beta) - \phi_n(\beta)) = 0$$

for all $\alpha \in L$. By induction, $\lambda_i(\phi_i(\beta) - \phi_n(\beta)) = 0$ for all $1 \leq i \leq n-1$. In particular, since $\phi_1(\beta) - \phi_n(\beta) \neq 0$, we have $\lambda_1 = 0$. Then we are left with

$$\lambda_2\phi_2(\alpha) + \cdots + \lambda_n\phi_n(\alpha) = 0.$$

Then by induction again, we know that all coefficients are zero. \square

Theorem. Let K be a field, $n \in \mathbb{N}$, $\text{char } K = 0$ or $0 < \text{char } K \nmid n$. Suppose K contains an n th primitive root of unity, and L/K is a cyclic extension of degree $[L : K] = n$. Then L/K is a Kummer extension.

Proof. Our objective here is to find a clever $\lambda \in K$ such that L is the splitting field of $t^n - \lambda$. To do so, we will have to hunt for a root β of $t^n - \lambda$ in L .

Pick ϕ a generator of $\text{Gal}(L/K)$. We know that if β were a root of $t^n - \lambda$, then $\phi(\beta) = \mu^{-1}\beta$ for some primitive n th root of unity μ . Thus, we want to find an element that satisfies such a property.

By the previous lemma, we can find some $\alpha \in L$ such that

$$\beta = \alpha + \mu\phi(\alpha) + \mu^2\phi^2(\alpha) + \cdots + \mu^{n-1}\phi^{n-1}(\alpha) \neq 0.$$

Then, noting that ϕ^n is the identity and ϕ fixes $\mu \in K$, we see that β trivially satisfies

$$\phi(\beta) = \phi(\alpha) + \mu\phi^2\alpha + \cdots + \mu^{n-1}\phi^n(\alpha) = \mu^{-1}\beta,$$

In particular, we know that $\phi(\beta) \in K(\beta)$.

Now pick $\lambda = \beta^n$. Then $\phi(\beta^n) = \mu^{-n}\beta^n = \beta^n$. So ϕ fixes β^n . Since ϕ generates $\text{Gal}(L/K)$, we know all automorphisms of L/K fixes β^n . So $\beta^n \in K$.

Now the roots of $t^n - \lambda$ are $\beta, \mu\beta, \dots, \mu^{n-1}\beta$. Since these are all in β , we know $K(\beta)$ is the splitting field of $t^n - \lambda$.

Finally, to show that $K(\beta) = L$, we observe that $\text{id}, \phi|_{K(\beta)}, \dots, \phi^n|_{K(\beta)}$ are distinct elements of $\text{Aut}_K(K(\beta))$ since they do different things to β . Recall our previous theorem that

$$[K(\beta) : K] \geq |\text{Aut}_K(K(\beta))|.$$

So we know that $n = [L : K] = [K(\beta) : K]$. So $L = K(\beta)$. So done. \square

3.3 Radical extensions

Lemma. Let L/K be a Galois extension, $\text{char } K = 0$, $\gamma \in L$ and F the splitting field of $t^n - \gamma$ over L . Then there exists a further extension E/F such that E/L is radical and E/K is Galois.

Proof. Since we know that L/K is Galois, we would rather work in K than in L . However, our γ is in L , not K . Hence we will employ a trick we've used before, where we introduce a new polynomial f , and show that its coefficients are fixed by $\text{Gal}(L/K)$, and hence in K . Then we can look at the splitting field of f or its close relatives.

Let

$$f = \prod_{\phi \in \text{Gal}(L/K)} (t^n - \phi(\gamma)).$$

Each $\phi \in \text{Gal}(L/K)$ induces a homomorphism $L[t] \rightarrow L[t]$. Since each $\phi \in \text{Gal}(L/K)$ just rotates the roots of f around, we know that this induced homomorphism fixes f . Since all automorphisms in $\text{Gal}(L/K)$ fix the coefficients of f , the coefficients must all be in K . So $f \in K[t]$.

Now since L/K is Galois, we know that L/K is normal. So L is the splitting field of some $g \in K[t]$. Let E be the splitting field of fg over K . Then $K \subseteq E$ is normal. Since the characteristic is zero, this is automatically separable. So the extension $K \subseteq E$ is Galois.

We have to show that $L \subseteq E$ is a radical extension. We pick our fields as follows:

- $E_0 = L$
- $E_1 =$ splitting field of $t^n - 1$ over E_0
- $E_2 =$ splitting field of $t^n - \gamma$ over E_1
- $E_3 =$ splitting field of $t^n - \phi_1(\gamma)$ over E_2
- ...
- $E_r = E$,

where we enumerate $\text{Gal}(L/K)$ as $\{\text{id}, \phi_1, \phi_2, \dots\}$.

