Part II – Galois Theory

Based on lectures by Dr C. Brookes
Notes taken by Bhavik Mehta

Michaelmas 2017

0 Introduction

0.1 Course overview

1 Field Extensions

Theorem 1.1 (Tower law)**.** Suppose $K \leq L \leq M$ are field extensions. Then $|M : K| = |M : L|\,|L : K|$.

Proof. Assume that $|M : L| < \infty$, and $|L : K| < \infty$. Take an L-basis of M, given by $\{ f_1, \dots, f_b \}$, and a K-basis of L given by $\{ e_1, \dots, e_a \}$. Take $m \in M$, so $m = \sum_{i=1}^{b} \mu_i f_i$ for some $\mu_i \in L$. Similarly, $\mu_i = \sum_{j=1}^{a} \lambda_{ij} e_j$ for some $\lambda_{ij} \in K$, so

$$m = \sum_{i=1}^{b} \sum_{j=1}^{a} \lambda_{ij} e_j f_i$$

Thus $\{ e_j f_i \mid 1 \leq j \leq a, 1 \leq i \leq b \}$ span M.

Linear independence: It's enough to show that if $0 = m = \sum\sum \lambda_{ij} e_j f_i$ then λ_{ij} are all zero. However if $m = 0$ the linear independence of f_i forces each $\mu_i = 0$. Then the linear indepedence of e_j forces λ_{ij} all to be zero, as required. □

1.1 Motivatory Example

1.2 Review of GRM

Lemma 1.2. Let $K \leq L$ be a finite field extension. Then L is algebraic over K.

Proof. Let $|L : K| = n$, and take $\alpha \in L$. Consider $1, \alpha, \alpha^2, \dots, \alpha^n$, which must be linearly dependent in the n-dimensional K–vector space L. So, $\sum_{i=0}^{n} \lambda_i \alpha^i = 0$ for some $\lambda \in K$ not all zero, and hence α is a root of $f(t) = \sum_{i=0}^{n} \lambda_i t^i$, so α is algebraic over K. α was arbitrary, so L is algebraic over K. □

Lemma 1.3. Suppose $K \leq L$ is a field extension, $\alpha \in L$ and α is algebraic over K. Then the minimal polynomial $f_\alpha(t)$ of α over K is irreducible in $K[t]$ and I_α is a prime ideal.

Proof. Suppose $f_\alpha(t) = p(t)q(t)$. We aim to show $p(t)$ or $q(t)$ is a unit in $K[t]$. But $0 = f_\alpha(\alpha) = p(\alpha)q(\alpha)$, so $p(\alpha) = 0$ or $q(\alpha) = 0$, without loss of generality take $p(\alpha) = 0$, thus $p(t) \in I_\alpha$.

But $I_\alpha = (f_\alpha(t))$, so $p(t) = f_\alpha(t)r(t)$, giving $f_\alpha(t) = f_\alpha(t)r(t)q(t)$ and so $r(t)q(t) = 1$ in $K[t]$, and $q(t)$ is a unit, as required. Recall from GRM that irreducible elements of $K[t]$ are prime and hence generate prime ideals of $K[t]$. So I_α is a prime ideal. □

Theorem 1.4. Suppose $K \leq L$ is a field extension and $\alpha \in L$ is algebraic over K. Then

(i) $K(\alpha) = K[\alpha]$

(ii) $|K(\alpha) : K| = \deg f_\alpha(t)$ where $f_\alpha(t)$ is the minimal polynomial of α over K.

Proof.

(i) Clearly $K[\alpha] \leq K(\alpha)$. We aim to show that any non-zero element β of $K[\alpha]$ is a unit, so $K[\alpha]$ is a field.

By definition of $K[\alpha]$, we have $\beta = g(\alpha)$ for some $g(t) \in K[t]$. Since $\beta = g(\alpha) \neq 0$, $g(t) \notin I_\alpha = (f_\alpha(t))$. Thus $f_\alpha(t) \nmid g(t)$.

From Lemma 1.3, $f_\alpha(t)$ is irreducible and $K[t]$ is a PID, we know $\exists r(t), s(t) \in K[t]$ with

$$r(t)f_\alpha(t) + s(t)g(t) = 1 \in K[t].$$

Hence $s(\alpha)g(\alpha) = 1$ in $K[\alpha]$, and so $\beta = g(\alpha)$ is a unit, as required.

(ii) Let $n = \deg f_\alpha(t)$ We'll show that $T = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a K–vector space basis of $K[\alpha]$.

Spanning: If $f_\alpha(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ with $a_i \in K$, then $\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0$. This implies α^n is a linear combination of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, and an easy induction shows that α^m for $m \geq n$ is likewise a linear combination of $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, so we have spanning.

Linear independence: Suppose $\lambda_{n-1}\alpha^{n-1} + \ldots + \lambda_0 = 0$. Let $g(t) = \lambda_{n-1}t^{n-1} + \ldots + \lambda_0$. Since $g(\alpha) = 0$, we have $g(t) \in I_\alpha = (f_\alpha(t))$. So $g(t) = 0$ or $f_\alpha(t) \mid g(t)$. The latter is not possible since $\deg f_\alpha(t) > \deg g_\alpha(t)$ so $g(t) = 0$ in $K[t]$ and all the λ_i's are zero. □

Corollary 1.5. If $K \leq L$ is a field extension and $\alpha \in L$, then α is algebraic over K if and only if $K \leq K(\alpha)$ is finite.

Proof.

($\Rightarrow$) By Theorem 1.4, $|K(\alpha) : K| = \deg f_\alpha(t) \leq \infty$.

($\Leftarrow$) Lemma 1.2

□

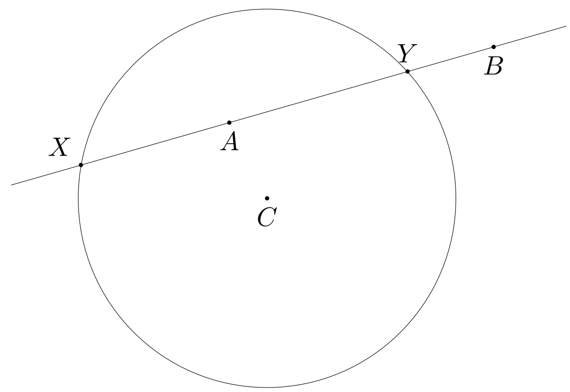
Corollary 1.6. Let $K \leq L$ be a field extension with $|L : K| = n$. Let $\alpha \in L$, then $\deg f_\alpha(t) \mid n$.

Proof. Use the Tower law on $K \leq K(\alpha) \leq L$. We deduce that $|K(\alpha) : K|$ divides $|L : K|$. Theorem 1.4(ii) gives $\deg f_\alpha(t) = |K(\alpha) : K|$. □

1.3 Digression on (Non-)Constructibility

Lemma 1.7. x_i, y_i are both roots in K_i of quadratic polynomials in $K_{i-1}[t]$.

Proof. There are three cases for $\mathbf{r_i}$: line meets line, line meets circle, circle meets circle. We do the second case only here.



The line is defined by two points $A = (p, q)$ and $B = (r, s)$ while the circle is defined with a centre $C = (t, u)$ and radius w. Then, points X and Y satisfy the equation of the line $\frac{x-p}{r-p} = \frac{y-q}{s-q}$, and the equation of the circle $(x - t)^2 + (y - u)^2 = w^2$. Solving these together gives coordinates of X and Y satisfying quadratic polynomials over K_{i-1}. The other two cases are left as an exercise for the reader. □

Theorem 1.8. If $\mathbf{r} = (x, y)$ is constructible from a set P_0 of points in $\mathbb{R}^2$ and if K_0 is the subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and the coordinates of the points in P_0, then the degrees $|K_0(x) : K_0|$ and $|K_0(y) : K_0|$ are powers of two.

Proof. Continue with the previous notation of $K_i = K_{i-1}(x_i, y_i)$. By the Tower law,

$$|K_i : K_{i-1}| = |K_{i-1}(x, y) : K_{i-1}(x)|\,|K_{i-1}(x) : K_{i-1}|$$

But Lemma 1.7 tells us that $|K_{i-1}(x) : K_{i-1}|$ must be 1 or 2 depending on whether the quadratic polynomial arising in the lemma is reducible or not, using Theorem 1.4(ii). Similarly, $|K_{i-1}(x, y) : K_{i-1}(x)|$ is 1 or 2.

So $|K_i : K_{i-1}| = 1, 2$ or 4, (but in fact 4 cannot happen), hence by the Tower law, $|K_n : K_0| = |K_n : K_{n-1}|\,|K_{n-1} : K_{n-2}| \dots |K_1 : K_0|$ is a power of two.

If $r = (x, y)$ is constructible from P_0, then

$$\begin{aligned} x, y \in K_n \quad \text{and} \quad & K_0 \leq K_0(x) \leq K_n \\ & K_0 \leq K_0(y) \leq K_n \end{aligned}$$

and the Tower Law again gives that $|K_0(x) : K_0|$ and $|K_0(y) : K_0|$ are also powers of 2. □

Theorem 1.9. Let $f(t)$ be a primitive integral polynomial. Then $f(t)$ is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[t]$.

Proof. A special case of Gauss' lemma from GRM. □

Theorem 1.10 (Eisenstein's criterion)**.** Let $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \in \mathbb{Z}[t]$. Suppose there is a prime p such that

(i) $p \nmid a_n$

(ii) $p \mid a_{n-1}$, $p \mid a_{n-2}, \dots, p \mid a_0$

(iii) $p^2 \nmid a_0$

Then $f(t)$ is irreducible in $\mathbb{Z}[t]$

Proof. Recall from GRM. □

Theorem 1.11. The cube cannot be duplicated by ruler and compasses.

Proof. The problem amounts to whether given a unit distance, one can construct points distance α apart, where α satisfies $t^3 - 2 = 0$. Starting with points $P_0 = \{(0,0),(1,0)\}$ can we produce $(\alpha, 0)$?

