Galois theory

Shing Tak Lam

April 28, 2023

Contents

1 Symmetric polynomials

Let R be a ring. Then we have a (right) action of S_n on $R[X_1, \dots, X_n]$, given by

$$f \cdot \sigma = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

Definition 1.1 (symmetric polynomial)
$f \in R[X_1, \dots, X_n]$ is symmetric if $\mathrm{Orb}(f) = f$. Equivalently,

$$f = f \cdot \sigma = f(X_{\sigma(1)}, \dots, f_{\sigma(n)})$$

for all $\sigma \in S_n$.

Definition 1.2 (elementary symmetric polynomials)
The elementary symmetric polynomials are

$$S_{n,r} = \sum_{1 \le i_1 < \dots < i_r \le n} X_{i_1} \cdots X_{i_r}$$

We write S_r for $S_{n,r}$ if n is clear from context.

Theorem 1.3. Define a homomorphism $\theta : R[Y_1, \dots, Y_n] \to R[X_1, \dots, X_n]$ by $\theta(Y_r) = S_r$ and $\theta = \mathrm{id}$ on R. Then

1. $\ker(\theta) = 0$,
2. and $\mathrm{im}(\theta) = \{\text{symmetric polynomials}\}$.

Proof. First we consider (ii). Necessarily $f \in \mathrm{im}(\theta)$ is symmetric, so suffices to show that any symmetric polynomial is in $\mathrm{im}(\theta)$.

Let $d = \deg(f)$, and $x^\alpha = \mathrm{lm}(f)$ be the leading monomial of f, with coefficient $c = \mathrm{lc}(f) \in R$. As f is symmetric, we must have that $\alpha = (\alpha_1, \dots, \alpha_n)$, with $\alpha_1 \ge \dots \alpha_n$, otherwise we can permute the variables and get a larger term[1]. So we can write

$$x^\alpha = x_1^{\alpha_1 - \alpha_2}(x_1 x_2)^{\alpha_2 - \alpha_3} \cdots (x_1 \cdots x_n)^{\alpha_n}$$

Consider $g = S_1^{i_1 - i_2} S_2^{i_2 - i_3} \cdots S_n^{i_n}$. Then $\mathrm{lm}(g) = x^\alpha$, g is symmetric, so $f - cg$ is symmetric, with leading monomial strictly smaller than x^α. As the lexicographic order is a well-ordering on monomials, this terminates.

For (i), we want to show that the representation is unique. Suppose there exists $G \in R[Y_1, \dots, Y_n]$ such that $G(S_{n,1}, \dots, S_{n,n}) = 0$. We want to show that $G = 0$. The base case $n = 1$ is trivial.

Now suppose we have $G = Y_n^m H$, where $y_n \not| H$. Then $S_{n,n}^k H(S_{n,1}, \dots, S_{n,n}) = 0$, but $S_{n,n}$ is not a zero divisor, so $H(S_{n,1}, \dots, S_{n,n}) = 0$. So we can assume wlog that $Y_n \not| G$. Consider the map $\phi : R[X_1, \dots, X_n] \to R[X_1, \dots, X_{n-1}]$, given by $\phi(f) = f(X_1, \dots, X_{n-1}, 0)$. Then

$$\phi(S_{n,r}) = \begin{cases} S_{n-1,r} & \text{if } r \le n-1 \\ 0 & \text{if } r = n \end{cases}$$

So $\phi(\theta(G)) = G(S_{n-1,1}, \dots, S_{n-1,n-1}, 0) = 0$. But then we can embed this into $R[X_1, \dots, X_{n-1}]$, and by the inductive hypothesis, we have that $G(Y_1, \dots, Y_{n-1}, 0) = 0$. But $Y_n \not| G$. Contradiction. ☐

Definition 1.4 (power sum)
The power sum polynomials are

$$P_{n,k} = \sum_{i=1}^{n} X_i^k$$

Theorem 1.5 (Newton's formula)**.** Let $n \ge 1$, then for all $k \ge 1$,

$$P_k - S_1 P_{k-1} + \cdots + (-1)^{k-1} S_{k-1} P_1 + (-1)^k S_k = 0$$

[1] With respect to the lexicographic ordering on monomials.

where we define $S_0 = 1$ and $S_r = 0$ for $r > n$.

Proof. Since the coefficients in the above are 1 and -1, suffices to prove this in the case $R = \mathbb{Z}$. In fact, we can consider the case $R = \mathbb{R}$, so we can use calculus. Consider the function

$$F(T) = \prod_{i=1}^{n}(1 - X_i T) = \sum_{r=0}^{n}(-1)^r S_r T^r$$

Taking the derivative of $\log(F)$, we get that

$$\frac{F'(T)}{F(T)} = \sum_{i=1}^{n} \frac{-X_i}{1 - X_i T} = \frac{-1}{T} sum_{i=1}^{n} \sum_{r=1}^{\infty} X_i^r T^r = \frac{-1}{T} \sum_{r=1} \infty P_r T^r$$

Evaluating separately, we get that

$$-TF'(T) = S_1 T - 2S_2 T^2 + \cdots + (-1)^{n-1} n S_n T^n$$
$$F(T) \sum_{r=1}^{\infty} P_r T^r = (S_0 - S_1 T + \cdots + (-1)^n S_n T^n)(P_1 T + P_2 T^2 + \dots)$$

Comparing the coefficients of T^k gives the required result. □

1.1 Discriminant

Notation 1.6. In this course, we have Disc $= \Delta^2$, whereas in Number Fields, we have Disc $= \Delta$. The actual definitions are the same.

Definition 1.7 (discriminant polynomial)
The discriminant polynomial is $D(X_1, \dots, X_n) = \Delta(X_1, \dots, X_n)^2$, where

$$\Delta = \prod_{i<j}(X_i - X_j)$$

D is a symmetric polynomial, so $D(X_1, \dots, X_n) = d(S_1, \dots, S_n)$ for some poly $d \in \mathbb{Z}[Y_1, \dots, Y_n]$.

Definition 1.8 (discriminant of a polynomial)
Let $f = T^n + \sum_{i=0}^{n-1} a_i T^i$ be a monic polynomial. Then define

$$\mathrm{Disc}(f) = d(-a_1, a_2, \dots, (-1)^n a_n)$$

Proposition 1.9. If $f = \prod_{i=1}^{n}(T - x_i)$, then $a_r = (-1)^r S_r(x_1, \dots, x_n)$, and

$$\mathrm{Disc}(f) = \prod_{i \neq j}(x_i - x - J)^2 = D(x_1, \dots, x_n)$$

Proposition 1.10. If $R = k$ is a field, f is a product of linear factors, then $\mathrm{Disc}(f) = 0$ if and only if f has a repeated root.

2 Field theory

2.1 Field extensions

Definition 2.1 (prime subfield)

Given a field K, we call the smallest subfield of K the prime subfield of K, which is isomorphic to $\mathbb{Q}$ if $\mathrm{char}(K) = 0$ and $\mathbb{F}_p$ if $\mathrm{char}(K) = p$ prime.

Definition 2.2 (field extension)

Let $K \subseteq L$ be fields, or equivalently $K \hookrightarrow L$. We say that K is a subfield of L, or L is an extension of K. We write L/K for the field extension.

Proposition 2.3. If L/K is a field extension, then L is a K-vector space.

Definition 2.4 (finite extension, degree)

An extension L/K is finite if $\dim_K(L) < \infty$. We write $[L : K] = \dim_K(L)$ for the degree of the extension.

Theorem 2.5. If L/K is an extension, V is an L-vector space, then V is a K-vector space, and

$$\dim_K(V) = [L : K]\dim_L(V)$$

Proof. Suppose $d = \dim_L(V) < \infty$. Then as $V \simeq L^d$ as L-vector spaces, they must be isomorphic as K-vector spaces as well. Suppose $[L : K] = n < \infty$. Then $L \simeq K^d$ as K-vector spaces, so

$$V \simeq \bigoplus_{i=1}^{d} K^n = K^{nd}$$

If $\dim_K(V) < \infty$, as K is a subfield of L, necessarily $\dim_L(V) < \infty$. Taking the contrapositive, if $\dim_L(V) = \infty$ then $\dim_K(V) = \infty$. Likewise, if $[L : K] = \infty$ and $V \neq 0$, then V has an infinite linearly independent subset over K, so $\dim_K(V) = \infty$. □

Corollary 2.6 (tower law). If $M/L/K$ are field extensions, then M/K is finite if and only if $[M : L]$ and $[L : K]$ are finite. In this case, we have that

$$[M : K] = [M : L][L : K]$$

2.2 Characteristic p and the Frobenius endomorphism

Proposition 2.7. Suppose K is a finite field. Than $\mathrm{char}(K) = p$ is prime, and $|K| = p^n$ for some n.

Proposition 2.8.

(i) Let K be a field, G a finite subgroup of $K^\times$. Then G is cyclic.

(ii) If K is finite, then $K^\times$ is cyclic.

Proof. From Lagrange's theorem, we have that for some m[2], $x^m = 1$ for all $x \in G$. So G is contained in the subgroup of m-th roots of unity, which is cyclic. □

Definition 2.9 (primitive root modulo p)
$a \in \mathbb{F}_p^\times$ such that $\mathbb{F}_p = \{0\} \cup \{a, a^2, \ldots, a^{p-1}\}$ is called a primitive root modulo p.

Corollary 2.10. Primitive roots modulo p always exist.

Definition 2.11 (Frobenius endomorphism)
Let R be a ring, $p \cdot 1_R = 0$. Then $\phi_p(x) = x^p$ is a ring homomorphism $R \to R$, called the Frobenius endomorphism of R.

2.3 Algebraic elements and extensions

Definition 2.12 (algebraic, transcendental)
Let L/K be a field extension, $x \in L$ is algebraic over K if there exists $f \in K[T]$ nonzero such that $f(x) = 0$. If no such f exists, we say that x is transcendental over K.

Definition 2.13 (minimum polynomial)
Suppose $x \in L$, then $\phi : f \mapsto f(x)$ defines a ring homomorphism $K[T] \to L$. Then $\ker(\phi) = (g)$ for some monic g. We call g the minimal polynomial of x over K, and we write $m_{x,K} = g$.

Proposition 2.14. $m_{x,K}$ is well defined, that is, g exists and is unique. Furthermore, $m_{x,K}$ is irreducible.

Proof. Since $K[T]$ is a PID, $\ker(\phi)$ is principal, and there is a unique monic generator of a principal ideal. Furthermore, as $\operatorname{im}(\phi)$ is a subring of a field, it is an integral domain, so $\ker(\phi)$ is prime. Thus, g is irreducible. □

Definition 2.15 (degree)
The degree of an algebraic element x over K is

$$\deg_K(x) = \deg(x/K) = \deg(m_{x,K})$$

Proposition 2.16. Let L/K be a field extension, $x \in L$, then the following are equivalent.

(i) x is algebraic over K,

(ii) $[K(x) : K] < \infty$,

(iii) $\dim_K(K[x]) < \infty$,

[2] m is a multiple of the exponent of G, for example $m = |G|!$ works.

(iv) $K[x] = K(x)$,

(v) $K[x]$ is a field.

If any of these hold, then $\deg_K(x) = [K(x) : K]$.