We then have the sequence of extensions

$$L = E_0 \subseteq E_1 \subseteq E_2 \subseteq \dots \subseteq E_r$$

Here $E_0 \subseteq E_1$ is a cyclotomic extension, and $E_1 \subseteq E_2, E_2 \subseteq E_3$ etc. are Kummer extensions since they contain enough roots of unity and are cyclic. By construction, $F \subseteq E_2$. So $F \subseteq E$. \square

Theorem. Suppose L/K is a radical extension and $\text{char } K = 0$. Then there is an extension E/L such that E/K is Galois and there is a sequence

$$K = E_0 \subseteq E_1 \subseteq \dots \subseteq E$$

where $E_i \subseteq E_{i+1}$ is cyclotomic or Kummer.

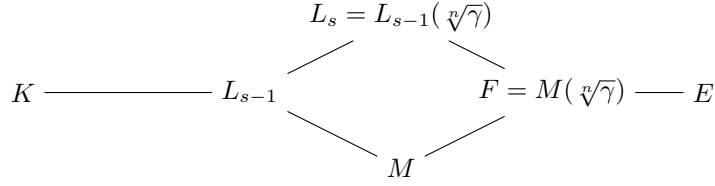
Proof. Note that this is equivalent to proving the following statement: Let

$$K = L_0 \subseteq L_1 \subseteq \dots \subseteq L_s$$

be a sequence of cyclotomic or Kummer extensions. Then there exists an extension $L_s \subseteq E$ such that $K \subseteq E$ is Galois and can be written as a sequence of cyclotomic or Kummer extensions.

We perform induction on s . The $s = 0$ case is trivial.

If $s > 0$, then by induction, there is an extension M/L_{s-1} such that M/K is Galois and is a sequence of cyclotomic and Kummer extensions. Now L_s is a splitting field of $t^n - \gamma$ over L_{s-1} for some $\gamma \in L_{s-1}$. Let F be the splitting field of $t^n - \gamma$ over M . Then by the lemma and its proof, there exists an extension E/M that is a sequence of cyclotomic or Kummer extensions, and E/K is Galois.



However, we already know that M/K is a sequence of cyclotomic and Kummer extensions. So E/K is a sequence of cyclotomic and Kummer extension. So done. \square

3.4 Solubility of groups, extensions and polynomials

Lemma. Let G be a finite group. Then

- (i) If G is soluble, then any subgroup of G is soluble.
- (ii) If $A \triangleleft G$ is a normal subgroup, then G is soluble if and only if A and G/A are both soluble.

Proof.

- (i) If G is soluble, then by definition, there is a sequence

$$G_r = \{1\} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G,$$

such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic.

Let $H_i = H \cap G_i$. Note that H_{i+1} is just the kernel of the obvious homomorphism $H_i \rightarrow G_i/G_{i+1}$. So $H_{i+1} \triangleleft H_i$. Also, by the first isomorphism theorem, this gives an injective homomorphism $H_i/H_{i+1} \rightarrow G_i/G_{i+1}$. So H_i/H_{i+1} is cyclic. So H is soluble.

- (ii) (\Rightarrow) By (i), we know that A is solvable. To show the quotient is soluble, by assumption, we have the sequence

$$G_r = \{1\} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G,$$

such that G_{i+1} is normal in G_i and G_i/G_{i+1} is cyclic. We construct the sequence for the quotient in the obvious way. We want to define E_i as the quotient G_i/A , but since A is not necessarily a subgroup of E , we instead define E_i to be the image of quotient map $G_i \rightarrow G/A$. Then we have a sequence

$$E_r = \{1\} \triangleleft \cdots \triangleleft E_0 = G/A.$$

The quotient map induces a surjective homomorphism $G_i/G_{i+1} \rightarrow E_i/E_{i+1}$, showing that E_i/E_{i+1} are cyclic.

- (\Leftarrow) From the assumptions, we get the sequences

$$A_m = \{1\} \triangleleft \cdots \triangleleft A_0 = A$$

$$F_n = A \triangleleft \cdots \triangleleft F_0 = G$$

where each quotient is cyclic. So we get a sequence

$$A_m = \{1\} \triangleleft A_1 \triangleleft \cdots \triangleleft A_0 = F_n \triangleleft F_{n-1} \triangleleft \cdots \triangleleft F_0 = G,$$

and each quotient is cyclic. So done. \square

Lemma. Let L/K be a Galois extension. Then L/K is soluble if and only if $\text{Gal}(L/K)$ is soluble.

Proof. (\Leftarrow) is clear from definition.

(\Rightarrow) By definition, there is some $E \subseteq L$ such that E/K is Galois and $\text{Gal}(E/K)$ is soluble. By the fundamental theorem of Galois theory, $\text{Gal}(L/K)$ is a quotient of $\text{Gal}(E/K)$. So by our previous lemma, $\text{Gal}(L/K)$ is also soluble. \square

Theorem. Let K be a field with $\text{char } K = 0$, and L/K is a radical extension. Then L/K is a soluble extension.