No. If we could, Theorem 1.8 would say $|\mathbb{Q}(\alpha) : \mathbb{Q}|$ is a power of 2. But $|\mathbb{Q}(\alpha) : \mathbb{Q}| = 3$ since $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f_\alpha(t)$ where $f_\alpha(t)$ is the minimal polynomial of α over $\mathbb{Q}$. α satisfies $t^3 - 2$, which is irreducible over $\mathbb{Z}$ by Eisenstein's criterion hence irreducible over $\mathbb{Q}$. So $t^3 - 2$ is the minimal polynomial $f_\alpha(t)$. □

Theorem 1.12. The circle cannot be squared using ruler and compasses.

Proof. Starting with $(0,0)$ and $(1,0)$, we must construct $(\sqrt{\pi}, 0)$ so that we have a square of side length $\sqrt{\pi}$ and hence area π. But π and hence $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$ (Lindemann - not proved here). Theorem 1.8 tells us we can't do this construction. □

1.4 Return to theory development

Lemma 1.13. Let $K \leq L$ be a field extension. Then

(i) $\alpha_1, \dots, \alpha_n \in L$ are algebraic over K if and only if $K \leq K(\alpha_1, \dots, \alpha_n)$ is a finite field extension.

(ii) If $K \leq M \leq L$ such that $K \leq M$ is finite, then there exist $\alpha_1, \dots, \alpha_n \in L$ such that $K(\alpha_1, \dots, \alpha_n) = M$.

Proof.

(i) By Corollary 1.5, α is algebraic over K if and only if $K \leq K[\alpha]$ is a finite field extension. α_i is algebraic over K and hence algebraic over $K(\alpha_1, \dots, \alpha_{i-1})$ and so

$$|K(\alpha_1, \dots, \alpha_i) : K(\alpha_1, \dots, \alpha_{i-1})| < \infty.$$

By the Tower law applied to

$$K \leq K(\alpha_1) \leq K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \dots, \alpha_n),$$

we get $|K(\alpha_1, \dots, \alpha_n) : K| < \infty$.

Conversely, consider $K \leq K(\alpha_i) \leq K(\alpha_1, \dots, \alpha_n)$. Then the tower law says that if $|K(\alpha_1, \dots, \alpha_n) : K| < \infty$ then $|K(\alpha_i) : K| < \infty$ and by Corollary 1.5, α_i is algebraic over K.

(ii) If $|M : K| = n$ then M is an n-dimensional K-vector space, so there exists a K-basis $\alpha_1, \dots, \alpha_n$ over M. Then $K(\alpha_1, \dots, \alpha_n) \leq M$. However, any element of M is a K-linear combination of $\alpha_1, \dots, \alpha_n$ and so lies in $K(\alpha_1, \dots, \alpha_n)$, so $M = K(\alpha_1, \dots, \alpha_n)$. □

Lemma 1.14. Suppose $K \leq L$, $K \leq L'$ are field extensions. Then

(i) Any K-homomorphism $\phi : L \to L'$ is injective and $K \leq \phi(L)$ is a field extension.

(ii) If $|L : K| = |L' : K| < \infty$ then any K-homomorphism $\phi : L \to L'$ is a K-isomorphism.

Proof.

(i) L is a field and $\ker \phi$ is an ideal of L.

Note $1 \mapsto 1$ and so $\ker \phi$ can't be the whole of L, hence $\ker \phi = \{0\}$. So $\phi(L)$ is a field and $K \leq \phi(L)$ is a field extension.

(ii) ϕ is an injective K-linear map, so $|\phi(L) : K| = |L : K|$. In general, $|\phi(L) : K| \leq |L' : K|$, but since $|L : K| = |L' : K|$ by assumption, we have $|\phi(L) : K| = |L' : K|$, hence $\phi(L) = L'$ and ϕ is a K-isomorphism $L \to L'$. (If $L' = L$ then ϕ would be a K-automorphism also.) □

Theorem 1.15 (Existence of splitting fields)**.** Let K be a field and $f(t) \in K[t]$. Then there exists a splitting field for f over K.

Proof. If $\deg f = 0$ then K is the splitting field for f over K.

Suppose $\deg f > 0$ and pick an irreducible factor $g(t)$ of $f(t)$ in $K[t]$, noting that $K \leq K[t]/(g(t))$ is a field extension.

Take

$$\alpha_1 = t + (g(t)) \in K[t]/(g(t)),$$

then $K[t]/(g(t)) = K(\alpha_1)$ and $g(\alpha_1) = 0$ in $K(\alpha_1)$. Therefore $f(\alpha_1) = 0$ in $K(\alpha_1)$ and we can write $f(t) = (t - \alpha_1)h(t)$ in $K(\alpha_1)[t]$.

Repeat, noting that $\deg h(t) < \deg f(t)$ and so we get

$$f(t) = a(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n)$$

where a is a constant in K. Thus, we have a factorisation of $f(t)$ in $K(\alpha_1, \ldots, \alpha_n)[t]$, and so $K(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f over K. □

Theorem 1.16 (Uniqueness of splitting fields)**.** If K is a field and $f(t) \in K[t]$, then the splitting field for f over K is unique up to K-isomorphism, that is, if there are two such splitting fields L and L', there is a K-isomorphism $\phi : L \to L'$.

Proof. Suppose L and L' are splitting fields for $f(t) \in K[t]$ over K. We need to show that there is a K-isomorphism $L \to L'$.

Suppose $K \leq M \leq L$ and there exist M' with $K \leq M' \leq L'$ and a K-isomorphism $\psi : M \to M'$. Clearly some M exists (we can take $M = K$), so we pick M so that $|M : K|$ is maximal among all such M, M', ψ.

We must show $M = L$ and $M' = L'$. Note that if $M = L$ then $f(t)$ splits over M:

$$f(t) = a(t - \alpha_1) \cdots (t - \alpha_n) \in M[t]$$

Apply ψ, we get an induced map $M[t] \to M'[t]$.

$$f(t) = \psi(f(t)) = \psi(a)(t - \psi(\alpha_1)) \cdots (t - \psi(\alpha_n))$$

Thus $f(t)$ splits over $\psi(M) = M'$. But L' is a splitting field and $M' \leq L'$, so $M' = L'$.

So, suppose $M \neq L$ and we'll get a contradiction of maximality of M. Since $M \neq L$, there is a root α of $f(t)$ in L which isn't in M. Factorise $f(t) = g(t)h(t)$ in $M[t]$ so that $g(t)$ is irreducible in $M[t]$ while $g(\alpha) = 0$ in L. Then there exists a K-homomorphism $M[t]/(g(t)) \to L$ given by $t + (g(t)) \mapsto \alpha$ which has image $M(\alpha)$.

The K-isomorphism $M[t] \to M'[t]$ induced by ψ maps $g(t) \in M[t]$ to $\gamma(t) \in M'[t]$. $f(t) = g(t)h(t)$ in $M[t]$ yields $f(t) = \gamma(t)\delta(t)$ in $M'[t]$.

We have a field extension $M' \leq M'[t]/(\gamma(t))$ and there exists a M'-homomorphism $M'[t]/(\gamma(t)) \to L'$ given by $t + (\gamma(t))$ by picking a root α' of $\gamma(t)$ in L'. However $\gamma(t) \mid f(t)$ in $M'[t]$ and hence in $L'[t]$ and so α' is also a root of $f(t)$ in L'. The M'-homomorphism gives a K-isomorphism

$$M'[t]/(\gamma(t)) \to M'(\alpha')$$

and so we have a K-isomorphism $M(\alpha) \to M'(\alpha')$. This contradicts the maximality of M, since $M \subsetneqq M(\alpha)$. □

Theorem 1.17. Let $K \leq L$ be a finite field extension. Then $K \leq L$ is normal $\iff$ L is the splitting field for some $f(t) \in K[t]$.

Proof. Later. □

Theorem 1.18. Let G be a finite subgroup of the multiplicative group of a field K. Then G is cyclic. In particular, the multiplicative group of a finite field is cyclic.

Proof. Let $|G| = n$. By the structure theorem of finite abelian groups from GRM,

$$G \cong C_{q_1^{m_1}} \times C_{q_2^{m_2}} \times \cdots \times C_{q_r^{m_r}}$$

with q_i prime, not necessarily distinct. However if $q = q_i = q_j$ for some $i \neq j$, there are at least q^2 distinct solutions of $t^q - 1 = 0$ in K (since $C_q \times C_q \cong$ subgroup of G). But in a field (or even an integral domain), a polynomial of degree q has at most q roots, a contradiction. So all the q_i are distinct and hence G is cyclic, generated by $(g_1, \dots, g_r)$ where g_i generates $C_{q_i^{m_i}}$ using the Chinese Remainder Theorem. □

2 Separable, normal and Galois extensions

Lemma 2.1. Let K be a field and $f(t), g(t) \in K[t]$. Then:

(a) $D(f(t)g(t)) = f'(t)g(t) + f(t)g'(t)$ (Leibniz' rule)

(b) Assume $f(t) \neq 0$. Then $f(t)$ has a repeated root in a splitting field L if and only if $f(t)$ and $f'(t)$ have a common irreducible factor in $K[t]$.

Proof.

(a) D is a K-linear map and so we only need to check for $f(t) = t^n$, $g(t) = t^m$. Left as an exercise.

(b) Let α be a repeated root in a splitting field L, then

$$f(t) = (t-\alpha)^2 g(t) \in L[t]$$
$$f'(t) = (t-\alpha)^2 g'(t) + 2(t-\alpha)g(t)$$

and so $f'(\alpha) = 0$. Therefore the minimal polynomial $f_\alpha(t)$ of α in $K[t]$ divides both $f(t)$ and $f'(t)$ and thus $f_\alpha(t)$ is a common irreducible factor of $f(t)$ and $f'(t)$.

Conversely, let $h(t)$ be a common irreducible factor of $f(t)$ and $f'(t)$ in $K[t]$. Pick a root α in L of $h(t)$.

So $f(\alpha) = 0 = f'(\alpha)$, thus $f(t) = (t-a)g(t)$ in $L[t]$, and $f'(t) = (t-a)g'(t) + g(t)$. Since $f'(\alpha) = 0$ we have $(t-a) \mid f'(t)$. and so $(t-a) \mid g(t)$. Hence $(t-a)^2 \mid f(t)$ and we have a repeated root. ☐

Corollary 2.2. If K is a field and $f(t) \in K[t]$ is irreducible:

(i) If the characteristic of K is 0, then $f(t)$ is separable over K.

