University of
Cambridge

Mathematics Tripos

Part II

Galois Theory

Michaelmas, 2017

Lectures by
C. Brookes

Notes by
Qiangru Kuang

Contents

0 History

The primary motivation of this course is to study polynomial equations in one variable and to consider whether there is a formula involving roots, i.e. solution by *radicals*.

Quadratics have been well understood since long long time ago and we have already studied them at school. For cubics and quartics, it took long time before people discovered how to solve them by radicals. In 1770 Lagrange studied why it worked. However, In 1799 Ruffini claimed that there were some quintics that *can't* be solved by radicals, i.e. there is no general formula, although his proof had gaps.

In 1824, Abel (1802 – 1829) first accepted proof of insolubility using existing ideas about permutations of roots. In 1831, Galois (1811 – 1832) first explained why some polynomials are soluble by radicals and others are not. He made use of a *group of permutations* of the roots and he realised in particular the importance of *normal subgroups*.

Galois' work was not known in his lifetime — it was only published by Liouville in 1846 who realised that it fit in well with the work of Cauchy on permutations.

Galois had submitted his work for various competitions and for entry into the École Polytechnique. He died in a duel, leaving a $6\frac{1}{2}$ page letter indicating his thoughts about future development.

Most of this course is Galois Theory but it is presented in a slightly more modern way in terms of field extensions.

Recall from IB Groups, Rings and Modules that if $f(t)$ is an irreducible polynomial in $K[t]$ for some field K then $K[t]/(f(t))$ is a field where $f(t)$ is the ideal generated by $f(t)$. This is the starting point of this course.

This course requires quite a lot of IB Groups, Rings and Modules but no content about module is required except in one place where it is useful to know the Structural Theorem of Finitely Generated Abelian Groups.

1 Field Extensions

1.1 Field Extensions

Definition (field extension)**.** A *field extension* $K \leq L$ is the inclusion of a field K into another field L, with the same 0 and 1 and the restriction of $+$ and $\cdot$ in L to K gives $+$ and $\cdot$ in K.

Example. $\mathbb{Q} \leq \mathbb{R}, \mathbb{R} \leq \mathbb{C}, \mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) = \{\lambda + \mu\sqrt{2} : \lambda, \mu \in \mathbb{Q}\}$ and $\mathbb{Q}(i) = \{\lambda + \mu i : \lambda, \mu \in \mathbb{Q}\} \leq \mathbb{C}$ are all field extensions.

Suppose $K \leq L$ is a field extension. Then L is a K-vector space with addition given by the field and scalar multiplication given by the multiplication in the field L.

Definition (degree of extension)**.** The *degree* of L over K is $\dim_k L$, the dimension of the K-vector space L. It is denoted by $|L : K|$. It may or may not be finite.

Definition (finite extension)**.** If $|L : K| < \infty$ the extension is *finite*. Otherwise it is *infinite*.

Example.

1. $|\mathbb{C} : \mathbb{R}| = 2$ since $\{1, i\}$ is a basis.
2. Similarly $|\mathbb{Q}(i) : \mathbb{Q}| = 2$.
3. $\mathbb{Q} \leq \mathbb{R}$ is an infinite extension.

Theorem 1.1 (Tower Law)**.** *Suppose $K \leq L \leq M$ are field extensions. Then*

$$|M : K| = |M : L||L : K|.$$

Proof. Assume $|M : L| < \infty, |L : K| < \infty$. Then we take an L-basis $\{f_i\}_{i=1}^b$ and a K-basis $\{e_j\}_{j=1}^a$.

Now take $m \in M$. $m = \sum_{i=1}^b \mu_i f_i$ for some $\mu_i \in L$. For each μ_i, we can write $\mu_i = \sum_{j=1}^\infty \lambda_{ij} e_j$ for some $\lambda_{ij} \in K$. Thus

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

so $\{f_i e_j\}$ span M.

To show linear independence, it suffices to show that if $m = 0$ then each of the λ_{ij} is zero. When $m = 0$, the linear independence of f_i forces each μ_i to be zero. Then the linear independence of e_i forces λ_{ij} to be zero as required.

The proof for infinite extensions is omitted. Observe (not very rigorously) that if M is an infinite extension of L then it is an infinite extension of K, and if L is an infinite extension of K then the larger field M must also be an infinite extension of K. □

Example. Consider

$$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{2}, i).$$

$\mathbb{Q}(\sqrt{2})$ has $\{1, \sqrt{2}\}$ as a $\mathbb{Q}$-basis. $\mathbb{Q}(\sqrt{2}, i)$ has $\{1, i\}$ as a $\mathbb{Q}(\sqrt{2})$-basis. Now $\mathbb{Q}(\sqrt{2}, i)$ has basis $\{1, \sqrt{2}, i, i\sqrt{2}\}$ over $\mathbb{Q}$. Thus

$$|\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}| = 4 = 2 \cdot 2 = |\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})||\mathbb{Q}(\sqrt{2}) : \mathbb{Q}|.$$

What are the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(i, \sqrt{2})$? Obviously we have $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{2})$. Are there any more?

To answer, this, the Galois correspondence arising in the Fundamental Theorem of Galois Theory gives an *order-reversing* bijection between the lattice of intermediate subfields and the subgroups of a group of ring automorphisms of the extension field ($\mathbb{Q}(i, \sqrt{2})$ here) that fix the smaller field element-wise.

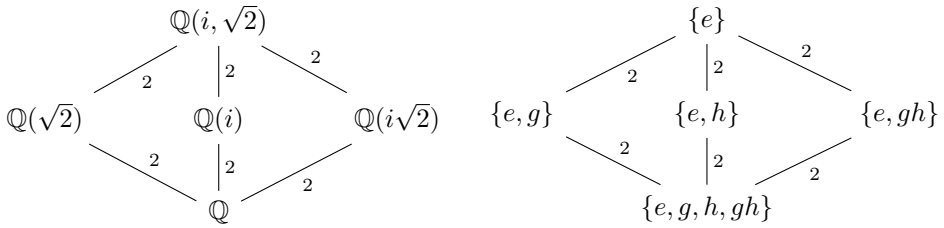
Ring automorphisms of $\mathbb{Q}(i, \sqrt{2})$ that fixes $\mathbb{Q}$ include the identity $e : \sqrt{2} \mapsto \sqrt{2}, i \mapsto i$ and complex conjugation $g : \sqrt{2} \mapsto \sqrt{2}, i \mapsto -i$. Notice that i and $-i$ play the same role in the field $\mathbb{Q}(i, \sqrt{2})$ — they are both roots of $t^2 + 1 = 0$. There is another automorphism

$$\begin{aligned} h : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto i \end{aligned}$$

which switches the roots of $t^2 - 2 = 0$. Notice that the composition

$$\begin{aligned} gh : \sqrt{2} &\mapsto -\sqrt{2} \\ i &\mapsto -i \end{aligned}$$

These form a group of order 4, which equals to $|\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}|$.



The recipe for producing an intermediate subfield from a subgroup is to take the elements of $\mathbb{Q}(i, \sqrt{2})$ which are fixed by all elements of the subgroup. For example, $\mathbb{Q}(i\sqrt{2})$ is the field of elements fixed by both e and gh. This correspondence doesn't always work for all finite field extensions: it only works for *Galois extensions*.

In the correspondence, normal extensions correspond to normal subgroups. In this example all subgroups are normal and hence the extensions are normal.

We will also prove Primitive Element Theorem, which in the context of finite extensions of $\mathbb{Q}$ tells us that they are necessarily of the form $\mathbb{Q}(\alpha)$ for some α. For example, $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(i + \sqrt{2})$.

We now do a review of IB Groups, Rings and Modules. Suppose $K \leq L$ is a field extension. Take $\alpha \in L$. Define

$$I_\alpha = \{f \in K[t] : f(\alpha) = 0\}.$$

Definition (algebraic, transcendental)**.** α is *algebraic* over K if $I_\alpha \neq \{0\}$. Otherwise α is *transcendental* over K.

Definition (algebraic extension)**.** L is *algebraic over* K if for all $\alpha \in L$, α is algebraic over K.

Remark. I_α is the kernel of the ring homomorphism

$$\begin{aligned} K[t] &\to L \\ f &\mapsto f(\alpha) \end{aligned}$$

evaluation at α. It follows that I_α is an ideal of $K[t]$.

Example.

1. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since it is a root of $t^2 - 2$.
2. π is transendental over $\mathbb{Q}$.

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

Proof. Let $|L : K| = n$. Take $\alpha \in L$. Consider $1, \alpha, \alpha^2, \ldots, \alpha^n$. These must be linearly dependent in the n-dimensional K-vector space L so

$$\sum_{i=0}^{n} \lambda_i \alpha^i = 0$$

for some $\lambda_i \in K$ not all zero. Then α is a root of $f(t) = \sum_{i=0}^{n} \lambda_i t^i$. Thus α is algebraic over K. □

The non-zero ideal I_α (where α is algebraic over K) is principal since $K[t]$ is a PID. Then

Definition (minimal polynomial)**.** $I_\alpha = (f_\alpha(t))$ and $f_\alpha(t)$ can be assumed to be monic. Such a monic $f_\alpha(t)$ is the *minimal polynomial* of α over K.

Remark. Multiplication by α within the field L gives a K-linear map $L \to L$, an automorphism of L if $\alpha \neq 0$.

In IB Groups, Rings and Modules, we proved that the minimal polynomial of a linear map is unique.

Example.

1. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$.
2. The minimal polynomial of $\sqrt{2}$ over $\mathbb{R}$ is $t - \sqrt{2}$.

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

Proof. Suppose not and $f_\alpha(t) = p(t)q(t)$. We must show that either $p(t)$ or $q(t)$ is a unit in $K[t]$. Note that $0 = f(\alpha) = p(\alpha)q(\alpha)$ and so $p(\alpha) = 0$ or $q(\alpha) = 0$. Assume wlog $p(\alpha) = 0$. Thus $p(t) \in I_\alpha$ and so $p(t) = f_\alpha(t)r(t)$ since $I_\alpha = (f_\alpha(t))$. Thus $f_\alpha(t) = f_\alpha(t)r(t)q(t)$ and so $r(t)q(t) = 1$ in $K[t]$. Thus $q(t)$ is a unit as required.

Recall that irreducible elements in an integral domain are prime and generate prime ideals of $K[t]$. Thus I_α is a prime ideal. □

Definition (generated field)**.** Suppose $K \leq L$ is a field extension and $\alpha \in L$. $K(\alpha)$ is defined to be the smallest subfield of L containing K and α. It is called the *field generated* by K and α.

Definition (simple extension)**.** L is a *simple extension* if $L = K(\beta)$ for some $\beta \in L$.

Given $\alpha_1, \ldots, \alpha_n \in L$, $K \leq L$, $K(\alpha_1, \ldots, \alpha_n)$ is the smallest intermediate field containing $\alpha_1, \ldots, \alpha_n$. It is the field generated by K and $\alpha_1, \ldots, \alpha_n$. On the other hand, $K[\alpha] = \mathrm{im}(K[t] \to L, f \mapsto f(\alpha))$ is the ring generated by K and α.

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

1. *$K(\alpha) = K[\alpha] = \mathrm{im}(f \mapsto f(\alpha))$.*
2. *$|K(\alpha) : K| = \deg f_\alpha(f)$ where $f_\alpha(t)$ is the minimal polynomial of α over K.*

Proof.

1. Clearly $K[\alpha] \leq K(\alpha)$. We need to show that if $0 \neq \beta \in K[\alpha]$ then it is a unit in $K[\alpha]$ and so $K[\alpha]$ is a field. Let $\beta = g(\alpha)$ for some $g(t) \in K[t]$. Since $\beta = g(\alpha) \neq 0$, $g(t) \notin I_\alpha = (f_\alpha(t))$. Therefore $f_\alpha(t) \nmid g(t)$. Since $f_\alpha(t)$ is irreducible and $K[t]$ is a PID, there exists $r(t), s(t) \in K[t]$ with
$$r(t)f_\alpha(t) + s(t)g(t) = 1 \in K[t].$$
Thus $s(\alpha)g(\alpha) = 1 \in K[\alpha]$ and thus $\beta = g(\alpha)$ is a unit as required.
2. Let $n = \deg f_\alpha(t)$. We will show that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a K-vector space basis of $K[\alpha]$.
   - spanning: suppose
   $$f_\alpha(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$$
   with $a_i \in K$. Then
   $$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$
   This implies that α^n is a linear combination of $\{\alpha^i\}_0^{n-1}$. An easy induction shows that a^m for $m \geq n$ is likewise a linear combination of $\{\alpha^i\}_0^{n-1}$. Spanning thus follows.

- linear independence: suppose there is a relation $\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0$. Let $g(t) = \sum_{i=0}^{n-1} \lambda_i t^i$. Since $g(\alpha) = 0$, we have $g(t) \in I_\alpha = (f_\alpha(t))$. Thus $g(t) = 0$ or $f_\alpha(t) \mid g(t)$. The latter is not possible by degree consideration. Thus $g(t) = 0 \in K[\alpha]$ and all the λ_i's are zero.

□

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

Proof. Straightforward by combining previous results. □

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

Proof. By Tower Law on $K \leq K(\alpha) \leq L$, we deduce that $|K(\alpha) : K|$ divides $|L : K|$. The result follows from the corollary above. □

1.2 Digression on (non-)constructability

In schedules it mentions "other classical problems" and we are in a position to tackle some of these using Corollary 1.6.

A classical problem from Greek geometry concerns the existence or otherwise of constructions using ruler and compasses. Here "ruler" means single unmarked straightedge. If you're an expert you can divide a line between two points into arbitrarily many equal segments, bisect an angle and produce parallel lines. In addition, given a polygon, you can produce a square of the same area or double the area. However, you cannot

1. duplicate the cube (i.e. given a cube you cannot produce a cube of double the volume);
2. trisect the angle $\pi/3$;
3. square a circle (i.e. given a circle you cannot construct a square of the same area).

Assume we are given a set P_0 of points in $\mathbb{R}^2$,

- *ruler operation* draws a straight line through any points in P_0,
- *compass operation* draws a circle with centre being a point in P_0 and radius being distance between a pair of points in P_0.

Definition (constructible number)**.** The points of intersection of any two distinct lines or circles drawn using these operations are *constructible* in one step from P_0.

A point $r \in \mathbb{R}^2$ is *constructible* from P_0 if there is a finite sequence $r_1, r_2, \ldots, r_n = r$ such that r_i is constructible in one step from $P_0 \cup \{r_1, \ldots, r_{i-1}\}$.

Exercise. Construct the midpoint of a line between two points.

Let K_0 be the subfield of $\mathbb{R}$ generated by $\mathbb{Q}$ and the coordinates of points in P_0. Let $r_0 = (x_i, y_i)$. Set $K_i = K_{i-1}(x_i, y_i)$. Then

$$K_0 \leq K_1 \leq \cdots \leq K_n \leq \mathbb{R}.$$

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

Proof. There are three cases:

- line intersects line.
- circle intersects circle,
- circle intersects circle.

For the line intersecting circle case, the line passes through $A = (p, q)$ and $B = (r, s)$ and the circle centres at $C = (t, u)$ and has radius w. Then the equation of line is

$$\frac{x-p}{r-p} = \frac{y-q}{s-q}$$

and the equation of circle is

$$(x-t)^2 + (y-u)^2 = w^2.$$

Solving gives coordinates of the intersection satisfying quadratic polynomials over K_{i-1}.

The other cases are similar. □

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

Proof. Use the previous notation $K_i = K_{i-1}(x_i, y_i)$. By Tower Law,

$$|K_i : K_{i-1}| = |K_{i-1}(x_i, y_i) : K_{i-1}(x_i)||K_{i-1}(x_i) : K_{i-1}|.$$

But the previous lemma tells us that $|K_{i-1}(x_i) : K_{i-1}| = 1$ or 2, depending on whether the quadratic polynomial satisfied by the point of intersection is irreducible or not. Similarly y_i satisfies a quadratic polynomial over K_{i-1}, and hence over $K_{i-1}(x_i)$ and so $K_{i-1}(x_i, y_i) : K_{i-1}(x_i)| = 1$ or 2. Therefore $|K_i : K_{i-1}| = 1, 2$ or 4 (but in fact 4 does not happen). Therefore by Tower Law,

$$|K_n : K_0| = |K_n : K_{n-1}| \cdots |K_1 : K_0|$$

is a power of 2.