Proof. We have already shown that if we have a radical extension L/K , then there is a finite extension $K \subseteq E$ such that $K \subseteq E$ is a Galois extension, and there is a sequence of cyclotomic or Kummer extensions

$$E_0 = K \subseteq E_1 \subseteq \cdots \subseteq E_r = E.$$

Let $G_i = \text{Gal}(E/E_i)$. By the fundamental theorem of Galois theory, inclusion of subfields induces an inclusion of subgroups

$$G_0 = \text{Gal}(E/K) \geq G_1 \geq \cdots \geq G_r = \{1\}.$$

In fact, $G_i \triangleright G_{i+1}$ because $E_i \subseteq E_{i+1}$ are Galois (since cyclotomic and Kummer extensions are). So in fact we have

$$G_0 = \text{Gal}(E/K) \triangleright G_1 \triangleright \cdots \triangleright G_r = \{1\}.$$

Finally, note that by the fundamental theorem of Galois theory,

$$G_i/G_{i+1} = \text{Gal}(E_{i+1}/E_i).$$

We also know that the Galois groups of cyclotomic and Kummer extensions are abelian. Since abelian groups are soluble, our previous lemma implies that L/K is soluble. \square

Corollary. Let K be a field with $\text{char } K = 0$, and $f \in K[t]$. If f can be solved by radicals, then $\text{Gal}(L/K)$ is soluble, where L is the splitting field of f over K .

Proof. We have seen that L/K is a Galois extension. By assumption, L/K is thus a radical extension. By the theorem, L/K is also a soluble extension. So $\text{Gal}(L/K)$ is soluble. \square

Lemma. Let K be a field, $f \in K[t]$ of degree n with no repeated roots. Let L be the splitting field of f over K . Then L/K is Galois and there exist an injective group homomorphism

$$\text{Gal}(L/K) \rightarrow S_n.$$

Proof. Let $\text{Root}_f(L) = \{\alpha_1, \dots, \alpha_n\}$. Let P_{α_i} be the minimal polynomial of α_i over K . Then $P_{\alpha_i} \mid f$ implies that P_{α_i} is separable and splits over L . So L/K is Galois.

Now each $\phi \in \text{Gal}(L/K)$ permutes the α_i , which gives a map $\text{Gal}(L/K) \rightarrow S_n$. It is easy to show this is an injective group homomorphism. \square

Lemma. Let p be a prime, and $\sigma \in S_p$ have order p . Then σ is a p -cycle.

Proof. By IA Groups, we can decompose σ into a product of disjoint cycles:

$$\sigma = \sigma_1 \cdots \sigma_r.$$

Let σ_i have order $m_i > 1$. Again by IA Groups, we know that

$$p = \text{order of } \sigma = \text{lcm}(m_1, \dots, m_r).$$

Since p is a prime number, we know that $p = m_i$ for all i . Hence we must have $r = 1$, since the cycles are disjoint and there are only p elements. So $\sigma = \sigma_1$. Hence σ is indeed an p cycle. \square

Theorem. Let $f \in \mathbb{Q}[t]$ be irreducible and $\deg f = p$ prime. Let $L \subseteq \mathbb{C}$ be the splitting field of f over \mathbb{Q} . Let

$$\text{Root}_f(L) = \{\alpha_1, \alpha_2, \dots, \alpha_{p-2}, \alpha_{p-1}, \alpha_p\}.$$

Suppose that $\alpha_1, \alpha_2, \dots, \alpha_{p-2}$ are all real numbers, but α_{p-1} and α_p are not. In particular, $\alpha_{p-1} = \bar{\alpha}_p$. Then the homomorphism $\beta : \text{Gal}(L/\mathbb{Q}) \rightarrow S_n$ is an isomorphism.

Proof. From IA groups, we know that the cycles $(1\ 2\ \dots\ p)$ and $(p-1\ p)$ generate the whole of S_n . So we show that these two are both in the image of β .

As f is irreducible, we know that $f = P_{\alpha_1}$, the minimal polynomial of α_1 over \mathbb{Q} . Then

$$p = \deg P_{\alpha_1} = [\mathbb{Q}(\alpha_1) : \mathbb{Q}].$$

By the tower law, this divides $[L : \mathbb{Q}]$, which is equal to $|\text{Gal}(L/\mathbb{Q})|$ since the extension is Galois. Since p divides the order of $\text{Gal}(L/\mathbb{Q})$, by Cauchy's theorem of groups, there must be an element of $\text{Gal}(L/\mathbb{Q})$ that is of order p . This maps to an element $\sigma \in \text{im } \beta$ of order exactly p . So σ is a p -cycle.

On the other hand, the isomorphism $\mathbb{C} \rightarrow \mathbb{C}$ given by $z \mapsto \bar{z}$ restricted to L gives an automorphism in $\text{Gal}(L/\mathbb{Q})$. This simply permutes α_{p-1} and α_p , since it fixes the real numbers and α_{p-1} and α_p must be complex conjugate pairs. So $\tau = (p-1\ p) \in \text{im } \beta$.

