3202 Galois Theory Notes

Based on the 2013 spring lectures by Dr M L Roberts

This includes:

1) establishes a one-to-one structure preserving correspondance between extensions of fields and groups.

2) analyzing the solution of polynomial equations $f(x) = 0$ in terms of (1). In particular, show that the quintic has no solution "by radicals".

3) provides solutions to some classical geometric problems such as trisecting the angle.

Field extensions and groups

This is the main goal of this course: The Fundamental Theorem of Galois Theory. This associates to a field extension $F \leq K$ (for example $\mathbb{R} \leq \mathbb{C}$), a group G called the Galois Group of the extension, and (under certain conditions) a 1-1 correspondance between intermediate fields $F \leq M \leq K$ and subgroups of G.

This construction fits into two important general ideas in algebra:

1) G is the group of automorphisms of K, such that this groups fixes F ($\Leftrightarrow \sigma(x) = x \ \forall x \in F$). For almost any structure we can look at the group of automorphisms of it, and this provides information about the structure.

2) The more general idea of attaching a group in some way to a structure is also important. (for example: the homotopy group of a space - in algebraic topology).

Solving polynomial equations

If you take a quadratic equation: $ax^2 + bx + c = 0$, we know that we can find the solution, by:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

The solution is given as an expression in the coefficients, involving only $+, -, \div, \times$ and $\sqrt{\ }$. This is called a "solution by radicals".

The cubic and quartic can in fact be solved similarly, though a lot more difficult.

For example: $t^3 + at^2 + bt + c = 0$

Make a change of variable $y = t + a/3$. The equation becomes:

$$y^3 + py + q = 0$$

Here p, q are expressions in a, b, c.

write $y = U + V$

Then $(U+V)^3 + p(U+V) + q = 0$

$$\Rightarrow \quad U^3 + 3U^3V + 3UV^2 + V^3 + p(U+V) + q = 0$$

$$\Rightarrow \quad [U^3 + V^3 + q] + (U+V)[3UV + p] = 0$$

$$U^3 + V^3 + q = 0$$
$$3UV + p = 0$$

$$u = U^3, \quad v = V^3$$

then
$$u + v = -q$$
$$27uv = -p^3$$

$$u - \frac{p^3}{27u} = -q \iff u^2 + qu - \frac{p^3}{27} = 0$$

$$\Rightarrow u = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

$$\Rightarrow y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Then just minus $a/3$ for the solution x!

A quartic can be solved similarly (by reducing to a cubic), so a natural hypothesis would be that all polynomial equations can be solved by radicals. However, Galois Theory can show that this is not true for the quintic.

The method:

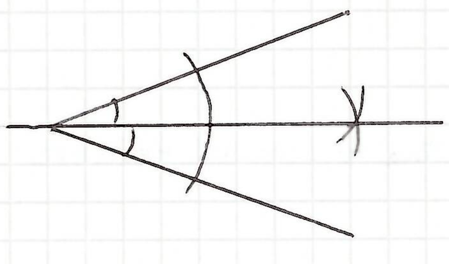
1) attach a field extension $\mathbb{Q} \subseteq L$ to a polynomial, $f(x) \in \mathbb{Q}[x]$.
2)
2) If the equation $f(x) = 0$ is soluble by radicals, then there is a chain of intermediate fields $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \dots \subseteq F_n \subseteq L$ with certain properties.

3) By the fundamental theorem, this corresponds to a chain of subgroups of the Galois Group G.

4) Show that, for the quintic, G doesn't have such a chain of subgroups.

<u>Geometric Problems</u>

These are "ruler and compass" problems for example bisecting an angle by ruler and compass



The question of which geometrical constructions can be done by ruler and compass goes back more that 2000 years to classical Greek mathematicians.

Three famous unsolved problems that were only answered in the 19th century are as follows:

1) trisecting an angle.

2) "squaring the circle" : can you construct $\sqrt{\pi}$?

area = 1   area = 1

3) "duplicating the cube" : can you construct $\sqrt[3]{2}$?

volume = 1   volume = 2

These can be solved fairly easily using the idea of a field extension and dimension.

<u>What do you need to know?</u>

1) Basic linear algebra
- vector spaces, bases, dimensions.

2) Group theory
- idea of a group, idea of a subgroup, Lagrange's theorem, permutation groups, normal subgroups, statement of Sylow's Theorem.

3) Some abstract algebra
- ideals in rings, quotient rings, other abstractions.

4) Need to be ok with quite complicated algebraic calculations.

<u>Structure of the course.</u>

Set book: Stewart, Galois Theory (3rd edition).

Project: 10% of the overall grade, based solely on presentation, in groups of 5-6. Maybe presentation help, maybe not!

Coursework: 10% of the course, split over 3 pieces of coursework.

<u>Handout 1</u>

(i) $f(t) = 2t^3 + t^2 + t + 1$ is irreducible $/\mathbb{Z}[t]$

$(f(t) \in \mathbb{Z}[t] \Rightarrow f(t) = a_n t^n + \dots + a_1 t + a_0$

a_n coprime to p. Then $\bar{f}(t)$ is irreducible in $\mathbb{Z}_p[t]$
$\Rightarrow f$ is irreducible in $\mathbb{Z}[t]$)

$\bar{f}(t) \in \mathbb{Z}_3[t]$

$\bar{f}(\bar{0}) = \bar{1} \neq \bar{0}$
$\bar{f}(\bar{1}) = \bar{2} \neq \bar{0}$
$\bar{f}(\bar{2}) = \bar{2} \neq \bar{0}$

$\Rightarrow \bar{f}$ is ~~not~~ irreducible in $\mathbb{Z}_3[t]$
$\Rightarrow f$ is irreducible in $\mathbb{Z}[t]$

a) $f(t) = t^3 + 7t^2 - 8t + 1$ is irreducible

f is a cubic, so reducible $\Leftrightarrow$ has a root.

Root could only be ± 1 but:
$f(1) \neq 0$
$f(-1) \neq 0$

$\Rightarrow$ irreducible $/\mathbb{Q}$.

b) $f(t) = t^4 - t^2 + 2t - 1$

$f(1) \neq 0$
$f(-1) \neq 0$

Try quadratics to get:

$f(t) = (t^2 - t + 1)(t^2 + t - 1)$
$\Rightarrow$ reducible!

c) $f(t) = t^4 + t^3 + t^2 + t + 1$

$$f(t) = \frac{t^5 - 1}{t - 1}$$

$\omega = e^{2\pi i/5}$
$\omega^5 = 1$

Put $t = s + 1$

$$f(s+1) = \frac{(s+1)^5 - 1}{(s+1) - 1} = \frac{(s+1)^5 - 1}{s} = \frac{s^5 + 5s^4 + 10s^3 + 10s^2 + 5s + 1 - 1}{s}$$

$$= s^4 + 5s^3 + 10s^2 + 10s + 5$$

Apply Eisenstein's with $p = 1$

$5 \nmid 1$
$5 \mid 5, 10, 10, 5$
$5^2 \nmid 5$

$\Rightarrow$ $f(s+1)$ is irreducible
$\Rightarrow$ $f(t)$ is irreducible $\square$

Note

$(x+y)^p$

$p \mid {}^pC_r$ (for $1 \leq r \leq p-1$)

3.17

a) F $(t-1)^2$
b) T
c) F
d) F $(t|t)$
e) T
f) T
g) F $(t^4 - 2 \in \mathbb{Z}[t])$
h) T (Gauss's Lemma)
i) F
j) ~~F~~ T

Chapter 4 - Field Extensions

Example: $f(t) = t^4 - 4t^2 - 5$

Roots are $f(t) = (t^2-5)(t^2+1)$
$\Rightarrow \pm\sqrt{5}, \pm i$

Consider $\{a + b\sqrt{5} + ci + di\sqrt{5} : a, b, c, d \in \mathbb{Q}\} = P$

It turns out that P is a field.
Consider $\mathbb{Q} \subseteq P$

Definition

A field extension is a field monomorphism $i : K \longrightarrow L$ where K, L are subfields of $\mathbb{C}$.

$K \cong \mathrm{im}(K)$ and usually we can identify K and $i(K)$, so normally we have $K \subseteq L$.

Write $L : K$ and call L the large field and K the small field.

$$\begin{array}{c} \mathbb{C} \\ | \\ L \\ | \\ K \\ | \\ \mathbb{Q} \end{array}$$

Examples

1) $\mathbb{R} : \mathbb{Q}$
2) $\mathbb{C} : \mathbb{R}$

Definition

22nd January 2013

Let $X \subseteq \mathbb{C}$. Then the field generated by X is the intersection of all subfields of $\mathbb{C}$ containing X.

$$= \bigcap_{X \subseteq F \subseteq \mathbb{C}} F$$

This is the same as:

1) The smallest subfield of $\mathbb{C}$ containing X.

2) The set of all elements obtained by combining elements of X algebraically. ($\Leftrightarrow$ the result of a finite sequence of field operations).

(Note that $X \neq \{0\}, \varphi \}$

Proposition 4.4

Any subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

Proof

Let F be a subfield.
Then $1 \in F$, so $\forall n \in \mathbb{N}$, $n = 1 + \dots + 1 \in F$
$\Rightarrow$ $-n \in F$ due to additive inverses.

Then $\forall m, n \neq 0 \in \mathbb{Z}$, $m/n \in F$ by multiplicative inverses.