Proof. Since $K[x] \leq K(x)$ is a subring, (ii) $\implies$ (iii) and (iv) $\iff$ (v) are clear.

(iii) $\implies$ (ii) and (iv). Let $y \in K[x]$ be nonzero. Then consider the map $K[x] \to K[x]$ given by $z \mapsto yz$. This is K-linear, and as $y \neq 0$ it is injective. So it is an isomorphism. Therefore, there exists $z \in K[x]$ such that $yz = 1$, so $K[x]$ is a field, i.e. $K[x] = K(x)$, and so

$$[K(x) : K] = \dim_K(K(x)) = \dim_K(K[x]) < \infty$$

(v) $\implies$ (i). Let $x \neq 0$. Then $x^{-1} = a_0 + a_1 x + \cdots + a_n x^n$, with $a_i \in K$, $a_n \neq 0$. Multiplying through by x, we get that

$$a_n x^{n+1} + \cdots + a_0 x - 1 = 0$$

So x is algebraic over K.

(i) $\implies$ (iii) and the degree formula. $\mathrm{im}(\mathrm{eval}_x : K[T] \to L) = K[x] \leq L$. If x is algebraic, then $\ker(\mathrm{eval}_x) = (m_{x,K})$ is maximal, as $(m_{x,K})$ is irreducible. So by the isomorphism theorem, we have that

$$K[x] \simeq \frac{K[T]}{(m_{x,K})}$$

Say $\deg(m_{x,K}) = d$. Then $K[T]/(m_{x,K})$ has basis $1, T, \ldots, T^{d-1}$. This means that $\dim_K(K[x]) = d < \infty$, which proves (iii) and the degree formula. □

Corollary 2.17.

(i) $x_1, \ldots, x_n$ are all algebraic over K if and only if $L = K(x_1, \ldots, x_n)$ is a finite extension. If so, every element of L is algebraic over K.

(ii) If x, y are algebraic over K, then so are $x \pm y$, xy, $1/x$,

(iii) Let L/K be any extension, then the set

$$\{x \in L \mid x \text{ algebraic over } K\}$$

is a subfield of L.

Proof. (i) If x_n is algebraic over K, then it must also be algebraic over $K(x_1, \ldots, x_{n-1})$, so $[L : K(x_1, \ldots, x_{n-1})] < \infty$. By induction and the tower law, we get that $[L : K] < \infty$. Conversely, if $[L : K] < \infty$, then $[K(x_i) : K] < \infty$, so x_i is algebraic over K. (ii) and (iii) follows immediately from (i). □

Definition 2.18 (algebraic extension)
An extension L/K is algebraic if any $x \in L$ is algebraic over K.

Proposition 2.19.

(i) Finite extensions are algebraic,

(ii) $K(x)/K$ is algebraic if and only if x is algebraic over K,

(iii) If $M/L/K$ are extensions, M/K is algebraic if and only if M/L and L/K are algebraic.

Proof. (i) and (ii) follows from the tower law and the previous proposition. For (iii), suppose M/K is algebraic, then M/L is algebraic and L/K is algebraic as $K \leq L \leq M$. For the coverese, choose $f = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in L[T]$ such that $f \neq 0$, $f(x) = 0$. Let $L_0 - K(a_0, \ldots, a_{n-1})$. As each $a_i \in L$ is algebraic over K, $[L_0 : K] < \infty$. Furthermore, $f \in L_0[T]$ and $f(x) = 0$, so x is algebraic over L_0. So $[l_0(x) : L_0] < \infty$, and $[L_0(x) : K] < \infty$ by the tower law. So $[K(x) : K] < \infty$, so x is algebraic over K. □

2.4 Splitting fields

Theorem 2.20. Let $f \in K[T]$ be monic irreducible, $L_f = K[T]/(f)$, $t = T + (f)$. Then L_f/K is a finite extension of fields, $[L_f : K] = \deg(f)$ and f is the minimal polynomial of t over K.

Definition 2.21 (K-homomorphism)

Suppose K is a field, L/K, M/K are extensions of K. A K-homomorphism $L \to M$ is a field homomorphism $\sigma : L \to M$ such that $\sigma|_K = \mathrm{id}_K$.

Theorem 2.22. Given $f \in K[T]$ irreducible, L/K an arbitary extension, then

(i) If $x \in L$ is a root of f, then there exists a unique K-homomorphism $\sigma : L_f \to L$, with $\sigma(t) = x$.

(ii) Every K-homomorphism $L_f \to L$ is of the above form.

That is, we have a bijection

$$\{K\text{-homomorphisms } L_f \to L\} \leftrightarrow \{\text{roots of } f \text{ in } L\}$$

In particular, there is at most $\deg(f)$ such σ.

Proof. (i) Consider the homomorphism $\phi : K[T] \to L$, given by $\phi(g) = g(x)$. Then as x is a root of f, we have that $(f) \subseteq \ker(\phi)$. As f is irreducible, (f) is maximal, and $\ker(\phi) \neq K[T]$, so $\ker(\phi) = (f)$. Hence we have an induced map

$$\varphi : \frac{K[T]}{(f)} = L_f \to L$$

which is a K-homomorphism as ϕ is one, and $\varphi(t) = x$. Uniqueness is immediate since φ is a ring homomorphism and we have specified the image of K and t.

(ii) Given a K-homomorphism $\sigma : L_f \to L$, let $x = \sigma(t)$. We want to show that $f(x) = 0$. But $f(x) = f(\sigma(t)) = \sigma(f(t))$ as σ is a K-homomorphism, and $f(t) = 0 \in L_f$. So $f(x) = 0$. The fact that σ is of the form in (i) follows immediately from uniqueness in (i). □

Corollary 2.23. If $L = K(x)$ with x algebraic over K, then there exists a unique isomorphism $\sigma : L_f \to K(x)$ such that $\sigma(t) = x$, where $f = m_{x,K}$.

Proof. Take $L = K(x)$ in the above theorem. □

Definition 2.24 (K-conjugate)

If x, y are algebraic over K (but x, y need not be in the same field), we say that x and y are K-conjugate if they have the same minimal polynomial.

Corollary 2.25. x, y are K-conjugate if and only if there exists a K-isomorphism $\sigma : K(x) \to K(y)$, with $\sigma(x) = y$.

Proof. For ($\implies$), we have that $K(x) \simeq L_f \simeq K(y)$. For the converse, notice that for all $g \in K[T]$, $\sigma(g(x)) = g(\sigma(x))$, so they have the same minimal polynomial. □

Definition 2.26 (σ-homomorphism, extension and restrictions of homomorphisms)
Let L/K, L'/K' be field extensions, $\sigma : K \to K'$ be a field homomorphism, $\tau : L \to L'$ is a homomorphism such that $\tau(x) = \sigma(x)$ for all $x \in K$. We say that τ is a σ-homomorphism, or τ extends σ, or σ is the restriction of τ.

Theorem 2.27. If $f \in K[T]$ is irreducible, $\sigma : K \to L$ is any field homomorphism, let $\sigma f \in L[T]$ be given by $\sigma f = \sigma_*(f)$, where $\sigma_* : K[T] \to L[T]$ is the induced map on coefficients. Then

(i) if x is a root of f, then there is a unique σ-homomorphism $\tau : L_f \to L$ such that $\tau(t) = x$.

(ii) every σ-homomorphism $\tau : L_f \to L$ is of the above form.

That is, we have a bijection

$$\{\sigma\text{-homomorphisms } L_f \to L\} \leftrightarrow \{\text{roots of } f \text{ in } L\}$$

Proof. Same as the above. □

Definition 2.28 (splitting field)
Let $f \in K[T]$ be a nonzero polynomial. We say that an extension L/K is a splitting field for f over K if

(i) f is a product of linear factors in $L[T]$,

(ii) L is minimal, that is, $L = K(x_1, \ldots, x_n)$, where the x_i are the roots of f in L.

Theorem 2.29. Every nonzero $f \in K[T]$ has a splitting field.

Proof. We prove this by induction on $\deg(f)$, but note that we will need to allow the field to vary[3]. That is, we will prove:

$$\forall n \in \mathbb{N}, \forall \text{ fields } K, \forall f \in K[T] \text{ with } \deg(f) = n, f \text{ has a splitting field.}$$

Base case: $n \leq 1$. In this case, K itself is a splitting field for f.

Inductive case: Now let g be an irreducible factor of f. Consider $K' = L_g = K[T]/(g)$. Let $x_1 = T \bmod (g)$. Then $g(x_1) = 0$, so $f(x_1) = 0$. Hence $f = (T - x_1)f_1$ where $f_1 \in K'[T]$ has $\deg(f_1) < \deg(f)$. By the inductive hypothesis, f_1 has a splitting field L/K'. Let $x_2, \ldots, x_n$ be the roots of f_1 in L, then f splits into linear factors in L, with roots $x_1, \ldots, x_n$, $L = K'(x_2, \ldots, x_n) = K(x_1, \ldots, x_n)$. So L is a splitting field for f over K. □

[3] Let us ignore any potential set theoretic nonsense here. This proof goes through just fine without quantifying over all fields, it's just that the proof is a bit longer. What we need is that each time we add a root the degree decreases, so this process terminates, and we end up with a finite tower $L = K_n/K_{n-1}/\ldots/K_1/K_0 = K$, where each $K_{i+1} = K_i(x_{i+1})$, $x_1, \ldots, x_n$ roots of f.

Another way out of set theory hell is to notice that all of these extensions are algebraic, so we are only quantifying over subfields $K \leq K' \leq \overline{K}$ of the algebraic closure.

Theorem 2.30 (uniqueness of splitting fields). Suppose $f \in K[T]$ is nonzero, L/K is a splitting field for f. Let $\sigma : K \hookrightarrow M$ be an extension such that $\sigma f \in M[T]$ splits into linear factors. Then

(i) σ can be extended to a homomorphism $\tau : L \to M$,

(ii) if M is a splitting field for σf over σK, then any τ in (i) is an isomorphism. In particular, any two splitting fields for f over K are K-isomorphic.

Proof. (i) By induction on $n = [L : K]$. If $n = 1$, then $L = K$ and f is a product of linear factors in $K[T]$ so we are done.

Now let $x \in L \setminus K$ be a root of an irreducible factor $g \in K[T]$ of f, with $\deg(g) > 1$. Let y be a root of $\sigma g \in M[T]$. Since σf splits in M, such a root exists. Thus, there exists $\sigma_1 : K(x) \to M$ such that $\sigma_1(x) = y$ and σ_1 extends σ. Now note that $[L : K(x)] < [L : K]$ by tower law, and L is a splitting field for f over $K(x)$. Furthermore, $\sigma_1 f = \sigma f$ splits in M. Thus, by induction we can extend σ_1 to a homomorphism $\tau : L \to M$.

(ii) Assume M is a splitting field for σf over σK, and τ be as in (i). Let $\{x_i\}$ be the roots of f in L, then the roots of σf in M are just $\{\tau(x_i)\}$. Since M is a splitting field, $M = \sigma K(\tau(x_1), \ldots, \tau(x_n)) = \tau L$ as $L = K(x_1, \ldots, x_n)$. So τ is an isomorphism. If $K \subseteq M$, σ is the inclusion, then τ is a K-isomorphism $L \simeq M$. □

2.5 Normal extensions

Definition 2.31 (normal extension)

An extension L/K is normal if it is algebraic and for every $x \in L$, $m_{x,K}$ splits into distinct linear factors over L.