If $r = (x, y)$ is contrucible from P_0 then $x, y \in P_n$ for some n and therefore

$$K_0 \leq K_0(x) \leq K_n$$
$$K_0 \leq K_0(y) \leq K_n$$

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

To use this for proofs about non-constructibility we need to be reasonably expert at working out minimal polynomials. Recall from IB Groups, Rings and Modules

Theorem 1.9 (Gauss' Lemma)**.** *Let $f(t)$ be a primitive integral polynomial. Then $f(t)$ is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[t]$.*

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

- $p \nmid a_n$,
- $p \mid a_{n-1}, p \mid a_{n-2}, \ldots, p \mid a_0$,
- $p^2 \nmid a_0$,

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

Example. Suppose p is prime. Then

$$f(t) = t^{p-1} + t^{p-2} + \cdots + 1$$

is irreducible over $\mathbb{Q}$ by considering $f(t+1)$ and using p as the prime in Eisenstein.

Another method to determine reducibility is to consider an integral polynomials $f(t) \pmod p$. If $f(t)$ is reducible in $\mathbb{Z}[t]$ then it is reducible over $\mathbb{Z}/p\mathbb{Z}$. So if we find a prime p such that $f(t) \pmod p$ is irreducible then $f(t)$ is irreducible in $\mathbb{Z}[t]$.

Example. $t^3 + t + 1$ is irreducible mod 2: if it were reducible it would have a linear factor and so the polynomial would have a root mod 2, but $0, 1$ are not roots. So $t^3 + t + 1$ is irreducible in $\mathbb{Z}[t]$ and hence irreducible in $\mathbb{Q}[t]$.

Remark. On example sheet we will meet an irreducible polynomials in $\mathbb{Z}[t]$ which is reducible mod p for all primes p.

Now back to construcibility.

Theorem 1.11. *The cube cannot be duplicated by rulers and compasses.*

Proof. The problem amounts to whether given a unit distance one can construct points distance α apart where α satisfies $t^3 - 2 = 0$. Starting with points $P_0 = \{(0,0), (1,0)\}$. Can we produce $(\alpha, 0)$? No. If we could, $|\mathbb{Q}(\alpha) : \mathbb{Q}|$ would be a power of 2. We show $|\mathbb{Q}(\alpha) : Q| = 3$: since α satisfies $t^3 - 2$, which by Eisenstein is irreducible over $\mathbb{Z}$ and hence over $\mathbb{Q}$. Thus it is the minimal polynomials of α over $\mathbb{Q}$. □

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

Proof. Starting with $(0,0)$ and $(1,0)$, can we construct $(\sqrt{\pi}, 0)$ so that we have a square of side length $\sqrt{\pi}$, and hence the area of the square equals to the are of the unit circle?

The answer is no since π and hence $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$. □

Now return to further theory develpment.

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

1. *$\alpha_1, \ldots, \alpha_n \in L$ are algebraic over K if and only if $K \leq K(\alpha_1, \ldots, \alpha_n)$ is a finite extension.*
2. *If $K \leq M \leq L$ is such that $K \leq M$ is finite, then there exists $\alpha_1, \ldots, \alpha_n \in L$ such that $K(\alpha_1, \ldots, \alpha_n) = M$.*

Proof.

1. We know α is algebraic over K if and only if $K \leq K(a)$ is a finite extension. Suppose for each i, α_i is algebraic over K, hence over $K(\alpha_1, \ldots, \alpha_{i-1})$ and so $|K(\alpha_1, \ldots, \alpha_i) : K(\alpha_1, \ldots, \alpha_{i-1})| < \infty$. By Tower Law applied to

$$K \leq K(\alpha_1) \leq \cdots \leq K(\alpha_1, \ldots \alpha_n),$$

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

   Conversely, consider

$$K \leq K(\alpha_i) \leq K(\alpha_1, \ldots, \alpha_n).$$

   Then the Tower Law says that if $|K(\alpha_1, \ldots, \alpha_n) : K| < \infty$ then $|K(\alpha_i) : K| < \infty$ and so α_i is algebraic over K.

2. If $|M : K| = n$ then M is an n-dimensional K-vector space so there exists a K-basis $\{\alpha_1, \ldots, \alpha_n\}$ of M. Then $K(\alpha_1, \ldots, \alpha_n) \leq M$. However, any elements of M is a K-linear combination of $\alpha_1, \ldots, \alpha_n$ and so lies in $K(\alpha_1, \ldots, \alpha_n)$ so equality.

□

Definition (K-homomorphism)**.** Suppose $K \leq L, K \leq L'$ are field extensions. A *K-homomorphism* $\phi : L \to L'$ is a ring homomorphism such that $\phi|_K = \mathrm{id}$.

Notation. Let

$$\mathrm{Hom}_K(L, L') = \{K\text{-homomorphisms } L \to L'\}.$$

A K-homomorphism $\phi : L \to L'$ is a *K-isomorphism* if it is a ring isomorphism.

Notation. $\mathrm{Aut}_K(L) = \{K\text{-isomorphism } L \to L'\}$ which has a group structure.

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

1. *any K-homomorphism $\phi : L \to L'$ is injective and $K \leq \phi(L)$ is a field extension;*
2. *if $|L : K| = |L' : K| < \infty$, then a K-homomorphism $\phi : L \to L'$ is a K-isomorphism.*

Proof.

1. L is a field and $\ker\phi$ is an ideal of L. Note $1 \mapsto 1$ and so $\ker\phi \neq L$, so $\ker\phi = 0$. Therefore $\phi(L)$ is a field and $K \leq \phi(L)$ is a field extension.

2. ϕ is an injective K-linear map and so $|\phi(L) : K| = |L : K|$, which, by considering the dimensions of K-vector spaces, is smaller than $|L' : K| = |L : K|$ by assumption. Thus $\phi : L \to L'$ is a K-isomorphism. In particular if $L = L'$ then ϕ is a K-automorphism of L.

□

Notation. If $K \leq L$ is a field extension and if $f(t) \in K[t]$, we denote the set of roots of f in L by $\mathrm{Root}_f(L)$.

Definition (splitting polynomial, splitting field)**.** Let $K \leq L$ be a field extension and $f(t) \in K[t]$. We say f *splits over* L if

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

where $a \in K, \alpha_1, \ldots, \alpha_n \in L$.

We say L is a splitting field for f over K if $L = K(\alpha_1, \ldots, \alpha_n)$.

Remark. This is equivalent to saying that L is a splitting field for f over K if and only if

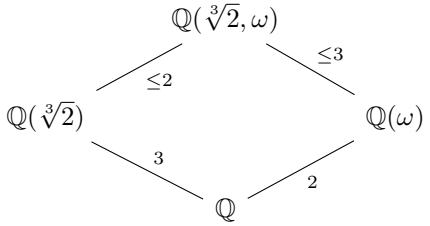
1. f splits over L,

2. if $K \leq M \leq L$ and f splits over M then $M = L$.

Example.

1. $f(t) = t^3 - 2$ over $\mathbb{Q}$: $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field over $\mathbb{Q}$ but $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is where ω is a primitive cubic root of unity, e.g. $\omega = e^{\frac{2\pi}{3}i}$. Note that $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

   As $\sqrt[3]{2}$ satisfies $t^3 - 2$ over $\mathbb{Q}$ and hence over $\mathbb{Q}(\omega)$, we have $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)| \leq 3$. ω satisfies $t^2 + t + 1$ over $\mathbb{Q}$ and hence over $\mathbb{Q}(\sqrt[3]{2})$ and so $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| \leq 2$. Since $t^3 - 2$ and $t^2 + t + 1$ are irredcuible over $\mathbb{Q}$, $|\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}| = 3$ and $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$ so by tower law we conclude that equality holds, i.e. $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\omega)| = 3$ and $|\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}(\sqrt[3]{2})| = 2$.



2. $f(t) = (t^2 - 3)(t^3 - 1)$ over $\mathbb{Q}$: the splitting field is

$$\mathbb{Q}(\sqrt{3}, \sqrt{-3}, \omega, \omega^2, 1) = \mathbb{Q}(\sqrt{3}, \omega) = \mathbb{Q}(\sqrt{3}, i)$$

   as $\omega = \frac{-1+i\sqrt{3}}{2}$.

3. $t^2 - 3$ and $t^2 - 2t - 2$ both have $\mathbb{Q}(\sqrt{3})$ as the splitting field over $\mathbb{Q}$.

4. $f(t) = t^2 + t + 1$ over $\mathbb{F}_2[t]$: $f(t)$ is irreducible over $\mathbb{F}_2$ since it has no roots and hence no linear factors. Thus $\mathbb{F}_2[t]/(t^2 + t + 1)$ is a field. Set $\alpha = t + (t^2 + t + 1) \in \mathbb{F}_2[t]/(t^2 + t + 1)$, Then $F_2[t]/(t^2 + t + 1) = \mathbb{F}_2(\alpha)$. The elements are $0, 1, \alpha$ and $1 + \alpha$. Note that $\alpha^2 = \alpha + 1$ since $\mathbb{F}_2$ has characteristic 2. Now $f(t)$ splits over $\mathbb{F}_2(\alpha)$ as

$$f(t) = (t - \alpha)(t - 1 - \alpha)$$

so $\mathbb{F}_2(\alpha)$ is a splitting field of f over $\mathbb{F}_2$.

We use the following construction to produce splitting field in general.

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

Proof. Induction of $\deg f$. If $\deg f = 1$ then K is the splitting field of f over K. Suppose $\deg f > 1$ and pick an irreducible factor $g(t)$ of $f(t)$ over K. Note that $K \leq K[t]/(g(t))$ is a field extension. Let $\alpha_1 = t + (g(t)) \in K[t]/(g(t))$ so $K[t]/(g(t)) = K(\alpha_1)$ and $g(\alpha_1) = 0$ in $K(\alpha_1)$. Therefore $f(\alpha_1) = 0$ in $K(\alpha_1)$ and we can write $f(t) = (t - \alpha_1)h(t)$ in $K(\alpha_1)[t]$. Repeat, note that $\deg h < \deg f$, and we get

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

where a is a constant which is in K (by considering the top coefficient of f). Thus we have a factorisation of $f(t)$ in $K(\alpha_1, \dots, \alpha_n)[t]$. $K(\alpha_1, \dots, \alpha_n)$ is a splitting field for f over K. □

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

Proof. Suppose L and L' are splitting fields for $f(t) \in K[t]$ over K. We need to show that there is a K-isomorphism $L \to L'$. Suppose $K \leq M \leq L$ and there exists $K \leq M' \leq L'$ and a K-isomorphism $\psi : M \to M'$. Clearly we can take $M = K$ so such intermediate fields exist. Pick M so that $|M : K|$ is maximal among such M, M' and ψ.

Now we want to show that $M = L$ and $M' = L'$. Note that if $M = L$ then $f(t)$ splits over M, say

$$f(t) = a(t - \alpha_1) \dots (t - \alpha_m) \in M[t].$$

Apply ψ we get an induced map $M[t] \to M'[t]$ which maps $f(t)$ to

$$\psi(f)(t) = \psi(a)(t - \psi(\alpha_1) \dots (t - \psi(\alpha_m))$$

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

Now suppose $M \neq L$ and we'll arrive at a contradition of maximality of M. Since $M \neq L$, there is a root α of $f(t)$ in L which isn't in M. Factorise $f(t) = g(t)h(t) \in M[t]$ so that $g(t) \in M[t]$ is irreducible and $g(\alpha) = 0$ in L. Then there exists a K-homomorphism

$$\begin{aligned} M[t]/(g(t)) &\to L \\ t + (g(t)) &\mapsto \alpha \end{aligned}$$

The image of the map is $M(\alpha)$. The K-isomorphism $M[t] \to M'[t]$ induced by ψ maps $g(t) \in M[t]$ to some irreducible $\gamma(t) \in M'[t]$ so

$$f(t) = g(t)h(t) \in M[t]$$

yields

$$f(t) = \gamma(t)\delta(t) \in M'[t].$$

We have a field extension $M' \leq M'[t]/(\gamma(t))$ and there exists an M'-homomorphism

$$\begin{aligned} M'[t]/(\gamma(t)) &\to L' \\ t + (\gamma(t)) &\mapsto \alpha' \end{aligned}$$

by picking a root α' of $\gamma(t)$ in L'. However $\gamma(t) \mid f(t)$ in $M'[t]$ and hence in $L'[t]$ and so α' is also a root of $f(t)$ in L'.

The M'-homomorphism gives a K-isomorphism $M'[t]/(\gamma(t)) \to M'(\alpha')$ and we have a K-homomorphism $M(\alpha) \to M'(\alpha')$, contradicting the maximality of M. □

Definition (normal extension)**.** An algebraic field extension $K \leq L$ is *normal* if for every $\alpha \in L$, the minimal polynomial $f_\alpha(t)$ of α over K splits over L.

Theorem 1.17. *Let $K \leq L$ be a finite field extension, then $K \leq L$ is normal if and only if L is the splitting field for some $f(t) \in K[t]$.*

Proof. Later. □

Example. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = m$. $\mathbb{F}$ has characteristic p for some prime p and $\mathbb{F}_p \leq \mathbb{F}$. Therefore $m = p^r$ for some r.

The nonzero elements of $\mathbb{F}$ form the multiplicative group or order $n = m - 1$ and they satisfy $t^n - 1$ so they are roots of $t^n - 1$. Thus $t^n - 1 = \prod_{i=1}^{n}(t - \alpha_i)$ where the α_i's are the nonzero elements of $\mathbb{F}$. Thus $\mathbb{F}$ is the splitting field for $t^n - 1$ over $\mathbb{F}_p$.

By uniqueness of splitting field, any other field with m elements is $\mathbb{F}_p$-isomorphic to $\mathbb{F}$. (We will later show that there *exists* a field of m elements.)

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

In particular the multiplicative group of a finite field is cyclic.

Proof. Let $|G| = n$. By the structure theorem of finite abelian groups from IB Group, Rings and Modules,

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

with q_i's (not necessarily distinct) prime.

If $q = q_i = q_j$ for some $i \neq j$ then there are at least q^2 distinct solutions of $t^q - 1$ in K (since $C_q \times C_q$ is isomorphic to a subgroup of G). However, in a field, which is an integral domain, a polynomial of degree q has at most q roots, contradiction.

Thus all the q_i's are distinct and G is cyclic and is generated by $g_1 \dots g_r$ where each g_i generates $C_{q_i^{m_i}}$. □

2 Separable, Normal and Galois Extensions

2.1 Separable Extension

Definition (separable polynomial)**.** Let K be a field and $f(t) \in K[t]$. Suppose $f(t)$ is irreducible in $K[t]$ and L is a splitting field of $f(t)$ over K. Then $f(t)$ is *separable* over K if $f(t)$ has no repeated roots in L. For general $f(t)$, we say $f(t)$ is *separable* over K if every irreducible factor in $K[t]$ is separable over K.

All constant polynomials are deemed to be separable.

Definition (formal differentiation)**.** If K is a field, the *formal differentiation* is the K-linear map

$$\begin{aligned} D : K[t] &\to K[t] \\ t^n &\mapsto nt^{n-1} \end{aligned}$$

Notation. Denote $D(f(t))$ by $f'(t)$.

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

$$(f(t)g(t))' = f'(t)g(t) + f(t)g'(t)$$

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

Proof. D is a K-linear map so we only need to check for $f(t) = t^n$. It is left as an exercise.

