Galois Theory

Dr P.M.H. Wilson[1]

Michaelmas Term 2000

[1] LaTeXed by James Lingard — please send all comments and corrections to `james@lingard.com`

These notes are based on a course of lectures given by Dr Wilson during Michaelmas Term 2000 for Part IIB of the Cambridge University Mathematics Tripos.

In general the notes follow Dr Wilson's lectures very closely, although there are certain changes. In particular, the organisation of Chapter 1 is somewhat different to how this part of the course was lectured, and I have also consistently avoided the use of a lower-case k to refer to a field — in these notes fields are always denoted by upper-case roman letters.

These notes have not been checked by Dr Wilson and should not be regarded as official notes for the course. In particular, the responsibility for any errors is mine — please email me at `james@lingard.com` with any comments or corrections.

James Lingard
October 2001

Contents

1 Revision from Groups, Rings and Fields

1.1 Field extensions

Suppose K and L are fields. Recall that a non-zero ring homomorphism $\theta : K \to L$ is necessarily injective (since $\ker\theta \lhd K$ and so $\ker\theta = \{0\}$) and satisfies $\theta(a/b) = \theta(a)/\theta(b)$. Therefore θ is a homomorphism of fields.

Definition

A *field extension* of K is given by a field L and a non-zero homomorphism $\theta : K \hookrightarrow L$. Such a θ will also be called an *embedding* of K into L.

Remark

In fact, we often identify K with its image $\theta(K) \subseteq L$, since $\theta : K \to \theta(K)$ is an isomorphism, and denote the extension by L/K or $K \hookrightarrow L$.

Lemma 1.1

If $\{K_i\}_{i\in I}$ is any collection of subfields of a field L, then $\bigcap_{i\in I} K_i$ is also a subfield of L.

Proof

Easy exercise from the axioms. $\square$

Definition

Given a field extension L/K and an arbitrary subset $S \subseteq L$, the subfield of L *generated* by K and S is

$$K(S) = \bigcap\{\text{subfields } M \subseteq L \mid M \supseteq K, M \supseteq S\}.$$

The lemma above implies that it is a subfield — it is the smallest subfield containing K and S.

Notation

If $S = \{\alpha_1, \dots, \alpha_n\}$ we write $K(\alpha_1, \dots, \alpha_n)$ for $K(S)$.

Definition

A field extension L/K is *finitely generated* if for some n there exist $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$. If $L = K(\alpha)$ for some $\alpha \in L$, the extension is *simple.*

Definition

Given a field extension L/K, an element $\alpha \in L$ is *algebraic* over K if there exists a non-zero polynomial $f \in K[X]$ such that $f(\alpha) = 0$ in L. Otherwise, α is *transcendental* over K.

If α is algebraic, the monic polynomial

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

of smallest degree such that $f(\alpha) = 0$ is called the *minimal polynomial* of f. Clearly such an f is unique and irreducible.

Definition

A field extension L/K is *algebraic* if every $\alpha \in L$ is algebraic over K. It is *pure transcendental* if every $\alpha \in L \setminus K$ is transcendental over K.

1.2 Classification of simple algebraic extensions

Given a field K and an irreducible polynomial $f \in K[X]$, recall that the quotient ring $K[X]/(f)$ is a field. Therefore we have a simple algebraic field extension $K \hookrightarrow K(\alpha) = K[X]/(f)$, α denoting the image of X under the quotient map.

Also, for any simple algebraic field extension $K \hookrightarrow K(\alpha)$ let f be the minimal polynomial of α over K. We then have a commutative diagram

$$\begin{tikzcd} K \arrow[r] \arrow[dr] & K[X] \arrow[d] \\ & K(\alpha) \end{tikzcd}$$

inducing an isomorphism of fields $K[X]/(f) \cong K(\alpha)$. Thus up to field isomorphisms, any simple algebraic extension of K is of the form $K \hookrightarrow K[X]/(f)$ for some irreducible $f \in K[X]$.

Therefore, classifying simple algebraic extensions of K (up to isomorphism) is equivalent to classifying irreducible monic polynomials in $K[X]$.

1.3 Tests for irreducibility

Let R be a UFD and K its field of fractions, e.g. $R = \mathbb{Z}$, $K = \mathbb{Q}$.

Lemma 1.2 (Gauss' Lemma)

A polynomial $f \in R[X]$ is irreducible in $R[X]$ iff it is irreducible in $K[X]$.

Theorem 1.3 (Eisenstein's Criterion)

Suppose

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in R[X]$$

and there exists an irreducible $p \in R$ such that $p \nmid a_n$, $p \mid a_i$ for $i = n-1, \ldots, 0$ and $p^2 \nmid a_0$. Then f is irreducible in $R[X]$ and hence irreducible in $K[X]$.

Proofs

See 'Groups, Rings and Fields'.

1.4 The degree of an extension

Definition

If L/K is a field extension, then L has the structure of a vector space over K. The dimension of the vector space is called the *degree* of the extension, written $[L : K]$.

We say that L is *finite* over K if $[L : K]$ is finite.

Theorem 1.4

Given a field extension L/K and an element $\alpha \in L$, α is algebraic over K iff $K(\alpha)/K$ is finite. When α is algebraic, $[K(\alpha) : K]$ is the degree of the minimal polynomial of α.

Proof

($\Leftarrow$) If $[K(\alpha) : K] = n$, then $1, \alpha, \ldots, \alpha^n$ are linearly dependent over K, so there exists a polynomial $f \in K[X]$ with $f(\alpha) = 0$, as claimed.

($\Rightarrow$) If α is algebraic over K with minimal polynomial f, then

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \tag{$*$}$$

in L.

Suppose $g \in K[X]$ with $g(\alpha) \neq 0$. Since f is irreducible we have $\mathrm{hcf}(f, g) = 1$. Euclid's algorithm implies that there exist $x, y \in K[X]$ such that $xf + yg = 1$ and so $y(\alpha)g(\alpha) = 1$ in L (since $f(\alpha) = 0$). So $g(\alpha)^{-1} \in \langle 1, \alpha, \alpha^2, \ldots \rangle$, the subspace of L generated by powers of α.

Now $K(\alpha)$ consists of all elements of the form $h(\alpha)/g(\alpha)$ for $h, g \in K[X]$ polynomials, $g(\alpha) \neq 0$, and so $K(\alpha)$ is spanned as a K-vector space by $1, \alpha, \alpha^2, \ldots$ and hence from relation $(*)$ by $1, \alpha, \ldots, \alpha^{n-1}$.

Minimality of n implies that the spanning set $1, \alpha, \ldots, \alpha^{n-1}$ is a basis and hence $[K(\alpha) : K] = n$. $\square$

Proposition 1.5 (Tower Law)

Given a tower *of field extensions $K \hookrightarrow L \hookrightarrow M$,*

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

Proof

Let $(u_i)_{i \in I}$, be a basis for M over L and let $(v_j)_{j \in J}$, be a basis for be a basis for L over K. We shall show that $(u_i v_j)_{i \in I, j \in J}$ is a basis for M over K, from which the result follows.

First we show that the $u_i v_j$ span M over K. Now any vector $x \in M$ may be written as a linear combination of the u_i, that is

$$x = \sum_{i \in I} \mu_i u_i$$

for some $\mu_i \in L$. But since the v_j span L over K we can write each μ_i as a linear combination of the v_j, that is

$$\mu_i = \sum_{j \in J} \lambda_{ij} v_j$$

for some $\lambda_{ij} \in K$. But then

$$x = \sum_{\substack{i \in I \\ j \in J}} \lambda_{ij} u_i v_j$$

as required.

Now we shall show that the $u_i v_j$ are linearly independent over K. Suppose that we have

$$\sum_{\substack{i \in I \\ j \in J}} \lambda_{ij} u_i v_j = 0$$

for some $\lambda_{ij} \in L$. But then

$$\sum_{i \in I} \left(\sum_{j \in J} \lambda_{ij} v_j \right) u_i = 0$$

and then since the u_i are linearly independent over L we must have

$$\sum_{j \in J} \lambda_{ij} v_j = 0$$

for each $j \in J$. But then since the v_j are linearly independent over K we must have that $\lambda_{ij} = 0$ for each $i \in I, j \in J$, as required. $\square$

Corollary 1.6

If L/K is finitely generated, $L = K(\alpha_1, \ldots, \alpha_n)$, with each α_i algebraic over K, then L/K is a finite extension.

Proof

Each α_i is algebraic over $K(\alpha_1, \ldots, \alpha_{i-1})$ and so by (1.4) we have that for each i, $[K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})]$ is finite. Induction and the Tower Law give the required result. $\square$

1.5 Splitting fields

Recall that if L/K is a field extension and $f \in K[X]$ we say that f *splits* (completely) over L if it may be written as a product of linear factors

$$f = k(X - \alpha_1) \cdots (X - \alpha_n),$$

where $k \in K$ and $\alpha_i \in L$. L is called a *splitting field* for f if f fails to split over any proper subfield of L, that is, if $L = K(\alpha_1, \ldots, \alpha_n)$.

Remark

Splitting fields always exist.

For if g is any irreducible factor of f, then $K[X]/(g) = K(\alpha)$ is an extension of K for which $g(\alpha) = 0$, where α denotes the image of X. The remainder theorem implies that g (and hence f) splits off a linear factor. Induction implies that there exists a splitting field L for f, with $[L : K] \leq n!$ ($n = \deg f$) by (1.5).

Splitting fields are unique up to isomorphisms over K.

Proposition 1.7

Suppose $\theta : K \to K'$ is an isomorphism of fields, with the polynomial $f \in K[X]$ corresponding to $g = \theta(f) \in K'[X]$. Then any splitting field L of f over K is isomorphic over θ to any splitting field L' of g over K', and we have the commutative diagram

$$\begin{tikzcd} L \arrow[r, "\tilde{\theta}"] & L' \\ K \arrow[u] \arrow[r, "\theta"] & K' \arrow[u] \end{tikzcd}$$

Proof

Since f splits in L, so does any irreducible factor f_1. Let $g_1 = \theta(f_1)$ be the corresponding irreducible factor of g. Observe that g, and hence g_1, splits in L'. Choose a root $\alpha \in L$ of f_1 and a root $\beta \in L'$ of g_1.

Then there exists an isomorphism of fields, θ_1, determined by the commutative diagram

$$\begin{tikzcd} K(\alpha) \arrow[r, "\theta_1"] & K'(\beta) \\ K[X]/(f_1) \arrow[u] \arrow[r] & K'[X]/(g_1) \arrow[u] \end{tikzcd}$$

with $\theta_1(\alpha) = \beta$. Hence we have the diagram

$$\begin{tikzcd} L & L' \\ K(\alpha) \arrow[u] \arrow[r, "\theta_1"] & K'(\beta) \arrow[u] \\ K \arrow[u] \arrow[r, "\theta"] & K' \arrow[u] \end{tikzcd}$$

Now set $f = (X - \alpha)h \in K(\alpha)[X]$ and $g = (X - \beta)l \in K'(\beta)[X]$. Then

1. $l = \theta_1(h)$ under the induced isomorphism $K(\alpha)[X] \to K'(\beta)[X]$.
2. L is a splitting field for h over $K(\alpha)$ and L' is a splitting field for l over $K'(\beta)$.

Therefore the required result follows by induction on the degree of the polynomial. □

Remark

Thus we have proved existence and uniqueness of splitting fields for any finite set of polynomials — just take the splitting field of the product.