Now for every $1 \leq i < p$, we know that σ^i again has order p , and hence is a p -cycle. So if we change the labels of the roots $\alpha_1, \dots, \alpha_p$ and replace σ with σ^i , and then waffle something about combinatorics, we can assume $\sigma = (1\ 2\ \dots\ p-1\ p)$. So done. \square

3.5 Insolubility of general equations of degree 5 or more

Theorem (Symmetric rational function theorem). Let K be a field, $L = K(x_1, \dots, x_n)$. Let F the field fixed by the automorphisms that permute the x_i . Then

(i) L is the splitting field of

$$f = t^n - e_1 t^{n-1} + \dots + (-1)^n e_n$$

over F .

- (ii) $F = L^{S_n} \subseteq L$ is a Galois group with $\text{Gal}(L/F)$ isomorphic to S_n .
- (iii) $F = K(e_1, \dots, e_n)$.

Proof.

- (i) In $L[t]$, we have

$$f = (t - x_1) \cdots (t - x_n).$$

So L is the splitting field of f over F .

- (ii) By Artin's lemma, L/K is Galois and $\text{Gal}(L/F) \cong S_n$.
- (iii) Let $E = K(e_1, \dots, e_n)$. Clearly, $E \subseteq F$. Now $E \subseteq L$ is a Galois extension, since L is the splitting field of f over E and f has no repeated roots.

By the fundamental theorem of Galois theory, since we have the Galois extensions $E \subseteq F \subseteq L$, we have $\text{Gal}(L/F) \leq \text{Gal}(L/E)$. So $S_n \leq \text{Gal}(L/E)$. However, we also know that $\text{Gal}(L/E)$ is a subgroup of S_n , we must have $\text{Gal}(L/E) = \text{Gal}(L/F) = S_n$. So we must have $E = F$. \square

Theorem. Let K be a field with $\text{char } K = 0$. Then the general polynomial over K of degree n cannot be solved by radicals if $n \geq 5$.

Proof. Let

$$f = t^n + u_1 t^{n-1} + \cdots + u_n.$$

be our general polynomial of degree $n \geq 5$. Let N be a splitting field of f over $K(u_1, \dots, u_n)$. Let

$$\text{Root}_f(N) = \{\alpha_1, \dots, \alpha_n\}.$$

We know the roots are distinct because f is irreducible and the field has characteristic 0. So we can write

$$f = (t - \alpha_1) \cdots (t - \alpha_n) \in N[t].$$

We can expand this to get

$$\begin{aligned} u_1 &= -(\alpha_1 + \cdots + \alpha_n) \\ u_2 &= \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \cdots + \alpha_{n-1} \alpha_n \\ &\vdots \\ u_i &= (-1)^i (\textit{i} \text{th elementary symmetric polynomial in } \alpha_1, \dots, \alpha_n). \end{aligned}$$

Now let x_1, \dots, x_n be new variables, and e_i the i th elementary symmetric polynomial in x_1, \dots, x_n . Let $L = K(x_1, \dots, x_n)$, and $F = K(e_1, \dots, e_n)$. We know that $F \subseteq L$ is a Galois extension with Galois group isomorphic to S_n .

We define a ring homomorphism

$$\begin{aligned} \theta : K[u_1, \dots, u_n] &\rightarrow K[e_1, \dots, e_n] \subseteq K[x_1, \dots, x_n] \\ u_i &\mapsto (-1)^i e_i. \end{aligned}$$

This is our equations of u_i in terms α_i , but with x_i instead of α_i .

We want to show that θ is an isomorphism. Note that since the homomorphism just renames u_i into e_i , the fact that θ is an isomorphism means there are no

“hidden relations” between the e_i . It is clear that θ is a surjection. So it suffices to show θ is injective. Suppose $\theta(h) = 0$. Then

$$h(-e_1, \dots, (-1)^n e_n) = 0.$$

Since the x_i are just arbitrary variables, we now replace x_i with α_i . So we get

$$h(-e_1(\alpha_1, \dots, \alpha_n), \dots, (-1)^n (e_n(\alpha_1, \dots, \alpha_n))) = 0.$$

Using our expressions for u_i in terms of e_i , we have

$$h(u_1, \dots, u_n) = 0,$$

But $h(u_1, \dots, u_n)$ is just h itself. So $h = 0$. Hence θ is injective. So it is an isomorphism. This in turns gives an isomorphism between

$$K(u_1, \dots, u_n) \rightarrow K(e_1, \dots, e_n) = F.$$

We can extend this to their polynomial rings to get isomorphisms between

$$K(u_1, \dots, u_n)[t] \rightarrow F[t].$$

In particular, this map sends our original f to

$$f \mapsto t^n - e_1 t^{n-1} + \dots + (-1)^n e_n = g.$$

Thus, we get an isomorphism between the splitting field of f over $K(u_1, \dots, u_n)$ and the splitting field g over F .