$\Rightarrow \mathbb{Q} \subseteq F$. $\square$

Corollary 4.5

Let $X \subseteq \mathbb{C}$, $(X \neq \varphi, \{0\})$, then the subfield generated by $X \supseteq \mathbb{Q}$

Remark

We write $\mathbb{Q}(X)$ for the subfield of $\mathbb{C}$ generated by X.

Example

What is $\mathbb{Q}(\sqrt{2})$?

If $a, b \in \mathbb{Q}$, then $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

$\Rightarrow$ If $M = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, then $M \subseteq \mathbb{Q}(\sqrt{2})$

M is closed under addition and multiplication:

$$(a_1 + a_2\sqrt{2}) + (b_1 + b_2\sqrt{2}) = (a_1 + b_1) + (a_2 + b_2)\sqrt{2} \in M$$
$$(a_1 + a_2\sqrt{2})(b_1 + b_2\sqrt{2}) = (a_1 b_1 + 2a_2 b_2) + (a_2 b_1 + a_1 b_2)\sqrt{2} \in M.$$

$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \neq 0$ since $\sqrt{2}$ is irrational.

$$(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) = 1$$

$\Rightarrow (a + b\sqrt{2})^{-1} \in M$

$\Rightarrow$ M is a subfield of $\mathbb{C}$ containing $\sqrt{2}$.
$\Rightarrow$ $M = \mathbb{Q}(\sqrt{2})$. $\square$

(so $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$)

Generally finding these are a lot more complicated, for example:

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a,b,c \in \mathbb{Q}\}$$

So in the next chapter we develop theory about $\mathbb{Q}(X)$.

Definition 4.7

Let $L:K$ be a field extension and $Y \subseteq L$. Then the subfield of L generated by $K \cup Y$ is written $K(Y)$.

clearly $K(Y) \subseteq L$.

Here $K(y)$ means $K(\{y\})$ and $K(y_1, \dots, y_n)$ means $K(\{y_1, \dots, y_n\})$

Example

$\mathbb{Q}(i, \sqrt{3}) = \{a + bi + c\sqrt{3} + di\sqrt{3} : a,b,c,d \in \mathbb{Q}\}$
$\rightarrow$ quite hard work to show this!

what about $\mathbb{Q}(i)(\sqrt{3})$?

well, $\mathbb{Q}(i)(\sqrt{3}) = \mathbb{Q}(i, \sqrt{3})$!

4.2 - Rational Functions

These are of the form:

$\frac{p(t)}{q(t)}$ where $p(t), q(t)$ are polynomials.

For example: $\frac{t}{t^2 - 1}$

Definition

Given any field K, we can define the polynomial ring $K[t]$
$= \{(a_0, a_1, a_2, \dots) : a_i \in K$, only finitely many $a_i \neq 0\}$.

Add and multiply by:

$$(a_i) + (b_i) = (a_i + b_i)$$
$$(a_i)(b_i) = (c_i)$$

where $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

This makes $K[t]$ into a ring.

We usually write: $(a_0, a_1, a_2, \dots)$ as $a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n = p(t)$ say.

We can then think of $p(t)$ as a function $K \rightarrow K$ in the ordinary way.

Note: $K[t]$ is an integral domain.

Recall

An integral domain means: $pq=0 \Rightarrow p=0 \vee q=0$.

Definition

Given an integral domain, R, we can construct a field K containing R called the field of fractions of R.

Elements of K are of the form: rs^{-1} $(r, s \in R,\ s \neq 0)$

Example

Simplest example is $\mathbb{Z} \subseteq \mathbb{Q}$.

(a,b), but $2/4 = 1/2$.

Consider $\sim$ on $R \times R^* = \{(r,s) : r \in R,\ s \in R^* = R \setminus \{0\}\}$ by:

$$(r,s) \sim (r', s') \text{ if } rs' = r's.$$

Let $[r,s]$ be the equivalence class of (r,s), and let F be the set of equivalence classes.

($\mathbb{Q}$: For example: $[1,2] = \{(1,2), (2,4), (3,6), \dots, (-4,-8), \dots\}$)

Then we can define $+$ and $\times$ on F by:

$$[r,s] + [t,u] = [ru+ts, su]$$
$$[r,s] \cdot [t,u] = [rt, su]$$

Check F is a field under these operations.

We can identify R with $\{[r,1] : r \in R\}$ and every element of F is of the form $rs^{-1} = [r,1][s,1]^{-1} = [r,1][1,s] = [r,s]$

$\Rightarrow F$ is the field of fractions of R.

If you apply this method to $\mathbb{Z}$, you get $\mathbb{Q}$.

→ 1st Exercise sheet: Fill in the details to the above proof.

We apply this to $K[t]$, we get the field of fractions:

$$K(t) = \left\{ \frac{f(t)}{g(t)} : f(t), g(t) \in K[t] \right\}$$

We can now think of elements of $K(t)$ as "functions" $K \to K$, defined almost everywhere.

Example

$\mathbb{F}_p[t]$.

$f(t) = t^p - t$

As the function $f : \mathbb{F}_p \to \mathbb{F}_p$:

$f(\alpha) = \alpha^p - \alpha$

But by Fermat's Little Theorem, $\alpha^p = \alpha \Rightarrow f(\alpha) = 0$ so we can't think of f as a function.

4.3 - Simple Extensions

Definition

A field extension $L:K$ is simple if $\exists \alpha \in L$ such that $L = K(\alpha)$

Example 1

$\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ is simple, but these may not be this obviously simple.

$\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$, let $\alpha = \sqrt{2}+\sqrt{3}$

claim $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$.

clearly $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$

$(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2}) = 1$
$\Rightarrow \alpha^{-1} = \sqrt{3}-\sqrt{2} \in \mathbb{Q}(\alpha)$
$\Rightarrow \alpha + \alpha^{-1} = 2\sqrt{3} \in \mathbb{Q}(\alpha)$
$\Rightarrow \sqrt{3} \in \mathbb{Q}(\alpha)$.

$\alpha - \sqrt{3} = \sqrt{2} \in \mathbb{Q}(\alpha)$
$\Rightarrow \sqrt{2},\sqrt{3} \in \mathbb{Q}(\alpha)$
$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$ is in fact simple, with $\alpha = \sqrt{2}+\sqrt{3}$. $\square$

Example 2

if $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}):\mathbb{Q}$ simple?

Let $\alpha = \sqrt{2}\cdot\sqrt[3]{3}$

$\alpha^3 = 6\sqrt{2} \in \mathbb{Q}(\alpha)$
$\alpha^4 = 12\sqrt[3]{3} \in \mathbb{Q}(\alpha)$

$\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}):\mathbb{Q}$ is simple $\square$!

Example 3

$\mathbb{R}:\mathbb{Q}$ is not simple.

$\mathbb{R}$ is uncountable
$\mathbb{Q}(\alpha)$ is countable

$\Rightarrow \mathbb{R} \neq \mathbb{Q}(\alpha)$
$\Rightarrow \mathbb{R}:\mathbb{Q}$ is not simple! $\square$

Example 4

$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \dots, \sqrt[n]{2})$: $\mathbb{Q}$ is not simple.

Suppose $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \dots, \sqrt[n]{2}) = \mathbb{Q}(\alpha)$,
α is some expression in $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots, \sqrt[n]{2}$.

$\Rightarrow \alpha = f(\sqrt[N]{2})$ for some N.

$\Rightarrow \sqrt[N+1]{2} \in \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt[N]{2})$ which is impossible (a more precise proof later).

Definition 4.12

Let $i: K \to \hat{K}$ and $j: J \to \hat{J}$ to be two field extensions. Then an isomorphism between these two field extensions is a pair (λ, μ) where

$$\begin{tikzcd} \hat{K} \arrow[r, "\mu"] & \hat{J} \\ K \arrow[u, "i"] \arrow[r, "\lambda"'] & J \arrow[u, "j"'] \end{tikzcd}$$

$\lambda: K \longrightarrow L$ is a field isomorphism
$\mu: \hat{K} \longrightarrow \hat{L}$ is a field isomorphism

This diagram $(\rightarrow)$ commutes. This means that:

$$\mu i(k) = j\lambda(k) \quad \forall k \in K$$
$$\Leftrightarrow \mu i = \lambda j.$$

we usually think of i, j as inclusions:

$$\begin{array}{ccc} \hat{K} & \longrightarrow & \hat{L} \\ \cup\!\mid & & \cup\!\mid \\ K & \longrightarrow & L \end{array}$$

Such that $\mu I_K = \lambda$.

Often also, $K = L$ and $\lambda = Id$.

$$\begin{tikzcd} \hat{K} \arrow[r, "\mu"] & \hat{L} \\ K \arrow[u, dash] \arrow[r, "id"'] & K \arrow[u, dash] \end{tikzcd}$$

Here, $\mu \cdot I_K = Id$

$\Leftrightarrow$ μ fixes each element of K.

Example

$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ \cup\!\mid & & \cup\!\mid \\ \mathbb{R} & \xrightarrow[id]{} & \mathbb{R} \end{array}$$

where $c(a+bi) = a-bi$ is an isomorphism of field extensions.

Exercise 4.10

a) True
b) True
c) True
d) False
e) False
f) True
g) True
h) False
i) False : $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$

CHAPTER 5 - Simple Extensions

we want to classify extensions $K(\alpha) : K$.

Definition 5.1

Let $K \subseteq \mathbb{C}$ and $\alpha \in \mathbb{C}$. Then α is called algebraic over K if $\exists p(t) \in K[t]$, $p \neq 0$, such that $p(\alpha) = 0$.