With appropriate use of Zorn's Lemma (see §3) we can prove existence and uniqueness of splitting fields for any set of polynomials.

2 Separability

2.1 Separable polynomials and formal differentiation

Definition

An irreducible polynomial $f \in K[X]$ is *separable* over K if it has distinct zeros in a splitting field L, that is

$$f = k(X - \alpha_1) \cdots (X - \alpha_n)$$

in $L[X]$, with $k \in K$ and $\alpha_i \in L$ all distinct. By uniqueness (up to isomorphism) of splitting fields, this is independent of any choices.

An arbitrary polynomial $f \in K[X]$ is *separable* over K if all its irreducible factors are. If f is not separable, it is called *inseparable*.

Definition

Formal differentiation is a linear map $D : K[X] \to K[X]$ of vector spaces over K, defined by

$$D(X^n) = nX^{n-1}$$

for all $n \geq 0$.

Claim

If $f, g \in K[X]$, then

$$D(fg) = fD(g) + gD(f).$$

Proof

Using linearity we can reduce the theorem to the case when f and g are monomials, when it is a trivial check.

Notation

From now on, we write f' for $D(f)$.

Lemma 2.1

A non-zero polynomial $f \in K[X]$ has a repeated zero in a splitting field L iff f and f' have a common factor in $K[X]$ of degree ≥ 1.

Proof

($\Rightarrow$) Suppose f has a repeated zero in a splitting field L, that is $f = (X - \alpha)^2 g$ in $L[X]$. Then $f' = (X - \alpha)^2 g' - 2(X - \alpha)g$. So f and f' have a common factor $(X - \alpha)$ in $L[X]$, and so f and f' have a common factor in $K[X]$, namely the minimal polynomial for α over K.

($\Leftarrow$) Suppose f has no repeated zeros in a splitting field L. We shall show that f and f' are coprime in $L[X]$ and hence also in $K[X]$.

Since f splits in L it is sufficient to prove that $(X - \alpha) \mid f$ in $L[X]$ implies $(X - \alpha) \nmid f'$. Writing $f = (X - \alpha)g$, we observe that $(X - \alpha) \nmid g$, but $f' = (X - \alpha)g' + g$ and so $(X - \alpha) \nmid f'$. □

Suppose now that $f \in K[X]$ is irreducible. Then (2.1) says that f has repeated zeros iff $f' = 0$. But if

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

then

$$f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + a_1$$

and therefore $f' = 0$ iff $i a_i = 0$ for all $i > 0$. So if $\deg f = n > 0$ then $f' = 0$ iff $\operatorname{char} K = p > 0$ and $p \mid i$ whenever $a_i \neq 0$.

So if $\operatorname{char} K = 0$, all polynomials are separable. If $\operatorname{char} K = p > 0$, an irreducible polynomial $f \in K[X]$ is inseparable iff $f \in K[X^p]$.

2.2 Separable extensions

Definition

Given a field extension L/K and an element $\alpha \in L$, α is *separable* over K if its minimal polynomial $f_\alpha \in K[X]$ is separable.

The extension is called *separable* if α is separable for all $\alpha \in L$. Otherwise the extension is called *inseparable*.

Example

Let $L = \mathbb{F}_p(t)$, the field of rational functions over the finite field $\mathbb{F}_p$ with p elements. Let $K = \mathbb{F}_p(t^p)$.

Then the extension L/K is finite but inseparable, since the minimal polynomial of t over K is $X^p - t^p$, which splits as $(X - t)^p$ over $L[X]$.

Lemma 2.2

If $K \hookrightarrow L \hookrightarrow M$ is a tower of field extensions with M/K separable, then both M/L and L/K are separable.

Proof

Obviously L/K is separable, since any element $\alpha \in L$ is separable over K as an element of M.

Now given $\alpha \in M$, the minimal polynomial of α over L divides the minimal polynomial of α over K, and so has distinct zeros in any splitting field. $\square$

Proposition 2.3

Let $K(\alpha)/K$ be a finite simple extension, with $f \in K[X]$ the minimal polynomial for α. Given a field extension $\theta : K \hookrightarrow L$, the number of embeddings $\tilde{\theta} : K(\alpha) \hookrightarrow L$ extending θ is precisely the number of distinct roots of $\theta(f)$ in L.

In particular, there exist at most $n = [K(\alpha) : K]$ such embeddings, with equality iff $\theta(f)$ splits completely over L and f is separable.

Proof

An embedding $K(\alpha) \hookrightarrow L$ extending θ must send α to a zero of $\theta(f)$, and it is determined by this information.

Furthermore, if β is a root of $\theta(f)$ in L then the ring homomorphism $K[X] \to L$ sending g to $\theta(g)(\beta)$ factors to give an embedding $K(\alpha) \cong K[X]/(f) \hookrightarrow L$ extending θ.

Therefore the embeddings $K(\alpha) \hookrightarrow L$ extending θ are in one-to-one correspondence with the roots of $\theta(f)$ in L. So there exist at most $n = \deg(f) = [K(\alpha) : K]$ (by (1.4)) such embeddings, with equality iff $\theta(f)$ has n distinct roots in L iff $\theta(f)$ splits completely over L and f is separable. □

Theorem 2.4

Suppose $L = K(\alpha_1, \ldots, \alpha_r)$ is a finite extension of K, and M/K is any field extension for which the minimal polynomials of the α_i all split. Then

1. *The number of embeddings $L \hookrightarrow M$ extending $K \hookrightarrow M$ is at most $[L : K]$. If each α_i is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$ then we have equality.*
2. *If the number of embeddings $L \hookrightarrow M$ extending $K \hookrightarrow M$ is $[L : K]$ then L/K is separable.*

Hence if each α_i is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$ then L/K is separable. (By (2.2) *this happens, for example, when each α_i is separable over K.)*

Proof

1. This follows by induction on r:

   (2.3) implies that the claim holds for $r = 1$.

   Suppose that it is true for $r - 1$ ($r > 1$). Then there exist at most $[K(\alpha_1, \ldots, \alpha_{r-1}) : K]$ embeddings $K(\alpha_1, \ldots, \alpha_{r-1}) \hookrightarrow M$ extending $K \hookrightarrow M$, with equality if each α_i ($i < r$) is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$.

   Now for each embedding $K(\alpha_1, \ldots, \alpha_{r-1}) \hookrightarrow M$, (2.3) implies that there exist at most $[K(\alpha, \ldots, \alpha_r) : K(\alpha_1, \ldots, \alpha_{r-1})]$ embeddings $K(\alpha_1, \ldots, \alpha_r) \hookrightarrow M$ extending the given one, with equality if α_r separable over $K(\alpha_1, \ldots, \alpha_{r-1})$.

   The Tower Law then gives the result.

2. Suppose $\alpha \in L$. Then (2.3) implies that there exist at most $[K(\alpha) : K]$ embeddings $K(\alpha) \hookrightarrow M$ extending $K \hookrightarrow M$ and (1) implies that for each such embedding, there exist at most $[L : K(\alpha)]$ embeddings $L \hookrightarrow M$ extending it. By the Tower Law, our assumption implies that both these must be equalities. In particular, (2.3) implies that α must be separable. □

Corollary 2.5

If $K \hookrightarrow L \hookrightarrow M$ is a tower of finite extensions with M/L and L/K separable, then so too is M/K.

Proof

Let $\alpha \in M$ with (separable) minimal polynomial $f \in L[X]$ over L. Write

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

where each a_i is separable over K.

The minimal polynomial of α over $K(a_0, \ldots, a_{n-1})$ is still f, and so α is separable over $K(a_0, \ldots, a_{n-1})$. But then (2.4) implies that $K(a_0, \ldots, a_{n-1}, \alpha)/K$ is separable, and so α is separable over K. $\square$

2.3 The Primitive Element Theorem

Lemma 2.6

If K is a field and G is a finite subgroup of K^*, the group of units of K, then G is cyclic.

Proof

See 'Groups, Rings and Fields'.

Theorem 2.7 (Primitive Element Theorem)

1. *If $L = K(\alpha, \beta)$ is a finite extension of K with β separable over K, then there exists $\theta \in L$ such that $L = K(\theta)$.*
2. *Any finite separable extension is simple.*

Proof

1. $\Rightarrow$ 2. If L/K is a finite separable extension, then $L = K(\alpha_1, \ldots, \alpha_r)$ with each α_i separable over K, so (2) follows from (1) by induction.

1. If K is finite then so too is L, and so (2.6) implies that L^* is cyclic, say $L^* = \langle \theta \rangle$. Then $L = K(\theta)$, as required.

   So assume that K is infinite, and let f and g be the minimal polynomials for α and β respectively.

   Let M be a splitting field extension for fg over L. Identifying L with its image in M, the distinct zeros of f are $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$, where $r \leq \deg f$. Since β is separable over K, g splits into distinct linear factors over M and has zeros $\beta = \beta_1, \beta_2, \ldots, \beta_s$, where $s = \deg g$.

   Then choose $c \in K$ such that the elements $\alpha_i + c\beta_j$ are distinct (this is possible since there are only finitely many values $\alpha_i - \alpha_{i'}$, $\beta_j - \beta_{j'}$) and set $\theta = \alpha + c\beta$.

   Let $F \in K(\theta)[X]$ be given by $F(X) = f(\theta - cX)$. We have $g(\beta) = 0$ and $F(\beta) = f(\alpha) = 0$. So F and g have a common zero, namely β. Any other common zero would be a β_j with $j > 1$, but then $F(\beta_j) = f(\alpha + c(\beta - \beta_j))$. Since by assumption $\alpha + c(\beta - \beta_j)$ is never an α_i, this cannot be zero.

   The linear factors of g being distinct, we deduce that $(X - \beta)$ is the h.c.f. of F and g in $M[X]$. However, the minimal polynomial h of β over $K(\theta)$ then divides both F and g in $K(\theta)[X]$ and hence also in $M[X]$. This implies that $h = X - \beta$ and so $\beta \in K(\theta)$.

   Therefore $\alpha = \theta - c\beta \in K(\theta)$ and so $K(\alpha, \beta) = K(\theta)$, as required. $\square$

2.4 Trace and norm

Definition

Let L/K be a finite field extension and let $\alpha \in L$. Multiplication by α defines a linear map $\theta_\alpha : L \to L$ of vector spaces over K. The *trace* and *norm* of α, $\mathrm{Tr}_{L/K}(\alpha)$ and $\mathrm{N}_{L/K}(\alpha)$, are defined to be the trace and determinant of θ_α, i.e. of any matrix representing θ_α with respect to some basis for L/K.

Proposition 2.8

Suppose $r = [L : K(\alpha)]$ *and*

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

is the minimal polynomial of α *over* K. *If we define* $b_i = (-1)^{(n-i)}a_i$, *then*

$$\mathrm{Tr}_{L/K}(\alpha) = rb_{n-1} \qquad \text{and} \qquad \mathrm{N}_{L/K}(\alpha) = {b_0}^r.$$

Proof

This follows from the claim that the characteristic polynomial of θ_α is f^r.

We prove this first for the case $r = 1$, i.e. $L = K(\alpha)$. Take a basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ ($n = [K(\alpha) : K]$) for L/K. With respect to this basis, θ_α has the matrix

$$M = \begin{pmatrix} & & & & -a_0 \\ 1 & & & & -a_1 \\ & 1 & & & -a_2 \\ & & \ddots & & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}.$$

The characteristic polynomial of θ_α is then

$$\det \begin{pmatrix} X & & & & a_0 \\ -1 & X & & & a_1 \\ & -1 & X & & a_2 \\ & & \ddots & \ddots & \vdots \\ & & & -1 & X + a_{n-1} \end{pmatrix} = \det \begin{pmatrix} & & & & f \\ -1 & X & & & a_1 \\ & -1 & X & & a_2 \\ & & \ddots & \ddots & \vdots \\ & & & -1 & X + a_{n-1} \end{pmatrix}$$

which equals f, as claimed.