The splitting field of f over $K(u_1, \dots, u_n)$ is just N by definition. From the symmetric rational function theorem, we know that the splitting field of g over F is just L , and So $N \cong L$. So we have an isomorphism

$$\text{Gal}(N/K(u_1, \dots, u_n)) \rightarrow \text{Gal}(L/F) \cong S_n.$$

Since S_n is not soluble, f is not soluble. □

Theorem. Let K be a field with $\text{char } K = 0$. If L/K is a soluble extension, then it is a radical extension.

Proof. Let $L \subseteq E$ be such that $K \subseteq E$ is Galois and $\text{Gal}(E/K)$ is soluble. We can replace L with E , and assume that in fact L/K is a soluble Galois extension. So there is a sequence of groups

$$\{0\} = G_r \triangleleft \dots \triangleleft G_1 \triangleleft G_0 = \text{Gal}(L/K)$$

such that G_i/G_{i+1} is cyclic.

By the fundamental theorem of Galois theory, we get a sequence of field extension given by $L_i = L^{G_i}$:

$$K = L_0 \subseteq \dots \subseteq L_r = L.$$

Moreover, we know that $L_i \subseteq L_{i+1}$ is a Galois extension with Galois group $\text{Gal}(L_{i+1}/L_i) \cong G_i/G_{i+1}$. So $\text{Gal}(L_{i+1}/L_i)$ is cyclic.

Let $n = [L : K]$. Recall that we proved a previous theorem that if $\text{Gal}(L_{i+1}/L_i)$ is cyclic, and L_i contains a primitive k th root of unity (with

$k = [L_{i+1} : L_i]$, then $L_i \subseteq L_{i+1}$ is a Kummer extension. However, we do not know if L_i contains the right root of unity. Hence, the trick here is to add an n th primitive root of unity to each field in the sequence.

Let μ an n th primitive root of unity. Then if we add the n th primitive root to each item of the sequence, we have

$$\begin{array}{ccccccccccc} L_0(\mu) & \subseteq & \cdots & \subseteq & L_i(\mu) & \subseteq & L_{i+1}(\mu) & \subseteq & \cdots & \subseteq & L_r(\mu) \\ \cup & & & & \cup & & \cup & & & & \cup \\ K = L_0 & \subseteq & \cdots & \subseteq & L_i & \subseteq & L_{i+1} & \subseteq & \cdots & \subseteq & L_r = L \end{array}$$

We know that $L_0 \subseteq L_0(\mu)$ is a cyclotomic extension by definition. We will now show that $L_i(\mu) \subseteq L_{i+1}(\mu)$ is a Kummer extension for all i . Then L/K is radical since $L \subseteq L_r(\mu)$.

Before we do anything, we have to show $L_i(\mu) \subseteq L_{i+1}(\mu)$ is a Galois extension. To show this, it suffices to show $L_i \subseteq L_{i+1}(\mu)$ is a Galois extension.

Since $L_i \subseteq L_{i+1}$ is Galois, $L_i \subseteq L_{i+1}$ is normal. So L_{i+1} is the splitting of some h over L_i . Then $L_{i+1}(\mu)$ is just the splitting field of $(t^n - 1)h$. So $L_i \subseteq L_{i+1}(\mu)$ is normal. Also, $L_i \subseteq L_{i+1}(\mu)$ is separable since $\text{char } K = \text{char } L_i = 0$. Hence $L_i \subseteq L_{i+1}(\mu)$ is Galois, which implies that $L_i(\mu) \subseteq L_{i+1}(\mu)$ is Galois.

We define a homomorphism of groups

$$\text{Gal}(L_{i+1}(\mu)/L_i(\mu)) \rightarrow \text{Gal}(L_{i+1}/L_i)$$

by restriction. This is well-defined because L_{i+1} is the splitting field of some h over L_i , and hence any automorphism of $L_{i+1}(\mu)$ must send roots of h to roots of h , i.e. L_{i+1} to L_{i+1} .

Moreover, we can see that this homomorphism is injective. If $\phi \mapsto \phi|_{L_{i+1}} = \text{id}$, then it fixes everything in L_{i+1} . Also, since it is in $\text{Gal}(L_{i+1}(\mu)/L_i(\mu))$, it fixes $L_i(\mu)$. In particular, it fixes μ . So ϕ must fix the whole of $L_{i+1}(\mu)$. So $\phi = \text{id}$.

By injectivity, we know that $\text{Gal}(L_{i+1}(\mu)/L_i(\mu))$ is isomorphic to a subgroup of $\text{Gal}(L_{i+1}/L_i)$. Hence it is cyclic. By our previous theorem, it follows that $L_i(\mu) \subseteq L_{i+1}(\mu)$ is a Kummer extension. So L/K is radical. \square

Corollary. Let K be a field with $\text{char } K = 0$ and $h \in K[t]$. Let L be the splitting of h over K . Then h can be solved by radicals if and only if $\text{Gal}(L/K)$ is soluble.