Proposition 2.32. The following are equivalent:

(i) L/K is normal,

(ii) for every $x \in L$, L contains a splitting field for $m_{x,K}$.

(iii) for every $f \in K[T]$ irreducible, if f has a root in L, then f splits over L.

Theorem 2.33 (splitting fields are normal). Let L/K be a finite extension. Then L is normal over K if and only if L is the splitting firld for some not necessarily irreducible $f \in K[T]$.

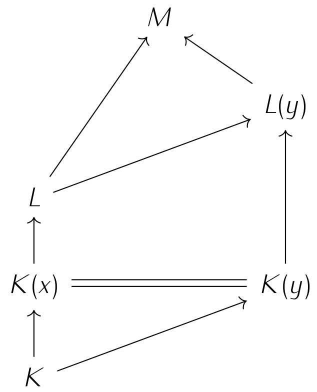
Proof. Suppose L/K is normal. Write $L = K(x_1, \ldots, x_n)$, then $m_{x_i,K}$ splits in L, so L is generated by the roots of $f = m_{x_1,K} \cdots m_{x_n,K}$. So L is a splitting field for f over K.

Conversely, suppose L is the splitting field for some $f \in K[T]$. Let $x \in L$, $g = m_{x,K}$. We want to show that g splits in L. Let M be the splitting field for g over L. $y \in M$ a root for g. We want to show that $y \in L$.

Since L is a splitting field for f over K, L is a splitting field for f over $K(x)$,, and $L(y)$ is a splitting field for f over $K(y)$. But x, y are K-conjugate, so there exists an isomorphism $K(x) \simeq K(y)$. By uniqueness of splitting fields, we have that

$$[L : K(x)] = [L(y) : K(y)]$$

As $[K(x) : K] = [K(y) : K]$, computing $[L(y) : K]$ along the different paths in



We find that $[L(y) : L] = 1$, so $L(y) = L$, i.e. $y \in L$. □

Corollary 2.34 (existence of normal closure)**.** Let L/K be a finite extension. Then there exists a finite extension M/L such that

(i) M/K is a normal extension,

(ii) if $L \leq M' \leq M$ with M'/K normal, then $M' = M$.

Moreover, any two such extensions are L-isomorphic. We call M the normal closure of L/K.

Proof. Write $L = K(x_1, \dots, x_k)$ and let $f = m_{x_1,K} \cdots m_{x_k,K}$. Let M be a splitting field for f over L. Then as the x_is are roots of f, M is also a splitting field for M/K. So M/K is normal. Now let M' be such that $L \leq M' \leq M$ with M'/K normal. Since $x_i \in M'$, $m_{x_i,K}$ splits in M' for all i. So $M' = M$ by the minimality of splitting fields.

For uniqueness, any such M satisfying (i) must contain a splitting field for f, and by the above, (ii) implies that M is a splitting field for f. The result follows by uniqueness of splitting fields. □

2.6 Separability

Definition 2.35 (separable polynomial)

$f \in K[T]$ is separable if it splits into distinct linear factors in a splitting field L. That is, it has $\deg(f)$ distinct roots in L.

Proposition 2.36. Suppose $f \in K[T]$, L/K is an extension, $x \in L$ is a root of f. Then x is a simple root, i.e. $(T-x)^2 \nmid f$ if and only if $f'(x) \neq 0$.

Proof. By the division algorithm, we can write $f = (T-x)g$, then $f' = g + (T-x)g'$, so $f'(x) = g(x)$. □

Corollary 2.37. f is separable if and only if $\gcd(f, f') = 1$.

Proof. Replacing K by a splitting field for f, we may assume f has all of its roots in K. Then it is separable if f, f' have no common zeroes, which is true if and only if $\gcd(f, f') = 1$. □

Theorem 2.38.

(i) Let $f \in K[T]$ be irreducible. Then f is separable if and only if $f' \neq 0$.

(ii) If $\mathrm{char}(K) = 0$, then every irreducible polynomial in $K[T]$ is separable.

(iii) If $\text{char}(K) = p > 0$, then an irreducible $f \in K[T]$ is inseparable if and only if $f = g(T^p)$ for some $g \in K[T]$.

Proof. (i) wlog f is monic. Then as f is irreducible, $\gcd(f, f') \mid f$ implies that $\gcd(f, f') = 1$ or f. If $\gcd(f, f') = f$, then $f \mid f'$. But $\deg(f') < \deg(f)$, so $f' = 0$ is the only possibility.

For (ii) and (iii), write $f = \sum_{i=0}^{d} a_i T^i$, then $f' = \sum_{i=1}^{d} i a_i T^{i-1}$. So $f' = 0$ if and only if $i a_i = 0$ for all $i = 1, \dots, d$.

In (ii), $\text{char}(K) = 0$, so this means that $a_i = 0$ for all $i \geq 1$, so f is constant, which is not irreducible.

In (iii), $a_i = 0$ for all $p \not| i$, so $f = g(T^p)$ for some $g \in K[t]$. □

Definition 2.39 (separable element, separable extension)

Let L/K be an extension. We say that $x \in L$ is separable over K if x is algebraic over K and $m_{x,K}$ is separable. We say that L/K is separable if every element of L is separable over K.

Theorem 2.40. Let x be algebraic over K, L/K any extension in which $m_{x,K}$ splits. Then x is separable over K if and only if there are exactly $\deg_K(x)$ K-homomorphisms $K(x) \to L$.

Proof. Recall that the number of such homomorphisms is the number of roots of $m_{x,K}$ in L, which is equal to $\deg_K(x)$ if and only if x is separable. □

Notation 2.41. Write $\text{Hom}_K(L, M)$ for the set of K-homomorphisms $L \to M$.

Theorem 2.42 (counting embeddings)**.** Let $L = K(x_1, \dots, x_k)$ be a finite extension of K, M/K any extension. Then $|\text{Hom}_K(L, M)| \leq [L : K]$, with equality if and only if

(i) for all i, $m_{x_i,K}$ splits into linear factors over M,

(ii) all x_i are separable over K.

if and only if all $m_{x_i,K}$ splits into distinct linear factors over M.

Remark 2.43. We will in fact prove the stronger statement that if $\sigma : K \to M$ is a homomorphism, then the number of σ homomorphisms $L \to M$ is less than $[L : K]$, with equality if and only if $\sigma m_{x_i,K}$ splits in M.

Proof. We induct on k. $k = 0$ is trivial, and for $k \geq 1$, set $K_1 = K(x_1)$, $\deg_X(x_1) = d = [K_1 : K]$. Then set

$$e = |\text{Hom}_K(K_1, M)| = |\{y \in M \mid m_{x_1,K}(y) = 0\}|$$

Necessarily, we have that $e \leq d$. Let $\sigma : K \to M$ be a K-homomorphism. Applying the induction hypothesis to L/K_1, we find that there are at most $[L : K_1]$ σ-homomorphisms $L \to M$. So the number of K-homomorphisms $L \to M$ is at most

$$e[L : K_1] \leq d[L : K_1] = [L : K]$$

If equality holds, then $d = e$, so $m_{x_i,K}$ splits into d distinct linear factors over M, so (i) and (ii) holds for x_1. But we can just permute the x_i, so (i) and (ii) holds for all x_i. Conversely, if (i) and (ii) holds, then by the previous theorem $|\text{Hom}_K(K_1, M)| = d$. So (i) and (ii) holds over K_1, so by induction each $\sigma : K_1 \to M$ has $[L : K_1]$ extensions ot a homomorphism $L \to M$. Hence $|\text{Hom}_K(L, M)| = [L : K]$ as required. □

Theorem 2.44 (separably generated is separable)**.** Let $L = K(x_1, \dots, x_n)$ be a finite extension of K, then

L/K is separable if and only if each x_i is separable.

Proof. If L/K is separable, then by definition the x_i are separable. Conversely, suppose the x_i are separable. Let M be a normal closure of L/K, i.e. M is the splitting field of $f = m_{x_1,K} \cdots m_{x_n,K}$. Equality holds when counting embeddings, so $|\mathrm{Hom}_K(L, M)| = [L : K]$. But if $x \in L$, then $L = K(x, x_1, \ldots, x_k)$, so x is separable, again by counting embeddings. □

Corollary 2.45. If L/K is a field extension, $x, y \in L$ are separable over K, then

$$\{x \in L \mid x \text{ is separable over } K\}$$

is a subfield of L.

Proof. The intermediate field extension $K(x, y/K)$ is separable. □

2.7 Primitive element theorem

Theorem 2.46 (primitive element theorem for separable extensions)**.** Let K be an infinite field, $L = K(x_1, \ldots, x_k)$ a finite separable extension. Then there exists $x \in L$ such that $L = K(x)$.

Proof. By induction, we only need to consider the case $k = 2$. Say $L = K(x, y)$, where x, y are separable over K. Let $n = [L : K]$ and M be a normal closure for L/K. Then there exists n distinct K-homomorphisms $\sigma_i : L \to M$. Let $a \in K$, and consider $z = x + ay$. We will choose $a \in K$ such that $L = K(z)$.

Since $L = K(x, y)$, $\sigma_i(x) = \sigma_j(x), \sigma_i(y) = \sigma_j(y)$ if and only if $i = j$. So consider $\sigma_i(z) = \sigma_i(x) + a\sigma_i(y)$. If $\sigma_i(z) = \sigma_j(z)$, then

$$\underbrace{(\sigma_i(x) - \sigma_j(x))}_{\text{(i)}} + a \underbrace{(\sigma_i(y) - \sigma_j(y))}_{\text{(ii)}} = 0$$

If $i \neq j$, then at least one of (i) and (ii) is nonzero, so there is at most one value of $a \in K$ such that equality holds. Since K is infinite, there exists $a \in K$ such that $\sigma_i(z)$ are distinct. But then $\deg_K(z) = n$, so $L = K(z)$. □

Theorem 2.47. Suppose L/K is an extension of finite fields, then $L = K(x)$ for some $x \in L$.

Proof. $L^\times$ is cyclic, so letting x be a generator of $L^\times$, $L = K(x)$. □

3 Galois theory

3.1 Automorphisms of fields

Definition 3.1 (automorphism of a field)

Let L be a field, $\sigma : L \to L$ is an automorphism of L if σ is a bijective homomorphism. Wrire $\mathrm{Aut}(L)$ for the group of automorphisms of L.

Definition 3.2 (fixed field)

If $S \subseteq \mathrm{Aut}(L)$ write

$$L^S = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in S\}$$

for the subfield of L fixed by S. We call this the fixed field of S.

Definition 3.3 (automorphism of a field extension)
Let L/K be an extension, define

$$\mathrm{Aut}(L/K) = \{K\text{-automorphisms of } L\} = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}\}$$

Theorem 3.4. Let L/K be finite. Then $|\mathrm{Aut}(L/K)| \leq [L : K]$.

Proof. Taking $M = L$ in the counting embeddings theorem, and noticing that $\mathrm{Hom}_K(L, L) = \mathrm{Aut}(L/K)$, since $\sigma \in \mathrm{Hom}_K(L, L)$ is an injective K-linear map $L \to L$ and L is a finite dimensional K-vector space. □

Proposition 3.5. $K = \mathbb{Q}$ and $K = \mathbb{F}_p$ have no nontrivial automorphisms, so for any L, $\mathrm{Aut}(L) = \mathrm{Aut}(L/K)$ where K is the prime subfield of L.