Let α be a repeated root in a splitting field L. Then $f(t) = (t-\alpha)^2 g(t) \in L[t]$ so $f'(t) = (t-\alpha)^2 g'(t) + 2(t-\alpha)g(t)$ and $f'(\alpha) = 0$. Therefore the minimal polynomial $f_\alpha(t)$ of α in $K[t]$ divides both $f(t)$ and $f'(t)$, so it is a common irreducible factor of $f(t)$ and $f'(t)$.

Conversely, let $h(t)$ be a common irreducible factor of $f(t)$ and $f'(t)$ in $K[t]$. Pick a root $\alpha \in L$ of $h(t)$. Then $f(\alpha) = f'(\alpha) = 0$. Then $f(t) = (t-\alpha)g(t) \in L[t]$ and $f'(t) = (t-\alpha)g'(t) + g(t)$. Since $f'(\alpha) = 0$, we have $(t-\alpha) \mid f'(t)$ so $(t-\alpha) \mid g(t)$. Hence $(t-\alpha)^2 \mid f(t)$. □

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

1. *if* $\operatorname{char} K = 0$ *then $f(t)$ is separable over K,*
2. *if* $\operatorname{char} K = p > 0$ *then $f(t)$ is not separable if and only if $f(t) \in K[t^p]$.*

Proof. By Lemma 2.1, $f(t)$ is not separable if and only if $f(t)$ and $f'(t)$ have a common irreducible factor. But since $f(t)$ is irreducible, the only possible factor is $f(t)$ itself, i.e. $f(t) \mid f'(t)$. $f'(t) = 0$ as it has a smaller degree. But if $f(t) = \sum_{i=0}^{n} a_i t^i$ then $f'(t) = \sum_{i=1}^{n} i a_i t^{i-1}$ so $f'(t) = 0$ if and only if $i a_i = 0$ for all $i \geq 1$. Thus

1. if $\operatorname{char} K = 0$, $f'(t) \neq 0$ for non-constant $f(t)$ so $f(t)$ is separable over K,
2. if $\operatorname{char} K = p > 0$, then if $f'(t) = 0$ we must have $ia_i = 0$ for all $i \geq 1$, i.e. $f(t)$ is not separable if and only if $f(t) \in K[t^p]$.

□

Definition (separable element)**.** If $K \leq L$ is a field extension, we say $\alpha \in L$ is *separable* over K if its minimal polynomial is separable over K.

Definition (purely inseparable)**.** If the minimal polynomial of α is $f_\alpha(t) = (t-\alpha)^n = t^n - \alpha^n$ where n is a power of $\operatorname{char} K$, α is said to be *purely inseparable* over K.

Definition (separable extension)**.** Given $K \leq L$, L is *separable* over K if all elements of L are separable over K.

Example.

1. Let $\mathbb{Q} \leq L$ be an algebraic extension. Then L is separable over $\mathbb{Q}$.
2. Let $L = \mathbb{F}_p(X)$, the field of rational functions in X over $\mathbb{F}_p$. It has $K = \mathbb{F}_p(X^p)$ as a subfield. Then $K \leq L$ is not separable:

   Proof. Observe that if $f(t) = t^p - X^p \in K[t]$ then $f'(t) = 0$. But $t^p - X^p = (t-X)^p \in L[t]$. However, $f(t) \in K[t]$ is irreducible: suppose $f(t) = g(t)h(t) \in K[t] \subseteq L[t]$, we get $g(t) = (t-X)^r$ for some $0 < r < p$ if the factorisation is non-trivial. But this would mean $X^r \in K$. However r and p are coprime so there exist $a, b \in \mathbb{Z}$ such that $ar + bp = 1$, so $X = (X^r)^a (X^p)^b \in K$. Thus we would have $X = u(X^p)/v(X^p)$, absurd.

   Thus $f(t) = t^p - X^p$ is the minimal polynomial of X over K. α is purely inseparable over K and it follows that $K \leq L$ is not separable. □

3. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = m$, a power of $\operatorname{char} \mathbb{F}$, and $f(t) = t^n - 1$ where $n = m - 1$. We know this is separable over $\mathbb{F}_p$ since we saw that $f(t)$ has distinct linear factors in $\mathbb{F}[t]$.

Remark. It is useful to have an alternative approach to separability of field extensions without having to check separability of minimal polynomials for all elements of the larger field. This is where we start thinking about K-homomorphisms.

Lemma 2.3. *Let $M = K(\alpha)$ where α is algebraic over K. Let $f_\alpha(t)$ be the minimal polynomial of α over K. For any field extension $K \leq L$, the number of K-homomorphisms $M \to L$ is equal to the number of distinct roots of $f_\alpha(t)$ in L. Thus*

$$|\operatorname{Hom}_K(M, L)| \leq \deg f_\alpha(t) = |K(\alpha) : K| = |M : K|.$$

Proof. We know that any K-homomorphism $M \to L$ is injective. Since $K(\alpha) \cong K[t]/(f_\alpha(t))$, for any root β of $f_\alpha(t)$ in L, we can define a K-homomorphism

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

Conversely, for any K-homomorphism $\phi : M \to L$, the image $\phi(\alpha)$ must satisfy $f_\alpha(\phi(\alpha)) = 0$. These two maps are inverses to each other. Thus there is a one-to-one correspondence

$$\{K\text{-homomorphism } M \to L\} \leftrightarrow \{\text{root of } f_\alpha(t) \text{ in } L\}.$$

□

Example. Let $K = \mathbb{Q}, L = \mathbb{Q}(\sqrt[3]{2})$. Then $\alpha = \sqrt[3]{2}$ has minimal polynomial $f_\alpha(t) = t^3 - 2$ over $\mathbb{Q}$. There is only one K-homomorphism $M = K(\sqrt[3]{2}) \to L$, i.e. the identity map.

Corollary 2.4. *In the previous lemma, the number of K-homomorphisms $K(\alpha) \to L$ equals to $\deg f_\alpha(t)$ if and only if L is large enough (so that it contains a splitting field for $f_\alpha(t)$) and α is separable over K.*

Proof. Trivial from Lemma 2.3. □

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

$$\{\textit{extension } \phi_1 : M_1 \to L \textit{ of } \phi\} \leftrightarrow \{\textit{root of } \phi(f(t)) \textit{ in } L\}.$$

Remark. Lemma 2.3 is a special case where $M = K$ and $\phi = \mathrm{id}_K$.

Proof. $f(t) \in M[t]$ is irreducible so $\phi(f(t)) \in \phi(M)[t]$ is irreducible. Any extension $\phi_1 : M_1 \to L$ of ϕ produces a root $\phi_1(\alpha)$ of $\phi(f(t))$.

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

$$M_1 = M(\alpha) \cong M[t]/(f(t)) \cong \phi(M)[t]/(\phi(f(t))) \cong \phi(M)(\gamma) \leq L$$

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

Corollary 2.6. *Given L contains a splitting field of $f(t)$, the number of ϕ_1 extending ϕ equals to the number of distinct roots of $f(t)$ in L.*

This equals to $|M_1 : M|$ if and only if α is separable over M.

Corollary 2.7. *Let $K \leq M \leq N$ be finite field extensions and $K \leq L$. Let $\phi : M \to L$ be a K-homomorphism. Then the number of extensions of ϕ to maps $\theta : N \to L$ is less than or equal to $|N : M|$.*

Moreover, such θ exists if L is large enough.

Proof. Pick $\alpha_1, \dots \alpha_n$ so that $N = M(\alpha_1, \dots, \alpha_r)$ and set $M_i = M(\alpha_1, \dots, \alpha_i)$. Thus we have got

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

Use Lemma 2.5 repeatedly, there are at most $|M_1 : M|$ extensions $\phi_1 : M_1 \to L$ of ϕ and $|M_{i+1} : M|$ extensions $\phi_{i+1} : M_{i+1} \to L$ of ϕ_i for $1 \leq i < r$ so by Tower Law the number of extensions $\theta : N \to L$ of ϕ is less than or equal to

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

The last bit come from the proof of Lemma 2.5 since we need L to contain a root. □

Remark. The proof shows that the number of extensions θ of ϕ is $|N : M|$ if and only if L is large enough and α_i is separable over $M(\alpha_1, \dots, \alpha_{i-1})$ for all i.

Theorem 2.8. *Let $K \leq N$ be a field extension with $|N : K| = n$ and $N = K(\alpha_1, \dots, \alpha_i)$, say. Then TFAE:*

1. *$K \leq N$ is separable.*
2. *Each α_i is separable over $K(\alpha_1, \dots, \alpha_{i-1})$.*
3. *If L is large enough then there are exactly n distinct K-homomorphisms $N \to L$.*

Proof.

- 1 $\Rightarrow$ 2: If $K \leq N$ is separable then each α_i is separable over K. As $K \leq K(\alpha_1, \dots, \alpha_{i-1})$, the minimal polynomial of α_i over $K(\alpha_1, \dots, \alpha_{i-1})$ divides that over K. So if the latter has distinct roots in a splitting field then the former does as well.
- 2 $\Rightarrow$ 3: Corollary 2.7.
- 3 $\Rightarrow$ 1: Suppose 3 is true and 1 is false, we shall get a contradiction. Suppose there exists $\beta \in N$ that is not separable over K. Then there are strictly less than $|K(\beta) : K|$ K-homomorphisms $\phi : K(\beta) \to L$. Each ϕ extends to at most $|N : K(\beta)|$ extensions $\theta : N \to L$. Thus there are stricly less than $|N : K(\beta)||K(\beta) : K| = |N : K| = n$ K-homomorphisms $N \to L$. Absurd.

□

Corollary 2.9. *A finite extension is separable if and only if it is separably generated.*

Proof. 1 $\Leftrightarrow$ 2 above. □

Lemma 2.10. *If $K \leq M \leq L$ are finite extensions then $M \leq L$ and $K \leq M$ are both separable if and only if $K \leq L$ is separable.*

Proof. Example sheet. □

Example. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = m$. Then the multiplicative group of order $n = m - 1$ is cyclic. Take a generator α, then $\mathbb{F} = \mathbb{F}(\alpha)$. Since $\alpha^n = 1$, the minimal polynomial of α divides $t^n - 1$.

Since $t^n - 1$ has distinct roots (all the non-zero elements of $\mathbb{F}$), the minimal polynomial of α is separable so $\mathbb{F} = \mathbb{F}(\alpha)$ is separable over $\mathbb{F}$.

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

Proof. If K is a finite field then M is also finite. So we can take α to be generator of the multiplicative group of M, which is cyclic.

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

Take $f(t)$ and $g(t)$ to be the minimal polynomials of α and β over K respectively. Let L be the splitting field for $f(t)g(t)$ over $K(\alpha, \beta)$. The distinct zeros of $f(t)$ in L are $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_a$ and those of $g(t)$ are $\beta_1 = \beta, \beta_2, \ldots, \beta_b$. By separability we know $b = \deg g(t)$. Choose $\lambda \in K$ such that all $\alpha_i + \lambda\beta_j$ are distinct (this is possible since K is infinite). Now we set $\gamma = \alpha + \lambda\beta$ (remember α is α_1 and β is β_1). Let $F(t) = f(\gamma - \lambda t) \in K(\gamma)[t]$. We have $g(\beta) = 0$ and $F(\beta) = f(\alpha) = 0$. Thus $F(t)$ and $g(t)$ have a common zero. Any other common zero would have to be β_j for some $j > 1$. But then $F(\beta_j) = f(\alpha + \lambda(\beta - \beta_j))$. By assumption $\alpha + \gamma(\beta - \beta_j)$ is never an α_i so $f(\beta_j) \neq 0$.

Now separability of $g(t)$ says that the linear factors are all disinct. So $t - \beta$ is a highest common factor of $F(t)$ and $g(t)$ in $L[t]$. However, the minimal polynomial $h(t)$ of β over $K(\gamma)$ divides $F(t)$ and $g(t)$ in $K(\gamma)[t]$, and hence in $L[t]$. This imples $h(t) = t - \beta$, and so $\beta \in K(\gamma)$. Therefore $\alpha = \gamma - \lambda\beta \in K(\gamma)$. So $K(\alpha, \beta) \leq K(\gamma)$. The other direction is obvious. □

Exercise. In our example on page 4 we have $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, i)$. We had intermediate subfields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$ and $\mathbb{Q}(i\sqrt{2})$. If we follow the procedure of the proof of Theorem 2.11, $\alpha = \sqrt{2}, \beta = i, f(t) = t^2 - 2$ and $g(t) = t^2 + 1$. Consider some $\sqrt{2} + \lambda i$ where $\pm\sqrt{2} \pm \lambda i$ are all distinct, for example $\lambda = 1$. The proof show that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

2.2 Trace & Norm

These will also be used in IID Number Fields.

Definition (trace, norm)**.** Let $K \leq M$ be a finite field extension and $\alpha \in M$. Multiplication by a is a K-linear map $\theta_\alpha : M \to M$. The *trace* of α over K is

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}\,\theta_\alpha \in K$$

and the *norm* of α over K is

$$\mathrm{N}_{M/K}(\alpha) = \det \theta_\alpha \in K.$$

Note. Trace and norm depend on the ground field.

Theorem 2.12. *Suppose $f_\alpha(t) = t^s + a_{s-1}t^{s-1} + \cdots + a_0$ is the minimal polynomial of α over K. Let $r = |M : K(\alpha)|$. Then the characteristic polynomial of θ_α is $(f_\alpha(t))^r$ and*

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

Proof. Regard M as a $K(\alpha)$-vector space with basis $\beta_1 = 1, \beta_2, \ldots, \beta_r$. Now take the K-vecotr space basis $1, \alpha, \alpha^2, \ldots, \alpha^{s-1}$ of $K(\alpha)$. Then $\{\alpha^i\beta_j\}_{i<s, j\leq r}$ is a K-vector space basis for M. Multiplication by α in $K(\alpha)$ is represented by the matrix

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

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

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

whose characteristic polynomial is $(f_\alpha(t))^r$. By inspecting the coefficients of the characteristic polynomial we get the trace and norm. □

Theorem 2.13. *Let $K \leq M$ be a finite separable field extension and $|M : K| = n$. Let $\alpha \in M$ and $K \leq L$ large enough so that there are n distinct K-homomorphisms $\sigma_1, \ldots, \sigma_n : M \to L$. Then the characteristic polynomial of $\theta_\alpha : M \to M$ is*

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

Thus

$$\mathrm{Tr}_{M/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$$
$$\mathrm{N}_{M/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

Proof. Let

$$f_\alpha(t) = \prod_{i=1}^{s}(t-\alpha_i) = t^s + a_{s-1}t^{s-1} + \cdots + a_0$$

be the minimal polynomial of α over K in $L[t]$ where L is large enough that $f_\alpha(t)$ splits in L. There are s K-homomorphisms $K(\alpha) \to L$, corresponding to maps sending α to α_i. Each of these extends in $r = |M : K(\alpha)|$ ways to give $K(\alpha)$-homomorphisms $M \to L$. However, each of such extension mapping $\alpha \mapsto \alpha_i$ still does so. So there are r maps sending $\alpha \to \alpha_i$ for each i. Thus if the $n = rs$ distinct K-homomorphism $M \to L$ are $\sigma_1, \ldots, \sigma_n$ then

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

since the sum of roots of $f_\alpha(t)$ is $-a_{s-1}$, and

$$\prod_{i=1}^{n}\sigma_i(\alpha) = ((-1)^s a_0)^r = \mathrm{N}_{M/K}(\alpha).$$

□

Recall from Theorem 2.12 that the characteristic polynomial of θ_α is $(f_\alpha(t))^r$ where $f_\alpha(t)$ is the minimal polynomial of α over K and $r = |M : K(\alpha)|$. The characteristic polynomial is $\prod_{n=1}^{s}(t-\alpha_i)^r$ where α_i are the roots of $f_\alpha(t)$ in a splitting field. We also saw that those root are $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ so the characteristic polynomial is

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

Theorem 2.14. *Let $K \leq M$ be a finite separable extension. We define a K-bilinear form*

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

where xy is the product in M. Then this is non-degenerate. In particular, the K-linear map $\mathrm{Tr}_{M/K} : M \to K$ is non-zero. Thus it is surjective.