Examples

1) $\sqrt{2}$ is algebraic over $\mathbb{Q}$.

$$f(t) = t^2 - 2 \in \mathbb{Q}[t], \text{ then } f(\sqrt{2}) = 0.$$

2) Let $\omega = e^{2\pi i/17}$ is algebraic over $\mathbb{Q}$.

$$f(t) = t^{17} - 1$$

Definition

If α is not algebraic, it is called transcendental.

Examples

3) π is transcendental over $\mathbb{Q}$
$\Rightarrow$ hard proof!

4) $\alpha = \sum_{n=0}^{\infty} 2^{-n!}$ is transcendental over $\mathbb{Q}$.

5) $\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$.

$$f(t) = t^2 - \pi \in \mathbb{Q}(\pi)[t].$$

Theorem 5.3

$K(t) : K$ is a transcendental field extension. ($K(t)$ is the field of rational functions).

Proof

Suppose t is algebraic $/K$.

$\Rightarrow \exists$ a polynomial $p(t) \in K[t]$ such that $p(t) = 0$.

This contradicts the definition of $K(t) \Rightarrow t$ is transcendental. $\square$

5.2 - Minimal Polynomial

Definition

A polynomial $f(t) = a_n t^n + \dots + a_0 \in K[t]$ is called monic if $a_n = 1$.

If $L:K$ and $\alpha \in L$ is algebraic over K, there exists $f(t) \in K[t]$ such that $f(\alpha) = 0$.

Example

$K = \mathbb{Q}, \ \alpha = i$

$f(t) = t^2 + 1$, then $f(i) = 0$
$g(t) = 4(t^4 - 1)$, then $g(i) = 0$.

There is a unique polynomial, which is monic, called $m(t) \neq 0$ of least degree such that $m(\alpha) = 0$.

- Pick polynomial of least degree such that $f(\alpha) = 0$.
- Divide by top coefficient to get a monic polynomial m?

Why is m unique?

If m' is another monic polynomial of degree n such that $m'(\alpha) = 0$.

Say $m' = t^n + a'_{n-1} t^{n-1} + \dots + a'_0$.
$m = t^n + a_{n-1} t^{n-1} + \dots + a_0$.

$m - m'$ is of degree $< n$ such that $(m - m')(\alpha) = 0$
$\Rightarrow m - m' = 0$
$\Rightarrow m = m'$ $\square$

m is called the minimal polynomial of α.

Lemma 5.6

Let α be algebraic over K with minimal polynomial m. Then m is irreducible and $f(\alpha) = 0 \Rightarrow m | f$.

($\Leftrightarrow$ if $I = \{ f \in K[t] : f(\alpha) = 0 \}$, then $I = mK[t]$ is a principle ideal with generator m).

Proof

Suppose $m = fg$.

Then $m(\alpha) = f(\alpha) g(\alpha) = 0$
$\Rightarrow f(\alpha) = 0$ or $g(\alpha) = 0$
$\Rightarrow \deg(f) \geq \deg(m)$ as m is the minimal polynomial.
$\Rightarrow \deg(g) = 0$ and g is a unit.
$\Rightarrow m$ has no non-trivial factorisation. $\square$ 1st part.

Suppose $f(\alpha) = 0$. Write $f = mq + r$, $\deg(r) < \deg(m)$.

Then $f(\alpha) = m(\alpha) q(\alpha) + r(\alpha)$

$\Rightarrow$ $m(\alpha) = 0$ as it is the minimal polynomial
$\Rightarrow$ $r(\alpha) = 0$
$\Rightarrow$ $r = 0$ as $\deg(r) < \deg(m)$
$\Rightarrow$ $f = mq$
$\Rightarrow$ $m \mid f$. $\square$ 2nd part

Exercise

What is the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

$$\alpha = \sqrt{2} + \sqrt{3}$$
$$\alpha^2 = 5 + 2\sqrt{6}$$
$$\alpha^2 - 5 = 2\sqrt{6}$$
$$(\alpha^2 - 5)^2 = 24$$
$$(\alpha^2 - 5)^2 - 24 = 0$$
$$\Rightarrow \quad \alpha^4 - 10\alpha^2 + 1 = 0$$

$\Rightarrow$ $f(t) = t^4 - 10t^2 + 1$ is the minimal polynomial.

Now we need to check that f is irreducible!

$f(1) \neq 0$
$f(-1) \neq 0$
$\Rightarrow$ no linear factors.

$$(t^2 + at + b)(t^2 + ct + d)$$
$$= t^4 + at^3 + bt^2 + ct^3 + act^2 + bct + dt^2 + adt + bd$$
$$= t^4 + (a+c)t^3 + (b+ac+d)t^2 + ad + bct + bd$$

$\Rightarrow$ $a + c = 0 \iff a = -c$
$b + d + ac = -10 \iff b + d - a^2 = -10$
$ad + bc = 0 \iff a(d-b) = 0$, $a \neq 0 \Rightarrow b = d$
$bd = 1 \Rightarrow b^2 = d^2 = 1$.

If $b = d = 1$ then $a^2 = 12$ | If $b = d = -1$ then $a^2 = 8$

$\Rightarrow f(t) = t^4 - 10t^2 + 1$ is irreducible.

Slightly easier way

Roots of f are $\pm\sqrt{2} \pm \sqrt{3}$

Quadratic factors would have to be $(t - \alpha_1)(t - \alpha_2)$.

α_1, α_2 are chosen from $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$.
But there is no way to combine the roots such that they lie in $\mathbb{Z}$, and so no quadratic factors.

$\Rightarrow$ $f(t) = t^4 - 10t^2 + 1$ is irreducible.
$\Rightarrow$ f must be the minimal polynomial of α.

5.3 - Simple algebraic extensions

$S = K[t]/(m)$, where $(m) = \{ m(t)f(t) : f(t) \in K[t] \}$

R, $I \triangleleft R$ $(i_1, i_2 \in I \Rightarrow i_1 + i_2 \in I,\ i \in I,\ r \in R \Rightarrow ir \in I)$

For example: $(2) \trianglelefteq \mathbb{Z}$ $\quad (2) = \{2a : a \in \mathbb{Z}\}$

$R/I = \{I + r : r \in R\}$
$(I+r)(I+s) = I + rs$
$(I+r) + (I+s) = I + (r+s)$

$I + r = \{i + r : i \in I\}$

Example

$\mathbb{Z}/5\mathbb{Z}$, $\quad 5\mathbb{Z} + r$.

$5\mathbb{Z} + 1 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$5\mathbb{Z} = \{\ldots, -5, 0, 5, \ldots\}$
$5\mathbb{Z} + 6 = \{\ldots, -9, -4, 1, 6, 11, \ldots\}$

Note that $5\mathbb{Z}+1 = 5\mathbb{Z}+6$.

$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}+0, 5\mathbb{Z}+1, 5\mathbb{Z}+2, 5\mathbb{Z}+3, 5\mathbb{Z}+4\}$
$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$K[t]/(m)$

Consider $K[t]/(m)$, where $(m) = \{m(t)f(t) : f \in K[t]\}$
$= \{(m) + f(t) : \deg(f) < \deg(m)\}$

Let $f(t) \in K[t]$. $f = mq + r$, $\deg(r) < \deg(m)$

$(m) + f = (m) + r$

Suppose $(m) + f = (m) + g$. $\deg(f), \deg(g) < \deg(m)$.

Then $f - g \in (m)$
$\Rightarrow f - g = ms$

But, $\deg(f-g) < \deg(m) \Rightarrow s = 0 \wedge f = g$.

And so every element of $K[t]/(m)$ can be written uniquely as $(m) + f(t) = \bar{f}(t)$

$\deg(f) < \deg(m)$

29th February

Recall

$\dfrac{K[t]}{(m)} = \{\bar{f} : \partial f < n\} = \{\overline{a_0 + a_1 + \cdots + a_{n-1}t^{n-1}} : a_i \in K\}$

Theorem 5.10

$K[t]/(m)$ is a field $\Leftrightarrow$ m is irreducible over K.

Proof

$\Rightarrow$ $\quad m = fg$

Then in $K[t]/(m)$, $\bar{m} = \bar{f}\bar{g}$. i.e. $\bar{0} = \bar{f} \cdot \bar{g}$

$K[t]/m$ is a field so $\bar{f} = 0$ or $\bar{g} = 0$

$\Rightarrow$ $f \in (m)$ or $g \in (m)$
$\Rightarrow$ f or g is a unit, and the factorisation is trivial.
$\Rightarrow$ m is irreducible.

$\underline{\Leftarrow}$ Let $\bar{f} \in K[t]/(m)$, $\bar{f} \neq \bar{0}$. Then $m \nmid f$

Let $d = HCF(m, f)$. d divides m and m is irreducible
$\Rightarrow$ $d = 1 \vee d = m$
$\Rightarrow$ $d = 1$ since $m \nmid f$ and so $d \neq m$.

$\Rightarrow$ $\exists h, k \in K[t]$ such that $mh + fk = 1$

In the quotient ring: $\bar{m}\bar{h} + \bar{f}\bar{k} = \bar{1}$
$\Rightarrow$ $\bar{f}\bar{k} = 1$
$\Rightarrow$ $\bar{f}$ has inverse $\bar{k}$.
$\Rightarrow$ $K[t]/(m)$ is a field $\square$

<u>Example</u>

$\dfrac{\mathbb{R}[t]}{(t^2+1)}$ is a field; as t^2+1 is irreducible / $\mathbb{R}[t]$. (by Theorem).