Definition 3.6 (Galois extension)
An extension L/K is Galois if L/K is algebraic, and $L^{\mathrm{Aut}(L/K)} = K$. If L/K is Galois, write $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$ for the Galois group of the extension L/K.

Theorem 3.7 (classification of finite Galois extensions)**.** Let L/K be a finite extension, and let $G = \mathrm{Aut}(L/K)$. Then the following are equivalent.

(i) L/K is Galois,

(ii) L/K is normal and separable,

(iii) L is the splitting field of a separable polynomial over K,

(iv) $|G| = [L : K]$.

If any of these hold, then the minimal polynomial of $x \in L$ is

$$m_{x,K} = \prod_{i=1}^{r}(T - x_i) = \prod_{z \in \mathrm{Orb}_G(x)} (T - z)$$

Proof. **(i) $\implies$ (ii) and the minimal polynomial.** Let $x \in L$, $\mathrm{Orb}(x) = \{x_1, \ldots, x_r\}$, $f = \prod_{i=1}^{r}(T - x_i) \in L[T]$. Clearly, $f(x) = 0$. As $\mathrm{Aut}(L/K)$ permutes the x_i, $f \in L^G[T] = K[T]$, so $m_{x,K} \mid f$. Also, since $m_{x,K}(\sigma(x)) = \sigma(m_{x,K}(x)) = 0$ for all σ, each x_i is a root of $m_{x,K}$. So $f = m_{x,K}$ and x is separable over K, $m_{x,K}$ splits in L. That is, L/K is normal and separable.

(ii) $\implies$ (iii). Since L/K is normal, L is a splitting field for some $f \in K[T]$. Write $f = \prod_i q_i^{e_i}$, where the q_i are distinct irreducible factors of f. Then as L/K is separable, the q_i are separable. So $g = \prod_i q_i$ is separable, and L is also a splitting field for g.

(iii) $\implies$ (iv). Say $L = K(x_1, \ldots, x_n)$ is the splitting field of some separable polynomial $f \in K[T]$ with roots x_i. As $m_{x_i,K} \mid f$, each $m_{x_i,K}$ splits into distinct linear factors over L. So by counting embeddings,

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

(iv) $\implies$ (i). Suppose $|G| = [L : K]$. Then

$$G \leq \mathrm{Aut}(L/L^G) \leq \mathrm{Aut}(L/K)$$

So $G = \mathrm{Aut}(L/L^G)$, hence by counting embeddings, we have

$$[L:K] = |G| \leq [L:L^G]$$

But $[L:K] = [L:L^G][L^G:K]$ by tower law, so $L^G = K$. □

Corollary 3.8. If L/K is a finite Galois extension, then $L = K(x)$ for some $x \in L$, x is separable over K with $\deg_K(x) = [L:K]$.

Proof. By (ii) in the theorem and the primitive element theorem for finite separable extensions. □

3.2 Galois correspondence

Theorem 3.9 (Galois correspondence). Suppose L/K is a finite Galois extension, $G = \mathrm{Gal}(L/K)$. If we have an intermediate extension $K \leq F \leq L$, then L/F is Galois, $\mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K)$ is a subgroup.

The map $\theta : \{\text{intermediate fields } K \leq F \leq L\} \to \{\text{subgroups } H \leq G\}$ defined by

$$\theta(F) = \mathrm{Gal}(L/F)$$

is an order reversing bijection, with inverse $\theta^{-1}(H) = L^H$. Furthermore, we have that

$$[F:K] = [G:\theta(F)]$$

Proof. Let $x \in L$, then $m_{x,F} \mid m_{x,K}$ in $F[T]$. As $m_{x,K}$ splits into distinct linear factors in K, so does $m_{x,F}$. So L/F is normal and separable, so L/F is Galois. By definition $\mathrm{Gal}(L/F) \leq G$.

Since L/F is Galois, $L^{\mathrm{Gal}(L/F)} = F$. So $\theta^{-1} \circ \theta = \mathrm{id}$. Conversely, since $H \leq \mathrm{Gal}(L/L^H)$ and $\left|\mathrm{Gal}(L/L^H)\right| \leq [L:L^H]$, suffices to show $[L:L^H] \leq |H|$. Choosing a primitive element, we can assume $L = L^H(x)$ and

$$f = \prod_{\sigma \in H} (T - \sigma(x)) \in L^H[T]$$

has x as a root. So $\deg_{L^H}(x) \leq \deg(f) = |H|$, so $[L:L^H] \leq |H|$. Hence $\theta \circ \theta^{-1} = \mathrm{id}$.

Order reversing is clear since if $K \leq F \leq F' \leq L$, then $\mathrm{Gal}(L/F') \leq \mathrm{Gal}(L/F)$. Finally, if $F = L^H$, then

$$[F:K] = \frac{[L:K]}{[L:F]} = \frac{|G|}{|H|} = [G:H]$$

as L/F and L/K are Galois. □

Proposition 3.10. Let $\sigma \in G$, $H \leq G$ be a subgroup. Then $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.

Proof.

$$\begin{aligned} L^{\sigma H \sigma^{-1}} &= \left\{x \in L \mid \sigma\tau\sigma^{-1}(x) = x \text{ for all } \tau \in H\right\} \\ &= \left\{x \in L \mid \tau\sigma^{-1}(x) = \sigma^{-1}(x)\right\} \\ &= \{\sigma(y) \mid y \in L, \tau(y) = y\} && = \sigma(L^H) \end{aligned}$$

□

Proposition 3.11 (normal subgroups and extensions). Fix $H \leq G$, then the following are equivalent.

(i) L^H/K is Galois,

(ii) L^H/K is normal,

(iii) for all $\sigma \in G$, $\sigma(L^H) = L^H$,

(iv) $H \leq G$ is normal.

If any of the above hold, then $\mathrm{Gal}(L^H/K) \cong G/H$.

Proof. Since L/K is separable, so is L^H/K. So (i) and (ii) are equivalent. Let $F = L^H$ and $x \in F$. Then the roots of $m_{x,K}$ in L is precisely (with multiplicity) $\mathrm{Orb}_G(x)$, since L/K is Galois.

Thus, $m_{x,K}$ splits in F if and only if for all $\sigma \in G$, $\sigma(x) \in F$. Therefore, we have that F/K is normal if and only if $\sigma F \subseteq F$. But $[\sigma F : K] = [F : K]$, so F is normal if and only if $\sigma F = F$. By the previous proposition, F is normal if and only if $H = \sigma H \sigma^{-1}$ for all σ, so (ii), (iii) and (iv) are equivalent.

If any of (i)-(iv) holds, then for all $\sigma \in G$, $\sigma F = F$. So we have a homomorphism $G \to \mathrm{Gal}(F/K)$ given by $\sigma \mapsto \sigma|_F$. This has kernel $\{\sigma \in G \mid \sigma \text{ fixes } F\} = H$, so by the isomorphism theorem,

$$G/H \;\sim \mathrm{im}(G \to \mathrm{Gal}(G/K)) \leq \mathrm{Gal}(F/K)$$

But we know the index, so $\mathrm{Gal}(F/K) \cong G/H$. □

3.3 Galois group of polynomials

Let $f \in K[T]$ be separable, $x_1, \dots, x_n$ the roots of f in a splitting field L, then G acts on $\{x_1, \dots, x_n\}$ by a permutation, since $\sigma(f(x)) = f(\sigma(x))$. Furthermore, if $\sigma(x_i) = x_i$ for all i, as $L = K(x_1, \dots, x_n)$, $\sigma = \mathrm{id}$. So we have an injective homomorphism $\iota : G \hookrightarrow S_n$.

Definition 3.12 (Galois group of a polynomial)
$\mathrm{Gal}(f/K) = \mathrm{im}(\iota) \leq S_n$ is called the Galois group of f over K.

Proposition 3.13. Suppose f is separable. The following are equivalent.

(i) f is monic and irreducible,

(ii) $\mathrm{Gal}(f/K)$ is a transitive subgroup,

(iii) for all $i, j \in \{1, \dots, n\}$, there exists $\sigma \in \mathrm{Gal}(f/K)$ such that $\sigma(i) = j$,

(iv) $\mathrm{Gal}(f/K)$ acting on $\{1, \dots, n\}$ has only one orbit.

Proof. We only need to show (i) and (ii) are equivalent, the rest are clear. Let x be a root of f in a splitting field L. $m_{x,K}$ divides f and is irreducible, so f is irreducible if and only if $m_{x,K} = f$. But the roots of $m_{x,K}$ is $\mathrm{Orb}(x)$ as L/K is Galois, since f is separable. So f is irreducible if and only if every root of f is in the orbit of x, if and only if G acts transitively on the roots of f. □

Proposition 3.14. f is separable if and only if $\mathrm{Disc}(f) \neq 0$.

Proof. Say f is monic, then in a splitting field L for f,

$$f = \prod_{i=1}^{n} (T - x_i)$$

so $\mathrm{Disc}(f) = 0$ if and only if f has repeated roots (in L). □

Proposition 3.15. Suppose $\mathrm{char}(K) \neq 2$, and L is a splitting field for $f \in K[T]$ separable, $G = \mathrm{Gal}(f/K)$. Then the the fixed field of $G \cap A_n = K(\Delta(x_1, \dots, x_n))$, where $x_1, \dots, x_n$ are the roots of f in L. So $\mathrm{Gal}(f/K) \leq A_n$ if and only if $\mathrm{Disc}(f)$ is a square in K.

Proof. Given $\pi \in S_n$, we have that

$$\prod_{i<j}(T_{\pi(i)} - T_{\pi(j)}) = \operatorname{sign}(\pi)\prod_{i<j}(T_i - T_j)$$

so if $\sigma \in G$, $\sigma\Delta = \operatorname{sign}(\sigma)\Delta$. Since $\operatorname{char}(K) \neq 2$, $1 \neq -1$. As $\Delta \neq 0$, this impliex that $\Delta \in K$ if and only if $G \subseteq A_n$ and Δ lies in the fixed field of $G \cap A_n$. As $[F : K] = [G : G \cap A_n] = 1$ or 2, $F = K(\Delta)$. □

4 Finite fields

Theorem 4.1 (existence and uniqueness of finite fields)**.** For all n, there exists a field F with order $q = p^n$. Any such field is a splitting field for the polynomial $f = T^q - T$ over $\mathbb{F}_p$. In particular, any two finite fields of the same order are isomorphic.

Proof. Suppose F is a field with $q = p^n$ elements. Then if $x \in F^\times$, $x^{q-1} = 1$ by Lagrange's theorem. So for every $x \in F$, $x^q = x$. Thus, $f = \prod_{x \in F}(T - x)$ splits into linear factors in F, and not in any proper subfield (as there are not enough elements). So F is a splitting field for f over $\mathbb{F}_p$. By uniqueness of splitting fields, any two such F are isomorphic.

On the other hand, let $L/\mathbb{F}_p$ be a splitting field for $f = T^q - T$, and let $F \subseteq L$ be the fixed field of $\phi_p^n : x \mapsto x^q$. Then $F = \{x \mid x^q = x\}$ is the roots of f in L. So $|F| = q$ and $F = L$. □

Notation 4.2. We write $\mathbb{F}_q$ for any finite field of order $q = p^n$.