In the general case, choose a basis $1 = \beta_1, \beta_2, \ldots, \beta_r$ for L over $K(\alpha)$ and take a basis for L/K given by

$$\begin{matrix} 1, & \alpha, & \alpha^2, & \ldots, & \alpha^{n-1} \\ \beta_2, & \alpha\beta_2, & \alpha^2\beta_2, & \ldots, & \alpha^{n-1}\beta_2 \\ & & \vdots & & \\ \beta_r, & \alpha\beta_r, & \alpha^2\beta_r, & \ldots, & \alpha^{n-1}\beta_r \end{matrix}$$

(c.f. proof of the Tower Law). With respect to this basis, θ_α has the matrix

$$\begin{pmatrix} M & & & \\ & M & & \\ & & \ddots^{(r \text{ times})} & \\ & & & M \end{pmatrix},$$

with characteristic polynomial f^r, which proves the claim and hence the proposition. $\square$

3 Algebraic Closures

3.1 Definitions

Definition

A field K is *algebraically closed* if any $f \in K[X]$ splits into linear factors over K.

This is equivalent to saying, "there do not exist non-trivial algebraic extensions of K", i.e. any algebraic extension $K \hookrightarrow L$ is an isomorphism.

An extension L/K is called an *algebraic closure* of K if L/K is algebraic and L is algebraically closed.

Lemma 3.1

If L/K is algebraic and every polynomial in $K[X]$ splits completely over L, then L is an algebraic closure of K.

Proof

It is required to prove that L is algebraically closed. Suppose $L(\alpha)/L$ is a finite extension and let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

be the minimal polynomial of α over L. Let $K' = K(a_0, \ldots, a_{n-1})$. Then the extension $K'(\alpha)/K'$ is finite, and since each $a_i \in L$ is algebraic over K the Tower Law implies that K'/K and hence $K'(\alpha)/K$ is finite. But then α is algebraic over K and so $\alpha \in L$ (since the minimal polynomial of α over K splits completely over L). $\square$

Example

Let A be the set of algebraic numbers in $\mathbb{C}$, i.e.

$$A = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}.$$

Then A is a subfield of $\mathbb{C}$. For if $\alpha, \beta \in A$, the Tower Law and (1.4) imply that $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ is a finite extension. Therefore for any combination $\gamma = \alpha+\beta, \alpha-\beta, \alpha\beta, \alpha/\beta$ (when $\beta \neq 0$) we have $[\mathbb{Q}(\gamma)/\mathbb{Q}]$ finite, and so γ is algebraic over $\mathbb{Q}$ and hence $\gamma \in A$.

Therefore $A = \bar{\mathbb{Q}}$, the algebraic closure of the rationals.

3.2 Existence and uniqueness of algebraic closures

Theorem 3.2 (Existence of algebraic closures)

For any field K there exists an algebraic closure.

Proof

Let A be the set of all pairs $\alpha = (f, j)$, where f is an irreducible monic polynomial in $K[X]$ and $1 \leq j \leq \deg f$. For each $\alpha = (f, j)$ we introduce an indeterminate $X_\alpha = X_{f,j}$ and consider the polynomial ring $K[X_\alpha \mid \alpha \in A]$ in all these indeterminates.

Let $b_{f,l}$, for $0 \leq l < \deg f$, denote the coefficients of

$$\tilde{f} = f - \prod_{j=1}^{\deg f} (X - X_{f,j})$$

in $K[X_\alpha \mid \alpha \in A]$. Let I be the ideal generated by all these elements $b_{f,l}$ over all f, l and set $R = K[X_\alpha \mid \alpha \in A]/I$.

The idea here is that we are forcing all the monic polynomials $f \in K[X]$ to split completely, with the indeterminates $X_{f,j}$ representing the roots of f.

Claim

$I \neq K[X_\alpha \mid \alpha \in A]$, and so $R \neq 0$.

Proof

If we did have equality, then there exists a finite sum

$$g_1 b_{f_1,l_1} + \cdots + g_N b_{f_N,l_N} = 1 \qquad (*)$$

in $K[X_\alpha \mid \alpha \in A]$. Let S be a splitting field extension for $f_1, \ldots, f_N$. For each i, f_i splits in S as

$$f_i = \prod_{j=1}^{\deg f_i} (X - \alpha_{ij}).$$

Let $\theta : K[X_\alpha \mid \alpha \in A] \to S$ be the evaluation map (a ring homomorphism) sending $X_{f_i,j}$ to α_{ij} for each i, j and all other indeterminates X_α to 0. Let $\tilde{\theta}$ be the homomorphism induced from $K[X_\alpha \mid \alpha \in A][X]$ to $S[X]$ by θ. Then

$$\tilde{\theta}(\tilde{f}_i) = \tilde{\theta}(f_i) - \prod_{j=1}^{\deg f} \tilde{\theta}(X - X_{f_i,j}) = f_i - \prod_{j=1}^{\deg f_i} (X - \alpha_{ij}) = 0.$$

But then $\theta(b_{f_i,j}) = 0$ for each i, j, since the $b_{f_i,j}$ are the coefficients of $\tilde{f}$. Then, taking the image of the relation $(*)$ under θ, we get $0 = 1$.

Thus $R \neq 0$, and we may use Zorn's Lemma to choose a maximal ideal m of R (see handout). Let $L = R/m$. This gives a field extension $K \hookrightarrow L$ as the composite of the ring homomorphisms

$$K \hookrightarrow K[X_\alpha \mid \alpha \in A] \to R \to L.$$

Claim

L is an algebraic closure of K with this inclusion map.

Proof

First observe that L/K is algebraic, since it is generated by the images $x_{f,j}$ of the $X_{f,j}$, which by construction satisfy $f(x_{f,j}) = 0$. Any element of L involves only finitely many of the $x_{f,j}$, and so by the Tower Law is algebraic over K.

Moreover, by assumption any $f \in K[X]$ splits completely over L, and so the result follows from (3.1). $\square$

Proposition 3.3

Suppose $i : K \hookrightarrow L$ is an embedding of K into an algebraicallly closed field L. For any algebraic field extension $\phi : K \hookrightarrow M$, there exists an embedding $j : M \hookrightarrow L$ extending i, i.e. such that the following diagram

$$\begin{tikzcd} & M \arrow[dr, "j"] & \\ K \arrow[ur, "\phi"] \arrow[rr, "i"'] & & L \end{tikzcd}$$

commutes.

Proof

Let S denote all pairs (A, θ), where A is a subfield of M containing $\phi(K)$ and θ is an embedding of A into L such that $\theta \circ \phi = i$. Clearly $S \neq \emptyset$, since $A = \phi(K)$ is a component of an element of S.

We shall use the partial order on S given by $(A_1, \theta_1) \leq (A_2, \theta_2)$ if A_1 is a subfield of A_2 and $\theta_2|_{A_1} = \theta_1$.

If $\mathcal{C}$ is a chain in S, let $B = \bigcup\{A \mid (A, \theta) \in \mathcal{C}\}$. Then B is a subfield of M. Moreover, we can define a function ψ from B to L as follows. If $\alpha \in B$, then $\alpha \in A$ for some $(A, \theta) \in \mathcal{C}$, and so we let $\psi(\alpha) = \theta(\alpha)$. This is clearly well-defined, and gives an embedding of B into L. Thus (B, ψ) is an upper bound for $\mathcal{C}$.

Therefore Zorn's Lemma implies that S has a maximal element (A, θ).

It is now required to prove that $A = M$. Given an element $\alpha \in M$, α is algebraic over A so let f be its minimal polynomial over A. Then $\theta(f)$ splits over L (since L is algebraically closed), say

$$\theta(f) = (X - \beta_1) \cdots (X - \beta_r).$$

Since $\theta(f)(\beta_1) = 0$, there exists an embedding $A(\alpha) \cong A[X]/(f) \hookrightarrow L$ extending θ and sending α to β_1 (c.f. proof of (2.3)). But then the maximality of (A, θ) implies that $\alpha \in A$ and hence $M = A$. $\square$

Corollary 3.4 (Uniqueness of algebraic closures)

If $i_1 : K \hookrightarrow L_1$, $i_2 : K \hookrightarrow L_2$ are two algebraic closures of K, then there exists an isomorphism $\theta : L_1 \to L_2$ such that the following diagram

$$\begin{tikzcd} & L_1 \arrow[dr, "\theta"] & \\ K \arrow[ur, "i_1"] \arrow[rr, "i_2"'] & & L_2 \end{tikzcd}$$

commutes.

Proof

By (3.3), there exists an embedding $\theta : L_1 \hookrightarrow L_2$ such that $i_2 = \theta \circ i_1$. Since L_2/K is algebraic, so too is L_2/L_1, but then since L_1 is algebraically closed, $L_2 \cong L_1$. $\square$

Remark

For general K the construction and uniqueness of the algebraic closure $\bar{K}$ has involved Zorn's Lemma, so it is preferable to avoid the use of $\bar{K}$ wherever possible (which for finite extensions we can).

Note, however, that we can construct $\mathbb{C}$ by 'bare hands', without the use of the Axiom of Choice, so our objection is not valid for $K = \mathbb{Q}$, any number field, or $\mathbb{R}$.

4 Normal Extensions and Galois Extensions

4.1 Normal extensions

Definition

An extension L/K is *normal* if every irreducible polynomial $f \in K[X]$ having a root in L splits completely over L.

Example

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since $X^3 - 2$ doesn't split completely over any real field.

Theorem 4.1

An extension L/K is normal and finite iff L is a splitting field for some polynomial $f \in K[X]$.

Proof

($\Rightarrow$) Suppose L/K is normal and finite. Then $L = K(\alpha_1, \ldots, \alpha_r)$, with α_i having minimal polynomial $f_i \in K[X]$, say.

Let $f = f_1 \cdots f_r$. We claim that L is the splitting field for f over K. For each f_i is irrreducible with a zero α_i in L and so each f_i, and hence f, splits completely over L, by the normality of L. Since L is generated by K and the zeros of f it is a splitting field for f over K.

($\Leftarrow$) Suppose L is the splitting field of some $g \in K[X]$. The extension is obviously finite.

To prove normality, it is required to prove that given an irreducible polynomial $f \in K[X]$ with a zero in L, f splits completely over L.

Suppose M/L is a splitting field extension for a polynomial f (thought of as an element of $L[X]$) and that α_1 and α_2 are zeros of f in M. Then we claim that $[L(\alpha_1) : L] = [L(\alpha_2) : L]$.

This yields the required result, since we may choose $\alpha_1 \in L$ by assumption and so for any root α_2 of f in M we have $[L(\alpha_2) : L] = 1$, i.e. $\alpha_2 \in L$, and so f splits completely over L.