$= \{a\bar{t} + b : a, b \in \mathbb{R}\}$
$\bar{t}^2 = \overline{(t^2+1)-1} = -1$

$= \{a\bar{t} + b : a, b \in \mathbb{R}, \bar{t}^2 = -1\}$

$\Rightarrow \dfrac{\mathbb{R}[t]}{(t^2+1)} \cong \mathbb{C}$

Classifying simple extensions

<u>Theorem 5.11</u>

- The transcendental case.
  we will skip this case!

<u>Theorem 5.12</u>

Let $K(\alpha) : K$ be a simple algebraic extension, and let m be the minimal polynomial of α over K.

Then $K(\alpha) \cong \dfrac{K[t]}{(m)}$

$$\begin{tikzcd} \varphi : \dfrac{K[t]}{(m)} \arrow[r, "\varphi", "\bar{t} \mapsto \alpha"'] \arrow[d, dash] & K(\alpha) \arrow[d, dash] \\ K \arrow[r, "Id"] & K \end{tikzcd}$$

<u>Proof</u>

Define $\psi : K[t] \longrightarrow K(\alpha)$ by $\psi(f(t)) = f(\alpha)$.

ψ is a ring homomorphism such that $\psi|_K = id$

~~ψ is surjective:~~
~~Note that every element of $K(\alpha)$ can~~

$$\ker\psi = \{ f(t) \in K[t] : f(\alpha) = 0 \} = (m(t))$$

By 1st isomorphism theorem: $\exists$ a map:

$$\phi : \frac{K[t]}{\ker\psi} \longrightarrow K(\alpha)$$

$$\varphi(\bar{f}) = \psi(f) = f(\alpha)$$

$$\varphi : \frac{K[t]}{(m)} \longrightarrow K(\alpha), \quad \varphi(\bar{f}(t)) = f(\alpha)$$

$\Rightarrow \varphi$ is injective.

$\operatorname{im}\varphi \cong \frac{K[t]}{(m)}$ is a field $\subseteq K(\alpha)$ and containing $\varphi(\bar{t}) = \alpha$ and K

By defining $K(\alpha)$, $\operatorname{Im}\varphi = K(\alpha)$

$\Rightarrow \varphi$ is the required isomorphism. $\square$

__Example__

$\mathbb{Q}(\sqrt{2})$

$\sqrt{2}$ has minimal polynomial $t^2 - 2$, so

$$\frac{\mathbb{Q}[t]}{(t^2-2)} \cong \mathbb{Q}(\sqrt{2})$$

Note $\frac{\mathbb{Q}[t]}{(t^2-2)} = \{ (t^2-2) + at + b : a, b \in \mathbb{Q} \}$

$$= \{ \overline{at+b} : a, b \in \mathbb{Q}, \ \bar{t}^2 = 2 \}.$$

__Lemma 5.14__

Let α be algebraic over K with minimal polynomial $m(t)$.

Then $K(\alpha) = \{ a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in K \}$
(where $n = \deg(m)$)

This expression is unique, so $\{1, \alpha, \dots, \alpha^{n-1}\}$ forms a K-basis for $K(\alpha)$.

In particular $[K(\alpha) : K] = n$

__Proof__

$$K(\alpha) \cong \frac{K[t]}{(m)} = \{ a_0 + a_1\bar{t} + \dots + a_{n-1}\bar{t}^{n-1} : a_i \in K \} \quad \square$$

Example

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a,b,c \in \mathbb{Q}\}$$

Corollary 5.13

Suppose α and β have the same minimal polynomial over K. Then:

$$K(\alpha) \cong K(\beta)$$

where $\varphi(\alpha) = \beta$ and $\varphi|_K = id$

$$\begin{tikzcd} K(\alpha) \arrow[r, "\varphi", "\alpha \mapsto \beta"'] \arrow[d, dash] & K(\beta) \arrow[d, dash] \\ K \arrow[r, "id"'] & K \end{tikzcd}$$

Proof

$$\begin{tikzcd} K(\alpha) \arrow[d, dash] & \frac{K[t]}{(m)} \arrow[l, "\varphi_1"'] \arrow[r, "\varphi_2"] \arrow[d, dash] & K(\beta) \arrow[d, dash] \\ K & K \arrow[l, "id"'] \arrow[r, "id"] & K \end{tikzcd}$$

$\varphi = \varphi_2 \varphi_1^{-1} : K(\alpha) \to K(\beta)$ is the required isomorphism $\square$

Example

$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\omega)$ with $\omega = e^{2\pi i/3}$.

clearly they are not the same ($\mathbb{Q}(\sqrt[3]{2})$ is real, while $\mathbb{Q}(\sqrt[3]{2}\omega)$ is not), but they are isomorphic.

Note

$K(\alpha) \cong K(\beta)$ does not imply α, β have the same minimal polynomial.

For example: $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{2}-1)$

check this

- minimal polynomial of $\sqrt{2}$ is t^2-2
- minimal polynomial of $\sqrt{2}-1$ is t^2+2t-1

If $\exists$ isomorphism $\varphi: K(\alpha) \to K(\beta)$ such that $\varphi(\alpha) = \beta$ and $\varphi|_K = id$, then α and β have same minimal polynomial

Definition

Let $i: K \longrightarrow L$ be a field monomorphism. Then there is a ring monomorphism:

$$\hat{\imath}: K[t] \longrightarrow L[t]$$
$$\hat{\imath}(a_n t^n + \dots + a_0) = i(a_n)t^n + \dots + i(a_0)$$

If i is a monomorphism and an isomorphism, so is $\hat{i}$.

We usually write i for $\hat{i}$.

Theorem 5.16

Let K, L be subfields of $\mathbb{C}$, $i: K \to L$ a field isomorphism. Let α have minimal polynomial m_α over K and β have minimal polynomial m_β over L.

Suppose $i(m_\alpha) = m_\beta$.

Then $\exists$ an isomorphism $j: K(\alpha) \longrightarrow L(\beta)$ such that $j(\alpha) = \beta$

(and $j|_K = i$)

$$\begin{tikzcd} K(\alpha) \arrow[r, "j"', "\alpha \mapsto \beta"] \arrow[d, dash] & K(\beta) \arrow[d, dash] \\ K \arrow[r, "i"] & L \end{tikzcd}$$

Proof

$K[t]/(m)$:

$$\begin{tikzcd} K(\alpha) \arrow[r, "\varphi_1"] \arrow[d, dash] & K[t]/(m) \arrow[r, "\psi"] \arrow[d, dash] & L[t]/(m_\beta) \arrow[r, "\varphi_2"] \arrow[d, dash] & L(\beta) \arrow[d, dash] \\ K & K \arrow[l, "id"'] \arrow[r, "i"] & L \arrow[r, "id"] & L \end{tikzcd}$$

$\alpha \leftarrow \bar{t}$ $\quad$ $\bar{t} \longleftrightarrow \bar{t}$ $\quad$ $\bar{t} \longmapsto \beta$

φ_1, φ_2 exist by 5.12

$K[t] \cong L[t] \xrightarrow{\pi} L[t]/(m_\beta)$

π is injective and:

$\ker(\pi i) = \{f(t) : i(f) \in (m_\beta)\} = (m_\alpha)$

$\Rightarrow \dfrac{K[t]}{(m_\alpha)} \cong \dfrac{K[t]}{(m_\beta)}$ $\square$

5.9

a) True $(K \subseteq K(t))$
b) False $(\mathbb{C})$
c) False $(\mathbb{C} \subseteq \mathbb{C}(t))$
d) False $(\mathbb{C}(S,t) : \mathbb{C})$ also $(\mathbb{C} : \mathbb{Q}$ by countability$)$.
e) False $(\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(\sqrt{5}))$
f) True $(K(\alpha) \cong K(\beta))$
g) True (by definition)
h) False $(t^2 - 1 = (t+1)(t-1))$
i) False $(2t^2 - 2 = 2 \cdot (t^2 - 1)$ reducible!$)$

Chapter 6 - Degrees of extensions

Theorem 6.1

If $L:K$ is a field extension, then L can be regarded as a vector space over K.

Definition

The degree of a field extension $L:K$ is the dimension of L as a vector space over K, denoted $[L:K]$.

Example

$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, because $\mathbb{Q}(\sqrt{2})$ has a $\mathbb{Q}$-basis: $\{1,\sqrt{2}\}$
$\Rightarrow$ dimension 2!

6.2 - The Tower Law

Let K, L, M be fields with $K \subseteq L \subseteq M$. Then:

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

$$\left.\begin{array}{rc} & M \\ {[M:L]} & | \\ & L \\ {[L:K]} & | \\ & K \end{array}\right\} [M:K]$$

Proof

Let $(x_i)_{i\in I}$ be a basis for L over K and let $(y_j)_{j\in J}$ be a basis for M over L.

$[L:K] = |I|$
$[M:L] = |J|$

Claim $(x_iy_j)_{i\in I, j\in J}$ is a K-basis for M.

#1) Spanning

Let $m\in M$. Since $(y_j)_{j\in J}$ spans M over L, so $\exists\, l_j \in L$ such that:

$$m = \sum_{j\in J} l_j y_j$$

Since $(x_i)_{i\in I}$ span L over K, then $\exists\, \alpha_{ij}\in K$ such that:

$$l_j = \sum_{j\in J} \alpha_{ij} x_i$$

$$\Rightarrow m = \sum_{j\in J} l_j y_j = \sum_{j\in J}\left(\sum_{i\in I} \alpha_{ij} x_i\right) = \sum_{i\in I, j\in J} \alpha_{ij} x_i y_j$$

$\Rightarrow (x_iy_j)_{i\in I, j\in J}$ spans M over K.