Remark. If $K \leq M$ is a finite extension which is not separable then $\mathrm{Tr}_{M/K}$ is always zero. It follows that T is degenerate. See example sheet.

Proof. By Primitive Element Theorem, separability implies that $M = K(\alpha)$ for some α. We have a K-basis $\{\alpha^i\}_{i=0}^{n-1}$ of $K(\alpha)$ where $n = |M : K|$. The K-bilinear form T is represented by the matrix

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

Let L be a splitting field of the minimal polynomial $f(t)$ of α over K. Then $f_\alpha(t) = \prod_{i=1}^{n}(t-\alpha_i)$ with $\alpha_1, \ldots, \alpha_n \in L$. The entries in A are of the form $\mathrm{Tr}_{M/K}(\alpha^\ell)$ which is $\alpha_1^\ell + \cdots + \alpha_n^\ell$ by Theorem 2.13.

Now consider $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$, the *Vandermonde determinant*, is the determinant of the *Vandermonde matrix*

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}$$

Observe that $A_{ij} = \sum_n \alpha_n^{i+j-2}, V_{ij} = \alpha_j^{i-1}$ so

$$\begin{aligned} (VV^T)_{ik} &= V_{ij}V_{kj} \\ &= \alpha_j^{i-1}\alpha_j^{k-1} \\ &= \sum_n \alpha_n^{i+k-2} \\ &= A_{ik} \end{aligned}$$

so $VV^T = A$. Thus $0 \neq D = \Delta^2 = |VV^T| = |A|$. Thus A is non-singular and therfore the bilinear form T is non-degenerate. □

Remark. We will meet D again shortly. It is the *discriminant* of the polynomial $f_\alpha(t)$.

2.3 Normal Extensions

We met this definition before:

> **Definition** (normal extension)**.** An extension $K \leq M$ is *normal* if for every $\alpha \in M$, the minimal polynomial $f_\alpha(t)$ of α over K splits over M.

> **Theorem 2.15.** *Let $K \leq M$ be a finite field extension. Then $K \leq M$ is normal if and only if M is the splitting field for some $f(t) \in K[t]$.*

Proof.

- $\Rightarrow$: suppose $K \leq M$ is normal. Pick $\alpha_1, \dots, \alpha_r \in M$ such that $M = K(\alpha_1, \dots, \alpha_k)$. Let $f_{\alpha_i}(t)$ be the minimal polynomial of α_i over K. Let $f(t) = \prod_{n=1}^k f_{\alpha_i}(t)$.

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

- $\Leftarrow$: suppose M is a splitting field for $f(t)$ over K. Then $M = K(\beta_1, \dots, \beta_m)$ where β_j are the roots of $f(t)$ over M. Take $\alpha \in M$. Let $f_\alpha(t)$ be the minimal polynomial of α over K. Let $M \leq L$ be large enough so that $f_\alpha(t)$ splits over L.

  Now consider a K-homomorphism $\phi : M \to L$: $\phi(\beta_j)$ is also a root of $f(t)$ and is therefore one of the β_j. Injectivity of K-homomorphisms implies

that ϕ permutes β_j. However, $M = K(\beta_1, \dots, \beta_m)$ and so ϕ is determined by the images of β_j, thus $\phi(M) = M$.

However, if α_i is a root of $f_\alpha(t)$ in L, then there is a K-homomorphism

$$\begin{aligned} K(\alpha) &\to K(\alpha_i) \\ \alpha &\mapsto \alpha_i \end{aligned}$$

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

□

Remark. As the same for separability, being normal is equivalent to being normally generated. We will show in example sheet that $K \leq L$ is a normal and finite extension if and only if $L = K(\alpha_1, \dots, \alpha_r)$ with the minimal polynomial of each adjoined element splitting over L.

Definition (K-automorphism group)**.** Let $K \leq M$ be a finite extension. Its *K-automorphism group* is

$$\mathrm{Aut}_K(M) = \mathrm{Hom}_K(M, M).$$

From before we know that such K-automorphisms are isomorphisms and thus have inverses (well, it name says so).

Lemma 2.16.

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

Proof. Corollary 2.7. □

Theorem 2.17. *Let $K \leq M$ be a finite field extension, then*

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

if and only if the extension is both normal and separable.

Definition (Galois extension)**.** A finite field extension that is normal and separable is a *Galois extension*.

Definition (Galois group)**.** Let $K \leq M$ be a Galois extension. Then the K-automorphism group of M is the *Galois group* of M over K, denoted by

$$\mathrm{Gal}(M/K).$$

Remark. Some authors use the term "Galois group" as a synonym for automorphism group even when the extension is not Galois.

Proof of Theorem 2.17. Suppose $|\operatorname{Aut}_K(M)| = |M : K| = n$. Let $M \leq L$ be large enough. The n distinct K-automorphisms $\phi : M \to M$ extend to n K-homomorphisms $\phi : M \to L$ and Theorem 2.8 says that M is separable over K.

For normality, pick $\alpha \in M$ with minimal polynomial $f_\alpha(t)$ over K. Take $M = K(\alpha_1, \ldots, \alpha_m)$ as in the proof of Corollary 2.7 with $\alpha = \alpha_1$ and $L = M$. We only get $|M : K|$ extensions of the inclusion $K \hookrightarrow M$ if each inequality in the proof is an equality. In particular, we need the number of K-homomorphisms $K(\alpha_1) \to M$ to be $|K(\alpha_1) : K|$. But then root correspondence says we have $|K(\alpha) : K|$ distinct roots of $f_\alpha(t)$ in M. Thus $f_\alpha(t)$ splits over M.

Conversely, suppose $K \leq M$ is separable and normal. Then for $K \leq M \leq L$ with L large enough, separability implies there are $|M : K|$ K-homomorphisms $\phi : M \to L$ by Theorem 2.8. However, $K \leq M$ is normal implies that it is the splitting field for some polynomial $f(t) \in K[t]$ and thus $M = K(\alpha_1, \ldots, \alpha_n)$ where $f(t) = \prod_{i=1}^{n}(t - \alpha_i)$. Note that $\phi(\alpha_j)$ is also a root of $\phi(f(t)) = f(t)$, and is therefore one of the α_j. Thus $\phi(M) = M$. Thus $|\operatorname{Aut}_K(M)| = |M : K|$. □

Remark. In the previous proof we have shown that if $K \leq M \leq L$, $\phi \in \operatorname{Hom}_K(M, L)$ and $K \leq M$ is normal then $\phi(M) = M$.

Example.

1. Consider $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, i)$, which is Galois:

$$\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) = \langle \sigma : \sqrt{2} \mapsto -\sqrt{2}, \tau : i \mapsto -i \rangle \cong C_2 \times C_2.$$

   All non-identity elements have order 2.

2. Let $f(t) = t^3 - 2$. The splitting field of $f(t)$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is a primitive cubic root of unity. Thus $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$ is Galois with $|\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}|) = |\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}| = 6$. The Galois group contains

$$\sigma : \sqrt[3]{2} \mapsto \omega\sqrt[3]{2},\ \omega \mapsto \omega$$
$$\tau : \sqrt[3]{2} \mapsto \sqrt[3]{2},\ \omega \mapsto \omega^2 \text{ (complex conjugation)}$$

   and is generated by these two elements. It is an exercise to show that $\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong D_6 \cong S_3$.

3 Fundamental Theorem of Galois Theory

Definition (fixed field)**.** Let $K \leq L$ be a field extension and $H \leq \mathrm{Aut}_K(L)$. The *fixed field* of H is

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

The fixed field is a field and $K \leq L^H \leq L$.

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

1. *There is a one-to-one correspondence*

$$\left\{ \begin{array}{c} \text{intermediate subfield} \\ K \leq M \leq L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroup} \\ H \leq \mathrm{Gal}(L/K) \end{array} \right\}$$
$$M \mapsto \mathrm{Aut}_M(L)$$
$$L^H \hookleftarrow H$$

2. *H is a normal subgroup of $\mathrm{Gal}(L/K)$ if and only if $K \leq L^H$ is normal if and only if $K \leq L^H$ is Galois.*

3. *If $H \trianglelefteq \mathrm{Gal}(L/K)$ then the map*

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

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

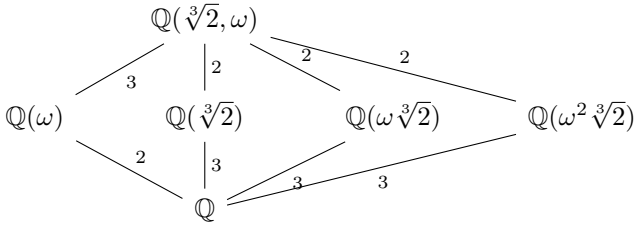
Remark.

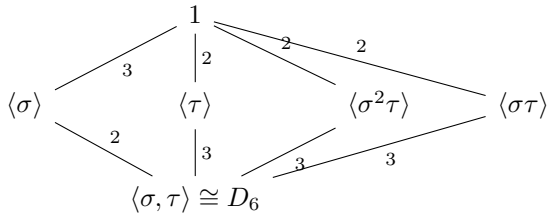
1. Observe that $M \leq L$ is Galois and so we could have written $\mathrm{Gal}(L/M)$ instead of $\mathrm{Aut}_M(L)$. To see this,
   - separability: follows from Lemma 2.10.
   - normality: if $\alpha \in L$ then the minimal polynomial of α over M divides the minimal polynomial of α over K. But the latter splits over L (see example sheet).
2. If $K \leq M$ is normal then the remark after proof of Theorem 2.17 says if $\sigma : L \to L$ then $\sigma(M) = M$ and so we can talk about the restriction of α to M giving an automorphism of M.

Example.

1. $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, i)$. We saw in example on page 4 the lattices of intermediate subfields and subgroups $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}) \cong C_2 \times C_2$ which is abelian. Thus all subgroups are normal and all intermediate subfields are normal extensions of $\mathbb{Q}$.

2. $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$.





The subgroup H of order 3 is normal but those of order 2 are not so the map $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$, i.e. $D_6 \to C_2$, generated by conjugation has kernel $\langle\sigma\rangle$.

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

Remark. This implies one way of Galois correspondence:

$$H \mapsto L^H \mapsto \mathrm{Gal}(L/L^H) = H.$$

Proof. Take $\alpha \in L$. We first show that $|M(\alpha) : M| \leq |H|$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be the distinct images of α under H, i.e. $\{\phi(\alpha) : \phi \in H\}$. Define $g(t) = \prod_{i=1}^{n}(t - \alpha_i)$. Each ϕ induces an endomorphism on $L[t]$ under which $g(t)$ is invariant since ϕ permutes the α_i. Thus the coefficients lie in $L^H = M$ and so $g(t) \in M[t]$. By definition $g(\alpha) = 0$ since α is one of the α_i. Hence the minimal polynomial $f_\alpha(t)$ of α over M divides $g(t)$. Thus

$$|M(\alpha) : M| = \deg f_\alpha(t) \leq \deg g(t) \leq |H|.$$

This step shows that α is algebraic over M and $f_\alpha(t)$ is separable since $g(t)$ is. Thus $M \leq L$ is a separable extension.

Next we show that $M \leq L$ is a simple extension. Pick $\alpha \in L$ with $|M(\alpha) : M|$ maximal. We will show that $L = M(\alpha)$ for this α. Suppose $\beta \in L$. Then $M \leq M(\alpha, \beta)$ is finite and separably generated and hence is a finite separable extension. By Primitive Element Theorem $M(\alpha, \beta) = M(\gamma)$ for some γ. But then

$$M \leq M(\alpha) \leq M(\gamma)$$

so by the maximality of $|M(\alpha) : M|$, $M(\alpha) = M(\gamma)$. Thus $\beta \in M(\gamma) = M(\alpha)$ so $L = M(\alpha)$.

It follows that $|L : M| \leq |H|$.

Finally, $H \leq \mathrm{Aut}_M(L)$ so

$$|L : M| = |M(\alpha) : M| \leq |H| \leq |\mathrm{Aut}_M(L)| \leq |L : M|$$

so we must have equality throughtout, i.e. $|L : M| = |\mathrm{Aut}_M(L)| = |H|$ so $M \leq L$ is a finite Galois extension and $H = \mathrm{Gal}(L/M)$. □

Theorem 3.3. *Let $K \leq L$ be a finite field extension. TFAE:*

1. *$K \leq L$ is Galois,*
2. *$L^H = K$ where $H = \mathrm{Aut}_K(L)$.*

Remark. The theorem allows some authors to give yet another definition of a Galois extension.

Proof.

1. $1 \Rightarrow 2$: Let $M = L^H$ where $H = \mathrm{Aut}_K(L)$. By Artin $M \leq L$ is a Galois extension. Now we have two Galois extensions, giving the equalities

$$\begin{aligned} |H| &= |\mathrm{Gal}(L/K)| = |L : K| \\ &= |\mathrm{Gal}(L/M)| = |L : M| \end{aligned}$$

   As $K \leq L^H = M$, equality.

2. $2 \Rightarrow 1$: Artin.

□

Proof of Fundamental Theorem of Galois Theory.

1. Composing the maps

$$\begin{aligned} H &\mapsto L^H \\ M &\mapsto \mathrm{Gal}(L/M) \end{aligned}$$

   gives $H \to H$ by Artin. Composition the other way $M \mapsto \mathrm{Gal}(L/M) \mapsto L^H$ where $H = \mathrm{Gal}(L/M)$ gives M by Theorem 3.3.

2. Take $H \leq \mathrm{Gal}(L/K)$. Then for $\phi \in \mathrm{Gal}(L/K)$, $L^{\phi H \phi^{-1}} = \phi(L^H)$ so by 1 $H \trianglelefteq \mathrm{Gal}(L/K)$ if and only if $\phi(L^H) = L^H$. Let $M = L^H$. We will show that $K \leq M$ is normal if and only if $\phi(M) = M$ for every $\phi \in \mathrm{Gal}(L/K)$:

   - $\Rightarrow$: remark 2 after Theorem 3.1.
   - $\Leftarrow$: suppose $\phi(M) = M$ for all $\phi \in \mathrm{Gal}(L/K)$. Pick $\alpha \in M$ and let $f_\alpha(t)$ be its minimal polynomial over K. We take β as a root for $f_\alpha(t)$ in L (which is possible by normality). Then there is a K-homomorphism

$$\begin{aligned} K(\alpha) &\to K(\beta) \\ \alpha &\mapsto \beta \end{aligned}$$

     This extends to a K-homomorphism $\phi : L \to L$. Since we assume $\phi(M) = M$, $\phi(\alpha) = \beta \in M$. Thus $K \leq M$ is normal.

Note that $K \leq M$ is separable since $K \leq M \leq L$ and $K \leq L$ is separable. Thus $K \leq M$ is Galois.

3. By remark 2 after Theorem 3.1, the restriction map $\theta : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L^H/K)$ is well-defined. Surjectivity follows from being able to extend a K-homomorphism $L^H \to L^H \leq L$ to a K-homomorphism $L \to L$. Clearly $H \leq \ker\theta$. However

$$\begin{aligned}\frac{|L:K|}{|\ker\theta|} &= \frac{|\mathrm{Gal}(L/K)|}{|\ker\theta|} \\ &= |\mathrm{Gal}(L^H/K)| \text{ by surjectivity of } \theta \\ &= |L^H : K| \text{ since } K \leq L^H \text{ is Galois} \\ &= \frac{|L:K|}{|L:L^H|} \text{ by Tower Law}\end{aligned}$$

Then

$$|\ker\theta| = |L:L^H| = |\mathrm{Gal}(L/L^H)| = |H|$$

by Artin. Thus $\ker\theta = H$.

□

3.1 Galois Group of Polynomials

Definition (Galois group)**.** Let $f(t) \in K[t]$ be a separable polynomial and $K \leq L$ with L a splitting field for $f(t)$. Then the *Galois group* of $f(t)$ over K is

$$\mathrm{Gal}(f) = \mathrm{Gal}(L/K).$$

Since L is a splitting field for $f(t)$, $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(t)$ in L. Observe that if $\phi \in \mathrm{Gal}(L/K)$ it maps bijectively roots of $f(t)$ to itself. Thus ϕ permutes the α_i.