To prove the claim, consider the following diagram of field extensions:

$$\begin{tikzcd}
 & M \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
L(\alpha_1) \arrow[dr, dash] \arrow[dd, dash] & & L(\alpha_2) \arrow[dl, dash] \arrow[dd, dash] \\
 & L \arrow[dd, dash] & \\
K(\alpha_1) \arrow[dr, dash] & & K(\alpha_2) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Observe the following:

1. Since f is irreducible, (1.4) implies that $K(\alpha_1) \cong K(\alpha_2)$ over K, and in particular $[K(\alpha_1) : K] = [K(\alpha_2) : K]$.
2. For $i = 1, 2$, $L(\alpha_i)$ is a splitting field for g over $K(\alpha_i)$, and so by (1.7)

$$\begin{tikzcd} L(\alpha_1) \arrow[r, "\cong"] & L(\alpha_2) \\ K(\alpha_1) \arrow[u] \arrow[r, "\cong"] & K(\alpha_2) \arrow[u] \end{tikzcd}$$

   In particular we deduce that $[L(\alpha_1) : K(\alpha_1)] = [L(\alpha_2) : K(\alpha_2)]$.

Now the Tower Law gives the result. $\square$

4.2 Normal closures

Definition

We know that any finite extension L/K is finitely generated, $L = K(\alpha_1, \ldots, \alpha_r)$ say. Let $f_i \in K[X]$ be the minimal polynomial for α_i.

Now let M/L be the splitting field for $f = f_1 \cdots f_r$. By (4.1) M/L is normal. We define M/K to be the *normal closure* of L/K.

Remark

Any normal extension N/L must split each of the f_i, and so for some $M' \subseteq N$, M'/L is a splitting field for f and so is isomorphic over L to M/L (by (1.7)).

Thus the normal closure of L/K is characterized as the minimal extension M/L such that M/K is normal, and it is unique up to isomorphism over L.

Definition

Let L/K and L'/K be field extensions. A *K-embedding* of L into L' is an embedding which fixes K.

In the case where $L = L'$ and L/K is finite, then the embedding is also surjective and so is an automorphism. In this case we call the K-embedding a *K-automorphism*. We denote the group of K-automorphisms of L/K by $\mathrm{Aut}(L/K)$.

Theorem 4.2

Let L/K be a finite extension, and let $\theta : L \hookrightarrow M$ with M/L normal. Let $L' = \theta(L) \subseteq M$. Then

1. *The number of distinct K-embeddings $L \hookrightarrow M$ is at most $[L : K]$, with equality iff L/K is separable.*
2. *L/K is normal iff every K-embedding $\phi : L \hookrightarrow M$ has image L' iff every K-embedding $\phi : L \hookrightarrow M$ is of the form $\phi = \theta \circ \alpha$ for some $\alpha \in \mathrm{Aut}(L/K)$.*

Proof

1. This follows directly from (2.4).
2. First observe that
   (a) L/K is normal iff L'/K is normal.
   (b) Any K-embedding $\phi : L \hookrightarrow M$ gives rise to a K-embedding $\psi : L' \hookrightarrow M$, where $\psi = \phi \circ \theta^{-1}$, and vice versa.
   (c) Any K-embedding $\phi : L \hookrightarrow M$ with image L' gives rise to an automorphism α of L/K such that $\phi = \theta \circ \alpha$. Conversely, any ϕ of this form is a K-embedding with image L'.

   Hence we are required to prove that L'/K is normal iff any K-embedding $\psi : L' \hookrightarrow M$ has image L'.

   ($\Rightarrow$) Suppose $\alpha \in L'$ with minimal polynomial $f \in K[X]$. If L'/K normal then f splits completely over L'. Now if $\psi : L' \hookrightarrow M$ is a K-embedding then $\psi(\alpha)$ is another root of f, and hence $\psi(\alpha) \in L'$. Thus $\psi(L') \subseteq L'$, but since L'/K is finite, $\psi(L') = L'$.

   ($\Leftarrow$) Suppose $f \in K[X]$ is an irreducible polynomial with a zero $\alpha \in L'$. By assumption, M contains a normal closure M' of L/K and so f splits completely over M'. Also, since L'/K is finite, $L' \subseteq M'$.

   Let $\beta \in M'$ be any other root of f. Then there exists an isomorphism over K, $K(\alpha) \cong K[X]/(f) \cong K(\beta)$. Since M' is a splitting field for some polynomial F over K, it is also a splitting field for F over $K(\alpha)$ or $K(\beta)$. So (1.7) implies that the isomorphism $K(\alpha) \cong K(\beta)$ extends to an isomorphism $K(\alpha) \subseteq M' \to M' \supseteq K(\beta)$ with $K(\alpha) \to K(\beta)$, which in turn restricts to a K-embedding $L' \hookrightarrow M$, sending α to β. Therefore, $\beta \in L'$.

   Since this is true for all roots of β, f splits completely over L', that is, L'/K is normal. □

Corollary 4.3

If L/K is finite then $|\operatorname{Aut}(L/K)| \leq [L : K]$ with equality iff L/K is normal and separable.

Proof

Let M/L be a normal extension. Then by (4.2),

$$\begin{aligned}
|\operatorname{Aut}(L/K)| &= |\{K\text{-embeddings } L \hookrightarrow M \text{ of the form } \theta \circ \alpha,\ \alpha \in \operatorname{Aut}(L/K)\}| \\
&\leq |\{K\text{-embeddings } L \hookrightarrow M\}| \\
&\leq [L : K],
\end{aligned}$$

with equality iff L/K is normal and separable. □

4.3 Fixed fields and Galois extensions

From now on, we'll only deal with field extensions L/K where $K \subseteq L$ — we don't lose any generality from doing this as for any extension L/K we can always identify K with its image in L.

Definition

If L is a field and G is any finite group of automorphisms of L then we write $L^G \subseteq L$ for the *fixed field*

$$L^G = \{x \in L \mid g(x) = x \text{ for all } g \in G\}.$$

It is easy to check that this is a subfield.

Definition

We say that a finite extension L/K is *Galois* if $K = L^G$ for some finite group of automorphisms G. If this is the case then it is clear that $G \leq \mathrm{Aut}(L/K)$. In fact we shall show that $G = \mathrm{Aut}(L/K)$.

Proposition 4.4

Let G be a finite group of automorphisms acting on a field L, with $K = L^G \subseteq L$. Then

1. *For every $\alpha \in L$ we have $[K(\alpha) : K] \leq |G|$.*
2. *L/K is separable.*
3. *L/K is finite with $[L : K] \leq |G|$.*

Proof

1, 2. Suppose $\alpha \in L$. We claim that its minimal polynomial f over K is separable of degree at most $|G|$.

For consider the set $\{\sigma(\alpha) \mid \sigma \in G\}$ and suppose its distinct elements are $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$. Let $g = \prod(X - \alpha_i)$. Then g is invariant under G, since its linear factors are just permuted by elements of G, and so $g \in K[X]$.

Since $g(\alpha) = 0$ we have $f \mid g$ and then f is clearly separable, with $\deg f \leq \deg g \leq |G|$.

3. By (1), we can find $\alpha \in L$ such that $[K(\alpha) : K]$ is maximal. We shall show that $L = K(\alpha)$, from which it follows that $[L : K] \leq |G|$, as claimed.

Let $\beta \in L$. It is required to prove that $\beta \in K(\alpha)$. By (1), β is algebraic over K and satisfies a polynomial of degree at most $|G|$ over K. Hence, by the Tower Law, $[K(\alpha, \beta) : K]$ is finite. However, (2) implies that $K(\alpha, \beta)/K$ is separable.

Now apply the Primitive Element Theorem and we get that there exists $\gamma \in L$ such that $K(\alpha, \beta) = K(\gamma)$. Now $[K(\gamma) : K] = [K(\gamma) : K(\alpha)][K(\alpha) : K]$. Hence $[K(\gamma) : K(\alpha)] = 1$, since $[K(\alpha) : K]$ is maximal, and so $\beta \in K(\alpha)$. $\square$

Theorem 4.5

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

1. *L/K is Galois,*
2. *K is the fixed field of $\mathrm{Aut}(L/K)$,*
3. *$|\mathrm{Aut}(L/K)| = [L : K]$,*
4. *L/K is normal and separable.*

Proof

$3 \Leftrightarrow 4$. This is just (4.3).

$2 \Rightarrow 1$. This is clear, since $\mathrm{Aut}(L/K)$ is finite by (4.3).

$1 \Rightarrow 2, 3$. Suppose now that $K = L^G$ for some finite group G. Then $[L : K] \leq |G|$, by (4.4). But $G \leq \mathrm{Aut}(L/K)$ and so $|G| \leq |\mathrm{Aut}(L/K)| \leq [L : K]$ by (4.3). Thus $|G| = [L : K]$ and $G = \mathrm{Aut}(L/K)$. Hence K is the fixed field of $\mathrm{Aut}(L/K)$ and $|\mathrm{Aut}(L/K)| = [L : K]$, as required.

$3 \Rightarrow 1$. Let $G = \mathrm{Aut}(L/K)$ be finite, and set $F = L^G$. Clearly $F \supseteq K$. Then L/F is Galois and so the previous argument shows that $|G| = [L : F]$. But by assumption $|G| = [L : K]$, and hence the Tower Law implies that $F = K$. □

Notation

If $K \subseteq L$ is Galois, we usually write $\mathrm{Gal}(L/K)$ for $\mathrm{Aut}(L/K)$, the *Galois group* of the extension.

4.4 The Galois correspondence

Let L/K be a finite extension of fields. The group $G = \mathrm{Aut}(L/K)$ has $|G| \leq [L : K]$ by (4.3). Let $F = L^G \supseteq K$. Then (4.5) implies that $|G| = [L : F]$.

1. If now H is a subgroup of G, then the fixed field $M = L^H$ is an intermediate field $F \subseteq M \subseteq L$ with L/M Galois, and then (4.5) implies that $\mathrm{Aut}(L/M) = H$.

2. For any intermediate field $F \subseteq M \subseteq L$, let $H = \mathrm{Aut}(L/M)$, a subgroup of G.

   Claim

   L/M is a Galois extension and $M = L^H$.

   Proof

   Since L/F is Galois, (4.5) implies that it is normal and separable. Since L/F is normal, so too is L/M (as by (4.1), L is the splitting field of some polynomial $f \in F[X]$, and so L is the splitting field of f over M). Since L/F is separable, so too is L/M (by (2.2)). Therefore L/M is Galois and $M = L^H$.

Conclusion

The operations

$$\begin{aligned} H \leq G &\longmapsto F \subseteq L^H \subseteq L \\ \mathrm{Aut}(L/M) \leq G &\longleftarrow F \subseteq M \subseteq L \end{aligned}$$

are mutually inverse.

Theorem 4.6 (Fundamental Theorem of Galois Theory)

With the notation as above,

1. *There exists an order-reversing bijection between subgroups H of G and the intermediate fields $F \subseteq M \subseteq L$, where H corresponds to its fixed field L^H and M corresponds to $\mathrm{Aut}(L/M)$.*
2. *A subgroup H of G is normal iff L^H/F is normal iff L^H/F is Galois.*
3. *If $H \lhd G$, then the map $\sigma \in G \mapsto \sigma|_{L^H}$ determines a group homomorphism of G onto $\mathrm{Gal}(L^H/F)$ with kernel H, and hence $\mathrm{Gal}(L^H/F) \cong G/H$.*

Proof

1. Already done.
2. If $M = L^H$, observe that the fixed field of a conjugate subgroup $\sigma H \sigma^{-1}$ ($\sigma \in G$) is just σM. From the bijection proved in (1), we deduce that $H \lhd G$ (i.e. $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$) iff $\sigma M = M$ for all $\sigma \in G$.