#2) Linearly independent

$$\sum_{j\in J} \underbrace{\left(\sum_{i\in I} \alpha_{ij} x_i\right)}_{\in L} y_j = 0$$

Since $(y_j)_{j\in J}$ are all LI over L.

$$\Rightarrow \sum_{i\in I} \alpha_{ij} x_i = 0$$

Since $(x_i)_{i\in I}$ are all LI over K, all $\alpha_{ij} = 0$

$$\Rightarrow [M:K] = |I \times J| = |I||J| = [M:L][L:K] \quad \square$$

Example

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

$\mathbb{Q}(\sqrt{2})(i)$

$|$

$\mathbb{Q}(\sqrt{2})$

$|$

$\mathbb{Q}$

$\mathbb{Q}(\sqrt{2})$ has basis $\{1, \sqrt{2}\}$ over $\mathbb{Q}$
$\mathbb{Q}(\sqrt{2})(i)$ has basis $\{1, i\}$ over $\mathbb{Q}(\sqrt{2})$

(if $a+bi = 0$, $a, b \in \mathbb{Q}(\sqrt{2})$, since $a, b \in \mathbb{R}$, then $a=0$ and we know anything in $K(i)$ is of the form $ai+b$, since $i^2+1=0$)

$$\Rightarrow \{1, \sqrt{2}, i, i\sqrt{2}\} \text{ is a } \mathbb{Q}\text{-basis for } \mathbb{Q}(\sqrt{2})(i)$$

Also: $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i), \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}]$
$= 2 \times 2 = 4.$

Corollary 6.6

Let $K_0, K_1, \dots, K_n$ be fields with $K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$.

Then $[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \dots [K_1 : K_0]$

Proof

Straight forward induction, read in book!

Proposition 6.7

i) If α is transcendental over K then $[K(\alpha) : K] = \infty$.

ii) If α is algebraic over K, then $[K(\alpha) : K] = \deg(m)$, where m is the minimal polynomial of α.

Proof

i) Claim $\{1, \alpha, \dots, \alpha^n\}$ is LI/K.

Suppose $\sum_{i=0}^{n} k_i \alpha^i = 0$, $(k_i \in K)$

Let $f(t) = \sum_{i=0}^{n} k_i t^i$ $\quad f(t) \in K[t]$.

and $f(\alpha) = 0$ since α is transcendental.

$\Rightarrow f = 0$
$\Rightarrow$ all $k_i = 0$

$\Rightarrow \quad [K(\alpha) : K] \geq n+1 \quad \forall n$
$\Rightarrow \quad [K(\alpha) : K] = \infty$

ii) Lemma 5.14: $\deg(m) = n$ then:

$\{1, \alpha, \dots, \alpha^{n-1}\}$ is a K-basis for $K(\alpha)$

$\Rightarrow \quad [K(\alpha) : K] = n = \deg(m) \quad \square$

Calculating degrees of extensions comes down to finding minimal polynomials and using the tower law.

Example

$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}]$?

$$\begin{array}{c} \mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5}) \\ | \\ \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ since the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$
- $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = \cancel{8}\,2$ as the minimal polynomial over $\mathbb{Q}(\sqrt{2})$ is $t^{\cancel{8}2} - 3$ (bit more work!)
- $[\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5}) : \mathbb{Q}(\sqrt{2})(\sqrt{3})] = 2$ as the minimal polynomial of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2})(\sqrt{3})$ is $t^2 - 5$

$\Rightarrow [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$

Definition — 31st January 2013

An extension $L : K$ is finite if its degree is finite.

we say that if α is algebraic over K, then $K(\alpha) : K$ is finite.

$L : K$ is called algebraic if every element of L is algebraic over K.

Lemma 6.11

The following are equivalent:

i) $L : K$ is algebraic and finitely generated over K.
(i.e. $\exists \alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$)
ii) $L : K$ is finite.

To say $K(\alpha) : K$ is simple algebraic could mean:

1) α is algebraic over K or
2) every element of $K(\alpha)$ is algebraic $/K$.

Proof of Lemma 6.11

$\Leftarrow$ Suppose $L : K$ is finite $\Leftrightarrow [L : K] < \infty$.
Let $l_1, \dots, l_m$ be a K-basis for L. Then $L = K(l_1, \dots, l_m)$.
$\Rightarrow$ L is finitely generated over K.

Let $x \in L$. The set $\{1, x, \dots, x^m\}$ where $m = [L : K]$.

$\{1, x, \dots x^m\}$ is a set of $m+1$ elements in a vector space of dimension m over K.

$\Rightarrow$ linearly dependent:

$$\Rightarrow \sum_{i=0}^{m} k_i x^i = 0 \quad (k_i \in K, \text{ not all } k_i = 0)$$

Let $f(t) = \sum_{i=0}^{n} k_i t^i \in K[t]$, $f \neq 0$ and $f(x) = 0$.

$\Rightarrow$ x is algebraic $/K$.

$\Rightarrow$ Suppose $L:K$ is algebraic and L is finitely generated $/K$.

Say $L = K(\alpha_1, \dots, \alpha_n)$. Consider the tower:

$$\begin{array}{c} L = K(\alpha_1, \dots, \alpha_n) \\ | \\ K = \dots \\ \vdots \\ K(\alpha_1)(\alpha_2) \\ | \\ K(\alpha_1) \\ | \\ K \end{array}$$

α_1 is algebraic over K, so by 5.14, $[K(\alpha):K] < \infty$.
α_2 is is algebraic over K, so α_2 is algebraic over $K(\alpha_1)$.
So by 5.14:

$$[K(\alpha_1)(\alpha_2) : K(\alpha_1)] < \infty.$$

Continuing in this way:

By the Tower Law: $[L:K] < \infty$.

6.17

a) False, for example $\mathbb{Q}(\sqrt{2}) \not\cong \mathbb{Q}(\sqrt{3})$ but both degree 2.
b) True
c) False
d) True
e) True, $[\mathbb{C}:\mathbb{R}] = 2 < \infty \Rightarrow$ algebraic by 6.11
f) False: $[\mathbb{R}(t):\mathbb{R}] \not< \infty$
g) Exercise 1, Question 3
h) $V \cong L$ as a vector space $\Leftrightarrow \dim V = \dim L$
i) –

chapter 7

Skip!
NOT examinable.

Chapter 8

We will only do 8.5 and 8.6.

8.5

Definition

Let $L:K$ be a field extension. A **K-automorphism** of L is a bijective field homomorphism $\alpha: L \longrightarrow L$ such that $\alpha|_K = \mathrm{id}$.

$$\begin{tikzcd} L \arrow[r, "\alpha"] & L \\ K \arrow[u, dash] \arrow[r, "\mathrm{id}"'] & K \arrow[u, dash] \end{tikzcd}$$

(we say that α **fixes** K)
$\Leftrightarrow \alpha(k) = k \quad \forall k \in K$

Example

Define $c: \mathbb{C} \longrightarrow \mathbb{C}$ by $c(a+ib) = a - ib$: complex conjugation.
Then c is an $\mathbb{R}$-automorphism of $\mathbb{C}$

c is bijective because:

$$c(z_1 z_2) = c(z_1)c(z_2)$$
$$c(z_1 - z_2) = c(z_1) - c(z_2)$$

For $z \in \mathbb{R}$, $c(z) = z$.

Theorem 8.2

The set of all K-automorphisms of L forms a group under composition of maps.

This is called the **Galois Group** of the extension $L:K$, denoted $\Gamma(L:K)$ or $\mathrm{Gal}(L:K)$

Galois Groups

5th February 13

Definition

Let $L:K$ be a field extension. Then the Galois Group, $\Gamma(L:K)$ is

$$\Gamma(L:K) = \{\text{group of } K\text{-automorphisms of } L, \text{ under composition}\}$$

Recall

An automorphism is a homomorphism $f: L \to L$ such that $f|_K = Id$, f is bijective.

Example 1

What is $\Gamma(\mathbb{C}:\mathbb{R})$? Let $\sigma: \mathbb{C} \longrightarrow \mathbb{C}$ be an $\mathbb{R}$-automorphism.

$$\sigma(a) = a \quad \forall a \in \mathbb{R}.$$

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$
$$\Rightarrow \sigma(i) = 1 \vee \sigma(i) = -1$$

If $\sigma(i) = i$, then $\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i) = a+bi$
$\Rightarrow \sigma = id$
id is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

If $\sigma(i) = -i$, then $\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i) = a-bi$
$\Rightarrow \sigma(z) = \bar{z}$.