(ii) If the characteristic of K is $p > 0$, then $f(t)$ is not separable if and only if $f(t) \in K[t^p]$.

Proof. By Lemma 2.1, $f(t)$ is not separable over K if and only if $f(t)$ and $f'(t)$ have a common irreducible factor. Since we're assuming $f(t)$ is irreducible, this is equivalent to saying $f'(t) = 0$.

$$f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$$
$$f'(t) = na_n t^{n-1} + \cdots + a_1$$

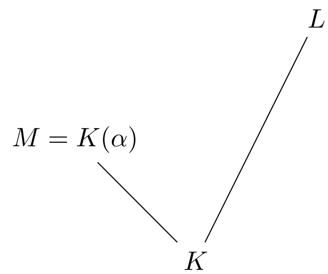
Thus $f'(t) = 0 \iff ia_i = 0$ for all $i > 0$.

(i) If $\operatorname{char} K = 0$ then $f'(t) \neq 0$ for any non-constant polynomial, so $f(t)$ is separable over K.

(ii) If $\operatorname{char} K = p > 0$ then if $f'(t) = 0$ we have $ia_i = 0$ for all $i > 0$, so $f(t)$ is not separable $\iff f(t) \in K[t^p]$. ☐

Lemma 2.3. Let $M = K(\alpha)$, where α is algebraic over K and let $f_\alpha(t)$ be the minimal polynomial of α over K.

Then, for any field extension $K \leq L$, the number of K-homomorphisms of M to L is equal to the number of distinct roots of $f_\alpha(t)$ in L. Thus this number is $\leq \deg f_\alpha(t) = |K(\alpha) : K| = |M : K|$.



Proof. We saw in Lemma 1.14 that any K-homomorphism $M \to L$ is injective, and we have

$$K(\alpha) \cong \frac{K[t]}{(f_\alpha(t))}.$$

For any root β of $f_\alpha(t)$ in L we can define a K-homomorphism

$$\begin{aligned} \frac{K[t]}{(f_\alpha(t))} &\to L \\ t + (f_\alpha(t)) &\mapsto \beta \end{aligned}$$

Thus we get a K-homomorphism $M \to L$.

Conversely, for any K-homomorphism $\phi : M \to L$ the image $\phi(\alpha)$ must satisfy

$$f_\alpha(\phi(\alpha)) = 0.$$

These processes are inverse to each other, giving a 1-1 correspondence

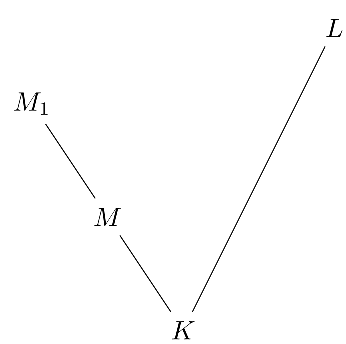
$$\{K \text{ homomorphisms } M \to L\} \longleftrightarrow \{\text{roots of } f_\alpha(t) \in L\}. \qquad \square$$

Corollary 2.4. The number of K-homomorphisms $K(\alpha) \to L = \deg f_\alpha(t) \iff L$ is large enough, in particular L contains a splitting field for $f_\alpha(t)$ and α is separable over K.

Proof. Immediate from Lemma 2.3. $\square$

Lemma 2.5. Let $K \leq M$ be a field extension and $M_1 = M(\alpha_1)$ (where α_1 is algebraic over M). Let $f(t)$ be the minimal polynomial of α_1 over M and let $K \leq L$. Let $\phi : M \to L$ be a K-homomorphism. Then there is a correspondence

$$\{\text{Extensions } \phi_1 : M_1 \to L \text{ of } \phi\} \longleftrightarrow \{\text{roots of } \phi(f(t)) \in L\}.$$



Proof. $f(t)$ is irreducible in $M[t]$, so $\phi(f(t))$ is irreducible in $\phi(M)[t]$. Any extension $\phi_1 : M \to L$ of ϕ produces a root $\phi_1(\alpha_1)$ of $\phi(f(t))$.

Conversely, given a root γ of $\phi(f(t))$ in L,

$$M_1 = M(\alpha_1) \cong \frac{M[t]}{(f(t))} \cong \frac{\phi(M)[t]}{(\phi(f(t)))} \cong \phi(M)(\phi) \leq L.$$

Thus we get an extension ϕ_1 of ϕ as required. □

Corollary 2.6. If L is large enough, the number of ϕ_1 which extend ϕ is equal to the number of distinct roots of $f(t)$ in L. This is equal to $|M_i : M| \iff \alpha$ is separable over M.

Proof. Immediate from Lemma 2.5. □

Corollary 2.7. Let $K \leq M \leq N$ be finite field extensions, $K \leq L$. Let $\phi : M \to L$ be a K-homomorphism. Then the number of extensions of ϕ to maps $\theta : N \to L$ is $\leq |N : M|$. Moreover, such a θ exists if L is large enough.

Proof. Pick $\alpha_1, \dots, \alpha_r$ so that $N = M(\alpha_1, \dots, \alpha_r)$ and set $M_i = M(\alpha_1, \dots, \alpha_i)$. Then we've got

$$M \leq M_1 \leq M_2 \leq \cdots \leq M_r = N.$$

Using Lemma 2.5, there are

$$\begin{aligned}
&\leq |M_1 : M| \ \text{ extensions } \phi_1 : M_1 \to L \text{ of } \phi \\
&\leq |M_2 : M_1| \ \text{ extensions } \phi_2 : M_2 \to L \text{ of } \phi_1 \\
&\vdots \\
&\leq |M_r : M_{r-1}| \ \text{ extensions } \phi_r : M_r \to L \text{ of } \phi_{r-1}
\end{aligned}$$

By the Tower law, the number of extensions $\theta : N \to L$ (recall $N = M_r$) of $\phi : M \to L$ is

$$\leq |M_r : M_{r-1}|\,|M_{r-1} : M_{r-2}| \cdots |M_1 : M| = |N : M|$$

where the last part comes from the proof of Lemma 2.5 - we need L to contain roots. □

Lemma 2.8. Let $K \leq N$ be a field extension with $|N : K| = n$ and $N = K(\alpha_1, \dots, \alpha_r)$ say. Then the following are equivalent:

(i) N is separable over K.

(ii) Each α_i is separable over $K(\alpha_1, \dots, \alpha_{i-1})$.

(iii) If $K \leq L$ is large enough there are exactly n distinct K-homomorphisms $N \to L$.

Proof. (i) ⇒ (ii). N is separable over $K \implies \alpha_i$ is separable over K. The minimal polynomial of α_i over $K(\alpha_1, \dots, \alpha_{i-1})$ divides the minimal polynomial of α_i over K (in $K(\alpha_1, \dots, \alpha_{i-1})[t]$).

So if the latter has distinct roots in a splitting field then the former does. So α_i separable over $K \implies \alpha_i$ separable over $K(\alpha_1, \dots, \alpha_{i-1})$.

(ii) ⇒ (iii) follows from **??**.

(iii) $\Rightarrow$ (i). Assume (iii) is true and (i) false, aiming for a contradiction. So, $\exists \beta \in N$ that is not separable over K, so there are $\lneq |K(\beta) : K|$ K-homomorphisms $\phi : K(\beta) \to L$ by Corollary 2.4.

By Corollary 2.7, ϕ extends to $\leq |N : K(\beta)|$ extensions $\theta : N \to L$, and so there are $\lneq |N : K(\beta)|\,|K(\beta) : K|$ K-homomorphisms $N \to L$, contradiction. ☐

Corollary 2.9. A finite extension is separable $\iff$ it is separably generated.

Proof. Lemma 2.8. ☐

Lemma 2.10. If $K \leq M \leq L$ finite field extensions, $M \leq L$, then

$$K \leq M,\ \ M \leq L \text{ are both separable } \iff K \leq L \text{ is separable}$$

Proof. Example sheet. ☐

Theorem 2.11 (Primitive Element Theorem)**.** Any finite separable extension $K \leq M$ is a simple extension, that is, $M = K(\alpha)$ for some α, called a primitive element.

Proof. First deal with the case where K is a finite field. Then M is also finite and we can take α to be a generator of the multiplicative group of M, which is cyclic.

Now assume K is an infinite field.

Since $K \leq M$ is a finite extension, $M = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some α_i. It is enough to show that any field $M = K(\alpha, \beta)$ with β separable over K is of the form $K(\gamma)$.

Take $f(t)$ and $g(t)$ to be the minimal polynomials of α and β over K and let L be the splitting field for $f(t)g(t)$ over $K(\alpha, \beta)$. Say the distinct zeros of $f(t)$ in L are $\alpha = \alpha_1, \ldots, \alpha_a$ and of $g(t)$ are $\beta = \beta_1, \ldots, \beta_b$.

By separability, $b = \deg g(t)$. Choose $\lambda \in K$ such that all $\alpha_i + \lambda\beta_j$ are distinct, which is possible since K is infinite. Set $\gamma = \alpha + \lambda\beta$.

Let $F(t) = f(\gamma - \lambda t) \in K(\gamma)[t]$. We have $g(\beta) = 0$ and $F(\beta) = f(\alpha) = 0$. Thus $F(t)$ and $g(t)$ have a common zero.

Any other common zero would have to be β_j for some $j > 1$. But then $F(\beta_j) = f(\alpha + \lambda(\beta - \beta_j))$. By assumption, $\alpha + \lambda(\beta - \beta_j)$ is never an α_i and so $F(\beta_j) \neq 0$. Separability of $g(t)$ says its linear factors are all distinct, so $(t - \beta)$ is a highest common factor of $F(t)$ and $g(t)$ in $L[t]$.

However the minimal polynomial $h(t)$ of β over $K(\gamma)$ then divides $F(t)$ and $g(t)$ in $K(\gamma)[t]$ and hence in $L[t]$. This implies $h(t) = t - \beta$ and so $\beta \in K(\gamma)$. Therefore $\alpha = \gamma - \lambda\beta \in K(\gamma)$ and so $K(\alpha, \beta) \subset K(\gamma)$ and equality holds since $\gamma \in K(\alpha, \beta)$. ☐

2.1 Trace and Norm

Theorem 2.12. With the above notation, suppose $f_\alpha(t) = t^s + a_{s-1}t^{s-1} + \cdots + a_0$ is the minimal polynomial for α over K. Let $r = |M : K(\alpha)|$, then the characteristic polynomial of θ_α is $(f_\alpha(t))^r$.