   Now observe that L is normal over F — in particular L is a splitting field for some polynomial $f \in F[X]$ — and so L contains a normal closure N of M/F. Any $\sigma \in G$ determines an F-embedding $M \hookrightarrow N$, and conversely any F-embedding $M \hookrightarrow N$ extends by (1.7) to an F-automorphism σ of the splitting field L of f. Thus (4.2) says that M/F is normal iff $\sigma M = M$ for all $\sigma \in G$.

   Finally, M/F is always separable (L/F is Galois and so use (2.2)) and so M/F is normal iff M/F is Galois.
3. Let $M = L^H$ and $H \lhd G$. Then we have $\sigma(M) = M$ for all $\sigma \in G$ and so $\sigma|_M$ is an F-automorphism of M. So there exists a group homomorphism $\theta : G \to \mathrm{Gal}(M/F)$ with $\ker\theta = \mathrm{Gal}(L/M)$. But $\mathrm{Gal}(L/M) = H$ by (4.5), and so $\theta(G) \cong G/H$. Thus $|\theta(G)| = |G : H| = |G|/|H| = [L : F]/[L : M] = [M : F]$.

   But $|\,\mathrm{Gal}(M/F)| = [M : F]$ by (4.5), since M/F is Galois, and so θ is surjective and induces an isomorphism $G/H \cong \mathrm{Gal}(M/F)$. $\square$

4.5 Galois groups of polynomials

Definition

Let $f \in K[X]$ be a separable polynomial and let L/K be a splitting field for f. We define the *Galois group* of f to be $\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$.

Suppose now f has distinct roots in L, say $\alpha_1, \ldots, \alpha_d$, and so $L = K(\alpha_1, \ldots, \alpha_d)$. Since a K-automorphism of L is determined by its action on the roots α_i, we have an injective homomorphism $\theta : G \hookrightarrow S_d$. Properties of f will be reflected in the properties of G.

Lemma 4.7

> *With the assumptions as above, $f \in K[X]$ is irreducible iff G acts transitively on the roots of f, that is, if $\theta(G)$ is a transitive subgroup of S_d.*

Proof

($\Leftarrow$) If f is reducible, say $f = gh$ with $g, h \in K[X]$ and $\deg g, h > 0$, let α_1 be a root of g, say. Then for any $\sigma \in G$, $\sigma(\alpha_1)$ is also a root of g. Hence G only permutes roots within the irreducible factors and so its action is not transitive.

($\Rightarrow$) If f is irreducible, then for any i, j there exists a K-automorphism $K(\alpha_i) \to K(\alpha_j)$. This isomorphism extends by (1.7) to give a K-automorphism σ of L (which is the splitting field of f) with the property that $\sigma(\alpha_i) = \alpha_j$. Therefore G is transitive on the roots of f. $\square$

So for low degree, the Galois groups of polynomials are very restrictive:

- $\deg f = 2$: if f is reducible then $G = 1$; otherwise $G = C_2$.
- $\deg f = 3$: if f is reducible then $G = 1$ or C_2; otherwise $G = S_3$ or C_3.

Definition

Let $f \in K[X]$ be a polynomial with distinct roots $\alpha_1, \ldots, \alpha_d$ in a splitting field L; for example, f may be irreducible and separable. Set $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Then the *discriminant* D of f is

$$D = \Delta^2 = (-1)^{d(d-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

D is fixed by all the elements of $G = \mathrm{Gal}(L/K)$ and hence is an element of K.

Remark

Suppose $\operatorname{char} K \neq 2$, and $f \in K[X]$ is irreducible and separable of degree d. Then $\Delta \neq 0$, and $\theta(G) \subseteq A_d$ iff Δ is fixed under G (since for any odd permutation σ, $\sigma(\Delta) = -\Delta$) iff D is a square in K.

Examples

1. Let $\operatorname{char} K \neq 2$ and let $f = X^2 + bX + c \in K[X]$. Then $\alpha_1 + \alpha_2 = -b$ and $\alpha_1\alpha_2 = c$, and so $D = (\alpha_1 - \alpha_2)^2 = b^2 - 4c$. So the quadratic splits iff $b^2 - 4c$ is a square (which we knew already).

2. Let $\operatorname{char} K \neq 2, 3$ and let $f = X^3 + bX^2 + cX + d \in K[X]$ be irreducible and separable. Let G be the Galois group of f. Then $G = A_3 (= C_3)$ iff $D(f)$ is a square, and $G = S_3$ otherwise.

   To calculate $D(f)$, set $g = f(X - b/3)$ — this is of the form $X^3 + pX + q$. Since α is a root of f iff $\alpha + b/3$ is a root of g, we deduce that $\Delta(f) = \Delta(g)$ and so $D(f) = D(g)$.

Lemma 4.8

Let $f \in K[X]$ be an irreducible, separable polynomial, and let M/K be a splitting field for f. Let $\alpha \in M$ be a root of f and let $L = K(\alpha) \subseteq M$. Then

$$D(f) = (-1)^{d(d-1)/2} N_{K/k}(f'(\alpha)).$$

Proof

Let $\sigma_1, \ldots, \sigma_d$ be the distinct K-embeddings of L into M. Then

$$\begin{aligned}
\prod_{i \neq j}(\alpha_i - \alpha_j) &= \prod_i \prod_{j \neq i}(\alpha_i - \alpha_j) \\
&= \prod_i f'(\alpha_i) \qquad\qquad (\text{since } f = \textstyle\prod(X - \alpha_j)) \\
&= \prod_i \sigma_i(f'(\alpha)) \\
&= N_{L/K}(f'(\alpha))
\end{aligned}$$

(see Examples Sheet 1, Question 14). □

Example

For the cubic $g = X^3 + pX + q$, as in the example above, set $y = g'(\alpha)$. Then $y = 3\alpha^2 + p = -2p - 3q\alpha^{-1}$ and so $\alpha = -3q(y + 2p)^{-1}$. Therefore the minimal polynomial of y is

$$(y + 2p)^3 - 3p(y + 2p)^2 - 27q^2,$$

whose constant term is

$$-4p^3 - 27q^2 = -N_{L/K}(y) = D(g).$$

Remark

When $K = \mathbb{Q}$, we can consider the spliting field of f an a subfield of $\mathbb{C}$. This may be useful.

For example, if $f \in \mathbb{Q}[X]$ is irreducible of degree d with precisely two complex roots, the Galois group contains a transposition (complex conjugation is an element of $\mathrm{Gal}(f)$ switching the two complex roots).

Elementary group theory shows that if $G \subseteq S_p$ (p prime) is transitive and contains a transposition, then it contains all transpositions and hence $G = S_p$.

So if f is irreducible of degree p with exactly two complex roots, then $\mathrm{Gal}(f) = S_p$.

The following proposition (whose proof is left as an exercise) may be helpful when calculating the Galois group of a polynomial.

Proposition 4.9

The transitive subgroups of S_4 are S_4, A_4, D_8, C_4, and V_4. The transitive subgroups of S_5 are S_5, A_5, G_{20}, D_{10} and C_5, where G_{20} is generated by a 5-cycle and a 4-cycle.

5 Galois Theory of Finite Fields

5.1 Finite fields

Recall

If F is a field with $|F| = q$, then $q = p^r$ for some r, where $p = \operatorname{char} F$.

Definition

Given such a finite field, there exists an $\mathbb{F}_p$-automorphism $\phi : F \to F$ given by $\phi(x) = x^p$ for all $x \in F$, called the *Fröbenius automorphism.*

Remarks

1. ϕ is an homomorphism since $1^p = p$, $(xy)^p = x^p y^p$ and $(x+y)^p = x^p + y^p$. It has kernel $\{0\}$ and so is injective, but then since F is finite it is surjective, and hence an automorphism. Also, for $x \in \mathbb{F}_p$ we have $x^p \equiv x \pmod{p}$, and so ϕ is a $\mathbb{F}_p$-automorphism.

2. Since $|F^*| = q - 1$ we have $a^{q-1} = 1$ and hence $a^q = a$ for all $a \in F$. That is, every element of F is a root of the polynomial $X^q - X$. But since $X^q - X$ is of degree q it has at most q roots, and so these are all the roots. Therefore F is the splitting field of $X^q - X$ over $\mathbb{F}_p$, and as such is unique.

3. If $q = p^r$, then there *does* exist a field of order q. For let F be the splitting field of $X^q - X$ over $\mathbb{F}_p$. Clearly F is finite, so let $\phi : F \to F$ be the Fröbenius automorphism. Let $F' \subseteq F$ be the fixed field of $\langle \phi^r \rangle$. But $x \in F'$ iff $\phi^r(x) = x$ iff x is a root of $X^q - X$. So F' contains all the roots of $X^q - X$ and so $X^q - X$ splits in F', and therefore $F = F'$. Thus F consists entirely of roots of $X^q - X$. These roots are distinct (since the derivative of $X^q - X$ is -1 and so it has no roots), and so $|F| = q$ as desired.

Notation

We denote the unique field of order $q = p^r$ by $\mathbb{F}_q$ or $\mathrm{GF}(q)$.

5.2 Galois groups of finite extensions of finite fields

Remarks

The subfields of $\mathbb{F}_{p^r}$ are just $\mathbb{F}_{p^s}$ for $s \mid r$, where for each such s there is a unique subfield of order p^s, being the fixed field of $\langle \phi^s \rangle$.

Now $\phi^r = \mathrm{id}$, but $\phi^i \neq \mathrm{id}$ for any $i < r$, since $X^{p^i} - X$ has only p^i roots. Hence ϕ generates a cyclic group $G = \langle \phi \rangle$ of order r of automorphisms of $\mathbb{F}_{p^r}$.

Since the subgroups of $G = \langle \phi \rangle$ are just those of the form $\langle \phi^s \rangle$ for $s \mid r$, we have the following:

1. Any finite extension of finite fields is of the form $L/K = \mathbb{F}_{p^r}/\mathbb{F}_{p^s}$, where $s \mid r$.
2. L/K is Galois with $\mathrm{Gal}(L/K)$ cyclic of order $[L : K] = r/s$, generated by ϕ^s.

3. For each t with $s \mid t$ and $t \mid r$ there exists an intermediate field $M = \mathbb{F}_{p^t}$ and a normal subgroup $H = \langle \phi^t \rangle$ such that $M = L^H$ and $H = \mathrm{Gal}(L/M)$. Further, these are the only intermediate fields of L/K and subgroups of G.

Thus we have verified the Fundamental Theorem of Galois Theory for finite fields.

Remarks

1. Let K is a finite field, with $f \in K[X]$ an irreducible polynimial of degree d. Then any finite extension L/K is normal, and so if L contains one root of f then it contains all the roots of f. Therefore, the splitting field L of f is of the form $K(\alpha)$, where f is the minimal polynomial for α.

   Moreover, $\mathrm{Gal}(f) = \mathrm{Gal}(K(\alpha)/K)$ is cyclic of degree d, and the generator of $\mathrm{Gal}(f)$ acts cyclically on the d roots of f.

2. If $K = \mathbb{F}_{p^s}$, then $L = \mathbb{F}_{p^{sd}}$ is unique, so it doesn't depend on the irreducible polynomial of degree d. That is, if we've split one irreducible polynomial of degree d then we've split them all.