Proof. (\Rightarrow) Proved before.

(\Leftarrow) Since L/K is a Galois extension, L/K is a soluble extension. So it is a radical extension. So h can be solved by radicals. \square

Corollary. Let K be a field with $\text{char } K = 0$. Let $f \in K[t]$ have $\deg f \leq 4$. Then f can be solved by radicals.

Proof. Exercise. \square

4 Computational techniques

4.1 Reduction mod p

Theorem.

$$G = \{\lambda \in S_n : \lambda \text{ preserves the irreducible factor corresponding to } G\}. \quad (\dagger)$$

Theorem. Let $f \in \mathbb{Z}[t]$ be monic with no repeated roots. Let E be the splitting field of f over \mathbb{Q} , and take $\bar{f} \in \mathbb{F}_p[t]$ be the obvious polynomial obtained by reducing the coefficients of f mod p . We also assume this has no repeated roots, and let \bar{E} be the splitting field of \bar{f} .

Then there is an injective homomorphism

$$\bar{G} = \text{Gal}(\bar{E}/\mathbb{F}_p) \hookrightarrow G = \text{Gal}(E/\mathbb{Q}).$$

Moreover, if \bar{f} factors as a product of irreducibles of length n_1, n_2, \dots, n_r , then $\text{Gal}(f)$ contains an element of cycle type (n_1, \dots, n_r) .

Proof. We apply the previous theorem twice. First, we take $K = \mathbb{Q}$. Then

$$\theta(R) \in \mathbb{Z}[u_1, \dots, u_n, t].$$

Let P be the irreducible factor of $\theta(R)$ corresponding to the Galois group G . Applying Gauss' lemma, we know P has integer coefficients.

Applying the theorem again, taking $K = \mathbb{F}_p$. Denote the ring homomorphism as $\bar{\theta}$. Then $\bar{\theta}(R) \in \mathbb{F}_p[u_1, \dots, u_n, t]$. Now let Q be the irreducible factor $\bar{\theta}(R)$ corresponding to \bar{G} .

Now note that $\theta(R_{(1)}) \mid P$ and $\bar{\theta}(R_{(1)}) \mid Q$, since the identity is in G and \bar{G} . Also, note that $\bar{\theta}(R) = \overline{\theta(R)}$, where the bar again denotes reduction mod p . So $Q \mid P$.

Considering the second action of S_n (i.e. permuting the u_i), we can show $\bar{G} \subseteq G$, using the characterization (\dagger) . Details are left as an exercise. \square

4.2 Trace, norm and discriminant

Lemma. Let $L/F/K$ be finite field extensions. Then

$$\text{tr}_{L/K} = \text{tr}_{F/K} \circ \text{tr}_{L/F}, \quad N_{L/K} = N_{F/K} \circ N_{L/F}.$$

Lemma. Let F/K be a field extension, and V an F -vector space. Let $T : V \rightarrow V$ be an F -linear map. Then it is in particular a K -linear map. Then

$$\det_K T = N_{F/K}(\det_F T), \quad \text{tr}_K T = \text{tr}_{F/K}(\text{tr}_F T).$$

Proof. For $\alpha \in F$, we will write $m_\alpha : F \rightarrow F$ for multiplication by α map viewed as a K -linear map.

By IB Groups, Rings and Modules, there exists a basis $\{e_i\}$ such that T is in rational canonical form, i.e. such that T is block diagonal with each diagonal looking like

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{r-1} \end{pmatrix}.$$

Since the norm is multiplicative and trace is additive, and

$$\det \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \det A \det B, \quad \text{tr} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \text{tr} A + \text{tr} B,$$

we may wlog T is represented by a single block as above.

From the rational canonical form, we can read off

$$\det_F T = (-1)^{r-1} a_0, \quad \text{tr}_F T = a_{r-1}.$$

We now pick a basis $\{f_j\}$ of F over K , and then $\{e_i f_j\}$ is a basis for V over K . Then in this basis, the matrix of T over K is given by

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_0} \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_1} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} & m_{a_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} & m_{a_{r-1}} \end{pmatrix}.$$

It is clear that this has trace

$$\text{tr}_K(m_{a_{r-1}}) = \text{tr}_{F/K}(a_{r-1}) = \text{tr}_{F/K}(\text{tr}_F T).$$

Moreover, writing $n = [L : K]$, we have

$$\begin{aligned} \det_K \begin{pmatrix} \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_0} \\ \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} & m_{a_1} \\ \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} & m_{a_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} & m_{a_{r-1}} \end{pmatrix} &= (-1)^{n(r-1)} \det_K \begin{pmatrix} m_{a_0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ m_{a_1} & \mathbf{1} & \mathbf{0} & \cdots & \mathbf{0} \\ m_{a_2} & \mathbf{0} & \mathbf{1} & \cdots & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m_{a_{r-1}} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1} \end{pmatrix} \\ &= (-1)^{n(r-1)} \det_K(m_{a_0}) \\ &= \det_K((-1)^{r-1} m_{a_0}) \\ &= N_{F/K}((-1)^{r-1} a_0) \\ &= N_{F/K}(\det_F T). \end{aligned}$$