Write $c(z) = \bar{z}$. $c: \mathbb{C} \to \mathbb{C}$ satisfies $c(zw) = c(z)c(w)$ and $c(z+w) = c(z) + c(w)$, and $c(a) = a \ \forall a \in \mathbb{R}$.
$\Rightarrow c$ is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

$$\Rightarrow \Gamma(\mathbb{C}:\mathbb{R}) = \{id, c\} \cong C_2 \qquad (c^2 = id)$$

Example 2

$$K = \mathbb{Q}, \ L = \mathbb{Q}(\alpha), \ \alpha = \sqrt[3]{2}$$

What is $\Gamma(\mathbb{Q}(\alpha):\mathbb{Q})$

Let $\sigma \in \Gamma$.
$\sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(2) = 2$
$\sigma(\alpha) \in \mathbb{Q}(\alpha) \leq \mathbb{R}$
$\Rightarrow \sigma(\alpha) = \alpha$ as the only cube root of 2 in $\mathbb{Q}(\alpha)$ is α.

$$\sigma(a + b\alpha + c\alpha^2) = \sigma(a) + \sigma(b)\sigma(\alpha) + \sigma(c)\sigma(\alpha^2)^2$$
$$= a + b\alpha + c\alpha^2$$

$$\Rightarrow \Gamma(\mathbb{Q}(\alpha):\mathbb{Q}) = \{id\}$$

Example 3

$$\Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q})$$

Let $f \in \Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3}):\mathbb{Q})$

f is determined by $f(\sqrt{2})$ and $f(\sqrt{3})$ (as $\sqrt{2}, \sqrt{3}$ generates $\mathbb{Q}(\sqrt{2}, \sqrt{3})$)

$$f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = 2$$
$$\Rightarrow f(\sqrt{2}) = \pm\sqrt{2}$$

$$f(\sqrt{3})^2 = f(\sqrt{3}^2) = f(3) = 3$$
$$\Rightarrow f(\sqrt{3}) = \pm\sqrt{3}$$

This gives us 4 potential elements of Γ.

These possibilities are:

1) id: $\sqrt{2} \to \sqrt{2}$, $\sqrt{3} \to \sqrt{3}$
2) f_1: $\sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to \sqrt{3}$
3) f_2: $\sqrt{2} \to \sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$
4) f_3: $\sqrt{2} \to -\sqrt{2}$, $\sqrt{3} \to -\sqrt{3}$

We need to check these are all $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$\sqrt{2}$ and $-\sqrt{2}$ have the same minimum polynomial over $\mathbb{Q}$. By 5.13,
$\exists\, \sigma : \mathbb{Q}(\sqrt{2}) \mapsto \mathbb{Q}(-\sqrt{2})$
$\sqrt{2} \mapsto -\sqrt{2}$

$$\sigma\, I_{\mathbb{Q}} = id.$$

$\sqrt{3}$ has minimum polynomial $t^2 - 3$ over $\mathbb{Q}(\sqrt{2})$ (because $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$)
check if:

$$\sqrt{3} = a + b\sqrt{2}$$
$$3 = a^2 + b^2 + 2ab\sqrt{2}$$

$\sqrt{2} \notin \mathbb{Q}$, so $ab = 0$.

$a = 0 \Rightarrow 3 = 2b^2 \Rightarrow b = \sqrt{\frac{3}{2}} \in \mathbb{Q}$: impossible
$b = 0 \Rightarrow 3 = a^2 \Rightarrow a = \sqrt{3} \in \mathbb{Q}$: impossible

$+\sqrt{3}$ has minimal polynomial $t^2 - 3 = \sigma(t^2 - 3)$ over $\mathbb{Q}(\sqrt{2})$.

By Theorem 5.16, there exist $f_1 : \mathbb{Q}(\sqrt{2})(\sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2})(\sqrt{3})$
such that:
$f_1(\sqrt{3}) = \sqrt{3}$ and $f_1\, I_{\mathbb{Q}(\sqrt{2})} = \sigma$

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2})(\sqrt{3}) \arrow[r] & \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\
\mathbb{Q}(\sqrt{2}) \arrow[u, dash] \arrow[r, "\sigma"] & \mathbb{Q}(\sqrt{2}) \arrow[u, dash] \\
\mathbb{Q} \arrow[u, dash] \arrow[r, "id"] & \mathbb{Q} \arrow[u, dash]
\end{tikzcd}$$

$f_1 : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \longrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3})$
$f_1(\sqrt{3}) = \sqrt{3}$
$f_1\, I_{\mathbb{Q}(\sqrt{2})} = \sigma$

$$f_1(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$$
$$f_1\, I_{\mathbb{Q}} = \sigma\, I_{\mathbb{Q}} = id$$

$\Rightarrow f_1 \in \Gamma(\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q})$

Similarly $f_2 \in \Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$

$f_1 \circ f_2 = f_3$, so $f_3 \in \Gamma$.
$\Rightarrow \Gamma = \{id, f_1, f_2, f_3\}$

$$f_1^2 = f_2^2 = f_3^2 = id \Rightarrow \Gamma = C_2 \times C_2 = \{id, f_1\} \times \{id, f_2\}$$

8.6

Definition

Let M be a field, and $L:K$ be a field extension. If $K \subseteq M \subseteq L$ it is called an intermediate field.

Consider $\mathcal{J}(L:K) = \{\text{set of intermediate fields}\}$
$= \{\text{set of subgroups of } \Gamma(L:K)\}$

If $M \in \mathcal{J}$, then $M^* = \{\sigma \in \Gamma : \sigma(m) = m \ \forall m \in M\}$

$M^* \leq \Gamma$ by definition. $*: \mathcal{J}(L:K) \longrightarrow \Gamma(L:K)$, $+: \Gamma(L:K) \rightarrow \mathcal{J}(L:K)$

It is fairly easy to show that M^* is a subgroup, and so:

$M^* = \Gamma(L:M)$
$\Rightarrow M^* \in \Gamma(L:K)$

If $H \in \Gamma(L:K)$, $H \leq G$. then $H^+ = \{x \in L : h(x) = x \ \forall h \in H\}$

Clearly $K \subseteq H^+ \subseteq L$. In fact H^+ is a subfield of L ($H^+ \leq L$).

(Let $x, y \in H^+$, then $\forall h \in H$, $h(y) = y$ and $h(x) = x$. Then:
$h(x+y) = h(x) + h(y) = x+y \ \forall h \in H$.
$\Rightarrow x+y \in H^+$
Similarly, $xy \in H^+$, $xy^{-1} \in H^+$, $x-y \in H^+$
$\Rightarrow H^+ \in \mathcal{J}$)

1) Suppose $M_1 \subseteq M_2$, then $M_2^* \subseteq M_1^*$

(Let $g \in M_2^*$, then $g(x) = x \ \forall x \in M_2$. Since $M_1 \subseteq M_2$, $g(y) = y$ $\forall y \in M_1 \Rightarrow g \in M_1^* \ \forall g \in M_1^*$.)

2) Suppose $H_1 \leq H_2$, then $H_1^+ \supseteq H_2^+$

(for the same/similar reason as above).

H^+ is called the fixed field of H.

3) We have $M \subseteq (M^*)^+ \ \forall M \subseteq \mathcal{J}$.

$M^* =$ things fixing M
$(M^*)^+ =$ things fixed by M^*
$=$ things fixed by (things fixing M).

Let $x \in M$, $g \in M^*$. By definition of M^*, $g(x) = x \ \forall g \in M^*$.
By definition of $+$, $x \in (M^*)^+$.

Remark

Under some circumstances, (normality and separability) $M = M^{*+}$ and $H = H^{+*}$.

$\Leftrightarrow$ $*$ and $+$ are mutual inverses.

In this case G is just $\mathcal{F}$ upside down.

This is the Galois correspondance.

<u>Example</u>

$\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}$ is a separable normal extension, so Galois correspondance holds.

$$\Gamma = \{id, \gamma_1\} \times \{id, \gamma_2\} \cong C_2 \times C_2$$
$$= \{id, \gamma_1, \gamma_2, \gamma_3\}$$

- $\gamma_1(\sqrt{2}) = -\sqrt{2}$ and $\gamma_1(\sqrt{3}) = \sqrt{3}$
- $\gamma_2(\sqrt{2}) = \sqrt{2}$ and $\gamma_2(\sqrt{3}) = -\sqrt{3}$
- $\gamma_3(\sqrt{2}) = -\sqrt{2}$ and $\gamma_3(\sqrt{3}) = -\sqrt{3}$

There are exactly 3 proper subgraps of $\Gamma(\mathbb{Q}(\sqrt{2},\sqrt{3}) ; \mathbb{Q})$

$$\langle \gamma_1 \rangle = \{id, \gamma_1\}$$
$$\langle \gamma_2 \rangle = \{id, \gamma_2\}$$
$$\langle \gamma_3 \rangle = \{id, \gamma_3\}$$

G (upside down):

$$\begin{tikzcd}
G & & \cancel{\Gamma}\ \{id\} \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\langle \gamma_1 \rangle \arrow[drr, dash] & & \langle \gamma_2 \rangle \arrow[d, dash] & & \langle \gamma_3 \rangle \arrow[dll, dash] \\
& & \cancel{\{id\}}\ \Gamma & &
\end{tikzcd}$$

F (right way up):

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{3},\sqrt{2}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

The obvious intermediate fields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$.
Quite a long calculation shows that there aren't any others.

$$\langle \gamma_1 \rangle^{+} = \{x \in \mathbb{Q}(\sqrt{2},\sqrt{3}) : \gamma(x) = x\}$$

$$x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \quad \text{with } a,b,c,d \in \mathbb{Q}$$

$$\gamma_1(x) = \gamma_1(a) + \gamma_1(b)\gamma_1(\sqrt{2}) + \gamma_1(c)\gamma_1(\sqrt{3}) + \gamma_1(d)\gamma_1(\sqrt{6})$$
$$= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$

$$\gamma_1(x) = x \iff b = -b \text{ and } d = -d$$
$$\iff b = 0,\ d = 0$$
$$\iff x = a + c\sqrt{3}$$

$$\Rightarrow \langle \gamma_1 \rangle^{+} = \mathbb{Q}(\sqrt{3})$$

$$\mathbb{Q}(\sqrt{3})^{*} = \{g \in \Gamma : g(x) = x \ \forall x \in \mathbb{Q}(\sqrt{3})\}$$
$$= \{g \in \Gamma : g(\sqrt{3}) = \sqrt{3}\}$$
$$= \{id, \gamma_1\} = \langle \gamma_1 \rangle.$$

$$\Rightarrow \langle \gamma_1 \rangle^{+} = \mathbb{Q}(\sqrt{3}) \text{ and } \mathbb{Q}(\sqrt{3})^{*} = \langle \gamma_1 \rangle$$
$$+(\langle \gamma_1 \rangle) = \mathbb{Q}(\sqrt{3}) \text{ and } *(\mathbb{Q}(\sqrt{3})) = \langle \gamma_1 \rangle.$$

In a similar way:

$$+(\langle \gamma_2 \rangle) = \mathbb{Q}(\sqrt{2}) \text{ and } *(\mathbb{Q}(\sqrt{2})) = \langle \gamma_2 \rangle$$
$$+(\langle \gamma_3 \rangle) = \mathbb{Q}(\sqrt{6}) \text{ and } *(\mathbb{Q}(\sqrt{6})) = \langle \gamma_3 \rangle$$

Also ~~†*~~ $\dagger: \Gamma \to \mathbb{Q}$
$*: \mathbb{Q} \to \Gamma$.