Consider the general situation of K a field,

$$f = X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \in K[X]$$

a polynomial with distinct roots $\alpha_1, \ldots, \alpha_n$ in a splitting field L, and $G = \mathrm{Gal}(f) = \mathrm{Gal}(L/K)$ regarded as a subset of S_n. Let $Y_1, \ldots, Y_n$ be independent indeterminates, and for $\sigma \in S_n$, let

$$H_\sigma = \big(X - (\alpha_{\sigma(1)}Y_1 + \cdots + \alpha_{\sigma(n)}Y_n)\big) \in L[Y_1, \ldots, Y_n][X].$$

We can define an action of σ on $H = X - (\alpha_1 Y_1 + \cdots + \alpha_n Y_n)$ by $\sigma H = H_{\sigma^{-1}}$. Set

$$\begin{aligned} F &= \prod_{\sigma \in S_n} \sigma H \\ &= \prod_{\sigma \in S_n} \big(X - (\alpha_1 Y_{\sigma(1)} + \cdots + \alpha_n Y_{\sigma(n)})\big) \\ &= \sum_{j=0}^{n!} \left(\sum_{i_1 + \cdots + i_n = n! - j} a_{i_1,\ldots,i_n} Y_1^{i_1} \cdots Y_n^{i_n} \right) X^j. \end{aligned}$$

Since S_n preserves F, it preserves the coefficients $a_{i_1,\ldots,i_n}$. The coefficients are in fact certain symmetric polynomials in the α_i (which could be given explicitly, independent of f) and hence are polynomials in the coefficients $c_0, \ldots, c_{n-1}$ (which could again can be given explicitly, independent of f) (c.f. the Symmetric Function Theorem). Hence $F \in K[Y_1, \ldots, Y_n][X]$.

Now factor $F = F_1 \cdots F_N$ into irreducibles in $K[Y_1, \ldots, Y_n][X]$, with each F_i irreducible in $K(Y_1, \ldots, Y_n)[X]$, by Gauss's Lemma.

Remark

In the case $K = \mathbb{Q}$ and $c_i \in \mathbb{Z}$, all the polynomials in the $c_0, \ldots, c_{n-1}$ have coefficients in $\mathbb{Z}$, and so $F \in \mathbb{Z}[Y_1, \ldots, Y_n][X]$ and we can take the factorization $F = F_1 \cdots F_N$ with $F_i \in \mathbb{Z}[Y_1, \ldots, Y_n][X]$ (by Gauss's Lemma).

Now choose one of the factors $H = H_\sigma$ of F_1. By reordering the F_i (or the roots $\alpha_1, \dots, \alpha_n$) we may assume without loss of generality that $H = (X - (\alpha_1 Y_1 + \cdots + \alpha_n Y_n))$.

Recall that the images σH are all distinct. Now consider $\prod_{g \in G} gH$, with g^{-1} acting on the coefficients of H. This has degree $|G|$ and is in $K[Y_1, \dots, Y_n][X]$, since it is invariant under the action of G.

Since H divides F_1 in $L[Y_1, \dots, Y_n][X]$, gH divides F_1 in $L[Y_1, \dots, Y_n][X]$ and so $\prod gH$ divides F_1 in $K[Y_1, \dots, Y_n][X]$. But F_1 is irreducible in $K[Y_1, \dots, Y_n][X]$, and hence $\prod gH = F_1$.

So $\deg F_1 = |G|$ and there are $N = n!/|G|$ irreducible factors F_i, permuted transitively by the action of S_n. Therefore, the orbit-stabilizer theorem implies that

$$\frac{n!}{|\operatorname{Stab}(F_1)|} = \frac{n!}{|G|},$$

so $|G| = |\operatorname{Stab}(F_1)|$. Since G fixes F_1, $G \le \operatorname{Stab}(F_1)$ and hence $G = \operatorname{Stab}(F_1)$, i.e. $\operatorname{Gal}(f)$ is isomorphic to the subgroup of S_n (acting on $Y_1, \dots, Y_n$) which fixes F_1.

Theorem 5.1

Suppose $f \in \mathbb{Z}[X]$ is a monic polynomial of degree n with distinct roots in a splitting field. Suppose p is a prime such that the reduction $\bar{f}$ of f modulo p also has distinct roots in a splitting field. If $\bar{f} = g_1 \cdots g_r$ is the the factorization of $\bar{f}$ in $\mathbb{F}_p[X]$, say $\deg g_i = n_i$, then $\operatorname{Gal}(f) \le S_n$ has an element of cyclic type $(n_1, \dots, n_r)$.

Proof

This will follow if we can show $\operatorname{Gal}(\bar{f}) \le \operatorname{Gal}(f) \le S_n$, since the action of Fröbenius ϕ on the roots of $\bar{f}$ clearly has the cyclic type claimed.

We now run the above programme twice: first over $K = \mathbb{Q}$, identifying $\operatorname{Gal}(f)$ as the subgroup of S_n fixing $F_1 \in \mathbb{Z}[Y_1, \dots, Y_n][X]$, and then with $\bar{f}$ over $K = \mathbb{F}_p$. The resulting polynomial we obtain,

$$\tilde{F} \in \mathbb{F}_p[Y_1, \dots, Y_n][X],$$

is just the reduction mod p of F, i.e. $\tilde{F} = \bar{F}$. But $\bar{F} = \bar{F}_1 \cdots \bar{F}_N$ in $\mathbb{F}_p[Y_1, \dots, Y_n][X]$, and we can factor $\bar{F}_1 = h_1 \cdots h_m$, with h_i irreducible.

With appropriate choice of the order of the roots $\beta_1, \dots, \beta_n$ of $\bar{f}$ in a splitting field, we may identify $\operatorname{Gal}(\bar{f})$ as the subgroup of S_n (acting on $Y_1, \dots, Y_n$) fixing h_1, say. Since, however, the linear factors of $\bar{F}$ are *distinct*, the subgroup of S_n fixing $\bar{F}_1$ is the same as the subgroup fixing F_1, and $\operatorname{Stab}(h_1)$ is a subgroup of $\operatorname{Stab}(\bar{F}_1) = \operatorname{Stab}(F_1)$. Thus $\operatorname{Gal}(\bar{f}) \le \operatorname{Gal}(f) \le S_n$ as claimed. $\square$

6 Cyclotomic Extensions

Suppose char $K = 0$ or p, where $p \nmid m$. The *mth cyclotomic extension* of K is just the splitting field L over K of $X^m - 1$.

Since mX^{m-1} and $X^m - 1$ have no common roots, the roots of $X^m - 1$ are distinct, the mth roots of unity. They form a finite subgroup μ_m of K^*, and hence by (2.6) a cyclic group $\langle \xi \rangle$. Thus $L = K(\xi)$ is simple.

An element $\xi' \in \mu_m$ is called a *primitive* mth root of unity if $\mu_m = \langle \xi' \rangle$. Choosing a primitive mth root of unity determines an isomorphism of cyclic groups

$$\begin{aligned} \mu_m &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ \xi^i &\longmapsto i. \end{aligned}$$

Recall that ξ^i is a generator of μ_m iff $(m, i) = 1$, and so the primitive roots correspond to elements of $U(m) = (\mathbb{Z}/m\mathbb{Z})^*$, the multiplicative group of units in the ring $\mathbb{Z}/m\mathbb{Z}$.

Since $X^m - 1$ is separable, L/K is Galois with Galois group G. An element $\sigma \in G$ sends the primitive mth root of untiy ξ to another primitive mth root ξ^i, with $(i, m) = 1$ (and knowing i determines σ).

Having chosen a primitive mth root of unity, we can define an injective map

$$\begin{aligned} \theta : G &\longrightarrow U(m) \\ \sigma &\longmapsto i, \end{aligned}$$

where $\sigma(\xi) = \xi^i$. If, however, $\theta(\sigma) = i$ and $\theta(\tau) = j$, then $(\sigma\tau)(\xi) = \sigma(\xi^i) = \xi^{ij}$, and so $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$. Hence θ is a homomorphism. Via this homomorphism, the Galois group may be considered as a subgroup of $U(m)$. θ is an isomorphism iff G acts transitively on the primitive mth roots of unity.

Definition

The *mth cyclotomic polynomial* is

$$\Phi_m = \prod_{i \in U(m)} (X - \xi^i).$$

Remark

Observe that

$$X^m - 1 = \prod_{i \in \mathbb{Z}/m\mathbb{Z}} (X - \xi^i) = \prod_{d \mid m} \Phi_d.$$

For example, when $K = \mathbb{Q}$, $\Phi_1 = X - 1$, $\Phi_2 = X + 1$, $\Phi_4 = X^2 + 1$, and

$$\begin{aligned} X^8 - 1 &= (X^4 - 1)(X^4 + 1) \\ &= (X^2 - 1)(X^2 + 1)(X^4 + 1) \\ &= (X - 1)(X + 1)(X^2 + 1)(X^4 + 1) \\ &= \Phi_1 \Phi_2 \Phi_4 (X^4 + 1), \end{aligned}$$

and so $\Phi_8 = X^4 + 1$.

Lemma 6.1

Φ_m is defined over the prime subfield of K (that is, over $\mathbb{Q}$ or $\mathbb{F}_p$). When $\operatorname{char} k = 0$*, Φ_m is defined over $\mathbb{Z}$.*

Proof

The proof is by induction on m. The result is trivial if $m = 1$. If $m > 1$ then

$$X^m - 1 = \Phi_m \prod_{\substack{d|m \\ d \neq m}} \Phi_d = \Phi_m g,$$

where g is monic and by the induction hypothesis is defined over the prime subfield of K (and over $\mathbb{Z}$ if $\operatorname{char} k = 0$). By Gauss' Lemma, or by direct argument using the Remainder Theorem, Φ_m is also defined over the prime subfield (and over $\mathbb{Z}$ if $\operatorname{char} k = 0$). □

Proposition 6.2

The homomorphism θ (defined above) is an isomorphism iff Φ_m is irreducible in $K[X]$.

Proof

Clear, since Φ_m is irreducible iff (by (4.7)) G acts transitively on the roots of Φ_m.

Proposition 6.3

If L is the mth cyclotomic extension of $K = \mathbb{F}_q$, where $q = p^r$, and $p \nmid m$, then the Galois group G is isomorphic to the cyclic subgroup of $U(m)$ generated by q.

Proof

G is generated by the Fröbenius automorphism $x \mapsto x^q$, and so

$$G \cong \theta(G) = \langle q \rangle \leq U(m). \qquad \square$$

Thus if $U(m)$ is not cyclic and K is any finite field, then θ is not an isomorphism, and so Φ_m is reducible over K.

Now consider the case $K = \mathbb{Q}$ (and so $\Phi_m \in \mathbb{Z}[X]$). If we can show that Φ_m is irreducible over $\mathbb{Z}$, then Φ_m must be irreducible over $\mathbb{Q}$ (by Gauss's Lemma) and so $G \cong U(m)$.

Proposition 6.4

For all $m > 0$, Φ_m is irreducible in $\mathbb{Z}[X]$.

Proof

Suppose not, and write $\Phi_m = fg$, where $f, g \in \mathbb{Z}[X]$ and f an irreducible monic polynomial with $1 \leq \deg f < \phi(m) = \deg \Phi_m$. Let $K/\mathbb{Q}$ be the mth cyclotomic extension, and let ϵ be a root of f in K.

Claim

If $p \nmid m$ is prime, then ϵ^p is also a root of f.

Proof

Suppose not. Then ϵ^p is a primitive mth root of unity and hence ϵ^p is a root of g. Define $h \in \mathbb{Z}[X]$ by $h(X) = g(X^p)$. Then $h(\epsilon) = 0$. But then since f is the minimal polynomial for ϵ over $\mathbb{Q}$, $f \mid h$ in $\mathbb{Q}[X]$ and Gauss' Lemma implies that we can write $h = fl$ with $l \in \mathbb{Z}[X]$ (since f is monic).