So the result follows. \square

Corollary. Let L/K be a finite field extension, and $\alpha \in L$. Let $r = [L : K(\alpha)]$ and let P_α be the minimal polynomial of α over K , say

$$P_\alpha = t^n + a_{n-1}t^{n-1} + \cdots + a_0.$$

with $a_i \in K$. Then

$$\text{tr}_{L/K}(\alpha) = -ra_{n-1}$$

and

$$N_{L/K}(\alpha) = (-1)^{nr} a_0^r.$$

Proof. We first consider the case $r = 1$. Write m_α for the matrix representing multiplication by α . Then P_α is the minimal polynomial of m_α . But since $\deg P_\alpha = n = \dim_K K(\alpha)$, it follows that this is also the characteristic polynomial. So the result follows.

Now if $r \neq 1$, we can consider the tower of extensions $L/K(\alpha)/K$. Then we have

$$\begin{aligned} N_{L/K}(\alpha) &= N_{K(\alpha)/K}(N_{L/K(\alpha)}(\alpha)) = N_{K(\alpha)/K}(\alpha^r) \\ &= (N_{K(\alpha)/K}(\alpha))^r = (-1)^{nr} a_0^r. \end{aligned}$$

The computation for trace is similar. \square

Theorem. Let L/K be a finite but not separable extension. Then $\text{tr}_{L/K}(\alpha) = 0$ for all $\alpha \in L$.

Proof. Pick $\beta \in L$ such that P_β , the minimal polynomial of β over K , is not separable. Then by the previous characterization of separable polynomials, we know $p = \text{char } K > 0$ with $P_\beta = q(t^p)$ for some $q \in K[t]$.

Now consider

$$K \subseteq K(\beta^p) \subseteq K(\beta) \subseteq L.$$

To show $\text{tr}_{L/K} = 0$, by the previous proposition, it suffices to show $\text{tr}_{K(\beta)/K(\beta^p)} = 0$.

Note that the minimal polynomial of β^p over K is q because $q(\beta^p) = 0$ and q is irreducible. Then $[K(\beta) : K] = \deg P_\beta = p \deg q$ and $\deg[K(\beta^p) : K] = \deg q$. So $[K(\beta) : K(\beta^p)] = p$.

Now $\{1, \beta, \beta^2, \dots, \beta^{p-1}\}$ is a basis of $K(\beta)$ over $K(\beta^p)$. Let R_{β^i} be the minimal polynomial of β^i over $K(\beta^p)$. Then

$$R_{\beta^i} = \begin{cases} t - 1 & i = 0 \\ t^p - \beta^{ir} & i \neq 0 \end{cases},$$

We get the second case using the fact that p is a prime number, and hence $K(\beta^p)(\beta^i) = K(\beta)$ if $1 \leq i < p$. So $[K(\beta^p)(\beta^i) : K(\beta^p)] = p$ and hence the minimal polynomial has degree p . Hence $\text{tr}_{K(\beta)/K(\beta^p)}(\beta^i) = 0$ for all i .

Thus, $\text{tr}_{K(\beta)/K(\beta^p)} = 0$. Hence

$$\text{tr}_{L/K} = \text{tr}_{K(\beta^p)/K} \circ \text{tr}_{K(\beta)/K(\beta^p)} \circ \text{tr}_{L/K(\beta)} = 0. \quad \square$$

Theorem. Let L/K be a finite separable extension. Pick a further extension E/L such that E/K is normal and

$$|\text{Hom}_K(L, E)| = [L : K].$$

Write $\text{Hom}_K(L, E) = \{\varphi_1, \dots, \varphi_n\}$. Then

$$\text{tr}_{L/K}(\alpha) = \sum_{i=1}^n \varphi_i(\alpha), \quad N_{L/K}(\alpha) = \prod_{i=1}^n \varphi_i(\alpha)$$

for all $\alpha \in L$.

Proof. Let $\alpha \in L$. Let P_α be the minimal polynomial of α over K . Then there is a one-to-one correspondence between

$$\text{Hom}_K(K(\alpha), E) \longleftrightarrow \text{Root}_{P_\alpha}(E) = \{\alpha_1, \dots, \alpha_d\}.$$

wlog we let $\alpha = \alpha_1$.

Also, since

$$|\mathrm{Hom}_K(L, E)| = [L : K],$$

we get

$$|\mathrm{Hom}_K(K(\alpha), E)| = [K(\alpha) : K] = \deg P_\alpha.$$

Moreover, the restriction map $\mathrm{Hom}_K(L, E) \rightarrow \mathrm{Hom}_K(K(\alpha), E)$ (defined by $\varphi \mapsto \varphi|_{K(\alpha)}$) is surjective and sends exactly $[K(\alpha) : K]$ elements to any particular element in $\mathrm{Hom}_K(K(\alpha), E)$.