Moreover if ϕ fixes each α_i it also fixes all elements of L and so it is the identity map. Thus $\mathrm{Gal}(f)$ may be regarded as a permutation group of the n roots, so in particular admitting a permutation representation in S_n.

Lemma 3.4. *Suppose separable $f(t) = g_1(t)\cdots g_s(t)$ with $g_i(t)$ irreducible in $K[t]$ is a factorisation in $K[t]$. Then the orbits of* $\mathrm{Gal}(f)$ *acting on the roots of $f(t)$ correspond to the factors $g_j(t)$: two roots are in the same orbit if and only if they are roots of the same $g_i(t)$.*

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

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

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

$$K(\alpha_k) \cong K[t]/(g_j(t)) \cong K(\alpha_\ell) \leq L$$

Denote by ϕ_0 the isomorphsim $K(\alpha_k) \to K(\alpha_\ell)$. ϕ_0 extends to $\phi \in \mathrm{Gal}(L/K)$. Thus α_k and α_ℓ are in the same orbit. □

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

n	
2	$S_2 \cong C_2$
3	$A_3 \cong C_3, S_3$
4	C_4, V_4, D_8, A_4, S_4
5	$C_5, D_{10}, H_{20}, A_5, S_5$

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

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

$$\mathrm{Gal}(f) \cong S_p.$$

Proof. $\mathrm{Gal}(f)$ acts on the p distinct roots of $f(t)$ in a splitting field L of $f(t)$ (in $\mathbb{C}$). By Lemma 3.4 the irreducibility of $f(t)$ implies that $\mathrm{Gal}(f)$ acts transitively on p roots so by orbit-stabiliser $p \mid |\mathrm{Gal}(f)|$ but

$$|\mathrm{Gal}(f)| \leq |S_p| = p!$$

and so $\mathrm{Gal}(f)$ has a Sylow p-subgroup of order p, necessarily cyclic. Thus $\mathrm{Gal}(f)$ contains a p-cycle. Supposition that there are exactly 2 non-real roots gives that complex conjugation yields a transposition in $\mathrm{Gal}(f)$. The p-cycle and the transposition generate S_p. □

Example. Let $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$, then claim $\mathrm{Gal}(f) \cong S_5$:

Proof. $f(t)$ is irreducible by Eisenstein with $p = 3$. We want to show that $f(t)$ has 3 real roots (so 2 non-real roots) and apply the previous theorem.

Now we apply knowledge from analysis:

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

and $f'(t) = 5t^4 - 6$ which has two real roots. Thus by Intermediate Value Theorem there are 3 real roots while by Rolle's Theorem there are at most 3 real roots. □

Definition (discriminant)**.** Let $f(t) \in K[t]$ have distinct roots $\alpha_1, \ldots, \alpha_n$ (in a splitting field) ($f(t)$ need not be irreducible). Set $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Then the *discriminant* of f is

$$D(f) = \Delta^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(\alpha_i - \alpha_j).$$

Remark. We have already met this in the proof of Theorem 2.14.

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

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

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

If $\sigma \in G$ then $\sigma(\Delta) = (\operatorname{sgn}\sigma)\Delta$ where we are regarding G as a subgroup of S_n and sgn is the signature (this is where we need $\operatorname{char} K \neq 2$). Thus if $G \leq A_n$ we got that Δ is fixed by all $\sigma \in G$. Thus $\Delta \in K = L^G$.

On the other hand if $G \not\leq A_n$ we get $\sigma(\Delta) = -\Delta$ if σ is odd and so $\Delta \notin K = L^G$. Finally note that if D has square roots they must be $\pm\Delta$. □

Example.

1. $n = 2$: $f(t) = t^2 + bt + c = (t - \alpha_1)(t - \alpha_2)$ has discriminant
$$D(f) = (\alpha_1 - \alpha_2)^2 - (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = b^2 - 4c$$
2. $n = 3$: $f(t) = t^3 + ct + d$ has discriminant
$$D(t) = -4c^3 - 27d^2$$

> **Remark.** Any general monic cubic $g(t)$ can be put into this form by a suitable substitution $f(t) = g(t_1 + \lambda)$ for suitable λ. Note $D(f) = D(g)$.

Example.

- $f(t) = t^3 - t - 1 \in \mathbb{Q}[t]$ irreducible in $\mathbb{Z}[t]$ since irreducible mod 2. $D(f) = -23$ which is not a square in $\mathbb{Q}$. Thus $\mathrm{Gal}(f) \cong S_3$.
- $f(t) = t^3 - 3t - 1 \in \mathbb{Q}[t]$ irredicible since irreducible mod 2. $D(f) = 81$ which is a square so $\mathrm{Gal}(f) \cong A_3$.

Now we move on to irreducible quartics. We saw that the possible Galois groups are
$$V_4, A_4, C_4, D_8, S_4$$
with the first two being subgroups of A_4. From looking at the discriminant one gets information as whether the group is one of V_4, A_4 or one of C_4, D_8, S_4. We need further methods to pin down which group we are dealing with.

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

Proof. See Remark after discussion about Galois groups over finite fields. The fact that $\mathrm{Gal}(\bar{f}) \hookrightarrow \mathrm{Gal}(f)$ is from IID Number Fields. Look at Tony Scholl's teaching page on Galois Theory. □

Example. Given a quartic of the form $f(t) = t^4 + dt + e$, its discriminant is $D(t) = -27d^4 + 256e^3$. Consider $f(t) = t^4 - t - 1$, irreducible since irreducible mod 2 and $D(f) = -283$ which is not a square.

Consider mod 7,

$$\overline{f}(t) = t^4 - t - 1 = (t+4)(t^3 + 3t^2 + 2t + 5)$$

the second factor is irreducible over $\mathbb{F}_7$ since it has no roots in $\mathbb{F}_7$. By Theorem 3.8 $\mathrm{Gal}(f)$ contains an element of cycle type $(1, 3)$, i.e. a 3-cycle. We deduce that $\mathrm{Gal}(f) \cong S_4$ as it is the only transitive subgroup of S_4 that contains an odd permutation and a 3-cycle.

3.2 Galois Theory of Finite Fields

Recall what we already know from **??**: a finite field $\mathbb{F}$ is of characteristic $p > 0$ where p is a prime and $|\mathbb{F}| = p^r$ for some r. The multiplicative group of $\mathbb{F}$ is cyclic. It is a splitting field for $t^n - 1$ over $\mathbb{F}_p$ where $n = p^r - 1$. By the uniqueness of splitting fields this is unique. Observe we could also describe $\mathbb{F}$ as the splitting field of $t^{p^r} - t$ over $\mathbb{F}_p$.

What we haven't shown yet is that for any p^r there is a field with $|\mathbb{F}| = p^r$.

Definition (Frobenius automorphism)**.** Let $\mathbb{F}$ be a finite field of characteristic p. The *Frobenius automorphism* of $\mathbb{F}$ is

$$\begin{aligned} \phi_p : \mathbb{F} &\to \mathbb{F} \\ \alpha &\mapsto \alpha^p \end{aligned}$$

Remark. $(\alpha + \beta)^p = \alpha^p + \beta^p$ since all terms in binomial expansion is divisible by p. Also $\mathbb{F}_p$ is fixed under this so this is an $\mathbb{F}_p$-automorphism.

Since $t^{p^r} - t$ splits as a product of linear factors $(t - \alpha)$ in $\mathbb{F}$, we have that $\mathbb{F}_p \leq \mathbb{F}$ is a Galois extension and so we consider $G = \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$. It has order r since $|\mathbb{F} : \mathbb{F}_p| = r$.

Theorem 3.9 (Galois group of finite fields)**.** *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = p^r$. Then $\mathbb{F}_p \leq \mathbb{F}$ is a Galois extension with*

$$\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) = \langle \phi_p \rangle \cong C_r.$$

Proof. It remains to show that the order of Frobenius automorphism is r. Suppose $\phi_p^s = \mathrm{id}$. Then $\alpha^{p^s} = \alpha$ for all $\alpha \in \mathbb{F}$. But $t^{p^s} - t$ has at most p^s roots in $\mathbb{F}$. So we conclude $s \geq r$. Observe that $\phi_p^r = \mathrm{id}$ since $\alpha^{p^r} = \alpha$ for all $\alpha \in \mathbb{F}$. □

Now apply Fundamental Theorem of Galois Theory,

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

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

But we know all about subgroups of a cyclic group with generator ϕ_p with order r. There is exactly one group of order s for each $s \mid r$ generated by $\phi_p^{r/s}$. The corresponding intermediate subfields are the fixed fields $\mathbb{F}^{\langle \phi_p^{r/s} \rangle}$ and $|\mathbb{F} : \mathbb{F}^{\langle \phi_p^{r/s} \rangle}| = s$. By Tower Law $|\mathbb{F}^{\langle \phi_p^{r/s} \rangle} : \mathbb{F}_p| = r/s$.

Observe that all subgroups of cyclic groups are normal and therefore all our intermediate fields are normal extensions of $\mathbb{F}_p$. Thus $\mathrm{Gal}(\mathbb{F}^{\langle\phi_p^{r/s}\rangle}/\mathbb{F}_p) \cong \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)/H$ where $H = \langle\phi_p^{r/s}\rangle$.

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

Proof. Set $n = r/s$. □

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

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

Remark (mod p reduction)**.** We will discuss in IID Number Fields that $\mathrm{Gal}(\overline{f}) \hookrightarrow \mathrm{Gal}(f)$ if $f(t) \in \mathbb{Z}[t]$. We factorised $\overline{f}(t) = \overline{g_1}(t) \cdots \overline{g_s}(t)$ as a product of irreducibles (actually $\overline{g_s}(t)$ lives in p-adic integers). We knew from Lemma 3.4 that the orbits of $\mathrm{Gal}(\overline{f})$ correspond to the factorisation. We know $\mathrm{Gal}(\overline{f})$ is cyclic generated by the Frobenius map, which must have cyclic type $(n_1, \ldots, n_s)$ where $n_j = \deg \overline{g_j}(t)$.

4 Cyclotomic and Kummer Extensions, Cubics and Quartics, Solution by Radicals

4.1 Cyclotomic Extensions

Definition (cyclotomic extension)**.** Suppose $\operatorname{char} K = 0$ or p is prime where $p \nmid m$. The *mth cyclotomic extension* of K is the splitting field L of $t^m - 1$.

Remark. $f(t) = t^m - 1$ and $f'(t) = mt^{m-1}$ have no common roots and so the roots of $f(t)$ are distinct, which are the mth roots of unity. They form a finite subgroup μ_m of $L^\times$ and hence by (1.28) **??** a cyclic group $\langle\zeta\rangle$. Thus $L = K(\zeta)$ is a simple extension.

Definition (primitive root of unity)**.** An element $\zeta \in \mu_m$ is a *primitive* mth root of unity if $\mu_m = \langle\zeta\rangle$.

Choosing a primitive mth root of unity determines an isomorphism

$$\mu_m \to \mathbb{Z}/m\mathbb{Z}.$$

Note that ζ^i is a generator of μ_m if and only if $(i, m) = 1$ and so the primitive roots of unity correspond to elements of $(\mathbb{Z}/m\mathbb{Z})^\times$, the unit group of $\mathbb{Z}/m\mathbb{Z}$.

Now consider Galois groups of cyclotomic extensions. We will see that they must be abelian. Observe $f(t) = t^m - 1$ is separable and so the extension $K \leq L$ is Galois. Let $G = \operatorname{Gal}(L/K)$. An element $\sigma \in G$ sends a primitive mth root of unity ζ to another mth root of unity ζ^i where $(i, m) = 1$. Then $\zeta \mapsto \zeta^i$ determines a K-homomorphism

$$K(\zeta) \to K(\zeta)$$

which is an injective map.

Definition. Define

$$\begin{aligned} \theta : G &\to (\mathbb{Z}/m\mathbb{Z})^\times \\ \sigma &\mapsto i \text{ where } \sigma(\zeta) = \zeta^i \end{aligned}$$

It is a group homomorphism since if $\sigma(\zeta) = \zeta^i, \phi(\zeta) = \zeta^j$ then $(\sigma\phi)(\zeta) = \sigma(\zeta^j) = \zeta^{ij}$.

Thus G is abelian and we regard G as a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$.

Definition (cyclotomic polynomial)**.** The *mth cyclotomic polynomial* is

$$\Phi_m(t) = \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} (t - \zeta^i),$$

the product of the linear factors of $t^m - 1$ corresponding to the primitive mth roots of unity.

Remark.

$$\begin{aligned} f(t) &= t^m - 1 \\ &= \prod_{i \in \mathbb{Z}/m\mathbb{Z}} (t - \zeta^i) \\ &= \prod_{d|m} \Phi_d(t) \end{aligned}$$

Example. Take $K = \mathbb{Q}$, then

$$\begin{aligned} \Phi_1(t) &= t - 1 \\ \Phi_2(t) &= t + 1 \\ \Phi_3(t) &= t^2 + t + 1 \\ \Phi_4(t) &= t^2 + 1 \end{aligned}$$

and from which we can deduce that

$$\Phi_8(t) = t^4 + 1$$

since $t^8 - 1 = (t-1)(t+1)(t^2+1)(t^4+1)$.

Lemma 4.1.

- $\Phi_m(t) \in \mathbb{Z}[t]$ *if* $\operatorname{char} K = 0$ *(i.e.* $\mathbb{Q} \hookrightarrow K$*).*
- $\Phi_m(t) \in \mathbb{F}_p[t]$ *if* $\operatorname{char} K = p$ *(i.e.* $\mathbb{F}_p \hookrightarrow K$*).*

Proof. By induction on m. If $m = 1$ then done.

For $m > 1$, consider

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

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

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

□

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

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

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

Proof. We know from Corollary 3.10 that G is generated by $\alpha \mapsto \alpha^{p^n}$ so

$$\theta(G) = \theta(\langle \alpha \mapsto \alpha^{p^n} \rangle) = \langle p^n \rangle = \langle q \rangle \leq (\mathbb{Z}/m\mathbb{Z})^\times.$$

□

Remark. If $(\mathbb{Z}/m\mathbb{Z})^\times$ is not cyclic then θ is not surjective for any finite field and $\Phi_m(t)$ is reducible over $\mathbb{F}$.

Example. Let $\mathbb{F} = \mathbb{F}_3$. Then

$$\Phi_8(t) = t^4 + 1 = (t^2 + t - 1)(t^2 - t - 1)$$

so $t^8 - 1$ factorises as a product of linear and quadratic polynomials mod 3. So $L = \mathbb{F}_9$, the unique field of order 9, whose multiplicative group is isomorphic to C_8. As $|\mathrm{Gal}(L/\mathbb{F}_3)| = 2$, it is isomorphic to C_2. But

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \cong C_2 \times C_2$$

so θ is not surjective and $\Phi_8(t)$ is reducible.

So far we have worked exclusively with finite fields with non-zero characteristic. The following theorem is a result regarding $\mathbb{Q}$:

Theorem 4.4. *For all $m > 0$, $\Phi_m(t)$ is irreducible in $\mathbb{Z}[t]$ and hence in $\mathbb{Q}[t]$. Thus θ is an isomorphism and*

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$$

where ζ is a primitive mth root of unity.

Remark. We already knew this when $m = p$ for p prime by substitution and Eisenstein.

Proof. Gauss' Lemma implies that irreducibility in $\mathbb{Z}[t]$ gives irreducibility in $\mathbb{Q}[t]$. Lemma 4.2 says that irreducibility corresponds to surjectivity of θ. Thus it is left to show that $\Phi_m(t)$ is irreducible in $\mathbb{Z}[t]$.