Now reduce modulo p to get $\bar{h} = \overline{fl}$ in $\mathbb{F}_p[X]$. Now $\bar{h}(X) = \bar{g}(X^p) = (\bar{g}(X))^p$. If $\bar{q}$ is any irreducible factor of $\bar{f}$ in $\mathbb{F}_p[X]$ then $\bar{q} \mid \bar{g}^p$ and so $\bar{q} \mid \bar{g}$. But then $\bar{q}^2 \mid \bar{f}\bar{g} = \bar{\Phi}_m$ and so there exists a repeated root of $\bar{\Phi}_m$ and thus a repeated root for $X^m - 1$ — but this is a contradiction since $(p, m) = 1$. $\square$

In general, consider now roots ξ of f and γ of g. Then $\gamma = \xi^r$ for some r with $(r, m) = 1$. Write $r = p_1 \cdots p_k$ as a product of (not necessarily distinct) primes, with $p_i \nmid m$ for each i.

Repeated use of our claim implies that γ is a root of f and so Φ_m has a repeated root — a contradiction. Hence Φ_m is irreducible over $\mathbb{Q}$. $\square$

Remark

When $m = p$ is prime, there is a simpler proof of (6.4). For Φ_p is irreducible iff $g(X) = \Phi_p(X + 1)$ is irreducible. But

$$g(X) = \frac{(X+1)^p - 1}{(X+1) - 1} = X^{p-1} + pX^{p-2} + \binom{p}{2}X^{p-3} + \cdots + p,$$

and so the result follows by Eisenstein's Criterion.

7 Kummer Theory and Solving by Radicals

7.1 Introduction

When is a Galois extension L/K a splitting field for a polynomial of the form $X^n - \theta$?

Theorem 7.1

Suppose $X^n - \theta \in K[X]$ and $\operatorname{char} K \nmid n$. Then the splitting field L contains a primitive nth root of unity ω and the Galois group of $L/K(\omega)$ is cyclic of order dividing n. Moreover, $X^n - \theta$ is irreducible over $K(\omega)$ iff $[L : K(\omega)] = n$.

Proof

Since $X^n - \theta$ and nX^{n-1} are coprime, $X^n - \theta$ has distinct roots $\alpha_1, \dots, \alpha_n$ in its splitting field L. Moreover, L/K is Galois.

Since $(\alpha_i\alpha_j^{-1})^n = \theta\theta^{-1} = 1$, the elements $1 = \alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \dots, \alpha_n\alpha_1^{-1}$ are n distinct nth roots of unity in L and so $X^n - \theta = (X - \beta)(X - \omega\beta)\cdots(X - \omega^{n-1}\beta)$ in $L[X]$. Hence $L = K(\omega, \beta)$

If $\sigma \in \operatorname{Gal}(L/K(\omega))$, it is determined by its action on β. $\sigma(\beta)$ is another root of $X^n - \theta$, say $\sigma(\beta) = \omega^{j(\sigma)}\beta$, for some $0 \le j(\sigma) < n$. If $\sigma, \tau \in \operatorname{Gal}(L/K(\omega))$,

$$\tau\sigma(\beta) = \tau(\omega^{j(\sigma)}\beta) = \omega^{j(\sigma)}\tau(\beta) = \omega^{j(\sigma)+j(\tau)}\beta.$$

Therefore the map $\sigma \mapsto j(\sigma)$ induces a homomorphism $\operatorname{Gal}(L/K(\omega)) \to \mathbb{Z}/n\mathbb{Z}$. As $j(\sigma) = \beta$ iff σ is the identity, the homomorphism is injective. So $\operatorname{Gal}(L/K(\omega))$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$ and hence is cyclic of order dividing n.

Finally, observe that $[L : K(\omega)] \le n$, with equality iff $X^n - \theta$ is irreducible over $K(\omega)$, since $L = K(\omega)(\beta)$. $\square$

Example

X^6+3 is irreducible over $\mathbb{Q}$ (by Eisenstein) but not over $\mathbb{Q}(\omega)$ (where $\omega = \frac{1}{2}(1+\sqrt{-3})$) since the splitting field $L = \mathbb{Q}((-3)^{1/6}, \omega) = \mathbb{Q}((-3)^{1/6})$ has degree 3 over $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$. In fact, $X^6 + 3 = (X^3 + \sqrt{-3})(X^3 - \sqrt{-3})$ over $\mathbb{Q}(\omega)$.

We now consider the converse problem to (7.1); we shall need a result proved on Example Sheet 1, Question 13.

Proposition 7.2

Suppose that K and L are fields and $\sigma_1, \dots, \sigma_n$ are distinct embeddings of K into L. Then there do not exist $\lambda_1, \dots, \lambda_n \in L$ (not all zero) such that $\lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0$ for all $x \in K$.

Proof

If such a relation did exist, choose one with the least number $r > 0$ of non-zero λ_i. Hence wlog $\lambda_1, \dots, \lambda_r$ are all non-zero and $\lambda_1\sigma_1(x) + \cdots + \lambda_r\sigma_r(x) = 0$ for all $x \in K$. Clearly we have $r > 1$, since if $\lambda_1\sigma_1(x) = 0$ for all x then $\lambda_1 = 0$. We now produce a relation with fewer than r terms, and hence a contradiction.

Choose $y \in K$, such that $\sigma_1(y) \neq \sigma_r(y)$. The above relation implies that $\lambda_1\sigma_1(yx) + \cdots + \lambda_r\sigma_r(yx) = 0$ for all $x \in K$. Thus $\lambda_1\sigma_1(y)\sigma_1(x) + \cdots + \lambda_r\sigma_r(y)\sigma_r(x) = 0$, so multiply the original relation by $\sigma_r(y)$ and subtract, to get

$$\lambda_1\sigma_1(x)(\sigma_1(y) - \sigma_r(y)) + \cdots + \lambda_{r-1}\sigma_{r-1}(x)(\sigma_{r-1}(y) - \sigma_r(y)) = 0$$

for all $x \in K$, which gives the required contradiction.

Definition

An extension L/K is called *cyclic* if it is Galois and $\mathrm{Gal}(L/K)$ is cyclic.

Theorem 7.3

Suppose L/K is a cyclic extension of degree n, where $\mathrm{char}\, K \nmid n$*, and that K contains a primitive nth root of unity ω, Then there exists $\theta \in K$ such that $X^n - \theta$ is irreducible over K and L/K is a splitting field for $X^n - \theta$. If β' is a root of $X^n - \theta$ in a splitting field then $L = K(\beta')$.*

Definition

Such an extension is called a *radical* extension.

Proof

Let σ be a generator of the cyclic group $\mathrm{Gal}(L/K)$. Since $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are distinct automorphisms of L, (7.2) implies that there exists $\alpha \in L$ such that

$$\beta = \alpha + \omega\sigma(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha) \neq 0.$$

Observe that $\sigma(\beta) = \omega^{-1}\beta$; thus $\beta \notin K$ and $\sigma(\beta^n) = \sigma(\beta)^n = \beta^n$. So let $\theta = \beta^n \in K$.

As $X^n - \theta = (X - \beta)(X - \omega\beta)\cdots(X - \omega^{n-1}\beta)$ in L, $K(\beta)$ is a splitting field for $X^n - \theta$ over K. Since $1, \sigma, \ldots, \sigma^{n-1}$ are distinct K-automorphisms of $K(\beta)$, (4.3) implies that $[K(\beta) : K] \geq n$, and hence $L = K(\beta)$. Thus $L = K(\beta')$ for any root β' of $X^n - \theta$, since $\beta' = \omega^i\beta$ for some $0 \leq i \leq n - 1$.

The irreducibility of $X^n - \theta$ over K follows since it is the minimal polynomial for β, and $[L : K] = n$. □

Definition

A field extension L/K is an *extension by radicals* if there exists a tower

$$K = L_0 \subset L_1 \subset \cdots \subset L_n = L$$

such that each extension L_{i+1}/L_i is a radical extension. A polynomial $f \in K[X]$ is said to be *soluble by radicals* if its splitting field lies in an extension of K by radicals.

7.2 Cubics

Let $\operatorname{char} K \neq 2, 3$ and let $f \in K[X]$ be an irreducible cubic. Let L be the splitting field for f over K. Let ω be a primitive cube root of unity, and let $D = \Delta^2$ be the discriminant.

Set $M = L(\omega)$ — then M is Galois over $K(\omega)$. We have a diagram with degrees as shown:

$$\begin{tikzcd}
& M = L(\omega) \arrow[dl, dash, "3"'] \arrow[dr, dash, "1 \text{ or } 2"] & \\
K(\Delta, \omega) \arrow[dr, dash, "1 \text{ or } 2"'] & & L \arrow[dl, dash, "3"] \\
& K(\Delta) \arrow[d, dash, "1 \text{ or } 2"] & \\
& K &
\end{tikzcd}$$

Hence $\operatorname{Gal}(M/K(\Delta, \omega)) = C_3$. Therefore, (7.3) implies that $M = K(\Delta, \omega)(\beta)$, where β is a root of an irreducible polynomial $X^3 - \theta$ over $K(\Delta, \omega)$.

In fact, the proof of (7.3) implies that $\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of f. Since all the extensions $K \subseteq K(\Delta) \subseteq K(\Delta, \omega) \subseteq M$ are radical, any cubic can by solved by radicals.

Explicitly, reduce down to the case of cubics $g(X) = X^3 + pX + q$. Then $D = -4p^3 - 27q^2$. Set

$$\begin{aligned}
\beta &= \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3, \\
\gamma &= \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.
\end{aligned}$$

Then

$$\begin{aligned}
\beta\gamma &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\omega + \omega^2)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\
&= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) \\
&= -3p
\end{aligned}$$

and so $\beta^3\gamma^3 = -27p^3$, and

$$\begin{aligned}
\beta^3 + \gamma^3 &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3 + (\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3)^3 + (\alpha_1 + \alpha_2 + \alpha_3)^3 \\
&= 3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3 \\
&= -27q,
\end{aligned}$$

since $\alpha_i^3 = -p\alpha_i - q$ and so $(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) = -3q$. So β^3 and γ^3 are roots of the quadratic $X^2 + 27qX - 27p^3$, and so are

$$-\frac{27}{2}q \pm \frac{3\sqrt{-3}}{2}(-27q^2 - 4p^3)^{1/2} = -\frac{27}{2}q \pm \frac{3\sqrt{-3}}{2}\sqrt{D}.$$

We can solve for β^3 and γ^3 in $K(\sqrt{-3D}) \subseteq K(\omega, \sqrt{D})$. We obtain β by adjoining a cube root of β^3, and then $\gamma = -3p/\beta$.

Finally, we solve in M for $\alpha_1, \alpha_2, \alpha_3$ — namely

$$\alpha_1 = \frac{1}{3}(\beta + \gamma), \qquad \alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma), \qquad \alpha_3 = \frac{1}{3}(\omega\beta + \omega^2\gamma).$$

7.3 Quartics

Recall there exists an action of S_4 on the set $\{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$ of unordered pairs of unordered pairs. So we have a surjective homomorphism $S_4 \to S_3$ with kernel $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, and hence an isomorphism $S_4/V \cong S_3$.

Suppose now that f is an irreducible separable quartic over K. Then the Galois group G is a transitive subgroup of S_4, with normal subgroup $G \cap V$ such that $G/(G \cap V)$ is isomorphic to a subgroup of S_3.