Example 2

$\mathbb{Q}(\alpha) : \mathbb{Q}$ where $\alpha = \sqrt[3]{2}$. Not normal:

$$\begin{tikzcd} & & \mathbb{Q}(\alpha) \arrow[dll, shift left, "*"] \arrow[d, dash] \\ \Gamma = \{id\} \arrow[urr, shift left, "\dagger"] & & \mathbb{Q} \arrow[ll, "*"] \end{tikzcd}$$

$\Gamma = \{id\}$

$\{id\}^{\dagger} = \{x \in \mathbb{Q}(\alpha) \;\; id(x) = x\}$
$= \mathbb{Q}(\alpha)$

$\mathbb{Q}(\alpha)^{*} = \{g \in \Gamma : g(\alpha) = \alpha\} = \{id\}$
$\mathbb{Q}^{*} = \{id\}$

Chapter 9

Definition

Let $K \subseteq \mathbb{C}$, $f(t) \in K[t]$. f splits over K if f factorizes into linear factors in $K[t]$.

$\Leftrightarrow$ f splits over K if all its roots in $\mathbb{C}$ lie in K.

If $f(t) \in K[t]$ and $K \subseteq L \subseteq \mathbb{C}$ then $f(t) \in L[t]$.

Every polynomial $f \in \mathbb{C}[t]$ splits by the Fundamental Theorem of Algebra.

Examples

1) $f(t) = t^2 - 5$ splits over $\mathbb{Q}(\sqrt{5})$
$(t^2 - 5 = (t+\sqrt{5})(t-\sqrt{5})$

2) $f(t) = t^2 - 2$ splits of $\mathbb{Q}(\sqrt{2})$

Definition

A field $\Sigma \subseteq \mathbb{C}$ is a splitting field for the polynomial $f(t) \in K[t]$ if $K \subseteq \Sigma$ and:

1) f splits over Σ
2) if $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ', then $\Sigma = \Sigma'$.
(smallest field such that it splits).

In fact if f has roots $\sigma_1, \ldots, \sigma_n \in \mathbb{C}$, then $\Sigma = K(\sigma_1, \ldots, \sigma_n)$.

Theorem 9.4

Let $K \subseteq \mathbb{C}$, $f \in K[t]$, then there exists a unique splitting field Σ for f over K and $[\Sigma : K] < \infty$.

Proof

$\Sigma = K(\sigma_1, \ldots, \sigma_n)$ is the unique splitting field.

Since Σ is finitely generated and algebraic over K, by Lemma 6.11, $[\Sigma : K] < \infty$.

Lemma 9.5

$$\begin{tikzcd} \Sigma \arrow[r, dashed, "j"', "(mono)"] \arrow[d, dash] & L \arrow[d, dash] \\ K \arrow[r, "i", "\cong"'] & K' \end{tikzcd}$$

$f \mapsto i(f)$

Σ is the splitting field for f over K.
L is the field over which $i(f)$ splits over K'.

in words

Let $K, K' \subseteq \mathbb{C}$, $i : K \to K'$ be a field isomorphism. Let $f \in K[t]$ with splitting field Σ, and let $K' \subseteq L$ be such that $i(f)$ splits over L.

Then $\exists$ field monomorphism $j : \Sigma \longrightarrow L$ such that $j|_K = i$.

Proof of Lemma 9.5

7th February 2013

Σ is a splitting field $\Rightarrow f(t) = k(t - \alpha_1) \dots (t - \alpha_n)$ where $\alpha_i \in \Sigma$.

Let m be the minimal polynomial of α_1 over K. m is irreducible and $m | f$. $\Rightarrow i(m) | i(f)$

$i(f)$ splits in $L \Rightarrow i(m)$ splits over L. say $i(m) = (t - \alpha_1) \dots (t - \alpha_r)$ where $\alpha_i \in L$

$$\begin{tikzcd} K(\alpha_1) \arrow[r, "j_1"] \arrow[d, dash] & K'(\alpha_1) \arrow[d, dash] \\ K \arrow[r] & K' \end{tikzcd}$$

By 5.16, since the minimal polynomial of α_1 over $K = m(t)$ and the minimal polynomial of α_1 over $K_1 = i(m)(t)$

$\Rightarrow \exists$ an isomorphism $j_1 : K(\alpha_1) \longrightarrow K'(\alpha_1)$ such that:

$j_1(\alpha_1) = \alpha_1$
$j_1 I_K = i$

$$\begin{tikzcd} \Sigma \arrow[r, "j"] \arrow[d, dash] & L \arrow[d, dash] \\ K(\alpha_1) \arrow[r, "j_1"] \arrow[d, dash] & K'(\alpha_1) \arrow[d, dash] \\ K \arrow[r, "i"] & K' \end{tikzcd}$$

$\Sigma =$ splitting field of $f(t)/t - \alpha_1$ over $K(\alpha_1)$

$i\left(\frac{f(t)}{t - \alpha_1}\right)$ splits over $K'(\alpha_1)$

By induction of the degree of f: $\exists$ a monomorphism $j : \Sigma \to L$, $\square$ (such that $j I_{K(\alpha_1)} = j_1$.

Theorem 9.6

Let $i : K \to K'$ be an isomorphism. Σ is a splitting field of f over K, Σ' is the splitting field of $i(f)$ over K'.

Then $\exists$ an isomorphism $j : \Sigma \longrightarrow \Sigma'$ such that $j I_K = i$

$(\Leftrightarrow \Sigma \cong \Sigma')$

Diagram

$$\begin{array}{ccc} \Sigma & \overset{j}{\underset{\cong}{- - \to}} & \Sigma' \\ | & & | \\ K & \xrightarrow{i} & K' \\ & \cong & \\ f & \longmapsto & i(f) \end{array}$$

Proof

By Lemma 9.5, $\exists$ a monomorphism $j : \Sigma \longrightarrow \Sigma'$ such that $j|_K = i$

Now $j(\Sigma) \subseteq \Sigma'$ and $i(f)$ splits over $j(\Sigma)$

~~E~~ ~~f~~ ($f = k(t-\alpha_1)\dots(t-\alpha_n) \in \Sigma[t]$ such that
$i(f) = j(f) = j(k)(t - j(\alpha_1))\dots(t - j(\alpha_n))$ in $j(\Sigma)[t]$)

By definition of a splitting field, $j(\Sigma) = \Sigma' \Rightarrow j$ is an automorphism.

$\square$

Normality

Definition 9.8

A field extension $L : K$ is normal if every irreducible polynomial polynomial over K with one root in L splits over L.

Examples

1) ~~$\mathbb{Q} : \mathbb{C}$~~ $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is normal, but this is not evident.

2) $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ is not normal.

Let $f(t) = t^3 - 2$. Then $f(t) \in \mathbb{Q}[t]$ and f is irreducible.
f has one root in $\mathbb{Q}(\sqrt[3]{2})$, namely $\sqrt[3]{2}$, but f does not split over $\mathbb{Q}(\sqrt[3]{2})$ as the 2 roots are not reals.

Theorem 9.9

$L : K$ is normal and finite $\Leftrightarrow$ L is the splitting field of some polynomial $f(t) \in K[t]$ over K.

Proof

$\Rightarrow$ Suppose $L : K$ is normal and finite. By Lemma 6.11,
$L : K$ is finite $\Rightarrow$ $L : K$ is algebraic.
$\Rightarrow \exists \alpha_1, \dots, \alpha_n$ algebraic over K s.t. $L = K(\alpha_1, \dots, \alpha_n)$

Let m_i = minimal polynomial of α_i over K.

Let $f = m_1 \dots m_n$. Then L is a splitting field of f over K.

(each m_i has one root $\alpha_i \in L$ and m_i is irreducible so by normality. m_i splits over L. Hence f splits in L. }

Also, L is generated by roots of f $(\alpha_1, \dots, \alpha_n) \Rightarrow L$ is a splitting field of f over K).

$\underline{\Leftarrow}$ Let L be the splitting field of $g(t) \in K[t]$, over K.