Theorem 4.3. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois, with Galois group $\cong C_n$, generated by ϕ_p.

Proof. $T^q - T = \prod_{x \in \mathbb{F}_q}(T - x)$ is separable, so $\mathbb{F}_q/\mathbb{F}_p$ is Galois. Let $G \leq \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ be the subgroup generated by ϕ_p. Then $\mathbb{F}_q^G = \{x \mid x^p = x\} = \mathbb{F}_p$. Thus by the Galois correspondence, $G = \operatorname{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. □

Corollary 4.4. $\mathbb{F}_{p^n}$ has a unique subfield of order p^m for each $m \mid n$, and no others. If $m \mid n$, then $\mathbb{F}_{p^m} \leq \mathbb{F}_{p^n}$ is the fixed field of ϕ_p^m.

Proof. By Galois correspondence. □

Theorem 4.5. Suppose $f \in \mathbb{F}_p[T]$ separable, $\deg(f) = n$, whose irreducible factors have degree $n_1, \dots, n_r$. Then $\operatorname{Gal}(f/\mathbb{F}_p) \leq S_n$ is cyclic, and generated by ana element of cycle type $(n_1, \dots, n_r)$. In particular, $\left|\operatorname{Gal}(f/\mathbb{F}_p)\right| = \operatorname{lcm}(n_1, \dots, n_r)$.

Proof. Let L be a splitting field for f over $\mathbb{F}_p$, where the roots of f are $x_1, \dots, x_N$. Then $\operatorname{Gal}(L/\mathbb{F}_p)$ is cyclic and generated by ϕ_p. As the irreducible factors of f are the minimal polynomials of the x_is, and the set of roots of $m_{x_i,K}$ is the orbit of ϕ_p on x_i, the cycle type of ϕ_p is $(n_1, \dots, n_r)$. □

Theorem 4.6 (reduction $\bmod p$)**.** Let $f \in \mathbb{Z}[T]$ be a monic separable polynomial, p prime, $n = \deg(f)$. Suppose the reduction $\overline{f} \in \mathbb{F}_p[T]$ is also separable, then $\operatorname{Gal}(\overline{f}/\mathbb{F}_p) \leq \operatorname{Gal}(f/\mathbb{Q})$ as subgroups of S_n.

Proof. Non examinable, so omitted. □

Corollary 4.7. With the same assumptions as in the theorem, suppose $\overline{f} = g_1 \cdots g_r$ product of irreducibles, with $\deg(g_i) = n_i$. Then $\mathrm{Gal}(f/\mathbb{Q})$ has an element with cycle type $(n_1, \ldots, n_r)$.

5 Cyclotomic and Kummer extensions

5.1 Primitive roots of unity

Lemma 5.1. Let $n > 1$, $a \in \mathbb{Z}$, $(a, n) = 1$, then the map $[a] : C_n \to C_n$ given by $g \mapsto g^a$ is an automorphism of C_n. Furthermore, the map $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(C_n)$ given by $a \mapsto [a]$ is an isomorphism.

Proof. $[a]$ is obviously a homomorphism, and it is an automorphism by Bezout's theorem. So we have an injection $(\mathbb{Z}/n\mathbb{Z})^\times \hookrightarrow \mathrm{Aut}(C)$ given by $a \mapsto [a]$, which is a homomorphism. To show that this is surjective, notice that if $\phi \in \mathrm{Aut}(C)$, then for a generator g of C, $\phi(g) = g^a$ for some a. So $\phi = [a]$. □

Definition 5.2 (roots of unity)
Let K be a field, $n > 1$, define the group of n-th roots of unity. This is a finite subgroup of $K^\times$, so it is cyclic, of order dividing n.

$$\mu_n(K) = \{x \in K \mid x^n = 1\}$$

Definition 5.3 (primitive root of unity)
We say that $\zeta \in \mu_n(K)$ is a primitive n-th root of unity if $\mathrm{ord}(\zeta) = n$ in $\mu_n(K)$.

Proposition 5.4. The following are equivalent:

(i) A primitive n-th root of unity ζ exists,

(ii) $|\mu_n(K)| = n$,

(iii) $f = T^n - 1$ splits into distinct linear factors in K,

In any of the above cases, we must have that $\mathrm{char}(K) \not| n$.

Proof. (i) and (ii) are equivalent by definition, and (ii) and (iii) are equivalent by definition. If $T^n - 1$ is separable, we must have $f' \neq 0$, i.e. $n \neq 0$, so $\mathrm{char}(K) \not| n$. □

Until the end of this subsection, assume either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p > 0$, $p \not| n$. So n-th roots of unity always exist (in some splitting field).

Definition 5.5 (cyclotomic extension)
Let L/K be a splitting field for $f = T^n - 1$. We call L/K a cyclotomic extension.

Proposition 5.6. Let L/K be a cyclotomic extension. Then

(i) L/K is Galois, say $G = \mathrm{Gal}(L/K)$,

(ii) $|\mu_n(L)| = n$, and so a primitive root of unity ζ_n exists.

(iii) $L = K(\zeta_n)$,

(iv) there exists an injective homomorphism $\chi_n : G \to (\mathbb{Z}/n\mathbb{Z})^\times$, such that if $\chi(a) = a \mod n$ then $\sigma(\zeta) = \zeta^a$. In particular, G is abelian.

(v) χ_n is an isomorphism if and only if G acts transitively on the set of primitive roots of unity in L.

We call χ_n the cyclotomic character of L/K.

Proof. For (i) and (ii) suffices to note that $T^n - 1$ is separable. The splitting field of a separable polynomial is Galois, and there are n distinct roots of $T^n - 1$, so $|\mu_n(L)| = n$.

For (iii), note that $\mu_n(L) = \langle\zeta\rangle$, so $L = K(1, \zeta, \dots, \zeta^{n-1}) = K(\zeta)$.

(iv) Consider the action of G on L. In permutes $\mu_n(L)$, and if ζ, ζ' are roots of unity, $\sigma \in G$, then $\sigma(\zeta\zeta') = \sigma(\zeta)\sigma(\zeta')$, so $\sigma \in \mathrm{Aut}(\mu_n(L))$. As $L = K(\zeta_n)$, $\sigma(\zeta_n) = \zeta_n$ if and only if $\sigma = \mathrm{id}$. So we have an injective homomorphism $G \to \mathrm{Aut}(\mu_n(L)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

(v) ζ_n^a is primitive if and only if $(a, n) = 1$, so by considering the G-orbit of ζ_n, we get the required result. □

Definition 5.7 (cyclotomic polynomial)
The n-th cyclotomic polynomial is

$$\Phi_n(T) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (T - \zeta_n^a)$$

Proposition 5.8.

(i) $\Phi_n \in K[T]$.

(ii) We have the recurrence formula

$$\Phi_n = \frac{T^n - 1}{\prod_{d|n, d<n} \Phi_d}$$

so in fact Φ_n does not depend on K.

Proof. For (i), as G permutes the primitive n-th roots of unity in L, Φ_n has coefficients in $L^G = K$.

For (ii), note that if $x^n = 1$, then x is a primitive d-th root of unity for some $d \mid n$, so we have that

$$T^n - 1 = \prod_{d|n} \Phi_d(T)$$

□

Theorem 5.9 (irreducibility of cyclotomic polynomials over $\mathbb{Q}$)**.** Let $K = \mathbb{Q}$, then χ_n is an isomorphism for every n. In particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, and Φ_n is irreducible over $\mathbb{Q}$.

Proof. The three statements are equivalent, so suffices to show any one of them. Note that χ_n is an isomorphism if and only if for all primes $p \not| n$, $p \mod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ is in the image of χ_n, by factoring a as a product of primes if a is coprime to n.

Fix a prime p with $p \not| n$. Let $f = m_{\zeta,\mathbb{Q}}$ and $g = m_{\zeta^p,\mathbb{Q}}$. If $f = g$, then $\zeta^p \in \mathrm{Orb}_G(\zeta)$, so $p \mod n \in \mathrm{im}(\chi_n)$ and we are done as p is arbitrary.

Suppose not. Then $(f, g) = 1$ and $f, g \mid T^n - 1$, so $fg \mid T^n - 1$. As ζ is a root of $g(T^p)$, $f \mid g(T^p)$. Reducing mod p, we get that

$$\overline{f} \mid \overline{g(T^p)} = \overline{g(T)^p}$$

Now $\overline{f}, \overline{g}$ divides $T^n - 1$ in $\mathbb{F}_p[T]$, which is separable as $p \not| n$, so $\overline{f} \mid (\overline{g})^p$ implies that $\overline{f} \mid \overline{g}$. But $\overline{f}^2 \mid \overline{f}\overline{g} \mid T^n - 1$. Contradiction as $T^n - 1$ separable. □

Proposition 5.10 (irreducibility of cyclotomic polynomials over $\mathbb{F}_p$). Let $K = \mathbb{F}_p$, $(n, p) = 1$. Then

(i) $\chi_n : G \to \langle p \mod n\rangle \leq (\mathbb{Z}/n\mathbb{Z})^\times$ is an isomorphism, with $\chi_n(\phi_p) = p \mod n$.

(ii) $r = [L : K] = |\langle p \mod n\rangle| = \mathrm{ord}(p \mod n)$,

(iii) ϕ_p has cycle type $(r, \dots, r)$ acting as a permutation of the roots of Φ_n.

Proof. $\phi_p(\zeta) = \zeta^p$, so $\chi_n(\phi_p) = p \mod n$, which implies that $\chi_n(G) = \langle p \mod n\rangle$ as $G = \mathrm{Gal}(L/K)$, L/K is an extension of finite fields, with G generated by ϕ_p. Then $[L : K] = |G| = |\langle p\rangle|$.

If $(a, n) = 1$, then

$$\phi_p^k(\zeta^a) = \zeta^{ak} \iff \phi_p^k(\zeta) = \zeta \iff r \mid k$$

so the orbits of ϕ_p acting on the primitive roots of unity all have size r. □

5.2 Artin's theorem

Theorem 5.11 (Artin's theorem on invariants). Let L be a field, $G \leq \mathrm{Aut}(L)$ be a finite subgroup. Then $L^G = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in G\}$ is a subfield of L, and $[L : L^G] = |G|$. In particular, L/L^G is a Galois extension with Galois group G.

Proof. Let $K = L^G$ and $x \in L$. Then if $\mathrm{Orb}_G(x) = \{\sigma_1(x), \dots, \sigma_r(x)\}$, x is a root of $f = \prod_{i=1}^r (T - \sigma_i(x)) \in L^G[T] = K[T]$. So x is separable over K, and $\deg_K(x) \leq |G|$. Furthermore, f is irreducible. Suppose there exists $f_1, f_2 \in K[T]$ such that $f = f_1 f_2$. Then

$$f_1 = \prod_{i \in I_1} (T - \sigma_i(x)) \quad \text{and} \quad f_2 = \prod_{i \in I_2} (T - \sigma_i(x))$$

where $I_1 \cup I_2 = \{1, \dots, r\}$, I_1, I_2 disjoint. Now for any $\sigma \in G$, $\sigma f_1 = f_1$, so σ fixes $\{\sigma_i(x) \mid i \in I_1\}$. Hence we must have that $I_1 = \varnothing$ or $I_1 = \{1, \dots, r\}$, i.e. one of f_1, f_2 is constant. So f is irreducible, and f is the minimal polynomial of x over K.