Note

$$|M : K| = |M : K(\alpha)|\,|K(\alpha) : K| = rs.$$

Then $\mathrm{Tr}_{M/K}(\alpha) = -ra_{s-1}$ and $N_{M/K} = ((-1)^s a_0)^r$.

Proof. Regard M as a $K(\alpha)$-vector space with basis $1 = \beta_1, \dots, \beta_r$. Now take the K-vector space basis $1, \alpha, \alpha^2, \dots, \alpha^{s-1}$ of $K(\alpha)$. So, $1, \alpha, \alpha^2, \dots, \alpha^{s-1}, \beta_2, \beta_2\alpha, \dots, \beta_2\alpha^{s-1}, \beta_3, \dots$ is a K-vector space basis for M. Multiplication by α in $K(\alpha)$ is represented by matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & 1 & \dots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{s-1} \end{pmatrix}$$

an $s \times s$ matrix whose characteristic polynomial is $f_\alpha(t)$.

Multiplication by α in M is represented by the $rs \times rs$ matrix

$$\begin{pmatrix} \mathbf{A} & 0 & 0 & \dots & 0 \\ 0 & \mathbf{A} & 0 & \dots & 0 \\ 0 & 0 & \mathbf{A} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \mathbf{A} \end{pmatrix}$$

whose characteristic polynomial is $(f_\alpha(t))^r$.

Look at the terms of this characteristic polynomial to get the trace and norm. □

Theorem 2.13. Let $K \leq M$ be a finite separable field extension and $|M : K| = n$, $\alpha \in M$. Let $K \leq L$ be large enough so that there are n distinct K-homomorphisms

$$\sigma_1, \sigma_2, \dots, \sigma_n : M \longrightarrow L.$$

Then the characteristic polynomial of $\theta_\alpha : M \to M$ (the multiplication map) is

$$\prod_{i=1}^{n} (t - \sigma_i(\alpha))$$

hence

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \qquad \text{and} \qquad N_{M/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

Proof. Write

$$\begin{aligned} f_\alpha(t) &= (t - \alpha_1) \dots (t - \alpha_s) \in L[t] \\ &= t^s + a_{s-1}t^{s-1} + \dots + a_0 \end{aligned}$$

the minimal polynomial of α over K (where L large enough implies $f_\alpha(t)$ splits in L). There are s K-homomorphisms $K[\alpha] \to L$ corresponding to maps sending α to α_i.

Each of these extends in $|M : K(\alpha)|$ ways to give K-homomorphisms $M \to L$ (by separability and Corollary 2.6).

However each of these extensions of a map sending $\alpha \to \alpha_i$ still sends $\alpha \to \alpha_i$. Set $r = |L : K(\alpha)|$. Thus there are r maps sending $\alpha \to \alpha_i$ for each i. Thus if the $n(= rs)$

distinct K-homomorphisms $M \to L$ are $\sigma_1, \dots, \sigma_n$, then

$$\sum_{i=1}^{n} \sigma_i(\alpha) = r(\alpha_1 + \alpha_2 + \cdots + \alpha_s) = -ra_{s-1} = \mathrm{Tr}_{M/K}(\alpha)$$
$$\prod_{i=1}^{n} \sigma_i(\alpha) = ((-1)^s a_0)^n = N_{M/K}(\alpha). \qquad \square$$

Theorem 2.14. Let $K \le M$ be a finite separable extension. Then we define a K-bilinear form

$$\begin{aligned} T : M \times M &\to K \\ (x, y) &\longmapsto \mathrm{Tr}_{M/K}(xy). \end{aligned}$$

Then this is non-degenerate and in particular the K-linear map $\mathrm{Tr}_{M/K} : M \to K$ is non-zero, and hence surjective.

Proof. Separability and finiteness give $M = K(\alpha)$ for some α, by Theorem 2.11. We have a K-basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ of $K(\alpha)$ where $n = |M : K|$. The K-bilinear form is represented by

$$A = \begin{pmatrix} \mathrm{Tr}_{M/K}(1) & \mathrm{Tr}_{M/K}(\alpha) & \dots \\ \mathrm{Tr}_{M/K}(\alpha) & \mathrm{Tr}_{M/K}(\alpha^2) & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}.$$

Let L be the splitting field of the minimal polynomial $f_\alpha(t)$ of α over K.

Thus $f_\alpha(t) = (t - \alpha_1) \cdots (t - \alpha_n)$ with $\alpha_1, \dots, \alpha_n \in L$. The entries in A are of the form $\mathrm{Tr}_{M/K}(\alpha^e)$ which is $\alpha_1^e + \cdots + \alpha_n^e$ using Theorem 2.13.

Now consider $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$, the discriminant of V:

$$V = \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{pmatrix}.$$

Observe that $VV^T = A$, and $0 \ne \Delta^2 = \left|VV^T\right| = |A|$, so A is non-singular and therefore the bilinear form T is non-degenerate. $\square$

2.2 Normal extensions

Proof. Assume $K \le M$ is normal. Pick $\alpha_1, \dots, \alpha_r \in M$ so that $M = K(\alpha_1, \dots, \alpha_r)$. Let $f_{\alpha_i}(t)$ be the minimal polynomial for α_i over K.

Let

$$f(t) = f_{\alpha_1}(t) f_{\alpha_2}(t) \dots f_{\alpha_r}(t).$$

By normality, each $f_{\alpha_i}(t)$ splits over M and therefore $f(t)$ splits over M. M is the splitting field of $f(t)$ over K since if $\beta_1, \dots, \beta_m$ are the roots of $f(t)$ then $M = K(\beta_1, \dots, \beta_m)$.

Conversely, suppose M is a splitting field for $f(t)$ over K. Thus $M = K(\beta_1, \dots, \beta_m)$ where the β_j are the roots of $f(t)$ in M.

Take $\alpha \in M$. Let $f(t)$ be the minimal polynomial of α over K. Let $M \leq L$ large enough so that $f_\alpha(t)$ splits in L and consider K-homomorphisms $\phi : M \to L$. $\phi(\beta_j)$ is also a root of $f(t)$ and is therefore one of the β_js. Injectivity of K-homomorphisms (Lemma 1.14) implies that ϕ generate the β_j.

$M = K(\beta_1, \ldots, \beta_m)$ and so ϕ is determined by the images of the β_j and thus $\phi(M) = M$. However if α_i is a root of $f_\alpha(t)$ in L, there is a K-homomorphism

$$\begin{aligned} K(\alpha) &\longrightarrow K(\alpha_i) \leq L \\ \alpha &\longmapsto \alpha_i. \end{aligned}$$

This extends by Corollary 2.7 to a K-homomorphism $\phi : M \to L$ with $\phi(\alpha) = \alpha_i$. But $\phi(M) = M$, so $\alpha_i \in M$. Thus M is normal over K. □

Lemma 2.15.

$$\mathrm{Aut}_K(M) \leq |M : K| .$$

Proof. Corollary 2.7. □

Theorem 2.16. Let $K \leq M$ be a finite field extension. Then $|\mathrm{Aut}_K(M)| = |M : K|$ iff the extension is both normal and separable.

Proof of Theorem 2.16. ($\Rightarrow$). Suppose $|\mathrm{Aut}_K(M)| = |M : K| = n$. Let L be large enough containing M.

The n distinct K-homomorphisms $\phi : M \to M \leq L$ give us n K-homomorphisms $\phi : M \to L$ and Lemma 2.8 says that M is separable over K. For normality, pick $\alpha \in M$ with minimal polynomial $f_\alpha(t)$ over K.

Take $M = K(\alpha_1, \ldots, \alpha_m)$ as in the proof of Corollary 2.7 with $\alpha = \alpha_1$ and $L = M$. We only get $|M : K|$ extensions of the inclusion $K \hookrightarrow M$ if each inequality in the proof is an equality. In particular we need the number of K-homomorphisms $K(\alpha_1) \to M$ to be $|K(\alpha_1) : K|$.

But then Lemma 2.3 says we have $|K(\alpha) : K|$ distinct roots of $f_\alpha(t)$ in M. Thus $f_\alpha(t)$ splits over M.

Conversely, suppose $K \leq M$ is separable and normal. Then for $K \leq M \leq L$ with L large enough, separability implies there are $|M : K|$ K-homomorphisms $\phi : M \to L$ by Lemma 2.8. However since $K \leq M$ is normal, it is the splitting field for some polynomial $f(t) \in K[t]$ (Theorem 1.17) and thus $M = K(\alpha_1, \ldots, \alpha_n)$, where $f(t) = (t - \alpha_1) \cdots (t - \alpha_n)$. Note that $\phi(a_j)$ is also a root of $\phi(f(t)) = f(t)$ and is therefore one of the α_js. Thus $\phi(M) = M$. Thus we have $|M : K|$ K-homomorphisms $\phi : M \to M$. □

3 Fundamental Theorem of Galois Theory

3.1 Artin's Theorem

Theorem 3.1 (Fundamental Theorem of Galois Theory)**.** Let $K \le L$ be a finite Galois extension. Then

(i) there is a 1 to 1 correspondence

$$\begin{aligned} \{\text{intermediate subfields } K \le M \le L\} &\longleftrightarrow \{\text{subgroups } H \text{ of } \mathrm{Gal}(L/K)\} \\ M &\longmapsto \mathrm{Aut}_M(L) \\ L^H &\longleftarrow\!\shortmid H \end{aligned}$$

This is called the Galois correspondence.

(ii) H is a normal subgroup of $\mathrm{Gal}(L/K)$ iff $K \le L^H$ is normal iff $K \le L^H$ is Galois.

(iii) If $H \lhd \mathrm{Gal}(L/K)$ then the map

$$\theta : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L^H/K)$$

given by restriction to L^H is a surjective group homomorphism with kernel H.

Theorem 3.2 (Artin's Theorem)**.** Let $K \le L$ be a field extension and H a finite subgroup of $\mathrm{Aut}_K(L)$. Let $M = L^H$. Then $M \le L$ is a finite Galois extension, and $H = \mathrm{Gal}(L/M)$.