Therefore

$$\sum \varphi_i(\alpha) = [L : K(\alpha)] \sum_{\psi \in \mathrm{Hom}_K(K(\alpha), E)} \psi(\alpha) = [L : K(\alpha)] \sum_{i=1}^d \alpha_i.$$

Moreover, we can read the sum of roots of a polynomial is the (negative of the) coefficient of t^{d-1} , where

$$P_\alpha = t^d + a_{d-1}t^{d-1} + \cdots + a_0.$$

So

$$\sum \varphi_i(\alpha) = [L : K(\alpha)](-a_{d-1}) = \mathrm{tr}_{L/K}(\alpha).$$

Similarly, we have

$$\begin{aligned} \prod \varphi_i(\alpha) &= \left(\prod_{\psi \in \mathrm{Hom}_K(K(\alpha), E)} \psi(\alpha) \right)^{[L:K(\alpha)]} \\ &= \left(\prod_{i=1}^d \alpha_i \right)^{[L:K(\alpha)]} \\ &= ((-1)^d a_0)^{[L:K(\alpha)]} \\ &= N_{L/K}(\alpha). \quad \square \end{aligned}$$

Corollary. Let L/K be a finite separable extension. Then there is some $\alpha \in L$ such that $\mathrm{tr}_{L/K}(\alpha) \neq 0$.

Proof. Using the notation of the previous theorem, we have

$$\mathrm{tr}_{L/K}(\alpha) = \sum \varphi_i(\alpha).$$

Similar to a previous lemma, we can show that $\varphi_1, \dots, \varphi_n$ are “linearly independent” over E , and hence $\sum \varphi_i$ cannot be identically zero. Hence there is some α such that

$$\mathrm{tr}_{L/K}(\alpha) = \sum \varphi_i(\alpha) \neq 0. \quad \square$$

Theorem. Let K be a field and $f \in K[t]$, L is the splitting field of f over K . Suppose $D_f \neq 0$ and $\mathrm{char} K \neq 2$. Then

- (i) $D_f \in K$.
- (ii) Let $G = \mathrm{Gal}(L/K)$, and $\theta : G \rightarrow S_n$ be the embedding given by the permutation of the roots. Then $\mathrm{im} \theta \subseteq A_n$ if and only if $\Delta_f \in K$ (if and only if D_f is a square in K).

Proof.

- (i) It is clear that D_f is fixed by $\text{Gal}(L/K)$ since it only permutes the roots.
- (ii) Consider a permutation $\sigma \in S_n$ of the form $\sigma = (\ell m)$, and let it act on the roots. Then we claim that

$$\sigma(\Delta_f) = -\Delta_f. \quad (\dagger)$$

So in general, odd elements in S_n negate Δ_f while even elements fix it. Thus, $\Delta_f \in K$ iff Δ_f is fixed by $\text{Gal}(L/K)$ iff every element of $\text{Gal}(L/K)$ is even.

To prove (\dagger) , we have to painstakingly check all terms in the product. We wlog $\ell < m$. If $k < \ell, m$. Then this swaps $(\alpha_k - \alpha_\ell)$ with $(\alpha_k - \alpha_m)$, which has no effect. The $k > m$ case is similar. If $\ell < k < m$, then this sends $(\alpha_\ell - \alpha_k) \mapsto (\alpha_m - \alpha_k)$ and $(\alpha_k - \alpha_m) \mapsto (\alpha_\ell - \alpha_m)$. This introduces two negative signs, which has no net effect. Finally, this sends $(\alpha_k - \alpha_m)$ to its negation, and so introduces a negative sign. \square

Theorem. Let K be a field, and $f \in K[t]$ be an n -degree monic irreducible polynomial with no repeated roots. Let L be the splitting field of f over K , and let $\alpha \in \text{Root}_F(L)$. Then

$$D_f = (-1)^{n(n-1)/2} N_{K(\alpha)/K}(f'(\alpha)).$$

Proof. Let $\text{Hom}_K(K(\alpha), L) = \{\varphi_1, \dots, \varphi_n\}$. Recall these are in one-to-one correspondence with $\text{Root}_f(L) = \{\alpha_1, \dots, \alpha_n\}$. Then we can compute

$$\prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Note that since f is just monic, we have

$$f = (t - \alpha_1) \cdots (t - \alpha_n).$$

Computing the derivative directly, we find

$$\prod_{j \neq i} (\alpha_i - \alpha_j) = f'(\alpha_i).$$

So we have

$$\prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i f'(\alpha_i).$$

Now since the φ_i just maps α to α_i , we have

$$\prod_{i \neq j} (\alpha_i - \alpha_j) = \prod_i \varphi_i(f'(\alpha)) = N_{K(\alpha)/K}(f'(\alpha)).$$

Finally, multiplying the factor of $(-1)^{n(n-1)/2}$ gives the desired result. \square