Now choose $y \in L$ with $\deg_K(y)$ maximal. We claim that $L = K(y)$. Suppose note, then choose $x \in L/K(y)$. By above, x, y are separable over K, so by the primitive element theorem, there exists $z \in L$ such that $K(z) = K(x, y) \supsetneq K(y)$. So $\deg_K(z) > \deg_K(y)$. Contradiction.

Finally, we want to show that the minimal polynomial of y over L^G has degree $|G|$. Equivalently, $|\mathrm{Stab}_G(y)| = 1$. But this is immediate since $\mathrm{Stab}_G(y)$ acts tirvially on L. □

Theorem 5.12. Let K be a field, $L = K(X_1, \dots, X_n)$ field of rational functions, $G = S_n$ acts on L by permuting the variables. Then $G \leq \mathrm{Aut}(L)$, with

$$L^G = k(S_1, \dots, S_n)$$

where S_k are the elementary symmetric polynomials.

Proof. $\supseteq$ is clear, so we will show the reverse inclusion. Given $f/g \in L^G$, $f, g \in k[X_1, \dots, X_n] = R$ so for every $\sigma \in G$, $f/g = (\sigma g)/(\sigma g)$. Gauss' lemma implies that R is a UDF,a nd the units in R are the constants. So $\sigma f = c_\sigma f$ and $\sigma g = c_\sigma g$ for some $c_\sigma \in K^\times$. As G is finite, of order $N = n!$, $f = \sigma^N f = c_\sigma^N f$, so $c_\sigma^N = 1$. But then $fg^{N-1}, g^N \in R^G = k[S_1, \dots, S_n]$, so $f/g \in \mathrm{Frac}(R^G) = k(S_1, \dots, S_n)$. □

Corollary 5.13. If $M = k(X_1, \dots, X_n)$ and $L = M^{S_n} = K(S_1, \dots, S_n)$, then L/K is a finite Galois extension with Galois group S_n. In particular, if

$$f = T^n - S_1 T^{n-1} + \dots + (-1)^n S_n \in L[T]$$

Then M is a splitting field for f over L and $\mathrm{Gal}(f/L) = S_n$.

Corollary 5.14. Given any finite group G, there exists a Galois extension L/K with Galois group G.

Remark 5.15. This is in general false if we fix K.

5.3 Constructible numbers

We will consider the following three plane geometry constructions.

(A): Intersection of lines

Given $P_1, P_2, Q_1, Q_2 \in \mathbb{R}^2$ with $P_i \neq Q_i$, we can construct the intersection of the lines P_1Q_1 and P_2Q_2, assuming the lines are not parallel.

(B): Intersection of circles

Given $P_1, P_2, Q_1, Q_2 \in \mathbb{R}^2$, we can construct the intersection of circles with centre P_i through Q_i.

(C): Intersection of line and circle

Given $P_1, P_2, Q_1, Q_2 \in \mathbb{R}^2$, we can construct the intersection of the line P_1Q_1 and the circle with centre P_2 through Q_2.

Definition 5.16 (constructible number)

We say that $(x, y) \in \mathbb{R}^2$ is constructible from $\{(x_1, y_1), \ldots, (x_n, y_n)\}$ if it can be obtained from a finite sequence of constructions (A), (B) and (C), involving the points (x_i, y_i) and any constructed in a previous step.

We say that $x \in \mathbb{R}$ is constructible if $(x, 0)$ is constructible from $\{(0, 0), (1, 0)\}$.

Definition 5.17 (constructible subfield)

Suppose $K \leq R$ is a subfield. We say that K is constructible if there exists fields

$$\mathbb{Q} = F_0 \leq F_1 \leq \cdots \leq F_n \leq \mathbb{R}$$

and $a_i \in F_i$ such that

(i) $K \leq F_n$,

(ii) $F_i = F_{i-1}(a_i)$,

(iii) $a_i^2 \in F_{i-1}$

Proposition 5.18. Suppose K is constructible. Then $[K : \mathbb{Q}] = 2^m$ for some m.

Proof. We have that $[F_n : \mathbb{Q}]$ is a power of 2 by the tower law, and that (ii) and (iii) imply that $[F_i, F_{i-1}] \leq 2$. Result follows by (i) and tower law. ☐

Theorem 5.19. If $x \in \mathbb{R}$ is constructible, then $K = \mathbb{Q}(x)$ is constructible.

Proof. Elementary geometry shows that (A) involves solving a linear equation, and (B) and (C) involves solving a quadratic equation. In both cases, the results can be obtained by adjoining (at most) one square root. ☐

Lemma 5.20. If m is a positive integer such that $2^m + 1$ is prime, then m is a power of 2.

Proof. If q is odd, then we have a nontrivial factorisation

$$2^{qr} + 1 = (2^r + 1)(2^{qr-r} - 2^{qr-2r} + \cdots + 1)$$

□

Theorem 5.21 (Gauss)**.** A regular n-gon is constructible, i.e. we can construct $\cos(2\pi/n)$ if and only if $n = 2^m p_1 \cdots p_k$, $p_1, \ldots, p_k$ distinct Fermat primes, i.e. primes of the form $2^{2^k} + 1$.

Proof. Let $x = \cos(2\pi/n)$, $\zeta_n = \exp(2\pi i/n)$. Then $\zeta_n^2 - 2x\zeta_n + 1 = 0$, so we have that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(x)] = 2$. Therefore, if x is constructible, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is a power of 2. But $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Let $n = p_1^{e_1} \cdots p_r^{e_r}$, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \prod p_i^{e_i - 1}(p-1)$. This is a power of two if and only if for all p_i odd, we haev $e_i = 1$ and $p - 1$ is a power of 2 so $\varphi(n)$ is a power of two if and only if n is of the required form.

Now suppose n has the required form, so $\varphi(n) = 2^m$, and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois, with Galois group $G \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, with 2^m elements. Then there exists subgroups

$$G = H_0 \geq H_1 \geq \cdots \geq H_m = 1$$

such that $[H_i : H_{i+1}] = 2$. This follows from GRM, where we showed a p-group has subgroups of all possible orders. Applying the Galois correspondence, we get $K_i = \mathbb{Q}(\zeta_n)^{H_i}$ and that $\mathbb{Q}(\zeta_n)$ is constructible. □

5.4 Kummer extensions

Theorem 5.22 (linear independence of characters)**.** Let G be a group, L a field, $\chi_1, \ldots, \chi_n : G \to L^\times$ be distinct group homomorphisms. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent.

Proof. By induction on n. $n = 1$ is trivial. Now suppose we have $y_1, \ldots, y_n \in L$ such that for all $g \in G$,

$$y_1\chi_1(g) + \cdots + y_n\chi_n(g) = 0 \qquad ((*))$$

As the homomorphisms are distinct, choose $h \in G$ such that $\chi_1(h) = \chi_n(h)$. As the χ_i are homomorphisms, putting hg into (*), we get

$$y_1\chi_1(h)\chi_1(g) + \cdots + y_n\chi_n(h)\chi_n(g) = 0$$

Now subtracting $\chi_n(h) \cdot (*)$, we get

$$y_1'\chi_1(g) + \cdots + y_{n-1}'\chi_{n-1}(g) = 0$$

where $y_i' = y_i(\chi_i(h) - \chi_n(h))$. By induction, all $y_i' = 0$, as $\chi_1(h) \neq \chi_n(h)$, so $y_1 = 0$. Hence by the induction hypothesis, $y_2 = \cdots = y_n = 0$. □

Corollary 5.23 (linear independence of field embeddings)**.** Suppose K, L are fields, $\sigma_1, \ldots, \sigma_n : K \to L$ are distinct field homomorphisms. If $y_1, \ldots, y_n \in L$ are such that $y_1\sigma_1(x) + \cdots + y_n\sigma_n(x) = 0$ for all $x \in K$, then $y_1 = \cdots = y_n = 0$.

Proof. Set $G = K^\times$ in the theorem. □

Theorem 5.24. Suppose K contains a primitive n-th root of unity $\zeta = \zeta_n$, and we have an extension $L = K(x)$, with $x^n = a \in K^\times$, then

(i) L/K is a splitting field for $f = T^n - a$, L/K is Galois with $\mathrm{Gal}(L/K)$ cyclic.

(ii) $[L:K] = \min\{m \geq 1 \mid x^m \in K\}$.

Proof. (i) As K has n distinct roots of unity ζ^i, f has n distinct roots in L, i.e. $f(T) = \prod_i (T - x\zeta^i)$. So L/K is a splitting field for the separable polynomial $T^n - a$, so L/K is Galois.

Now given $\sigma \in \mathrm{Gal}(L/K) = G$, $f(\sigma(x)) = 0$, so $\sigma(x) = x\zeta^i$ for some $i \in \{0, \ldots, n-1\}$. This gives us a map $\theta : G \to \mu_n(K) \simeq \mathbb{Z}/n\mathbb{Z}$, given by

$$\theta(\sigma) = \frac{\sigma(x)}{x} = \zeta^i$$

To see that this is a homomorphism, suppose $\sigma, \tau \in G$, as $\zeta \in K$, $\tau(\theta(\sigma)) = \theta(\sigma)$, so we have that

$$\theta(\tau\sigma) = \frac{\tau(\sigma(x))}{x} = \tau\left(\frac{\sigma(x)}{x}\right)\frac{\tau(x)}{x} = \tau(\theta(\sigma))\theta(\tau) = \theta(\sigma)\theta(\tau)$$

Furthermore, θ is injective, since $\theta(\sigma) = 1$ if and only if $\sigma(x) = x$, which is true if and only if $\sigma = \mathrm{id}$. So G is isomorphic to a subgroup of a cyclic group, so it is cyclic.

For (ii), if $m > 1$, since L/K is Galois,

$$x^m \in K \iff \forall \sigma \in G, \sigma(x^m) = x^m \iff \forall \sigma \in G, \theta(\sigma)^m = 1 \iff |G| = [L:K] \mid m$$

□

Corollary 5.25. Suppose K contains a primitive n-th root of unity ζ_N, then for $a \in K^\times$, $f = T^n - a$ is irreducible in $K[T]$ if and only if a is not a d-th power in K for any $d \mid n$, $d \neq 1$.

Proof. Let $L = K(x)$, where $x^n - a$. Then $m_{x,K}$ divides f, so f is irreducible if and only if $m_{x,K} = f$, which is true if and only if $|G| = [L:K] = n$. Now suppose $n = md$, $d > 1$. Then a is a d-th power in K if and only if $x^m \in K$, which is true if and only if $|G| \mid m$. □

Definition 5.26 (Kummer extension)

Extensions of the form $L = K(x)$, where $x^n = a \in K^\times$, and $\zeta_n \in K$ are called Kummer extensions.

Theorem 5.27. Suppose K contains a primitive n-th root of unity ζ, let L/K be a Galois extension, with $\mathrm{Gal}(L/K)$ cyclic of order n. Then $L = K(x)$ for some x such that $x^n = a \in K^\times$.

That is, if K contains a primitive n-th root of unity, then L/K is a Kummer extension if and only if L/K is Galois, with $\mathrm{Gal}(L/K)$ cyclic.