Proof of Artin's Theorem. Take $\alpha \in L$.
First step: Show that $|M(\alpha) : M| \le |H|$. Let

$$\underbrace{\{\alpha_1, \dots, \alpha_n\}}_{\text{all distinct}} = \{\, \phi(\alpha) \mid \phi \in H \,\}.$$

Define $g(t) = \prod_{i=1}^n (t - \alpha_i)$. Each ϕ induces a homomorphism $L[t] \to L[t]$ that sends $g(t)$ to itself, since ϕ is permuting the α_i. So the coefficients of $g(t)$ are fixed by all $\phi \in H$ and thus they all lie in $L^H = M$. Thus $g(t) \in M[t]$.

By definition, $g(\alpha) = 0$ since α is one of the α_i. Hence the minimal polynomial $f_\alpha(t)$ of α over M divides $g(t)$. Thus $|M(\alpha) : M| = \deg f_\alpha(t) \le \deg g(t) \le |H|$. We've shown that α is algebraic over M. Moreover, $f_\alpha(t)$ is separable since $g(t)$ is. Thus $M \le L$ is a separable extension.

Next step: Show that $M \le L$ is a simple extension. Pick $\alpha \in L$ with $|M(\alpha) : M|$ maximal. We'll show that $L = M(\alpha)$ for this choice of α. Suppose $\beta \in L$. Then $M \le M(\alpha, \beta)$ is finite and is separably generated and hence is a finite separable extension by Lemma 2.8.

By the Primitive Element Theorem, $M(\alpha, \beta) = M(\gamma)$ for some γ. But $M \le M(\alpha) \le M(\gamma)$. The maximality of $|M(\alpha) : M|$ forces $M(\alpha) = M(\gamma)$. Thus $\beta \in M(\gamma) = M(\alpha)$ and so $L = M(\alpha)$ so $|L : M| \le |H|$.

Finally,

$$|L : M| = |M(\alpha) : M| \le |H| \le |\mathrm{Aut}_M(L)| \underset{\substack{\uparrow \\ \text{Lemma 2.15}}}{\le} |L : M|$$

We must have equality throughout, and so $|L : M| = |\mathrm{Aut}_M(L)| = |H|$. Hence by Theorem 2.16 we have $M \le L$ is a finite Galois extension and $H = \mathrm{Gal}(L/M)$. ☐

Theorem 3.3. Let $K \leq L$ be a finite field extension. Then the following are equivalent:

(i) $K \leq L$ is Galois

(ii) $L^H = K$ when $H = \mathrm{Aut}_K(L)$

Proof. **(i) $\Rightarrow$ (ii):** Let $M = L^H$ where $H = \mathrm{Aut}_K(L)$. By Artin's Theorem, $M \leq L$ is a Galois extension, and $|L : M| = |\mathrm{Gal}(L/M)|$ and $H = \mathrm{Gal}(L/M)$.

However if $K \leq L$ is Galois then $|H| = |\mathrm{Aut}_K(L)| = |L : K|$ by Theorem 2.16. Thus $|L : M| = |L : K|$ and so $M = K$.

(ii) $\Leftarrow$ (i): Use Theorem 3.2. □

Proof of Fundamental Theorem of Galois Theory.

(i) Composing the maps $H \to L^H$ and $M \to \mathrm{Gal}(L/M)$ gives $H \to H$ by Theorem 3.2. Also $M \longrightarrow \mathrm{Gal}(L/M) \longrightarrow L^H$ where $H = \mathrm{Gal}(L/M)$ yields M since $M \leq L^H$ where $H = \mathrm{Gal}(L/M)$ and

$$\left|L : L^H\right| \underset{\substack{(2.16)\\(3.2)}}{=} |H| = |\mathrm{Gal}(L/M)| \underset{(2.16)}{=} |L : M|$$

So $M = L^H$.

(ii) Take $H \leq \mathrm{Gal}(L/K)$, then $L^{\phi H \phi^{-1}} = \phi(L^H)$ when $\phi \in \mathrm{Gal}(L/K)$. So by (i), H is normal iff $\phi(L^H) = L^H$. Set $M = L^H$.

We'll show that $K \leq M$ is normal iff $\phi(M) = M \quad \forall \phi \in \mathrm{Gal}(L/K)$. $K \leq M$ is normal $\implies$ $\phi(M) = M$ by remark 2 after the statement of Fundamental Theorem of Galois Theory.

Conversely if $\phi(M) = M \quad \forall \phi \in \mathrm{Gal}(L/K)$, pick $\alpha \in M$ and let $f_\alpha(t)$ be its minimal polynomial over K. Take β to be a root of $f_\alpha(t)$ in L (possible by normality). Then there is a K-homomorphism

$$\begin{array}{ccc} K(\alpha) \cong \frac{K[t]}{(f_\alpha(t))} & \longrightarrow & K(\beta) \cong \frac{K[t]}{(f_\alpha(t))} \leq L \\ \alpha & \longmapsto & \beta. \end{array}$$

This extends to a K-homomorphism $\phi : L \to L$.

However we are assuming $\phi(M) = M$ and so $\phi(\alpha) = \beta \in M$. Thus $K \leq M$ is normal. Note that $K \leq L^H$ is separable since $K \leq L^H \leq L$ and $K \leq L$ separable.

(iii) By remark 2 after statement of Theorem 3.1, the restriction map

$$\theta : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$$

is defined. Surjectivity follows from being able to extend a K-homomorphism $L^H \to L^H \leq L$ to a K-homomorphism $L \to L$ by Corollary 2.7. Clearly $H \leq \mathrm{Ker}\,\theta$. However

$$\begin{aligned} \frac{|L : K|}{|\mathrm{Ker}\,\theta|} &= \frac{\mathrm{Gal}(L/K)}{|\mathrm{Ker}\,\theta|} \\ &= \left|\mathrm{Gal}(L^H/K)\right| \quad \text{by surjectivity of } \theta \\ &= \left|L^H : K\right| \quad \text{since } K \leq L^H \text{ is Galois} \\ &= \frac{|L : K|}{|L : L^H|} \quad \text{by Tower law} \end{aligned}$$

So $|\operatorname{Ker}\theta| = \left|L : L^H\right| = \left|\operatorname{Gal}(L/L^H)\right| = |H|$ by Theorem 3.2, so $H = \operatorname{Ker}\theta$. $\square$

3.2 Galois groups of polynomials

Lemma 3.4. Suppose $f(t)$ is separable, $f(t) = g_1(t)\cdots g_s(t)$ with $g_i(t)$ irreducible in $K[t]$ is a factorisation in $K[t]$. Then the orbits of $\operatorname{Gal}(f)$ on the roots of $f(t)$ correspond to the factors $g_j(t)$.

$$\text{Two roots are in the same orbit} \iff \text{they are roots of the same } g_j(t).$$

In particular, if $f(t)$ is irreducible in $K[t]$ there is one orbit, i.e., $\operatorname{Gal}(f)$ acts transitively on the roots of $f(t)$.

Proof. Let α_k, α_l be in the same orbit under $\operatorname{Gal}(f)$. Thus there is $\phi \in \operatorname{Gal}(f)$ with $\alpha_l = \phi(\alpha_k)$. But if α_k is a root of $g_j(t)$ then $\phi(\alpha_k) = \alpha_l$ is also a root of $g_j(t)$.

Conversely, if α_k, α_l are roots of $g_j(t)$ then

$$\begin{tikzcd} K(\alpha_k) \arrow[rrrr, bend right, "\phi_0"'] & \cong & \frac{K[t]}{(g_j(t))} & \cong & K(\alpha_l) & \leq & L \end{tikzcd}$$

with $\phi_0(\alpha_k) = \alpha_l$. ϕ_0 extends to a $\phi : L \to L \in \operatorname{Gal}(L/K)$, thus α_k, α_l are in the same orbit. $\square$

Lemma 3.5. The transitive subgroups of S_n for $n \leq 5$ are

$$\begin{array}{ll} n = 2: & S_2\ (\cong C_2) \\ n = 3: & A_3\ (\cong C_3),\ S_3 \\ n = 4: & C_4,\ V_4,\ D_8,\ A_4,\ S_4 \\ n = 5: & C_5,\ D_{10},\ H_{20},\ A_5,\ S_5 \end{array}$$

where H_{20} is generated by a 5-cycle and a 4-cycle.

Proof. Exercise. $\square$

Theorem 3.6. Let p be a prime, and $f(t)$ irreducible $\in \mathbb{Q}[t]$ of degree p. Suppose $f(t)$ has exactly 2 non-real roots in $\mathbb{C}$. Then $\operatorname{Gal}(f)$ over $\mathbb{Q} \cong S_p$.

Proof. $\operatorname{Gal}(f)$ acts on the p distinct roots of $f(t)$ in a splitting field L of $f(t)$ (in $\mathbb{C}$). By Lemma 3.4, the irreducibility of $f(t)$ implies that $\operatorname{Gal}(f)$ is acting transitively on the p roots. By the orbit-stabiliser theorem, $p \mid |\operatorname{Gal}(f)|$ but $|\operatorname{Gal}(f)| \leq |S_p| = p!$ and so $\operatorname{Gal}(f)$ has a Sylow p-subgroup of order p, necessarily cyclic. Thus, $\operatorname{Gal}(f)$ contains a p-cycle.

The supposition that we have precisely 2 non-real roots gives that complex conjugation yields a transposition in $\operatorname{Gal}(f)$. The p-cycle and transposition generate the whole of S_p. $\square$

Proof. $f(t)$ is irreducible by Eisenstein's criterion with $p = 3$. We want to show that $f(t)$ has three real roots, two non-real ones and apply Theorem 3.6.

$$f(-2) = -17,\ f(-1) = 8,\ f(1) = -2,\ f(2) = 23$$

and $f'(t) = 5t^4 - 6$ which has two real roots. From the intermediate value theorem, f has at least three real roots, and by Rolle's theorem there are at most three real roots, so we are done. $\square$

Lemma 3.7. Let $f(t)$ be separable $\in K[t]$ of degree n with $\operatorname{char} K \neq 2$. Then

$$\mathrm{Gal}(f) \leq A_n \iff D(f) \text{ is a square in } K.$$

Proof. Let L be a splitting field of $f(t)$ over K. Then $D(f) \neq 0$ and is fixed by all elements of $G = \mathrm{Gal}(L/K)$ as the latter permutes the roots. Thus $D \in K$, since $L^G = K$ (by Galois correspondence).