Suppose not and $\Phi_m(t) = g(t)h(t)$ in $\mathbb{Z}[t]$, with $g(t)$ irreducible and monic with $\deg g(t) < \deg \Phi_m(t)$. Let $\mathbb{Q} \leq L$ be the mth cyclotomic extension and ζ be a primitive mth root and unity and also a root of $g(t)$. Claim that if $p \nmid m$ and p is prime then ζ^p is also a root of $g(t)$ in L:

Proof. Suppose not, then ζ^p is also a primitive mth root of unity (since $p \nmid m$) and a root of $\Phi_m(t)$. The supposition implies that ζ^p is a root of $h(t)$. Define

$$r(t) = h(t^p),$$

then $r(\zeta) = 0$. But $g(t)$ is the minimal polynomial of ζ over $\mathbb{Q}$ and so $g(t) \mid r(t)$ in $\mathbb{Q}[t]$. By Gauss' Lemma $r(t) = g(t)s(t)$ with $s(t) \in \mathbb{Z}[t]$. Now reduce mod p,

$$\overline{r}(t) = \overline{g}(t)\overline{s}(t).$$

But $\overline{r}(t) - \overline{h}(t^p) = (\overline{h}(t))^p$. If $\overline{a}(t)$ is any irreducible factor of $\overline{g}(t)$ in $\mathbb{F}_p[t]$ then $\overline{a}(t) \mid (\overline{h}(t))^p$ and so $\overline{a}(t) \mid \overline{h}(t)$. But then $(\overline{a}(t))^2 \mid \overline{g}(t)\overline{h}(T) = \overline{\Phi}_m(t)$. So $\overline{\Phi}_m(t)$ has a repeated root and thus $t^m - 1$ has repeated roots mod p. Absurd. □

So the claim is true. Now consider a root γ of $h(t)$. It is also a primitive mth root of unity and $\gamma = \zeta^i$ for some i coprime with m. Factorise it as $i = p_1 \cdots p_k$ with p_j prime and not necessarily distinct and $p_j \nmid m$. Apply the claim repeatedly, we get that γ is also a root of $g(t)$ and so $\Phi_m(t)$ has a repeated root. Absurd. Thus $\Phi_m(t)$ is irreducible over $\mathbb{Q}$. □

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

Definition (abelian extension)**.** An extension $K \leq L$ is *abelian* if the extension is Galois and $\mathrm{Gal}(L/K)$ is abelian.

Example.

1. We saw in Corollary 3.10 that for finite fields $\mathbb{F} \leq L$ is cyclic.
2. Cyclotomic extensions are abelian.
3. Theorem 4.4 says $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and so if $m = 8$, $\mathbb{Q} \leq \mathbb{Q}(\zeta)$ is a non-cyclic abelian extension.

4.2 Kummer Theory

Rather than consider the mth root of unity, in this section we consider Galois extensions $K \leq L$ where L is the splitting field of a polynomial of the form $t^m - \lambda$ where $\lambda \in K$.

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

Remark. We have the following Galois correspondence

$$\text{cyclic} \left\{ \begin{array}{cc} L & 1 \\ | & | \\ K(\zeta) & \mathrm{Gal}(L/K(\zeta)) \\ | & | \\ K & \mathrm{Gal}(L/K) \end{array} \right.$$

with $\mathrm{Gal}(L/K(\zeta)) \trianglelefteq \mathrm{Gal}(L/K)$. By Fundamental Theorem of Galois Theory

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(\zeta)) \cong \mathrm{Gal}(K(\zeta)/K)$$

which is abelian.

Proof. Since $t^m - \lambda$ and mt^{m-1} are coprime, we know that $t^m - \lambda$ has distinct roots, say $\alpha_1, \dots \alpha_m$ in the splitting field L. Thus $K \leq L$ is Galois. Since $(\alpha_i \alpha_j^{-1})^m = \lambda\lambda^{-1} = 1$, the elements

$$\alpha_1\alpha_1^{-1} = 1, \alpha_2\alpha_1^{-1}, \dots, \alpha_m\alpha_1^{-1}$$

are m distinct mth roots of unity in L and so

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

where $\beta = \alpha_1$ and ζ is a primitive mth root of unity. Thus

$$L = K(\zeta, \beta).$$

Let $\sigma \in \mathrm{Gal}(L/K(\zeta))$. It is determined by its action on β. Note that $\sigma(\beta)$ is also a root of $t^m - \lambda$ so $\sigma(\beta) = \zeta^{j(\sigma)}\beta$ where $0 \leq j(\sigma) < m$. Also if $\sigma, \tau \in \mathrm{Gal}(L/K(\zeta))$ then

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

where the second inequality comes from the fact that ζ is fixed by τ. Thus there is a group homomorphism

$$\begin{aligned} \Theta : \mathrm{Gal}(L/K(\zeta)) &\to \mathbb{Z}/m\mathbb{Z} \\ \sigma &\mapsto j(\sigma) \end{aligned}$$

Note that $j(\sigma) = 0$ only if σ is the identity and so Θ is injective. Thus $\mathrm{Gal}(L/K(\zeta))$ is isomorphic to a subgroup of $\mathbb{Z}/m\mathbb{Z}$, so a cyclic group of order dividing m.

Finally,

$$|L : K(\zeta)| = |\mathrm{Gal}(L/K(\zeta))| \leq m$$

with equality precisely when the action of $\mathrm{Gal}(L/K(\zeta))$ is transitive on the roots and that is when $t^m - \lambda$ is irreducible over $K(\zeta)$ by Lemma 3.4. □

Example.

1. $f(t) = t^6 + 3$ over $\mathbb{Q}$. Let $\zeta = -\omega$ be a primitive 6th root of unity where ω is a primitive cubic root of unity. Then

   $$\mathbb{Q}(\zeta) = \mathbb{Q}(\omega) = \mathbb{Q}(\frac{1}{2}(1+\sqrt{-3})) = \mathbb{Q}(\sqrt{-3}).$$

   $f(t)$ is irreducible over $\mathbb{Q}$ by Eisenstein with 3. However over $\mathbb{Q}(\zeta) = \mathbb{Q}(\sqrt{-3})$ $f(t)$ factorises as

   $$f(t) = (t^3 + \sqrt{-3})(t^3 - \sqrt{-3})$$

   so the Galois group of the splitting field L of $f(t)$ over $\mathbb{Q}(\zeta)$ is a proper subgroup of $\mathbb{Z}/6\mathbb{Z}$. We have the following Galois correspondence:

   $$\begin{array}{ccc} L & 1 & \\ | & | & 3 \\ \mathbb{Q}(\zeta) & \mathrm{Gal}(L/\mathbb{Q}(\zeta)) & \\ | & | & 2 \\ \mathbb{Q} & \mathrm{Gal}(L/\mathbb{Q}) & \end{array}$$

Note that

$$\begin{aligned}\mathrm{Gal}(L/\mathbb{Q}(\zeta)) &\cong \mathbb{Z}/3\mathbb{Z} \hookrightarrow \mathbb{Z}/6\mathbb{Z}\\ \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) &= \langle i \mapsto -i\rangle \cong \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

Let β be a root of $f(t)$. Then the roots are

β	$\zeta\beta$	$\zeta^2\beta$	$\zeta^3\beta$	$\zeta^4\beta$	$\zeta^5\beta$
β		$\omega^2\beta$		$\omega\beta$	
	$-\omega\beta$		$-\beta$		$-\omega^2\beta$

where a 3-cycle is given by permuting $\beta, \omega^2\beta, \omega\beta$ and the orbits are shown as the last two rows above. Denote the 3-cycle σ and complex conjugation τ, since

$$\tau\sigma\tau^{-1} = \sigma^{-1},$$

we get dihedral relation so $\mathrm{Gal}(L/\mathbb{Q})$ is dihedral of order 6.

2. $f(t) = t^5 - 2$ over $\mathbb{Q}$. It is irreducible by Eisenstein. Let L be the splitting field of $f(t)$ over $\mathbb{Q}$ and ζ be a primitive 5th root of unity. We have the following Galois correspondence:

$$\begin{array}{ccc} L & 1 & \\ | & | & 5 \\ \mathbb{Q}(\zeta) & \mathrm{Gal}(L/\mathbb{Q}(\zeta)) & \\ | & | & 4 \\ \mathbb{Q} & \mathrm{Gal}(L/\mathbb{Q}) & \end{array}$$

Let β be a root of $f(t)$. Then $\mathbb{Q} \leq \mathbb{Q}(\beta) \leq L$ so $5 \mid |L : \mathbb{Q}|$ and thus $5 \mid |\mathrm{Gal}(L/\mathbb{Q}(\zeta))|$. Since we also have $\mathrm{Gal}(L/\mathbb{Q}(\zeta)) \hookrightarrow \mathbb{Z}/5\mathbb{Z}$, it follows that $\mathrm{Gal}(L/\mathbb{Q}(\zeta)) \cong \mathbb{Z}/5\mathbb{Z}$.

We can thus deduce that $f(t)$ remains irreducible over $\mathbb{Q}(\zeta)$ and $|\mathrm{Gal}(L/\mathbb{Q})| = 20$. By irreducibility of $f(t)$ over $\mathbb{Q}$, $\mathrm{Gal}(L/\mathbb{Q})$ is a transitive subgroup of S_5. By Lemma 3.5, it is isomorphic to H_{20}, the subgroup generated by a 5-cycle and a 4-cycle. By Fundamental Theorem of Galois Theory,

$$\mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/\mathbb{Q}(\zeta)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$$

which is cyclic and contains a 4-cycle. Thus without a priori knowledge of H_{20} we know our subgroup of S_5 contains a 4-cycle.

Theorem 4.5 tells us the property of the splitting field of $t^m - \lambda$. The following theorem gives its converse:

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

Since we are going to restate the hypothesis in the theorem many times, we give it a name

Definition (Kummer extension)**.** A cyclic extension $K \leq L$ with $|L : K| = m$ where $\operatorname{char} K \nmid m$ and K contains a primitve mth root of unity is a *Kummer extension.*

We need the following to prove the theorem:

Lemma 4.7 (linear independence of group characters)**.** *Let $\phi_1, \dots, \phi_n$ be embeddings of a field K into a field L. Then there do not exist $\lambda_1, \dots, \lambda_n$ not all zero such that*

$$\lambda_1\phi_1(x) + \cdots + \lambda_n\phi_n(x) = 0$$

for all $x \in K$.

Proof. Example sheet 2 Q10. □

Proof of Theorem 4.6. Let $\operatorname{Gal}(G/K) = \langle\sigma\rangle$ which has order m. Observe that $\{\sigma^i\}_{i=0}^{m-1}$ are distinct maps $L \to L$ and we can apply linear independence of group characters: there exists $\alpha \in L$ such that

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

where ζ is a primitive mth root of unity.

Observe that $\sigma(\beta) = \zeta^{-1}\beta = \beta$ and so $\beta \in K$, the fixed field of $\operatorname{Gal}(L/K)$. Also $\sigma(\beta^m) = \sigma(\beta)^m = \beta^m$. Let $\lambda = \beta^m \in K$. Then

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

so $K(\beta)$ is the splitting field of $t^m - \lambda$ over K (recall $\zeta \in K$).

Observe also that $\{\sigma^i\}_{i=0}^{m-1}$ are distinct K-automorphisms and so $|K(\beta) : K| \geq m$. Therefore

$$L = K(\beta) = K(\zeta\beta).$$

□

$t^m - \lambda$ is the minimal polynomial of β over K and hence is irreducible.

Definition (radical extension)**.** A field extension $K \leq L$ is an *extension by racidals* if there exists

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

such that each $L_i \leq L_{i+1}$ is either cyclotomic or Kummer extension.

Definition (solubility by radicals)**.** A polynomial $f(t) \in K[t]$ is *soluble by radicals* if its splitting field lies in an extension by radicals.

4.3 Cubics

In this section and the following one we assume $\operatorname{char} K \neq 2$ for discussion about discriminant and $\operatorname{char} K \neq 3$ for cubic Kummer extension.

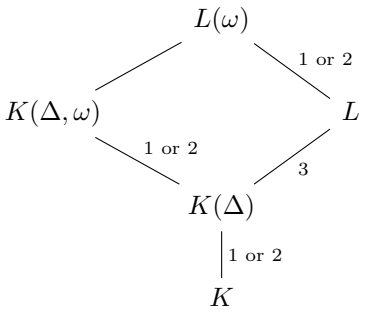
We have already seen that if $f(t)$ is a monic irreducible cubic in $K[t]$ with L its splitting field over K,

$$G = \operatorname{Gal}(f) = \operatorname{Gal}(L/K)$$

is either A_3 or S_3 since irreducibility implies that the action on roots is transitive. Thus we have the following correspondence:

$$\begin{array}{ccc} L & 1 & \\ | & | & 3 \\ K(\Delta) & G \cap A_3 & \\ | & | & 1 \text{ or } 2 \\ K & G & \end{array}$$

where $\Delta^2 = D(f)$ is the discriminant of f. But to see if we can solve f by radicals we want to make use of Theorem 4.6 and so we need to adjoin the appropriate roots of unity. So we get a bigger picture:



where ω is a primitive cubic root of unity. From the Tower Law $|L(\omega) : K(\Delta, \omega)| = 3$. Hence

$$\operatorname{Gal}(L(\omega)/K(\Delta, \omega)) \cong C_3.$$

We can now apply Theorem 4.6 to see that

$$L(\omega) = K(\Delta, \omega)(\beta)$$

where β is a root of an irreducible polynomial $t^3 - \lambda \in K(\Delta, \omega)[t]$.

In fact from the proof of Theorem 4.6 we see that

$$\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$$

where $\alpha_1, \alpha_2, \alpha_3$ are roots of $f(t)$. Now all the extensions

$$K \leq K(\Delta) \leq K(\Delta, \omega) \leq L(\omega)$$

are either cyclotomic or Kummer. Thus $f(t)$ is soluble by radicals.

Let's give a try to our theory. Given an irreducible cubic

$$f(t) = t^3 + at^2 + bt + c = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3),$$

we have $\alpha_1+\alpha_2+\alpha_3=-a$. But we don't actually need that many parameters: let $\alpha'=\alpha_i+\frac{a}{3}$ so that $\alpha_1'+\alpha_2'+\alpha_3'=0$ and the α''s are roots of the polynomial $g(t)=t^3+pt+q$ and most importantly,

$$K(\alpha_1,\alpha_2,\alpha_3)=K(\alpha_1',\alpha_2',\alpha_3')$$

so the splitting field for $g(t)$ is the same as that for $f(t)$. Thus we could work with $g(t)$ instead. The discriminant of $g(t)$ is $D(g)=-4p^3-27q^2$.

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

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

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

$$\begin{aligned}\beta^3+\gamma^3&=(\alpha_1'+\omega\alpha_2'+\omega^2\alpha_3')^3\\ &\quad+(\alpha_1'+\omega^2\alpha_2'+\omega\alpha_3')^3\\ &\quad+\underbrace{(\alpha_1'+\alpha_2'+\alpha_3')^3}_{=0}\\ &=3(\alpha_1'^3+\alpha_2'^3+\alpha_3'^3)+18\alpha_1'\alpha_2'\alpha_3'\\ &=-27q\end{aligned}$$

since $\alpha_1'^3=-p\alpha_1'-q$ and so $\alpha_1'^3+\alpha_2'^3+\alpha_3'^3=-3q$.

Thus after some messy algebra, we find that β^3 and γ^3 are roots of a quadratic

$$t^2+27qt-27p^3$$

and so are

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

We can solve for β^3 and γ^3 in $K(\sqrt{-3},\sqrt{D})=K(\omega,\Delta)$. From here we can get β by adjoining a cubic root of β^3 and set $\gamma=-\frac{3p}{\beta}$. Finally we solve in $L(\omega)$ for $\alpha_1',\alpha_2',\alpha_3'$

$$\begin{aligned}\alpha_1'&=\frac{1}{3}(\beta+\gamma)\\ \alpha_2'&=\frac{1}{3}(\omega^2\beta+\omega\gamma)\\ \alpha_3'&=\frac{1}{3}(\omega\beta+\omega^2\gamma)\end{aligned}$$

4.4 Quartics

As with the cubics, by making a substitution of the form $\alpha_i' = \alpha_i + \frac{a}{4}$ we may assume that the sum of the roots is zero and so the t^3 term vanishes, leaving a general quartic polynomial of the form

$$\begin{aligned} f(t) &= t^4 + bt^2 + ct + d \\ &= (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4) \end{aligned}$$

which we assume to be monic and irreducible.