Proof. Let $G = \mathrm{Gal}(L/K) = \{1, \sigma, \ldots, \sigma^{n-1}\}$. Define the Langrange resolvent

$$R(y) = \sum_{j=0}^{n-1} \zeta^{-j}\sigma^j(y) \in L$$

Then if $x = R(y)$, we have that

$$\sigma(x) = \sum_{j=0}^{n-1} \zeta^{-j}\sigma^{j+1}(y) = \sum_{j=0}^{n-1} \zeta^{1-j}\sigma^j(y) = \zeta x$$

So $\sigma(x^n) = \zeta^n x^n = x^n$, and $x^n \in K$. By linear independence of field emebeddings, there exists $y \in L$ such that $R(y) \neq 0$. As $\sigma^i(x) = \zeta^i(x)$, the $\sigma^i(x)$ are distinct. Hence $\deg_K(x) = n$ and $L = K(x)$. □

6 Trace and norm

Definition 6.1 (multiplication map)
Let L/K be a field extension, $x \in L$, then the map $U_x : L \to L$ given by $U_x(y) = xy$ is called the multiplication map. In particular, U_x is a K-linear map.

Definition 6.2 (trace, norm, characteristic polynomial)
Let L/K be a field extension. Then the trace and norm of $x \in L$ are

$$\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(U_x) \quad \text{and} \quad N_{L/K}(x) = \det(U_x)$$

and the characteristic polynomial of x is

$$f_{x,L/K} = \det(T \cdot I - U_x)$$

Lemma 6.3. For $x, y \in L$, $a \in K$, $n = [L : K]$, we have that

(i) $\mathrm{Tr}_{L/K}(x + y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$ and $N_{L/K}(xy) = a^N_{L/K}(x)N_{L/K}(y)$,

(ii) $N_{L/K}(x) = 0$ if and only if $x = 0$,

(iii) $\mathrm{Tr}_{L/K}(1) = n$ and $N_{L/K}(1) = 1$,

(iv) $\mathrm{Tr}_{L/K}(ax) = a\,\mathrm{Tr}_{L/K}(x)$ and $N_{L/K}(ax) = a^n N_{L/K}(x)$

So $\mathrm{Tr}_{L/K}$ is a K-linear map, and $N_{L/K} : L^\times \to K^\times$ is a group homomorphism.

Theorem 6.4 (tower law)**.** Let $M/L/K$ be finite extensions. Then for all $x \in M$, we have that

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) = \mathrm{Tr}_{M/K}(x) \quad \text{and} \quad N_{L/K}(N_{M/L}(x)) = N_{M/K}(x)$$

Proof. We will only prove the statement for the trace, as it is the only one we will need. Given $x \in M$, choose a basis $u_1, \ldots, u_n$ for M/L, and $v_1, \ldots, v_n$ for L/K. Then let (a_{ij}) be the matrix of $U_{x,M/L}$. Then $\mathrm{Tr}_{M/L}(x) = \sum_i a_i i$.
Now for each i, j, let the matrix of $U_{a_{ij},L/K}$ be A_{ij}, so that we get

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) = \sum_i \mathrm{Tr}_{L/K}(a_i i) = \sum_i \mathrm{Tr}(A_i i)$$

Now in terms of the basis $(u_i v_j)$ for M/K, in the order $u_1 v_1, u_1 v_2, \ldots$, the matrix of $U_{x,M/K}$ is

$$\begin{pmatrix} A_{11} & * & * \\ * & \ddots & * \\ * & * & A_{mm} \end{pmatrix}$$

So $\mathrm{Tr}_{M/K}(x) = \sum_i \mathrm{tr}(A_{ii})$. ∎

Proposition 6.5. Let $L = K(x)$, and $f = T^n + c_{n-1}T^{n-1} + \cdots + c_0$ be the minimal polynomial of x over K. Then $f_{x,L/K} = f$. Furthermore, $\mathrm{Tr}_{L/K}(x) = -c_{n-1}$ and $N_{L/K}(x) = (-1)^n c_0$.

Proof. By standard linear algebra we only need to prove the first statement. Now consider the basis $1, x, \ldots, x^{n-1}$ for L/K. The matrix of U_x is

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix}$$

which is just the companion matrix of f, so has characteristic polynomial f. □

Corollary 6.6. Suppose $\text{char}(K) = p > 0$, $L = K(x)$, where $x \notin K$, $x^p \in K$. Then for every $y \in L$, $\text{Tr}_{L/K}(y) = 0$ and $N_{L/K}(y) = y^p$.

Proof. Note that $[L : K] = p$, so suffices to prove that the minimal polynomial of x over K is $T^p - x^p$. If $y \in K$, then $\text{tr}(y) = py = 0$, and $N_{L/K}(y) = y^p$. Otherwise, sicne $[L : K]$ is prime, $L = K(y)$. So if $y = \sum_i a_i x^i$, then $b = y^p = \sum_i a_i^p x^{ip} \in K$, so the minimal polynomial of y is $T^p - b$ and we are done. □

Proposition 6.7. Let L/K be a finite separable extension of degree n, $\sigma_1, \dots, \sigma_n : L \to M$ be the distinct K-homomorphisms into a normal closure M for L/K. Then we have that

$$\text{Tr}_{L/K}(x) = \sum_i \sigma_i(x), \qquad N_{L/K}(x) = \prod_i \sigma_i(x) \quad \text{and} \quad f_{x,L/K} = \prod_i (T - \sigma_i(x))$$

Proof. Suffices to prove the statement for the minimal polynomial. Let (e_i) be a basis for L/K, and $P = (\sigma_i(e_j))_{i,j}$. Since the σ_i are linearly independent, there can't be $y_i \in M$ such that for all j, $\sum_i y_i \sigma_i(e_j) = 0$. So P is nonsingular.

Let $A = (a_{ij})$ be the matrix of U_x, i.e. $xe_j = \sum_r a_{rj} e_r$, so we get that for all i, j,

$$\sigma_i(x)\sigma_i(e_j) = \sum_r \sigma_i(e_r) a_{rj}$$

Now if S is a diagonal matrix with $S_{ii} = \sigma_i(x)$, then the above becomes $SP = PA$, so $A = P^{-1}SP$, and A and S have the same characteristic polynomial. □

Corollary 6.8. If L/K is a finite Galois extension, then

$$\text{Tr}_{L/K}(x) = \sum_{\sigma \in \text{Gal}(L/K)} (x)$$

and so on.

Theorem 6.9. Let L/K be a finite extension. Then L/K is separable if and only if $\text{Tr}_{L/K}$ is surjective, i.e. if and only if $\text{Tr}_{L/K}$ is nonzero.

Proof. If L/K is separable, let $\sigma_1, \dots, \sigma_n \in \text{Hom}_K(L, M)$ be the distinct field embeddings into a normal closure M for L/K, then $\text{Tr}_{L/K}(x) = \sum \sigma_i(x)$. As the σ_i are linearly independent, this can't be identically zero.

Conversely, if L/K is inseparable, then let $x \in L$ be such that$K(x^p) \subsetneq K(x)$, which exists[4]. Then we have that $\text{Tr}_{K(x)/K(x^p)} = 0$, so

$$\text{Tr}_{L/K} = \text{Tr}_{L/K(x)} \circ \text{Tr}_{K(x)/K(x^p)} = 0$$

□

[4]By examples sheet 2 question 7

7 Algebraic closure

Definition 7.1 (algebraically closed field)
A field K is algebraically closed if every polynomial with coefficients in K has a root in K. Equivalently, the only irreducibles in $K[T]$ are linear.

Proposition 7.2. The following are equivalent.

(i) K is algebraically closed.

(ii) if L/K is any extension, $x \in L$ algebraic over K, then $x \in K$,

(iii) if L/K is algebraic, then $L = K$.

Proof. **(i)** $\implies$ **(ii)**. Let $f = m_{x,K}$, then $f \in K[T]$ is irreducible, so it is linear, so $x \in K$.
(ii) $\implies$ **(iii)** is true by definition.
(iii) $\implies$ **(i)**. Let $f \in K[T]$ be irreducible, $L = L_f = K[T]/(f)$. Then L is algebraic over K, so $L = K$ and f is linear. □

Proposition 7.3. Let L/K be an algebraic extension such that every irreducible polynomial in $K[T]$ splits into linear factors over L. Then L is algebraically closed.
We call L an algebraic closure for K.

Proof. Let M/L be an extension, $x \in M$ algebraic over L. Then x is algebraic over K, so $m_{x,K}$ is an irreducible polynomial, so it splits into linear factors over L. Hence $x \in L$, and as x is arbitrary, L is algebraically closed. □

Theorem 7.4. If K is a countable field, then K has an algebraic closure.

Proof. $K[T]$ is also countable, so enumerate the monic irreducible polynomials $f_1, f_2, \dots$ in $K[T]$. Let $L_0 = K$, and for each $i \geq 1$, let L_i be a splitting field for f_i over L_{i-1}. We can assume without loss of generality that $L_{i-1} \leq L_i$. Let $L = \bigcup_{i=0}^{\infty} L_i$. Then L is a field, any by construction each f_i splits over L. So L is an algebraic closure of K. □

Proposition 7.5. Let L/K be an algebraic extension of K, M algebraically closed, $\sigma : K \to M$ a field homomorphism. Then there exists $\overline{\sigma} : L \to M$ such that $\overline{\sigma}|_K = \sigma$.

Proof. If $L = K(x)$ is algebraic over K, let $f = m_{x,K}$. Then $\sigma f \in M[T]$ splits into linear factos, so there exists $\overline{\sigma} : K(x) \to M$ extending σ. In fact, we have one for each root of σf in M.
For general L, assume $K \leq L$ is a subfield. Then let

$$\mathcal{S} = \{(F, \tau) \mid K \leq F \leq L, \tau : F \to M \text{ field homomorphism with } \tau|_K = \sigma\}$$

We write $(F, \tau) \leq (F', \tau')$ if $F \leq F'$ and $\tau'|_F = \tau$. Then $(\mathcal{S}, \leq)$ is a nonempty poset. If $T = (F_i, \tau_i)$ is a poset, define

$$F' = \bigcup_i F_i \quad \text{and} \quad \tau'(x) = \tau_i(x) \text{ if } x \in F_i$$

Since T is a chain, this is well defined and it is an upper bound for T. Hence by Zorn's lemma, $\mathcal{S}$ has a maximal element (F, τ). Suppose $F \neq L$, then choose $x \in L \setminus F$. Then $L/F(x)/F$ is algebraic, so we can extend to $F(x) > F$. Contradiction. □

Theorem 7.6 (maximal ideal)**.** Let R be a nonzero ring. Then R has a maximal ideal.

Proof. By Zorn's lemma. □

Theorem 7.7. Let K be a field, then K has an algebraic closure $\overline{K}$. If $\sigma : K \to K'$ is an isomorphism, and $\overline{K}, \overline{K'}$ algebraic closures of K, K' respectively, then there exists an isomorphism $\overline{\sigma} : \overline{K} \to \overline{K'}$ extending σ. So the algebraic closure is unique up to isomorphism.

Proof. **Existence of algebraic closure:** Let $\mathcal{P} = \{f \in K[T] \mid f \text{ monic irreducible}\}$. Then we construct K_1 such that every $f \in \mathcal{P}$ has a root in K_1.