Let M be the splitting field of f over K and let $L = M^{G\cap V}$. Since $V \subset A_4$, $L \supseteq M^{G\cap A_4} = K(\Delta)$, as observed before. Moreover, $\mathrm{Gal}(L/K(\Delta))$ is isomorphic to a subgroup of $A_4/V \cong C_3$, namely $G \cap A_4/G \cap V$ (FTGT).

Hence we have the tower of extensions:

$$
\begin{tikzcd}
M \arrow[d, dash] \\
L \arrow[d, dash, "1 \text{ or } 3"] \\
K(\Delta) \arrow[d, dash, "1 \text{ or } 2"] \\
K
\end{tikzcd}
$$

We claim that f can be solved by radicals.

For if we adjoin a primitive cube root of unity ω, then either f is reducible over $K(\omega)$, in which case we know already we can solve by radicals, or f is irreducible over $K(\omega)$. So, wlog, we may assume that K contains cube roots of unity.

Then $K(\Delta)/K$ is a radical extension. (7.3) implies that $L/K(\Delta)$ is a radical extension. So L/K is the composite of at most two radical extensions, and hence the claim follows.

We now see explicitly how this works. Assume that $\mathrm{char}\, K \neq 2, 3$. Wlog, we reduce to polynomials of the form

$$f = X^4 + pX^2 + qX + r.$$

Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ denote the roots of f in M (so $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$). Thus $M = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Set

$$\beta = \alpha_1 + \alpha_2, \qquad \gamma = \alpha_1 + \alpha_3, \qquad \delta = \alpha_1 + \alpha_4.$$

Then

$$
\begin{aligned}
\beta^2 &= (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\
\gamma^2 &= (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\
\delta^2 &= (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).
\end{aligned}
$$

Note that these are distinct — for example if $\beta^2 = \gamma^2$ then $\beta = \pm\gamma$ and so either $\alpha_2 = \alpha_3$ or $\alpha_1 = \alpha_4$.

Now $\beta^2, \gamma^2, \delta^2$ are permuted by G. They are invariant only under the elements of $G \cap V$, so $\mathrm{Gal}(M/K(\beta^2, \gamma^2, \delta^2)) = G \cap V$. Therefore $L = M^{G\cap V} = K(\beta^2, \gamma^2, \delta^2)$.

Consider now the polynomial $g = (X - \beta^2)(X - \gamma^2)(X - \delta^2)$. Since the elements of G can only permute these three factors, g must have coefficients fixed by G, and so $g \in K[X]$. g is called the *resolvant cubic.*

Explicit checks yield

$$\begin{aligned} \beta^2 + \gamma^2 + \delta^2 &= -2p && \text{(inspection)} \\ \beta^2\gamma^2 + \beta^2\delta^2 + \gamma^2\delta^2 &= p^2 - 4v && \text{(multiply out)} \\ \beta\gamma\delta &= -q. && \text{(inspection)} \end{aligned}$$

Thus the resolvant cubic is

$$X^3 + 2pX^2 + (p^2 - 4r)X - q^2.$$

L is the splitting field for g over K. So if we solve g for $\beta^2, \gamma^2, \delta^2$ by radicals, we can then solve for β, γ, δ by taking square roots (taking care to choose signs so that $\beta\gamma\delta = -q$). Then we solve for the roots

$$\alpha_1 = \frac{1}{2}(\beta + \gamma + \delta), \quad \alpha_2 = \frac{1}{2}(\beta - \gamma - \delta), \quad \alpha_3 = \frac{1}{2}(-\beta + \gamma - \delta), \quad \alpha_4 = \frac{1}{2}(-\beta - \gamma + \delta).$$

7.4 Insolubility of the general quintic by radicals

Definition

A group G is *soluble* if there exists a finite series of subgroups

$$1 = G_n \subset G_{n-1} \subset \cdots \subset G_0 = G$$

such that $G_i \lhd G_{i-1}$ with G_{i-1}/G_i cyclic, for each $1 \leq i \leq n$.

Examples

1. S_4 is soluble. For if $G_1 = A_4$, $G_2 = V$ and $G_3 = \langle(12)\rangle = C_2$, then

   $$1 = G_4 \leq G_3 \leq G_2 \leq G_1 \leq G_0 = S_4,$$

   and $G_0/G_1 \cong C_2$, $G_1/G_2 \cong C_3$ and $G_2/G_3 \cong G_3/G_4 \cong C_2$.

2. Using the structure theorem for abelian groups, it is easily seen that any finitely generated abelian group is soluble.

Theorem 7.4

1. *If G is a soluble group and A is a subgroup of G, then A is soluble.*
2. *If G is a group and $H \lhd G$, then G is soluble iff both H and G/H are soluble.*

Proof

1. We have a series of subgroups

$$1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G$$

   such that G_{i-1}/G_i is cyclic for $1 \le i \le n$. Let $A_i = A \cap G_i$ and $\theta : A_{i-1} \to G_{i-1}/G_i$ be the composite homomorphism $A_{i-1} \hookrightarrow G_{i-1} \hookrightarrow G_{i-1}/G_i$. Then

$$\begin{aligned} \ker\theta &= \{a \in A_{i-1} \mid aG_i = G_i\} \\ &= A_{i-1} \cap G_i \\ &= A \cap G_{i-1} \cap G_i \\ &= A \cap G_i \\ &= A_i. \end{aligned}$$

   So for each i, $A_i \lhd A_{i-1}$ and A_{i-1}/A_i is isomorphic to a subgroup of G_{i-1}/G_i and hence cyclic. Therefore A is soluble.

2. A similar but longer argument — see a book. □

Example

For $n \ge 5$, a standard result says that A_n is simple (i.e. there does not exist a proper normal subgroup) and hence non-soluble. Hence (7.4) implies that S_n is also non-soluble.

We now relate solubility of the Galois group to solubility of polynomial equations $f = 0$ by radicals. Assume for simplicity that $\operatorname{char} K = 0$. An argument similar to that used for the quartic in §7.3 shows that if f has a soluble Galois group, then f is soluble by radicals. (The basic idea is that if M/K is a splitting field for f, with $d = [M : K]$, we first adjoin a primitive dth root of unity and then repeatedly use (7.3).)

We're mainly interested in the converse. Suppose then $L = L_0 \subset L_1 \subset \cdots \subset L_r = N$ is an extension by radicals. Even if L contains all the requisite roots of unity and L_i/L_{i-1} is Galois and cyclic, it doesn't follow that N/L is Galois.

Proposition 7.5

Suppose that L/K is a Galois extension and that $M = L(\beta)$, with β a root of $X^n - \theta$ for some $\theta \in L$. Then there exists an extension by radicals N/M such that N/K is Galois.

Proof

If necessary we adjoin a primitive nth root of unity ϵ to M, so $X^n - \theta$ factorizes over $M(\epsilon)$ as $(X - \beta)(X - \epsilon\beta)\cdots(X - \epsilon^{n-1}\beta)$. $M(\epsilon)$ is a splitting field for $X^n - \theta$ over L, and so $M(\epsilon)/L$ is Galois. Let $G = \operatorname{Gal}(L/K)$ and define

$$f = \prod_{\sigma \in G} (X^n - \sigma(\theta)).$$

The coefficients of f are invariant under the action of G and so $f \in K[X]$.

Since L/K is Galois, it is the splitting field for some polynomial $g \in K[X]$. let N be the splitting field for fg — so N/K is normal. Moreover, N is obtained from M by first adjoining ϵ and then adjoining a root of each polynomial $X^n - \sigma(\theta)$ for $\sigma \in G$. So N/M is an extension by radicals. □

Corollary 7.6

Suppose M/K is an extension by radicals. Then there exists an extension by radicals N/M such that N/K is Galois.

Proof

We have $K = K_0 \subset K_1 \subset \cdots \subset K_r = M$, with $K_i = K_{i-1}(\beta_i)$ for some $\beta_i \in K_i$ satisfying $X^{n_i} - \theta_i = 0$ for some $\theta_i \in K_{i-1}$, $n_i \in \mathbb{N}$.

We now argue by induction on r. Suppose the Corollary to be true for $r-1$, so that there exists an extension by radicals N'/K_{r-1} such that N'/K is Galois. Let f_r be the minimal polynomial for β_r over K_{r-1} and let g_r be an irreducible factor of f_r considered as a polynomial in $N'[X]$. Let $N'(\gamma)/N'$ be the extension of N' obtained by adjoining a root γ of g_r. We consider $K_{r-1} \subseteq N' \subseteq N(\gamma)$, so that γ has minimal polynomial f_r over K_{r-1} (since $f_r(\gamma) = 0$ and by assumption f_r is irreducible). We may identify $K_r = K_{r-1}(\beta_r) \cong K_{r-1}(\gamma)$. Therefore $N'(\gamma)$ is an extension by radicals of $K_r = K_{r-1}(\gamma)$.

By assumption N'/K is Galois and contains a root of $X^{n_r} - \theta_r$, where $\theta_r \in K_{r-1} \subseteq N'$. So (7.5) implies that there exists an extension by radicals $N/N'(\gamma)$ — and so N is an extension by radicals of $K_r = M$ — such that N/K is Galois. $\square$

Theorem 7.7

Suppose that $f \in K[X]$ and that there exists an extension by radicals

$$K = K_0 \subset K_1 \subset \cdots \subset K_r = M,$$

where $K_i = K_{i-1}(\beta_i)$ and β_i is a root of $X^{n_i} - \theta_i$, over which f splits completely. Then $\mathrm{Gal}(f)$ *is soluble.*

Proof

By (7.6) we may assume that M/K is Galois. Let $n = \mathrm{lcm}(n_1, \ldots, n_r)$, and let ϵ be a primitive nth root of unity.

If $\mathrm{Gal}(M/K)$ is soluble, then the splitting field of f is an intermediate field $K \subseteq K' \subseteq M$ and $\mathrm{Gal}(f) = \mathrm{Gal}(K'/K)$ is a quotient of $\mathrm{Gal}(M/K)$ and hence soluble by (7.4).

So it remains to show that $\mathrm{Gal}(M/K)$ is soluble. Assume first that $\epsilon \in K$, and let $G_i = \mathrm{Gal}(M/K_i)$. Therefore $1 = G_r \leq G_{r-1} \leq \cdots \leq G_1 \leq G_0 = \mathrm{Gal}(M/K)$. Moreover, each extension $K_i = K_{i-1}(\beta)/K_{i-1}$ is a Galois extension (since $\epsilon \in K$) with cyclic Galois group (by (7.1)). So apply the fundamental theorem of Galois theory to the Galois extension M/K_{i-1} and we get that $G_i \lhd G_{i-1}$ with G_{i-1}/G_i cyclic. Therefore $G_0 = \mathrm{Gal}(M/K)$ is soluble.

If, however, $\epsilon \notin K$, set $L = K(\epsilon)$. Clearly $M(\epsilon)/K$ is Galois. Set $G' = \mathrm{Gal}(M(\epsilon)/L)$ — this is soluble by the previous argument (as $\epsilon \in L$). If $G = \mathrm{Gal}(M(\epsilon)/K)$, then $G/G' = \mathrm{Gal}(K(\epsilon)/K)$ is the Galois group of a cyclotomic extension, hence abelian, and hence soluble. So (7.4) implies that G is soluble and hence $\mathrm{Gal}(M/K)$ is also soluble. $\square$

Remark

There exist many irreducible quintics $f \in \mathbb{Q}[X]$ with Galois group S_5 (or A_5). Therefore (7.7) implies that we cannot in general solve quintics by radicals.