Let $L = K(\alpha_1, \ldots, \alpha_4)$ be the splitting field of $f(t)$ over K.

$$\begin{array}{cc} L & 1 \\ | & | \\ M & G \cap V_4 \trianglelefteq G \\ | & | \\ K(\Delta) & G \cap A_4 \\ | & | \\ K & G \end{array}$$

where M is the fixed field of the normal subgroup $G \cap V_4 \trianglelefteq G$, which is an normal extension of K. By Fundamental Theorem of Galois Theory,

$$\mathrm{Gal}(M/K) \cong G/(G \cap V_4).$$

To determine this group concretely, we use a little knowledge from group theory: there is a group isomorphism

$$S_4/V_4 \cong S_3.$$

Let $\theta : S_4 \to S_3$ denote the quotient map, which has kernel precisely V_4. Therefore $\theta|_G : G \to S_3$ induces an isomorphism

$$G/\ker\theta|_G = G/(G \cap V_4) \cong \operatorname{im}\theta|_G \leq S_3.$$

We therefore seek a cubic for which M is the splitting field. We introduce *resolvent cubic*: set

$$\begin{aligned} x &= \alpha_1 + \alpha_2 \\ y &= \alpha_1 + \alpha_3 \\ z &= \alpha_1 + \alpha_4 \end{aligned}$$

and so

$$\begin{aligned} \alpha_1 &= \frac{1}{2}(x+y+z) \\ \alpha_2 &= \frac{1}{2}(x-y-z) \\ \alpha_3 &= \frac{1}{2}(-x+y-z) \\ \alpha_4 &= \frac{1}{2}(-x-y+z) \end{aligned}$$

Thus

$$K(\alpha_1, \dots, \alpha_4) = K(x, y, z).$$

Remebering that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$,

$$\begin{aligned} x^2 &= (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ y^2 &= (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ z^2 &= (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_3 + \alpha_3) \end{aligned}$$

These are all distinct since for example if $y^2 = z^2$ then $y = \pm z$ so $\alpha_3 = \alpha_4$ or $\alpha_1 = \alpha_2$.

Now consider the *resolvent cubic*

$$g(t) = (t - x^2)(t - y^2)(t - z^2) \in K[t].$$

x^2, y^2 and z^2 are permuted by G and are fixed by $G \cap V_4$. Thus

$$K(x^2, y^2, z^2) \leq M = L^{G \cap V_4}.$$

We claim that we actually have equality here:

Proof. Check $D(f) = D(g)$ — this will be addressed on example sheet — so $K(\Delta) \leq K(x^2, y^2, z^2)$.

Now observe that

$$\mathrm{Gal}(L/(K(x^2, y^2, z^2)) = \mathrm{Gal}(K(x, y, z)/K(x^2, y^2, z^2))$$

and in

$$K(x^2, y^2, z^2) \leq K(x, y^2, z^2) \leq K(x, y, z^2) \leq K(x, y, z),$$

each extension is of degree either 1 or 2 so $|K(x, y, z) : K(x^2, y^2, z^2)|$ divides 8 so elements of $\mathrm{Gal}(L/K(x^2, y^2, z^2))$ have order dividing 8. But since

$$\mathrm{Gal}(L/K(x^2, y^2, z^2)) \leq G \cap A_4,$$

by checking the order of elements in A_4 we see that

$$\mathrm{Gal}(L/K(x^2, y^2, z^2)) \leq G \cap V_4.$$

Therefore by Fundamental Theorem of Galois Theory

$$M = K(x^2, y^2, z^2).$$

□

Consider the coefficients of $g(t)$: its roots x^2, y^2, z^2 are permuted by G and so it has coefficients in K. We can actually write down these coefficients:

$$\begin{aligned} x^2 + y^2 + z^2 &= -2b \\ x^2y^2 + x^2z^2 + y^2z^2 &= b^2 - 4d \\ xyz &= -c \\ x^2y^2z^2 &= c^2 \end{aligned}$$

so

$$g(t) = t^3 + 2bt^2 + (b^2 - 4d)t - c^2.$$

We know how to solve cubics so we can solve for x^2, y^2, z^2, from which we can solve for x, y, z. Finally we use formula $\alpha_1 = \frac{1}{2}(x + y + z)$ etc to recover the roots for the quartic. Whew, done!

Remark. In our map

$$\theta : S_4 \to S_3,$$

we have restriction

$$\theta|_{A_4} : A_4 \to A_3 \cong C_3$$

and

$$\theta|_{G\cap A_4} : G \cap A_4 \to A_3$$

so

$$G \cap A_4/(G \cap V_4) \leq A_3$$

which is either 1 or A_3, corresponding to $M/K(\Delta)$. If the resolvent cubic is irreducible then it is isomorphic to A_3. Otherwise it is the trivial group.

Example. Let $f(t) = t^4 + 4t^2 + 2$. As an aside even if we didn't study Galois theory we could solve it. Then the resolvent cubic $g(t) = t^3 + 8t^2 + 8t$. Note that $c = 0$ in $f(t)$ so $g(t)$ has no constant term and thus reducible. It follows that $M = K(\Delta)$.

4.5 Solubility by Radicals

Now suppose we have a Galois extension $K \leq L$ with

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

such that each $L_i \leq L_{i+1}$ is either cyclotomic or Kummer extension.

Let $G = \mathrm{Gal}(G/K)$. There is a corresponding chain of subgroups of G

$$G = G_0 \geq G_1 \geq \cdots \geq G_m = 1$$

with $G_i = \mathrm{Gal}(L/K_i)$ and, by Fundamental Theorem of Galois Theory, $L_i = L^{G_i}$. However each extension $L_i \leq L_{i+1}$ is Galois and we know

$$G_{i+1} = \mathrm{Gal}(L/L_{i+1}) \trianglelefteq \mathrm{Gal}(L/L_i) = G_i$$

and

$$G_i/G_{i+1} \cong \mathrm{Gal}(L_{i+1}/L_i)$$

which is abelian if $L_i \leq L_{i+1}$ is cyclotomic and cyclic if $L_i \leq L_{i+1}$ is Kummer. It is the perfect time to introduce some group theory:

Definition (soluble group)**.** A group is *soluble* if there is a chain of subgroups

$$1 \trianglelefteq G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G \qquad (*)$$

with G_i/G_{i+1} abelian.

Remark. Note that some authors use "cyclic" in the definition. While we will prove shortly that they are equivalent for a finite group G, in general they are different.

Example.

1. S_3 is soluble since
$$1 \trianglelefteq \langle(123)\rangle \trianglelefteq S_3.$$

2. S_4 is soluble since
$$1 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4.$$
and $A_4/V_4 \cong C_3$, $S_4/A_4 \cong C_2$.

3. A_5 is not soluble: we have proved in IA Groups and again in IB Groups, Rings and Modules that A_5 is simple, and therefore any normal subgroup is 1 or A_5. Then any chain of normal subgroups would have non-abelian quotients and thus A_5 is not soluble.

Lemma 4.8. *A finite group G is soluble if and only if*
$$1 = G_m \trianglelefteq G_{m-1} \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 = G \qquad (\dagger)$$
with G_i/G_{i+1} cyclic.

This says that we only have to consider cyclic extensions.

Proof. The if part is easy. For the only if part, from Structural Theorem of Finitely Generated Abelian Groups, if A is abelian then there is a chain
$$0 = A_r \trianglelefteq A_{r-1} \trianglelefteq \cdots \trianglelefteq A_0 = A$$
with A_r/A_{r+1} cyclic. Thus if we have a chain $(*)$ with abelian factors G_i/G_{i+1}, we can refine it to one of the form $(\dagger)$ by Third Isomorphism Theorem. □

Definition (derived subgroup)**.** The *derived subgroup* G' of a group G is the subgroup generated by all the commutators
$$g_1 g_2 g_1^{-1} g_2^{-1}$$
for $g_1, g_2 \in G$.

Note that it is the subgroup *generated* by all such elements since it is not obvious that they are closed.

Lemma 4.9. *Let $K \trianglelefteq G$. Then G/K is abelian if and only if $G' \leq K$.*

Proof. G/K is abelian if and only if
$$Kg_1Kg_2Kg_1^{-1}Kg_2^{-1} = K$$
for all $g_1, g_2 \in G$, if and only if
$$g_1 g_2 g_1^{-1} g_2^{-1} \in K$$
if and only if $G' \leq K$. □

Remark. Some interesting asides:

1. In IID Representation Theory we will prove Burnside's Theorem: if $|G| = p^a q^b$ with p, q distinct primes then G is soluble.

2. Feit-Thompson Theorem: if $|G|$ is odd then G is soluble.

3. There is an analogue of Sylow's Theorem due to Philip Hall: given a finite group G, for every m and n coprime and $|G| = mn$, there is a subgroup of order m if and only if G is soluble.

Definition (derived series)**.** The *derived series* $\{G^{(m)}\}$ of G is defined inductively as

$$G^{(0)} = G$$
$$G^{(i+1)} = (G^{(i)})'$$

Thus

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G$$

with $G^{(i)}/G^{(i+1)}$ abelian.

Lemma 4.10. *Given a finite group G, G is soluble if and only if $G^{(m)} = 1$ for some m.*

Proof. If $G^{(m)} = 1$ then the derived series gives a chain of the form $(*)$ as in the definition of solubility.

Conversely, if there is a chain of the form $(*)$

$$1 \trianglelefteq G_m \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G$$

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

Remark. The derived series is the fastest descending chain with abelian factors.

Lemma 4.11.

1. *Let $H \leq G$. If G is soluble then H is soluble.*

2. *Let $H \trianglelefteq G$. Then G is soluble if and only if H and G/H are both soluble.*

Proof.

1. G is soluble so there is some m such that $G^{(m)} = 1$. But $H^{(m)} \leq G^{(m)}$ and so H is soluble.

2. Let $H \trianglelefteq G$. Suppose G is soluble. Then by the previous line H is soluble. Let $G^{(m)} = 1$, observed that

$$(G/H)' = G'H/H \leq G/H$$

and inductively

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

Thus $(G/H)^{(m)} = H/H = 1$ so G/H is soluble.

Conversely, suppose both H and G/H are soluble, i.e. $H^{(r)} = 1$ and $(G/H)^{(s)} = H/H$. But from above $(G/H)^{(s)} = G^{(s)}H/H$ so $G^{(s)}H = H$ and thus $G^{(s)} \leq H$. Therefore

$$G^{(r+s)} \leq H^{(r)} = 1$$

so G is soluble.

□

Example. S_5 is not soluble since its subgroup A_5 is not soluble.

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

Remark. We don't need to restrict to $\operatorname{char} K = 0$. What we need to do for a particular $f(t)$ is to avoid a finite number of bad characteristics (to avoid characteristics smaller than $\deg f(t)$).

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

Example. In the example after Theorem 3.6 on page 29, $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$ has Galois group S_5 over $\mathbb{Q}$: recall that it has three real roots and so complex conjugation gives a transposition. $f(t)$ is irreducible and so $5 \mid |\operatorname{Gal}(f)|$ and so there is a 5-cycle. Together they generate S_5. Thus $f(t)$ is not soluble by radicals.

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

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

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

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

Proof. Suppose we have a sequence as above and want to extend this into a Galois extension of the same form (assume $\operatorname{char} K = 0$). By Primitive Element Theorem $L_m = K(\alpha_1)$ for some α_1. Let $g(t)$ be the minimal polynomial of α_1 over K with splitting field M. Thus $M = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are roots of $g(t)$. There are K-homomorphisms $\phi_i : M \to M, \alpha_1 \mapsto \alpha_i$ extending K-homomorphisms $K(\alpha_1) \to K(\alpha_i) \leq M$. The tower

$$K \leq \phi_1(K) \leq \phi_2(L_1) \leq \cdots \leq \phi_1(L_m) = K(\alpha_1)$$

has cyclotomic or Kummer extensions at each step as before. Consider

$$L_m = K(\alpha_1) \leq \phi_2(L_1)(\alpha_1) \leq \phi_2(L_2)(\alpha_1) \leq \cdots \leq \phi_2(L_m)(\alpha_1) = K(\alpha_1, \alpha_2).$$

Consider the extension $\phi_2(L_j)(\alpha_1) \leq \phi_2(L_{j+1})(\alpha_1)$ in this tower. There are two cases:

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

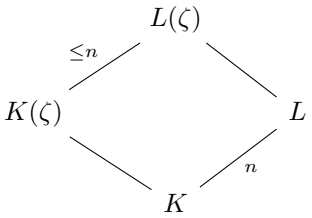
Now continue to get a suitable chain $K(\alpha_1, \alpha_2) \leq \cdots \leq K(\alpha_1, \alpha_2, \alpha_3)$ etc. Thus we get a suitable chain from K to $K(\alpha_1, \ldots, \alpha_n) = M$. Observe that $K \leq M$ is Galois. □

Assuming this lemma and so we may assume $K \leq L_m$ is Galois. By Fundamental Theorem of Galois Theory there is a corresponding chain of subgroups $\mathrm{Gal}(L_m/K)$. Previous discussion shows that $\mathrm{Gal}(L_m/K)$ is soluble. So to sum up we have $K \leq L \leq L_m$ with L_m Galois so by Fundamental Theorem of Galois Theory

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L_m/K)/\mathrm{Gal}(L_m/L)$$

But quotients of soluble group are soluble so $\mathrm{Gal}(L/K)$ is soluble.

Conversely, assume $\mathrm{char}\, K = 0$ and suppose $G = \mathrm{Gal}(f)$ over K is soluble. Let L be the splitting field of $f(t)$ over K and so $|G| = |L : K| = n$. Set $m = n!$ and let ζ be a primitive mth root of unity and consider $L(\zeta)$.



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

Note that $\mathrm{Gal}(L(\zeta)/L)$ is abelian since the extension is cyclotomic. Then $\mathrm{Gal}(L(\zeta)/K)$ is soluble since the subgroup $\mathrm{Gal}(L(\zeta)/L$ is soluble and the quotient group $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L(\zeta)/K)/\mathrm{Gal}(L(\zeta)/L)$ is also soluble. Then the subgroup $\mathrm{Gal}(L(\zeta)/K(\zeta))$ is soluble. Thus there is a chain of subgroups

$$1 = G_m \trianglelefteq \cdots \trianglelefteq G_1 \trianglelefteq G_0 \trianglelefteq \mathrm{Gal}(L(\zeta)/K(\zeta))$$

with G_i/G_{i+1} cyclic (since for a finite group cyclic is equivalent to abelian in the definition of a soluble group). Now use Fundamental Theorem of Galois Theory to get a corresponding chain of fields

$$L(\zeta) = K_m \geq \cdots \geq K_1 \geq K(\zeta)$$

with each $K_i \leq K_{i+1}$ Galois with cyclic Galois group.

By Theorem 4.6 all those extensions are Kummer (note all the extensions are of degree less than or equal to n and so we have the appropriate roots of unity, this is why we choose $m = n!$). Thus we have embedded L in an extension of K by radicals. □

Example.

1. Recall previously we had $f(t) = t^4 + 4t^2 + 2$ which is irreducible by Eisenstein over $\mathbb{Q}$. The resolvent cubic $g(t) = t^3 + 8t^2 + 8t$ is reducible. It actually has roots $0, -4 \pm 2\sqrt{2}$. We thus have

$$\begin{array}{c} L = K\left(\sqrt{-4+2\sqrt{2}}, \sqrt{-4-2\sqrt{2}}\right) \\ \Big| 4 \\ K(-4+2\sqrt{2}, -4-2\sqrt{2}) = K(\sqrt{2}) \\ \Big| 2 \\ K \end{array}$$

   so $|L : K| = 8$. The Galois group is a transitive subgroup of S_4 of order 8. It is the dihedral group.

   In particular the roots $\pm\sqrt{-2 \pm \sqrt{2}}$ are two conjugate pairs so complex conjugation gives double transposition.