On the other hand, if $\sigma \in G$ then $\sigma(\Delta) = (\mathrm{sgn}\sigma)\Delta$ where we're regarding G as a subgroup of S_n and the signature of σ:

$$\mathrm{sgn}\sigma = \begin{cases} +1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}$$

(This is where we need $\operatorname{char} K \neq 2$).

Thus if $G \leq A_n$ we get that Δ is fixed by all $\sigma \in G$. Thus $\Delta \in K = L^G$. Otherwise if $G \not\leq A_n$, we get $\sigma(A) = -\Delta$ if σ is an odd permutation, and so $\Delta \notin K = L^G$. Note that if D does have square roots, they must be $\pm\Delta$. $\square$

Theorem 3.8 (Mod p reduction)**.** Let $f(t) \in \mathbb{Z}[t]$ be monic of degree n with n distinct roots in a splitting field. Let p be a prime such that $\overline{f}(t)$, the reduction of $f(t)$ mod p also has n distinct roots in a splitting field. Let $\overline{f}(t) = \overline{g_1}(t) \cdots \overline{g_s}(t)$ be the factorisation into irreducibles in $\mathbb{F}_p[t]$ with $n_j = \deg \overline{g_j}(t)$. Then $\mathrm{Gal}(\overline{f}) \hookrightarrow \mathrm{Gal}(f)$ and has an element of cycle type $(n_1, n_2, \ldots, n_s)$.

Proof. We will talk about the last sentence after thinking about Galois groups of finite fields. The fact that $\mathrm{Gal}(\overline{f}) \hookrightarrow \mathrm{Gal}(f)$ is from Number Fields - see Tony Scholl's teaching page on Galois. $\square$

3.3 Galois Theory of Finite Fields

Theorem 3.9 (Galois groups of finite fields)**.** Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = p^r$. Then $\mathbb{F}_p \leq \mathbb{F}$ is a Galois extension with $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) = G$, a cyclic group with the Frobenius automorphism as generator.

Proof. It remains to show that the order of the Frobenius automorphism is r. Suppose $\phi^s = \mathrm{id}$. Then $\alpha^{p^s} = \alpha \ \forall \alpha \in \mathbb{F}$. But $t^{p^s} - t$ has at most p^s roots in $\mathbb{F}$, so we deduce that $s \geq r$. Observe that $\phi^r = \mathrm{id}$ since $\alpha^{p^n} = \alpha$, $\forall \alpha \in \mathbb{F}$.

Now apply the Fundamental Theorem of Galois Theory:

$$\{\mathbb{F}_p \leq M \leq \mathbb{F} \text{ intermediate fields } M\} \longleftrightarrow \{\text{subgroups } H \leq G\}$$

where $G = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ is cyclic.

But we know all about subgroups of a cyclic group with generator ϕ of order r. There is exactly one subgroup of order s for each $s \mid r$ generated by $\phi^{\frac{r}{s}}$. The corresponding intermediate subfields are the fixed fields $\mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle}$, and $\left| \mathbb{F} : \mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle} \right| = s$. By the Tower Law, $\left| \mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle} : \mathbb{F}_p \right| = \frac{r}{s}$. Observe that all subgroups of cyclic groups are normal and therefore all our intermediate fields are normal extensions of $\mathbb{F}_p$.

By Theorem 3.1 part (iii), $\mathrm{Gal}(\mathbb{F}^{\langle \phi^{\frac{r}{s}} \rangle}/F_p) \cong \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)/H$ where $H = \langle \phi^{\frac{r}{s}} \rangle$. $\square$

Corollary 3.10. Let $\mathbb{F}_p \leq M \leq \mathbb{F}$ be finite fields. Then $\mathrm{Gal}(\mathbb{F}/M)$ is cyclic, generated by ϕ^u, where ϕ is the Frobenius automorphism and $|M| = p^u$ and M is the fixed field of $\langle \phi^u \rangle$.

Proof. Set $n = \frac{r}{s}$. □

Theorem 3.11 (Existence of finite fields)**.** Let p be a prime and $u \geq 1$. Then there is a field of order p^u, unique up to isomorphism.

Proof. Consider the splitting field L of $f(t) = t^{p^u} - t$ over $\mathbb{F}_p$. It is a finite Galois extension $\mathbb{F}_p \leq L$. However the roots of $f(t)$ form a field, the fixed field of ϕ^u. Set $L = \mathbb{F}$ and $|\mathbb{F} : \mathbb{F}_p| = u$. □

4 Cyclotomic and Kummer extensions

4.1 Cyclotomic extensions

Lemma 4.1. $\Phi_m(t) \in \mathbb{Z}[t]$ if $\operatorname{char} K = 0$ (with $\mathbb{Q} \hookrightarrow K$, prime subfield). $\Phi_m(t) \in \mathbb{F}_p[t]$ if $\operatorname{char} K = p$ (with $\mathbb{F}_p \hookrightarrow K$, prime subfield).

Proof. Induct on m. $m = 1$ is clearly true.

For $m > 1$, consider

$$f(t) = t^m - 1 = \Phi_m(t) \left(\prod_{\substack{d|m \\ d \neq m}} \Phi_d(t) \right).$$

Note that $\prod_{\substack{d|m \\ d \neq m}} \Phi_d(t)$ is monic and is defined in $\mathbb{Z}[t]$ or $\mathbb{F}_p[t]$ by induction.

If $\operatorname{char} K = 0$, we deduce $\Phi_m(t) \in \mathbb{Q}[t]$ by division of polynomials and by Gauss' Lemma it is in $\mathbb{Z}[t]$. If $\operatorname{char} K = p > 0$, we deduce by division that $\Phi_m(t) \in \mathbb{F}_p[t]$. □

Lemma 4.2. The homomorphism $\theta : G \to (\mathbb{Z}/m\mathbb{Z})^\times$ defined in **??** is an isomorphism iff $\Phi_m(t)$ is irreducible.

Proof. We know from Lemma 3.4 that the orbits of $G = \operatorname{Gal}(L/K)$ correspond to the factorisation of $f(t)$ in $K[t]$. In particular, the primitive mth roots of unity form one orbit iff $\Phi_m(t)$ is irreducible. Then θ is surjective iff $\Phi_m(t)$ is irreducible. □

Theorem 4.3. Let L be the mth cyclotomic extension of finite field $\mathbb{F} = \mathbb{F}_q$ where $q = p^n$. Then the Galois group $G = \operatorname{Gal}(L/\mathbb{F})$ is isomorphic to the cyclic subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ generated by q.

Proof. We know from Corollary 3.10 that G is generated by $\alpha \mapsto \alpha^{p^n} = \alpha^q$ so $\theta(G) = \langle q \rangle \leq (\mathbb{Z}/m\mathbb{Z})^\times$. □

Theorem 4.4. For all $m > 0$, $\Phi_m(t)$ is irreducible in $\mathbb{Z}[t]$ and hence in $\mathbb{Q}[t]$. Thus θ in **??** is an isomorphism and thus $\operatorname{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ where ξ = primitive mth root of unity.

Proof of Theorem 4.4. Gauss' Lemma gives us that irreducibility in $\mathbb{Z}[t]$ implies irreducibility in $\mathbb{Q}[t]$. From Lemma 4.1, irreducibility corresponds to surjectivity of θ. It's left to show that $\Phi_m(t)$ is irreducible in $\mathbb{Z}[t]$.

Suppose not, and $\Phi_m(t) = g(t)h(t)$ in $\mathbb{Z}[t]$ with $g(t)$ irreducible. monic and $\deg g(t) \lneq \deg \Phi_m(t)$. Let $\mathbb{Q} \leq L$ be the mth cyclotomic extension and ξ be a root of $g(t)$, ξ primitive mth root of unity.

Claim: if $p \nmid m$, p prime, then ξ^p is also a root of $g(t)$ in L. Suppose not. Then ξ^p is also a primitive mth root of 1, since $p \nmid m$, as a root of $\Phi_m(t)$. By the supposition, ξ^p is a root of $h(t)$. Define $r(t) = h(t^p)$. Then $r(\xi) = 0$ but $g(t)$ is the minimal polynomial of ξ over $\mathbb{Q}$. So $g(t) \mid r(t)$ in $\mathbb{Q}[t]$.

By Gauss' Lemma, $r(t) = g(t)s(t)$ with $s(t) \in \mathbb{Z}[t]$. Now reduce mod p. $\overline{r}(t) = \overline{g}(t)\overline{s}(t)$. But $\overline{r}(t) = \overline{h}(t^p) = (\overline{h}(t))^p$. If $\overline{a}(t)$ is any irreducible factor of $\overline{g}(t)$ in $\mathbb{F}_p[t]$ then $\overline{a}(t) \mid (\overline{h}(t))^p$ and so $\overline{a}(t) \mid \overline{h}(t)$. But then $(\overline{a}(t))^2 \mid \overline{g}(t)\overline{h}(t) = \overline{\Phi_m}(t)$. Hence $\overline{\Phi_m}(t)$ has a repeated root and thus $t^m - 1$ has repeated root mod p. Contradiction, since $p \nmid m$, so claim is true.

Now consider a root γ of $h(t)$. Then it is also a primitive root of 1 and so $\gamma = \xi^i$ for some i with $(i, m) = 1$. Write $i = p_1 \cdots p_k$ factorisation with p_j prime, not necessarily distinct, $p_j \nmid m$. Applying the claim repeatedly we get that γ is a root of $g(t)$, and so $\Phi_m(t)$ has a repeated root.

Hence $\Phi_m(t)$ is irreducible over $\mathbb{Q}$. □

4.2 Kummer Theory

Theorem 4.5. Let $f(t) = t^m - \lambda \in K[t]$ and $\operatorname{char} K \nmid m$. Then the splitting field L of $f(t)$ over K contains a primitive mth root of unity ξ and $\operatorname{Gal}(L/K(\xi))$ is cyclic of order dividing m. Moreover $f(t)$ is irreducible over $K(\xi)$ iff $|L : K(\xi)| = m$.