Define $R = K[\{T_f\}_{f\in\mathcal{P}}]$, where we adjoin an element T_f for each $f \in \mathcal{P}$. Let $I \trianglelefteq R$, $I = (f(T_f) \mid f \in \mathcal{F})$. In R/I, $T_f \mod I$ is a root of f. We will now show R/I is nonzero. Suppose $R = I$. Then there exists a finite subset $\mathcal{Q} \subseteq \mathcal{P}$, $r_f \in R$ such that

$$\sum_{f\in\mathcal{Q}} r_f f(T_f) = 1$$

We can assume without loss of generality that r_f is a polynomial in $\left\{T_g \mid g \in \mathcal{Q}\right\}$. Let L/K be a splitting field for $\prod_{f\in\mathcal{Q}} f \in K[T]$, $a_f \in L$ a root for each $f \in \mathcal{Q}$.

Now consider $\phi : R \to L$ given by $\phi|_K = \text{id}$, and

$$\phi(T_f) = \begin{cases} a_f & f \in \mathcal{Q} \\ 0 & f \notin \mathcal{Q} \end{cases}$$

Then $1 = \phi(1) = \sum_{f\in\mathcal{Q}} \phi(r_f)\phi(f(T_f)) = \sum_{f\in\mathcal{Q}} \phi(r_f) f(a_f) = 0$. Contradiction.

Therefore, by the maximal ideal theorem, R/I has a maximal ideal. Equivalently, by the correspondence theorem there exists a maximal ideal J of R with $I \le J$. Let $K_1 = R/J$. Then this is a field, and let $x_f = T_f \mod J \in K_1$. Then K_1/K is generated by $\{x_f\}$, so K_1/K is an algebraic extension of K such that every $f \in \mathcal{P}$ has a root.

Now let $\mathcal{P}_1$ be the set of irreducibles in K_1, repeating the above process we get K_2 and so on, we obtain

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$$

such that if $f = K_n[T]$ is non-constant, then it has a root in $K_{n+1}[T]$, so it splits in $K_{n+\deg(f)}[T]$. Letting $\overline{K} = \bigcup_n K_n$, this is an algebraic closure of K.

Uniqueness of algebraic closure: Assume without loss of generality $K \le \overline{K}$ and $K' \le \overline{K'}$, $\sigma : K \to K'$ is an isomorphism. As $\overline{K}/K$ is algebraic, σ extends to $\overline{\sigma} : \overline{K} \to \overline{K'}$. Now $K' \le \sigma(\overline{K}) \le \overline{K'}$, so $\overline{K'}/\sigma(\overline{K})$ is algebraic, $\overline{K}$ is algebraically closed, so $\sigma(\overline{K})$ is also algebraically closed. Hence $\overline{K'} = \sigma(\overline{K})$, so $\overline{\sigma}$ is an isomorphism. □

8 Cubics, quartics and solubility by radicals

8.1 Cubics

Let $f \in K[T]$ be a monic separable cubic, $G = \text{Gal}(f/K) \le S_3$ acts on the roots x_1, x_2, x_3 in a splitting field L of K.

If f is reducible, then either

1. f is a product of distinct linear factors in K, so $G = 1$.

2. f is a product of a linear factor and an irreducible quadratic in K, so $G = S_2$.

Now suppose f is irreducible, and $\text{char}(K) \ne 2, 3$. Then $G = S_3$ or A_3, with $G = A_3$ if and only if $\text{Disc}(f)$ is a square in K.

Let $K_1 = K(\Delta)$, then L/K_1 is Galois, with Galois group C_3.

If $\omega \in K_1$ is a primitive root of unity, then by L/K_1 is a Kummer extension, that is, $L = K_1(y)$ with $y^3 \in K_1$. Otherwise, let $L(\omega)$ be a splitting field of $f \cdot (T^3 - 1)$ over K. Then $L(\omega)/K_1(\omega)$ is Galois, with Galois group C_3, so $L(\omega) = K_1(\omega, y)$ with $y^3 \in K_1(\omega)$. Hence the x_i lies in the field obtained by adjoining square roots and cube roots to K.

8.2 Quartics

Let $f \in K[T]$ be a monic separable quartic, $\text{char}(K) \neq 2, 3$. Then $G = \text{Gal}(f/K) \leq S_4$. Let $V = V_4$ be the Klein-4 group, the transitive subgroup of S_4 of order 4. Let f have splitting field L with distinct roots $x_1, \ldots, x_4$, and suppose without loss of generality $x_1 + \cdots + x_4 = 0$. So $f = T^3 + aT^2 + bT + c$. Since V is a normal subgroup of S_4, $G \cap V$ is a normal subgroup of G containing V. In particular, we have a homomorphism $G/(G \cap V) \to S_4/V \simeq S_3$. But $G/(G \cap V) = \text{Gal}(M/K)$, where $M = L^{G \cap V}$ is a cubic extension.

Write $y_{12} = x_1 + x_2$ etc. Then $V \cap G$ maps $y_{ij} \to \pm y_{ij}$. So $y_{12}^2, y_{13}^2, y_{14}^2$ are fixed under $V \cap G$. Furthermore, y_{ij}^2 are the roots of a separable cubic $g \in K[T]$, called the resolvent cubic. Then $M = L^{G \cap V}$ is the splitting field of g, and

$$x_1 = \frac{1}{2}(y_{12} + y_{13} + y_{14})$$

and so on, so $L = M(y_{12}, y_{13}, y_{14})$[5]. This means that we can solve a quartic by solving a cubic and taking square roots.

8.3 Solubility by radicals

Suppose throughout $\text{char}(K) = 0$, so an extension is Galois if and only if it is normal.

Definition 8.1 (soluble by radicals)
An irreducible polynomial $f \in K[T]$ is soluble by radicals over K if there exists a sequence of fields

$$K = K_0 \leq \cdots \leq K_m$$

with $x \in K_m$ a root of f, and each $K_i = K_{i-1}(y_i)$ with $y_i^{d_i} \in K_{i-1}$, $d_i \geq 2$.

Proposition 8.2. Suppose there exists $d \geq 1$, and a sequence of fields $K = K_0 \leq \cdots \leq K_m$ with

(i) f has a root $x \in K_m$,

(ii) for $i > 1$, $K_i = K_{i-1})(y_i)$ with $(y_i)^d = a_i \in K_{i-1}$,

(iii) $K_1 = K_0(\zeta)$, ζ is a primitive d-th root of unity.

Then f is soluble by radicals over K. The converse is also true.

Proof. The statement is immediate from definitions. The converse follows by letting $d = \text{lcm}(d_i)$ and adding the first field if necessary. □

Thus, we will assume throughout the above conditions. In particular, K_1/K_0 is a cyclotomic extension, so it is Galois with abelian Galois group, and by Kummer theory K_i/K_{i-1} is Galois with $\text{Gal}(K_i/K_{i-1}) \leq C_d$.

Let M be a normal closure of K_m/K. Then M will contain a splitting field for f over K, since $x \in M$ and f is irreducible. Let $K_i' \leq M$ be a normal closure of K_i/K.

Proposition 8.3.

$$K_i' = K_{i-1}' \left(\left\{ \sqrt[d]{\sigma(a_i)} \mid \sigma \in \text{Gal}(K_{i-1}'/K) \right\} \right)$$

Proof. As the extensions are all normal, we have that $\text{Gal}(K_{i-1}'/K)$ is a normal subgroup of $\text{Gal}(K_i'/K)$, so $\text{Gal}(K_{i-1}'/K)$ is a quotient of $\text{Gal}(K_i'/K)$. In particular, given $\sigma \in \text{Gal}(K_{i-1}'/K)$, there exists $\overline{\sigma} \in \text{Gal}(K_i'/K)$ such that $\overline{\sigma}|_{K_i'} = \sigma$. Then

$$\overline{\sigma}(y_i)^d = \overline{\sigma}(y_i^d) = \sigma(y_i^d) = \sigma(a_i)$$

[5]In fact, $L = M(y_{12}, y_{13})$ as $y_{12}y_{13}y_{14} = b \in K$.

So we have $\supseteq$. Suffices to show that the RHS is normal over K, as the LHS is a normal closure. But it is the splitting field over K'_{i-1} of

$$g_i = \prod_{\sigma} (T^d - \sigma(a_i)) \in K[T]$$

So if K'_{i-1} is the splitting field for g_{i-1} over K, the RHS is a splitting foeld for $g_i g_{i-1}$ over K, so it is normal over K. □

Proposition 8.4. $\mathrm{Gal}(K'_i/K'_{i-1})$ is abelian.

Proof. Let $A = \mathrm{Gal}(K'_i/K'_{i-1})$. Then for all $\tau \in A$, $\sigma \in \mathrm{Gal}(K'_{i-1}/K)$, we have that

$$\tau\left(\sqrt[d]{\sigma(a_i)}\right) = \zeta_d^{m_\sigma} \sqrt[d]{\sigma(a_i)}$$

for some $m_\sigma \in \mathbb{Z}/d\mathbb{Z}$. So we have a map $\tau \mapsto (m_\sigma) \in (\mathbb{Z}/d\mathbb{Z})^r$, where $r = |\mathrm{Gal}(K_{i-1'}/K)|$, which defines an injective homomorphism. This holds for $i > 1$. For $i = 1$, note that $K'_1 = K_1$ and so K'_1/K'_0 is just K_1/K_0, which has abelian Galois group. □

Definition 8.5 (soluble group)
A finite group G is solutble if there exists a chain of normal subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = G$$

such that N_i/N_{i-1} is abelian for all i.

Proposition 8.6. $G = \mathrm{Gal}(M/K)$ is soluble.

Proof. Notice that $M = K'_m$, so we have a chain of normal extensions over K,

$$K = K'_0 \leq K'_1 \leq \cdots \leq K'_{m-1} \leq K'_m = M$$

which by the Galois correspondence gives us a chain of normal subgroups of $\mathrm{Gal}(M/K)$,

$$1 = \mathrm{Gal}(K/K) \trianglelefteq \mathrm{Gal}(K'_1/K) \trianglelefteq \cdots \trianglelefteq \mathrm{Gal}(K'_{m-1}/K) \trianglelefteq \mathrm{Gal}(K'_m/K) = G$$

with

$$\frac{\mathrm{Gal}(K'_i/K)}{\mathrm{Gal}(K'_{i-1}/K)} = \mathrm{Gal}(K'_i/K'_{i-1})$$

abelian, so G is soluble. □

Lemma 8.7. Any subgroup and any quotient of a solble group is soluble.

Proof. Take $H \cap N_i$ and $N_i/(H \cap N_i)$ respectively. □

Theorem 8.8 (Abel-Ruffini)**.** If $f \in K[T]$ is soluble by radicals over K, then $\mathrm{Gal}(f/K)$ is soluble.

Proof.

$$\mathrm{Gal}(f/K) \simeq \mathrm{Gal}(L/K) \simeq \frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(L/K)}$$

is soluble. □

Proposition 8.9. If $n \geq 5$ then S_n and A_n are not soluble.

Proof. Both contain the non-abelian simple group A_5. □

Corollary 8.10. If $\deg(f) = n \geq 5$, with $A_n \leq \text{Gal}(f/K)$, then f is not soluble by radicals.