2. $f(t) = t^4 + 2t + 2$ which is irreducible by Eisenstein over $\mathbb{Q}$. A quick (hmm) calculation shows that the discriminant is $101 \cdot 4^2$ which is not a square. Thus the Galois group contains an odd permutation.

   The resolvent cubic $g(t) = t^3 - 8t - 4$ is irreducible mod 5. Therefore there is a 3-cycle in the Galois group. We deduce that $\mathrm{Gal}(f) = S_4$.

3. Finally a quintic: $f(t) = t^5 - t - 1$ is irreducible over $\mathbb{Q}$ since it is irreducible mod 5 and so the Galois group contains a 5-cycle and is a transitive subgroup of S_5. Reduction mod 2, $f(t)$ factorises as a product of irreducible cubic and an irreducible quadractic

$$\overline{f}(t) = (t^3 + t^2 + 1)(t^2 + t + 1)$$

   so $\mathrm{Gal}(\overline{f})$ is generated by an element of cycle type $(3, 2)$. Thus $\mathrm{Gal}(f)$ also contains an element of cycle type $(3, 2)$. Then g^3 is a transposition. A subgroup of S_5 containing a 5-cycle and a transposition must be S_5. Therefore $f(t)$ is not solvable by radicals.

5 Final Thoughts

5.1 Algebraic Closure

Definition (algebracially closed)**.** A field L is *algebraically closed* if any $f(t) \in L[t]$ splits into a product of linear factors in $L[t]$.

Remark. This is equivalent to saying that any $f(t) \in L[t]$ has a root in L, or that any algebraic extension of L is L itself.

Definition (algebraic closure)**.** An extension $K \leq L$ is an *algebraic closure* of K if $K \leq L$ is algebraic and L is algebraically closed.

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

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

The minimal polynomial of α over K must split over L and so $\alpha \in L$. Thus any algebraic extension of L is L itself. □

Example (algebraic number)**.** Let $\mathbb{A} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$. It is a subfield of $\mathbb{C}$: if α and β are algebraic over $\mathbb{Q}$ then $|\mathbb{Q}(\alpha, \beta) : \mathbb{Q}| < \infty$. So if $\gamma = \alpha + \beta, \alpha - \beta, \alpha\beta$ or α/β for $\beta \neq 0$ we get $\mathbb{Q}(\gamma) \leq \mathbb{Q}(\alpha, \beta)$ and so $|\mathbb{Q}(\gamma) : \mathbb{Q}| < \infty$ so γ is algebraic over $\mathbb{Q}$ and so $\gamma \in \mathbb{A}$. Therefore $\mathbb{A} = \overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Like construction of many other objects in this course, we want to prove the existence and uniqueness of algebraic closures. In general we need to appeal to Zorn's Lemma. This will be covered in IID Logic and Set Theory, and it fact it is equivalent to both Axiom of Choice and Well-ordering Principle.

We will do a quick ad hoc statement of Zorn's Lemma here and relegate the main discussion to IID Logic and Set Theory.

Definition (partial order)**.** $(\zeta, \leq)$ is a *partial order* on a set ζ is

1. reflexive: $x \leq x$ for all $x \in \zeta$.
2. transitive: $x \leq y$ and $y \leq z$ implies $x \leq z$.
3. antisymmetric: if $x \leq y$ and $y \leq x$ then $x = y$.

Definition (total order)**.** A partial order $(\zeta, \leq)$ is a *total order* if it is total: for any $x, y \in \zeta$, either $x \leq y$ or $y \leq x$.

Definition (chain)**.** A *chain* in a partially ordered set $(\zeta, \leq)$ is a totally ordered subset.

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

Recall a result derived from Zorn's Lemma in IB Groups, Rings and Modules:

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

Proof. Let ζ be the set of proper ideals of R. $\{0\}$ is a proper ideal so ζ is non-empty. Let ζ be partially orderd by inclusion.

Note that an ideal $I \trianglelefteq R$ is proper if and only if $1 \notin I$. Any chain of proper ideals has an upper bound in ζ, namely the union of the chain, so by Zorn's Lemma ζ has a maximal element, i.e. a maximal ideal of R. □

Theorem 5.4 (existence of algebraic closure)**.** *Any field has an algebraic closure.*

Proof. Let

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

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

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

Let $I \trianglelefteq K[X_s : s \in \zeta]$ be the ideal generated by coefficients of all the $\tilde{f}(t)$'s, which we denote by $a_{f,\ell}$ for $0 \leq \ell < \deg f$. Claim that $I \neq K[X_s : s \in \zeta]$:

Proof. Suppose $1 \in I$ for contradiction. We thus have a relation

$$b_1 a_{f_1,\ell_1} + \cdots + b_N a_{f_N,\ell_N} = 1 \in K[X_s : s \in \zeta]. \qquad (*)$$

Let L be a splitting field for the product $f_1(t) \cdots f_N(t)$.For each i, f_i splits over L so write

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

Define a K-linear ring homomorphism which is identity on K

$$\begin{aligned} \theta : K[X_s : s \in \zeta] &\to L \\ X_{f_i,j} &\mapsto \alpha_{ij} \\ X_s &\mapsto 0 \text{ otherwise} \end{aligned}$$

This induces a map $\theta : K[X_s : s \in \zeta][t] \to L[t]$. Then

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

so $\theta(a_{f_i,j}) = 0$ since $a_{f_i,j}$ are the coefficients of $\tilde{f}_i(t)$. But applying θ to $(*)$ shows $0 = 1$. Absurd. □

We have thus shown that $I \trianglelefteq K[X_s : s \in \zeta]$ is proper. By Zorn's Lemma, there is a maximal ideal $P \trianglelefteq K[X_s : s \in \zeta]$ containing I. Set

$$L_1 = K[X_s : s \in \zeta]/P,$$

which is a field. We thus have a field extension $K \leq L_1$. Claim that L_1 is an algebraic closure of K:

Proof. We first show $K \leq L_1$ is algebraic. L_1 is generated by the images $x_{f,j}$ of the $X_{f,j}$. However $\tilde{f}(t)$ has coefficients in I and so its image in $L_1[t]$ is the zero polynomial. Thus in $L_1[t]$,

$$f(t) = \prod_{j=1}^{\deg f} (t - x_{f,j}) \tag{$\dagger$}$$

and so $f(x_{f,j}) = 0$. Thus the $x_{f,j}$'s are algebraic. Any element of L_1 involves only finitely many of the $x_{f,j}$'s and so is algebraic over K.

Moreover, from $(\dagger)$ any $f(t) \in K[t]$ splits completely over L_1. The claim thus follows from Lemma 5.1. □

□

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

Proof. Let

$$\zeta = \{(N, \phi) : K \leq N \leq M : \phi : N \to L \text{ homomorphism extending } \theta\}$$

and define a partial order $\leq$ on it by

$$(N_1, \phi_1) \leq (N_2, \phi_2) \text{ if } \begin{cases} N_1 \leq N_2 \\ \phi_2|_{N_1} = \phi_1 \end{cases}$$

$(K, \theta) \in \zeta$ so it is non-empty. If there is an ascending chain

$$(N_1, \phi_1) \leq (N_2, \phi_2) \leq \cdots$$

then set $N = \bigcup_\lambda N_\lambda$, which is a subfield of M and we can define a homomorphism $N \to L$ as follow: if $\alpha \in N$ then $\alpha \in N_\lambda$ for some λ and we send $\alpha \mapsto \phi_\lambda(\alpha)$. This is well-defined. Thus this is an upper bound for the chain in ζ. Zorn's Lemma thus says that there is an maximal element of ζ, (N, ϕ).

We now show that $N = M$. Given $\alpha \in M$, it is algebraic over K and hence over N. Let $f_\alpha(t)$ be its minimal polynomial over N. $\phi(f_\alpha(t)) \in L[t]$ and so splits completely since L is algebraically closed. Write

$$\phi(f_\alpha(t)) = (t - \beta_1) \cdots (t - \beta_r).$$

Since $\phi(f_\alpha(\beta_j)) = 0$ there is a map

$$\begin{aligned} N(\alpha) \cong N[t]/(f_\alpha(t)) &\to L \\ \alpha &\mapsto \beta_1 \end{aligned}$$

extending ϕ. Maximality of (N, ϕ) implies that $N(\alpha) = N$. Thus $\alpha \in N$ and $N = M$. □

With this theorem we can finally show

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

Proof. By the previous theorem there is a homomorphism $\phi : L_1 \to L_2$ extending the embedding of K in L_2. Since $K \leq L_2$ is algebraic, so is $K \leq \phi(L_1)$. But L_1 is algebraically closed and so $\phi(L_1)$ is algebraically closed. Thus $L_2 = \phi(L_1)$ and ϕ is an isomorphism. □

5.2 Symmetric Polynomials & Invariant Theory

In the build-up of Fundamental Theorem of Galois Theory we met Artin, which says that if $K \leq L$, H is a finite subgroup of $\mathrm{Aut}_K(L)$ and $M = L^H$ then $M \leq L$ is a Galois extension and $H = \mathrm{Gal}(L/M)$.

Example. Let $L = K(X_1, \ldots, X_n)$. Let S_n be the permutation group on the X_i's. These permutations induce K-automorphisms of L. By Artin, $M = L^{S_n} \leq L$ is Galois and $\mathrm{Gal}(L/M) = S_n$. Thus S_n is a Galois group of *some* field extension.

Since we can regard any finite group G as a subgroup of some S_n, any finite group is a Galois group of *some* finite field extension

$$\mathbb{Q} \leq K.$$

Finding the field extension is the *inverse Galois problem.*

Using notation from the previous example, let

$$f(t) = \prod_{i=1}^{n} (t - X_i) = t^n - s_1 t^{n-1} + s_2 t^{n-2} + \cdots + (-1)^n s_n \in M[t]$$

where

$$\begin{aligned} s_1 &= X_1 + \cdots + X_n \\ s_1 &= \sum_{i<j} X_i X_j \\ &\vdots \\ s_n &= X_1 X_2 \cdots X_n \end{aligned}$$

Definition (elementary symmetric polynomial)**.** The s_i's are the *elementary symmetric polynomials.*

Definition (algebraic independence)**.** $\alpha_1, \ldots, \alpha_n$ are *algebraically independent* over K if the ring homomorphism

$$\begin{aligned} K[Y_1, \ldots, Y_n] &\to K[\alpha_1, \ldots, \alpha_n] \leq L \\ Y_i &\mapsto \alpha_i \end{aligned}$$

is an isomorphism where $K[Y_1, \ldots, Y_n]$ is the polynomial ring in $Y_1, \ldots, Y_n$.

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

Proof. Certainly the s_i's are fixed by S_n so $M_1 = K(s_1, \ldots, s_n) \leq M$. Observe that L is the splitting field for $f(t) = \prod_{i=1}^{n}(t - X_i)$ over M_1. But $f(t)$ has degree n and so by a proposition we proved in example sheet, the degree of the splitting field over M_1 is at most $n!$. Artin implies that $|L : M| = |S_n| = n!$ so $M_1 = M$.

To show the algebraic independence of s_i's, we make use of the idea of transcendence bases and transcendence degree: we may consider the algebraically independent subsets of L and partially order them by inclusion. Note that the union of a chain is algebraically independent and thus an upper bound of the chain. By Zorn's Lemma there is a maximal algebraically independent subset, which is a *transcendence basis*. The *transcendence degree* of L over K is the cardinality of such a set, which is well-defined by Steinitz Exchange Lemma for infinite sets, and is denoted $\operatorname{trdeg}_K(L)$.

Since L is algebraic over M, we have $\operatorname{trdeg}_K(L) = \operatorname{trdeg}_K(M)$. If s_i's were algebraically dependent then $\operatorname{trdeg}_K(M) < n$ as M would be algebraic over a subfield generated by fewer elements and $\operatorname{trdeg}_K K(\alpha_1, \ldots, \alpha_n) \leq n$ by induction. Absurd. □

Polynomial invariant theory studies $K[X_1, \ldots, X_n]^H$ for a finite subgroup $H \leq S_n$ and as an aside, rather than confining ourselves to permutations of the variables, we may also consider $H \leq \mathrm{GL}(V)$ where V is the K-vector space generated by $X_1, \ldots, X_n$.

Question.

1. Is $K[X_1, \ldots, X_n]^H$ finitely generated?

2. Is $K[X_1, \ldots, X_n]^H$ isomormphic to any polynomial algebra?

We have shown above that the fixed field of $K(X_1, \ldots, X_n)$ is $K(s_1, \ldots, s_n)$. A similar result holds for the ring:

Theorem 5.8.
$$K[X_1, \ldots, X_n]^{S_n} = K[s_1, \ldots, s_n].$$

Definition (symmetric polynomial)**.** The elements of $K[s_1, \ldots, s_n]$ are the *symmetric polynomials*.

Proof. Let $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]^{S_n}$. The proof is by induction on the total degree of f. If the total degree is 0 then f is a constant polynomial and thus in K, so in $K[s_1, \ldots, s_n]$.

Suppose the total degree of f is positive. Let

$$\begin{aligned} \theta : K[X_1, \ldots, X_n] &\to K[X_1, \ldots, X_{n-1}] \\ g(X_1, \ldots, X_n) &\mapsto g(X_n, \ldots, X_{n-1}, 0) \end{aligned}$$

i.e. the projection of the first $n-1$ coordinates. Then $\ker\theta = (X_n)$. Since $f(X_1, \ldots, X_n)$ is fixed by S_n, by slight abuse of notation $\theta(f(X_1, \ldots, X_n)) = f(X_1, \ldots, X_{n-1})$ is fixed under the subgroup S_{n-1}, i.e. the subgroup that fixes n. Note that in particular

$$\theta(s_j(X_1, \ldots, X_n)) = s_j(X_1, \ldots, X_{n-1})$$

for $j \leq n-1$ where s_j is the jth elementary symmetric polynomial. Apply induction,

$$\theta(f(X_1, \ldots, X_n)) = p(s_1(X_1, \ldots, X_{n-1}), \ldots, s_{n-1}(X_1, \ldots, X_{n-1}))$$

where p is a polynomial. Rearrange,

$$\theta(f(X_1, \ldots, X_n) - p(s_1(X_1, \ldots, X_n), \ldots, s_{n-1}(X_1, \ldots, X_n))) = 0$$

so X_n divides the polynomial

$$f(X_1, \ldots, X_n) - p(s_1(X_1, \ldots, X_n), \ldots, s_{n-1}(X_1, \ldots, X_n)) \qquad (*)$$

which is a symmetric polynomial since it is fixed under S_n. It follows that X_i divides $(*)$ for all i. However, $K[X_1, \ldots, X_n]$ is a UFD and the X_i's are coprime so the product $X_1 \cdots X_n$ divides $(*)$. Write

$$f(X_1, \ldots, X_n) = g(X_1, \ldots, X_n)X_1 \cdots X_n + p(s_1(X_1, \ldots, X_n), \ldots, s_{n-1}(X_1, \ldots, X_n)).$$

Observe that the total degree of $g(X_1, \ldots, X_n)$ is smaller that that of $f(X_1, \ldots, X_n)$ and that $g(X_1, \ldots, X_n)$ is fixed under S_n. Applying induction to $g(X_1, \ldots, X_n)$ and so it is a polynomial in s_i's. Thus $f(X_1, \ldots, X_n) \in K[s_1, \ldots, s_n]$. □

Example. $K[X_1, \ldots, X_n]^{A_n}$ is generated by s_i's and

$$\Delta(X_1, \ldots, X_n) = \prod_{i<j}(X_i - X_j).$$

Emmy Noether in 1920s consider other subgroups of S_n and showed that the invariant rings are Noetherian.

Theorem 5.9 (Chevalley-Shephard-Todd)**.** $\mathbb{C}[X_1, \ldots, X_n]^H$ *where* $H \leq \mathrm{GL}(V)$ *finite is isomorphic to a polynomial algebra if and only if* H *is generated by pesudoreflections, whose* 1*-eigenspace has codimension* 1*.*

Index