Proof of Theorem 4.5. Since $t^m - \lambda$ and mt^{m-1} are coprime, we know that $t^m - \lambda$ has distinct roots $\alpha_1, \ldots, \alpha_m$ in the splitting field L. Since $(\alpha_i \alpha_j^{-1})^m = \lambda\lambda^{-1} = 1$, the elements $1 = \alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \ldots, \alpha_m\alpha_1^{-1}$ are m distinct mth roots of unity in L and so

$$t^m - \lambda = (t - \beta)(t - \xi\beta)(t - \xi^2\beta) \cdots (t - \xi^{m-1}\beta) \in L[t]$$

where $\beta = \alpha_1$ and ξ primitive mth root of unity.

So $L = K(\xi, \beta)$. Let $\sigma \in \operatorname{Gal}(L/K(\xi))$, which is determined by its action on β. Note that $\sigma(\beta)$ is another root of $t^m - \lambda$ and so $\sigma(\beta) = \xi^{j(\sigma)}\beta$, where $0 \le j(\sigma) < m$. Also, if $\sigma, \tau \in \operatorname{Gal}(L/K(\xi))$ then

$$\tau\sigma(\beta) = \tau(\xi^{j(\sigma)}\beta) = \xi^{j(\sigma)}\tau(\beta) = \xi^{j(\sigma)}\xi^{j(\tau)}\beta$$

since ξ is fixed by τ. Thus $\sigma \to j(\sigma)$ gives a group homomorphism

$$\theta : \operatorname{Gal}(L/K(\xi)) \to \mathbb{Z}/m\mathbb{Z}.$$

Note that $j(\sigma) = 1$, only if σ is the identity and so θ is injective. Hence $\operatorname{Gal}(L/K(\xi)) \cong$ subgroup of $\mathbb{Z}/m\mathbb{Z}$. Finally $|L : K(\xi)| = |\operatorname{Gal}(L/K(\xi))| \le m$ with equality exactly when the action of $\operatorname{Gal}(L/K(\xi))$ is transitive on the roots, i.e. when $t^m - 1$ is irreducible over $K(\xi)$ by Lemma 3.4. □

Theorem 4.6. Suppose $K \le M$ is a cyclic extension with $|L : K| = m$, where $\operatorname{char} K \nmid m$ and that K contains a primitive mth root of unity. Then $\exists \lambda \in K$ such that $t^m - \lambda$ is irreducible over K and K is the splitting field of $t^m - \lambda$ over K. If β is a root of $t^m - \lambda$ in L, then $L = K(\beta)$.

Lemma 4.7. Let $\phi_1, \ldots, \phi_n$ be embeddings of a field K into a field L. Then there do not exist $\lambda_1, \ldots, \lambda_n$ not all zero such that $\lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x) = 0 \ \forall x \in K$.

Proof. Example sheet 2, question 10. □

Proof of Theorem 4.6. Let $\operatorname{Gal}(L/K) = \langle\sigma\rangle$ of order m. Observe that $1, \sigma, \sigma^2, \ldots, \sigma^{m-1}$ are distinct maps $L \to L$, and we can apply Lemma 4.7. There exists $\alpha \in L$ such that

$$\beta = \alpha + \xi\sigma(\alpha) + \cdots + \xi^{m-1}\sigma^{m-1}(\alpha) \ne 0$$

where ξ is a primitive mth root of unity. Observe that $\sigma(\beta) = \xi^{-1}\beta \ne \beta$ and so $\beta \notin K$, the fixed field of $\operatorname{Gal}(L/K)$.

$\sigma(\beta^m) = (\sigma(\beta))^m = \beta^m$. Let $\lambda = \beta^m \in K$. But $t^m - \lambda = (t-\beta)(t-\xi\beta)\cdots(t-\xi^{m-1}\beta)$ in $L[t]$, and so $K(\beta)$ is the splitting field of $t^m - \lambda$ over K (recall $\xi \in K$). Observe that $1, \sigma, \dots, \sigma^{m-1}$ are distinct K-automorphisms of $K(\beta)$ and so $|K(\beta) : K)| \geq m$.

So $L = K(\beta) = K(\xi\beta)$ since $\xi \in K$. $t^m - \lambda$ is the minimal polynomial of β over K and hence is irreducible. □

4.3 Cubics

4.4 Quartics

4.5 Solubility by radicals

Lemma 4.8. A finite group G is soluble if and only if we have

$$\{e\} = G_m \lhd G_{m-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

with G_i/G_{i+1} cyclic.

Proof. ($\Leftarrow$) is immediate. ($\Rightarrow$). We know about the structure of finite abelian groups. If A abelian then there is a chain

$$\{e\} = A_r \lhd A_{r-1} \lhd \cdots \lhd A_0 = A$$

with A_r/A_{r+1} cyclic. Thus if we have a chain with abelian factors G_i/G_{i+1} we can refine it to have cyclic factors. □

Lemma 4.9. Let $K \lhd G$. Then G/K abelian $\iff G' \leq K$.

Proof.

$$\begin{aligned} G/K \text{ abelian} &\iff Kg_1Kg_2Kg_1^{-1}Kg_2^{-1} = K \quad \forall g_1, g_2 \in G \\ &\iff g_1g_2g_1^{-1}g_2^{-1} \in K \\ &\iff G' \leq K. \end{aligned}$$

□

Lemma 4.10. For G finite, G is soluble $\iff G^{(m)} = \{e\}$ for some m.

Proof. If $G^{(m)} = \{e\}$ then the derived series gives a chain in the definition of solubility.

Conversely if there is such a chain

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd G_m = \{e\}$$

with G_i/G_{i+1} abelian then an easy induction shows that $G^{(j)} \leq G_j$ and so $G^{(m)} = \{e\}$. □

Lemma 4.11.

(i) Let $H \leq G$, G soluble. Then H soluble.

(ii) Let $H \lhd G$, then G soluble $\iff H$ and G/H both soluble.

Proof.

(i) G soluble $\implies G^{(m)} = \{e\}$ by Lemma 4.10. But $H^{(m)} \leq G^{(m)}$ and so H soluble by Lemma 4.10.

(ii) Let $H \lhd G$, then G soluble $\implies$ H soluble by (i). G soluble $\implies$ $G^{(m)} = \{e\}$, say. Observe that

$$\left(\frac{G}{H}\right)' = \frac{G'H}{H} \leq \frac{G}{H}.$$

Similarly,

$$(\frac{G}{H})^{(j)} = \frac{G^{(j)}H}{H} \leq \frac{G}{H}.$$

Thus $(G/H)^{(m)} = H/H$, a trivial subgroup of G/H and so G/H soluble.

Now consider the converse. Suppose that H and G/H are soluble. $H^(r) = \{e\}$ and $(G/H)^{(s)} = H/H$. But

$$\left(\frac{G}{H}\right)^{(s)} = \frac{G^{(s)}H}{H}$$

so $G^{(s)}H = H$ thus $G^{(s)} \leq H$. Hence $G^{(r+s)} \leq H^{(r)} = \{e\}$. Thus G is soluble by Lemma 4.10.

□

Theorem 4.12. Let K be a field and $f(t) \in K[t]$. Assume $\operatorname{char} K = 0$. Then $f(t)$ is soluble by radicals over K $\iff$ $\operatorname{Gal} f$ over K is soluble.

Corollary 4.13. If $f(t)$ is a monic irreducible polynomial $\in K[t]$ with $\operatorname{Gal}(f) \cong A_5$ or S_5 then $f(t)$ is not soluble by radicals (with $\operatorname{char} K = 0$).

Lemma 4.14. If $K \leq N$ is an extension by radicals then $\exists N'$ with $N \leq N'$ with $K \leq N'$ is an extension by radicals, with $K \leq N'$ a Galois extension.

Proof of Theorem 4.12. Suppose $f(t)$ is soluble by radicals. Thus if L is the splitting field of $f(t)$ over K then L lies in an extension of K by radicals

$$K = L_0 \leq L_1 \leq \cdots \leq L_m$$

with each $L_i \leq L_{i+1}$ cyclotomic or Kummer.

With Lemma 4.14, we may assume L_m is Galois over K. By Fundamental Theorem of Galois Theory there is a corresponding chain of subgroups of $\operatorname{Gal}(L_m/K)$. Our previous discussion at the beginning of this section (before Lemma 4.7) we know that $\operatorname{Gal}(L_m/K)$ is soluble.

But $F \leq L \leq L_m$ with $K \leq L$ Galois. By the Fundamental Theorem of Galois Theory, $\operatorname{Gal}(L/K) \cong \operatorname{Gal}(L_m/K)/\operatorname{Gal}(L_m/L)$.

But quotients of soluble groups are soluble, so $\operatorname{Gal}(L/K)$ is soluble. □

Proof of Lemma 4.14. We have $K = L_0 \leq L_1 \leq \cdots \leq L_m$ with each $L_i \leq L_{i+1}$ cyclotomic or Kummer, and we want to embed this into a Galois extension of the same form.

Assume $\operatorname{char} K = 0$. By the Primitive Element Theorem, $L_m = K(\alpha_1)$ for some α_1. Let $g(t)$ be the minimal polynomial of α_1 over K with splitting field M. Thus $M = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are roots of $g(t)$.

There are K-homomorphisms

$$\begin{aligned} \phi_i : M &\longrightarrow M \\ \alpha_1 &\longmapsto \alpha_i \end{aligned}$$

extending the K-homs $K(\alpha_1) \to K(\alpha_i) \leq M$.

The tower $K \leq \phi_i(K) \leq \phi_i(L_1) \leq \cdots \leq \phi_i(L_m) = K(\alpha_i)$ with cyclotomic or Kummer extensions as before, Consider $L_m = K(\alpha_1) \leq \phi_2(L_1)(\alpha_1) \leq \phi_2(L_2)(\alpha_1) \leq \cdots \leq \phi_2(L_m)(\alpha_1) = K(\alpha_1, \alpha_2)$.

Consider the extension $\phi_2(L_j)(\alpha_1) \leq \phi_2(L_{j+1})(\alpha_1)$:

> **if** $L_j \leq L_{j+1}$ **is cyclotomic** then all the roots of unity adjoined are now in $L_m = K(\alpha_1)$ and so $\phi_2(L_j)(\alpha_1) = \phi_2(L_{j+1})(\alpha_1)$.
>
> **if** $L_j \leq L_{j+1}$ **is Kummer** then we obtain L_{j+1} by adjoining roots of an element of L_j and so we obtain $\phi_2(L_{j+1})$ by adjoining roots of an element in $\phi_2(L_j)$. Hence we get from $\phi_2(L_j)(\alpha_1)$ to $\phi_2(L_{j+1})(\alpha_1)$ by adjoining roots of an element of $\phi_2(L_j)$. So it's a Kummer extension.

Now continue to get suitable chain $K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \alpha_2, \alpha_3)$.

Thus we get a suitable chain from K to $K(\alpha_1, \ldots, \alpha_n) = M$. Observe that $K \leq M$ is Galois. □

Converse of Theorem 4.12. Suppose $G = \mathrm{Gal}(f)$ over K is soluble (and $\operatorname{char} K = 0$). Let L be the splitting field of $f(t)$ over K and so $|G| = |L : K| = n$. Set $m = n!$ and let ξ be a primitive root of unity and consider $L(\xi)$.

$$\begin{tikzcd}[arrows=dash]
 & L(\xi) & \\
K(\xi) \arrow[ur, "\leq n"] & & L \arrow[ul] \\
 & K \arrow[ul] \arrow[ur, "n"'] &
\end{tikzcd}$$

Our proof is similar to that used for cubics. Observe that $|L(\xi) : K(\xi)| \leq n$. By the Primitive Element Theorem $L = K(\alpha)$ for some α with minimal polynomial $g(t)$ say of degree n. Then $L(\xi) = K(\xi)(\alpha)$ and the minimal polynomial of α over $K(\xi)$ divides $g(t)$ and so is of degree $\leq n$.

Then $\mathrm{Gal}(L(\xi)/K)$ is soluble since $\mathrm{Gal}(L(\xi)/L)$ is soluble and $\mathrm{Gal}(L/K) \cong \frac{\mathrm{Gal}(L(\xi)/K)}{\mathrm{Gal}(L(\xi)/L)}$ soluble by Fundamental Theorem of Galois Theory and Lemma 4.11. Then the subgroup $\mathrm{Gal}(L(\xi)/K(\xi)) \leq \mathrm{Gal}(L(\xi)/K)$ is soluble by Lemma 4.11.

Thus there is a chain of subgroups

$$\mathrm{Gal}(L(\xi)/K(\xi)) = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{e\},$$

with G_i/G_{i+1} cyclic (using Lemma 4.8).

Now use the Fundamental Theorem of Galois Theory to get a corresponding chain of fields $K(\xi) \leq K_1 \leq \cdots \leq K_m = L(\xi)$, with each $K_i \leq K_{i+1}$ Galois, with cyclic Galois group. By Theorem 4.6, all these extensions are Kummer (not all the extensions are of degree $\leq n$ and so we have the appropriate roots of unity). Thus we've embedded L in an extension of K by radicals. □

5 Final Thoughts

5.1 Algebraic closure

Lemma 5.1. If $K \leq L$ is algebraic and every polynomial in $K[t]$ splits completely over L, then L is an algebraic closure of K.

Proof. We need to show L is algebraically closed. Suppose $L \leq L(\alpha)$ is a finite extension, and $f_\alpha(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ is the minimal polynomial of α over L. Let $M = K(a_0, a_1, \ldots, a_{n-1})$. Then $M \leq M(\alpha)$ is a finite extension. But each a_i is algebraic over K and so $|M : K| < \infty$. Hence $|M(\alpha) : K| < \infty$ by Tower law and so α is algebraic over K. The minimal polynomial over K must split over L, and so $\alpha \in L$. Thus any algebraic extension of L is L itself. □

Lemma 5.2 (Zorn's Lemma)**.** Let $(\mathcal{S}, \leq)$ be a non-empty partially ordered set. Suppose that any chain has an upper bound in $\mathcal{S}$. Then $\mathcal{S}$ has a maximal element.

Lemma 5.3. Let R be a ring. Then R has a maximal ideal.

Proof. Let $\mathcal{S}$ be the set of proper ideals of R. This is is non-empty, since (0) is proper. Partially order $\mathcal{S}$ by inclusion. Any ideal I is proper $\iff 1 \notin I$. Any chain of proper ideals has an upper bound in $\mathcal{S}$, namely the union of the chain. Zorn's Lemma gives that $\mathcal{S}$ has a maximal element, i.e. a maximal ideal of R. □

Theorem 5.4 (Existence of algebraic closures)**.** For any field K there is an algebraic closure.

Proof. Let

$$\mathcal{S} = \{\, (f(t), j) \mid f(t) \text{ irreducible, monic in } K[t], 1 \leq j \leq \deg f \,\}$$

For each pair $s = (f(t), j) \in \mathcal{S}$ we introduce an indeterminate $X_s = X_{f,j}$. Consider the polynomial ring $K[X_s : s \in \mathcal{S}]$ and set

$$\tilde{f}(t) = f(t) - \prod_{j=1}^{\deg g} (t - X_{f,j}) \in K[X_s : s \in \mathcal{S}][t].$$

Let $I \lhd K[X_s : s \in \mathcal{S}]$ generated by all the coefficients of all the $\tilde{f}(t)$. Denote the coefficents of $\tilde{f}(t)$ by $a_{f,l}$ for $0 \leq l \leq \deg f$.

Claim: $I \neq K[X_s : s \in \mathcal{S}]$. Proof: Suppose $1 \in I$ and aim for a contradiction.

$$b_1 a_{f_1,l_1} + \cdots + b_N a_{f_N,l_N} = 1 \quad \text{in } K[X_s : s \in \mathcal{S}]. \tag{+}$$

Let L be a splitting field for $f_1(t) \cdots f_N(t)$.

For each i, f_i splits over L. $f_i(t) = \prod_{j=1}^{\deg f_i} (t - a_{ij})$. Define a K-linear ring homomorphism, identity on K,

$$\begin{aligned} \theta : K[X_s : s \in \mathcal{S}] &\longrightarrow L \\ X_{f_i,j} &\longmapsto \alpha_{ij} \\ X_s &\longmapsto 0 \qquad \text{otherwise.} \end{aligned}$$

This induces a map $K[X_s : s \in \mathcal{S}] \to L[t]$. Then

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

But then $\theta(a_{f_i,j}) = 0$ since $a_{f_i,j}$ are the coefficients of $\tilde{f}_i(t)$. But applying θ to (+) we get $0 = 1$.

Then I is a proper ideal of $K[X_s : s \in \mathcal{S}]$. By Zorn's Lemma there is a maximal ideal P of $K[X_s : s \in \mathcal{S}]$ containing I. Set $L_1 = K[X_s : s \in \mathcal{S}]/P$, a field. Thus we have a field extension $K \leq L_1$.

Claim: L_1 is an algebraic closure of K. First show $K \leq L_1$ is algebraic: L_1 is generated by the maps $x_{f,j}$ of the $X_{f,j}$. However $\tilde{f}(t)$ has coefficients in I and so its image $L_1[t]$ is the zero polynomial. Thus in $L_1[t]$,

$$f(t) = \prod (t - x_{f,j}) \tag{$*$}$$

and so $f(x_{f,j}) = 0$. Thus the $x_{f,j}$ are algebraic.

Any element of L_1 involves only finitely many of the $x_{i,j}$ and so is algebraic over K. Moreover from ($*$) any $f(t) \in K[t]$ splits completely over L_1.

The result follows from Lemma 5.1. □

Theorem 5.5. Suppose $\theta : K \to L$ is a ring homomorphism and L is algebraically closed. Suppose $K \leq M$ is an algebraic extension. Then θ can be extended to a homomorphism $\theta : M \to L$ (i.e. $\phi|_K = \theta$).

Proof. Let

$$\xi = \{ (N, \phi) \mid K \leq N \leq M, \phi \text{ a homomorphism } N \to L \text{ extending } \theta \}.$$

Partially order ξ with $(N_1, \phi_1) \leq (N_2, \phi_2)$ if $N_1 \leq N_2$ and $\phi_2|_{N_2} = \phi_1$. ξ is non-empty since $(K, \theta) \in \xi$.

If there is a chain $(N_1, \phi_1) \leq \cdots$ then set $N = \bigcup N_\lambda$. This is a subfield of M, and we can define $\psi : N \to L$ as follows: if $\alpha \in N$ then $\alpha \in N_\lambda$ for some λ and we set $\psi(\alpha) = \phi_\lambda(\alpha)$. This is well defined.

Then (N, ψ) is an upper bound for our chain ξ.

Zorn's Lemma applies and gives a maximal element of ξ, (N, ϕ). We now show $N = M$. Given $\alpha \in M$, it is algebraic over K, and hence over N. Let $f_\alpha(t)$ be its minimal polynomial over N. But $\phi f(t)$ is in $L[t]$ and so splits completely over L, since L is algebraically closed.

So $\phi f(t) = (t - \beta_1) \cdots (t - \beta_r)$, say. Since $\phi f(B_\gamma) = 0$ then there is a map

$$\begin{aligned} N(\alpha) \cong \tfrac{N[t]}{(f\alpha(t))} &\longrightarrow L \\ \alpha &\longmapsto \beta_1 \qquad \text{extending} \phi \end{aligned}$$

Maximality of (N, ϕ) implies that $N(\alpha) = N$. So $\alpha \in N$, so $N = M$. □

Theorem 5.6 (Uniqueness of algebraic closures)**.** If $K \leq L_1$, $L \leq L_2$ are two algebraic closures of K then there exists an isomorphism $\phi : L_1 \to L_2$.

Proof. By Theorem 5.5 there is a homomorphism $\phi : L_1 \to L_2$ extending the embedding of K into L_2. Since $K \leq L_2$ is algebraic, so too is $\phi(L_1)$. But L_1 is algebraically closed and so $\phi(L_1)$ is algebraically closed. So $L_2 = \phi(L_1)$ and ϕ is an isomorphism. □

5.2 Symmetric polynomials and invariant theory

Theorem 5.7. The fixed field $M = L^{s_n} = K(s_1, \ldots, s_n)$ and the $s_1, \ldots, s_n$ are algebraically independent over K (in L).