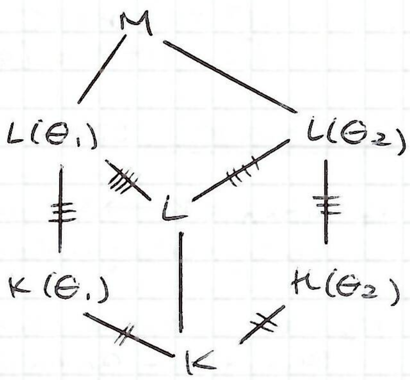
$L:K$ is finite (finitely generated algebraic extension) so need to prove that $L:K$ is normal.

Let $f(t) \in K[t]$ be an irreducible polynomial with one root in L, we must show that it splits in L.

Let $M \supseteq L$ be the splitting field for fg over K.

Let θ_1, θ_2 be two roots of f in M. We aim to prove that

$$[L(\theta_1) : L] = [L(\theta_2) : L]$$



$[K(\theta_1) : K] = [K(\theta_2) : K]$ because θ_1, θ_2 are roots of the same irred. polynomial f/K, so by 5.13, $K(\theta_1) : K \cong K(\theta_2) : K \Rightarrow$ the degrees are the same (6.7)

$L(\theta_i)$ is the splitting field of g over $K(\theta_i)$ $(i = 1, 2)$ (as L is the splitting field of g over K).

$\cancel{\Rightarrow}$ $K(\theta_1) \cong K(\theta_2)$
$\Rightarrow$ ~~[~~ $L(\theta_1) : K(\theta_1) \cong L(\theta_2) : K(\theta_2)$ (by 9.6)
$\Rightarrow$ $[L(\theta_1) : K(\theta_1)] = [L(\theta_2) : K(\theta_2)]$

By the Tower Law: $[L(\theta_1) : K] = [L(\theta_2) : K]$
$\Rightarrow$ $[L(\theta_1) : L][L : K] = [L(\theta_2) : L][L : K]$
$\Rightarrow$ $[L(\theta_1) : L] = [L(\theta_2 : L]$

Then if $\theta_1 \in L$, the degree is 1 and $\theta_2 \in L$ also
$\Rightarrow$ $L:K$ is normal. $\square$

<u>Recall</u> <u>19th January 2013</u>

If $K \subseteq \mathbb{C}$ is a field, then any irreducible polynomial over K is separable $\Leftrightarrow$ has no repeated roots.

$\Leftrightarrow$ a polynomial of degree n has n distinct roots.

The proof of this uses the idea of the derivative of f, in Lemma 9.1 (CORRECTION $K[t]$ not $\Sigma[t]$ at the end of the proof)

<u>Chapter 10 -</u>

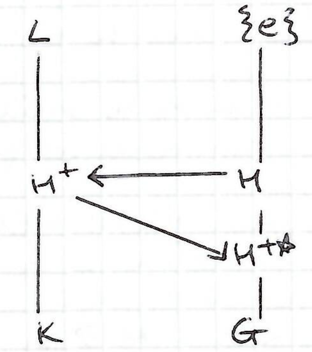
We are aiming at the following result:

If H is a finite group of automorphisms of a field L, then $[L : H^+] = |H|$

where $H^+ = \{x \in L : h(x) = x \ \forall h \in H\}$.

In chapter 11, we show that if $L:K$ is a finite normal (separable) extension then $|K^*| = [L:K]$

$$K^* = Gal(L:K)$$



From these two results, if $H \leq Gal(L:K)$ then:

$$|H^{+*}| = \cancel{[H^+ : K]} \ [L : H^+] = |H|$$

$$\text{since } H \subseteq H^{+*} \Rightarrow H = H^{+*}$$

Example

over $\mathbb{C}$, $H = \{id, c\}$ where $c(a+bi) = a - bi$. Then $|H| = 2$

$$H^+ = \{x \in \mathbb{C} : c(x) = x\} = \mathbb{R}$$
$$[\mathbb{C} : H^+] = [\mathbb{C} : \mathbb{R}] = 2$$

Lemma 10.1 (Dedekind's Lemma)

If $\lambda_1, \dots, \lambda_n \ \ K \longrightarrow L$ are distinct monomorphisms, then $\lambda_1, \dots, \lambda_n$ are linearly independent over L.

(if $a_1, \dots, a_n \in L$ then $a_1\lambda_1 + \dots + a_n\lambda_n : K \longrightarrow L$ is defined by
$(a_1\lambda_1 + \dots + a_n\lambda_n)(K) = a_1\lambda_1(K) + \dots + a_n\lambda_n(K)$
then $a_1\lambda_1 + \dots + a_n\lambda_n = 0 \Rightarrow$ all $a_i = 0$.

Example

Suppose length 3 shortest, say:

$$2\lambda_1 + 3\lambda_2 - 4\lambda_3 = 0$$
$$2\lambda_1(x) + 3\lambda_2(x) - 4\lambda_3(x) = 0 \quad \forall x. \quad (1)$$
$$2\lambda_1(y) + 3\lambda_2(y) - 4\lambda_3(y) = 0 \quad \forall y. \quad (2)$$

$$2\lambda_1(x)\lambda_1(y) + 3\lambda_2(x)\lambda_2(y) - 4\lambda_3(x)\lambda_3(y) = 0 \ \forall x, y. \quad (3)$$

$(1) \cdot \lambda_3(y)$: $\quad 2\lambda_1(x)\lambda_3(y) + 3\lambda_2(x)\lambda_3(y) - 4\lambda_3(x)\lambda_3(y) = 0 \quad (4)$

$(3) - (4)$: $\quad 2(\lambda_1(y) - \lambda_3(y))\lambda_1(x) + 3(\lambda_2(y) - \lambda_3(y))\lambda_2(x) = 0$
$\Rightarrow \quad 2(y_1(y) - \lambda_3(y))\lambda_1 + 3(\lambda_2(y) - \lambda_3(y))\lambda_2 = 0 \quad (5)$

Pick y such that $\lambda_1(y) \neq \lambda_3(y)$ then:
$2(\lambda_1(y) - \lambda_3(y)) \neq 0$
$3(\lambda_2(y) - \lambda_3(y)) \neq 0$ or $= 0$

(5) is a non-trivial relation of length < 3.

This is a contradiction. $\square$

You can't have a relation of length 1 as:

$$a_1\lambda_1 = 0$$
$$\Rightarrow a_1(\lambda_1)(1) = 0$$
$$\Rightarrow a_1 = 0 \Rightarrow a_1\lambda_1 \text{ is trivial.}$$

Example 1

Let $\alpha = \sqrt[4]{3}$
$K = \mathbb{Q}(\alpha, i)$, ~~let x = q0~~

K has $\mathbb{Q}$-basis $\{1, \alpha, \alpha^2, \alpha^3, \alpha i, \alpha^2 i, \alpha^3 i, i\}$

Let $\varphi: K \to K$ be given by $\varphi(\alpha) = i\alpha$, $\varphi(i) = -i$

$\varphi^2(\alpha) = \varphi(i\alpha) = \varphi(i)\varphi(\alpha) = -i \, i\alpha = \alpha$
$\varphi^2(i) = \varphi(-i) = -\varphi(i) = -(-i) = i$
$\Rightarrow \varphi^2(x) = x \quad \forall x \quad (\varphi^2 = id)$

$\Rightarrow G = \{id, \varphi\}$
$[K : K_0] = |G| = 2$

Example 2

$G = \{g_1, \dots, g_n\}$ for example $C_3 = \{e, x, x^2\}$
Then $G = \{gg_1, \dots, gg_n\}$

$xe = x$
$xx = x^2$
$xx^2 = x^3 = e$

Example 1 continued

Let $x = q_0 + q_1\alpha + q_2\alpha^2 + q_3\alpha^3 + q_4 i + q_5 i\alpha + q_6 i\alpha^2 + q_7 i\alpha^3$

$\varphi(x) = q_0 + q_1 i\alpha - q_2\alpha^2 + q_3 i\alpha^3 + q_4 i + q_5 i\alpha + q_6 i\alpha^2 + q_7 i\alpha^2$
– need to check this!

$x = \varphi(x) \Leftrightarrow$
$q_1 = q_5$
$q_2 = -q_2$
$q_3 = -q_7$
$q_4 = -q_4$
$q_5 = q_1$
$q_7 = -q_3$

So we have that:

$q_1 = q_5$
$q_2 = 0$
$q_7 = -q_3$
$q_4 = 0$

$\Rightarrow K^0 = \{q_0 + q_1\alpha + q_3\alpha^3 + q_1\alpha + q_6 i\alpha^2 - q_3 i\alpha^3\}$
$= \{q_0 + q_1(\alpha + \alpha i) + q_3(\alpha^3 - i\alpha^3) + q_6 i\alpha^2 : q_0, q_1, q_3, q_6 \in \mathbb{Q}\}$

$\Rightarrow [K^0 : \mathbb{Q}] = 4$
$\Rightarrow [K : K_0] = 8/4 = 2 = |G|$.

Theorem 10.5

Let G be a finite group of automorphisms of a field K and let $K_0 = \{x \in K : g(x) = x \ \forall g \in G\}$ be the fixed field.

Then $[K:K_0] = |G|$

<u>Proof</u>

Let $G = \{g_1, \dots, g_n\}$, so $|G| = n$.

Let $\{x_1, \dots, x_m\}$ be a K_0-basis for K, so $[K:K_0] = m$.
$\Rightarrow$ we must prove that $m = n$

<u>case 1)</u> Suppose $m < n$

Then $\exists\, y_1, \dots, y_m \in K$ not all zero such that:
$y_1 g_1(x_1) + y_2 g_2(x_1) + \dots + y_n g_n(x_1) = 0$
$y_1 g_1(x_2) + y_2 g_2(x_2) + \dots + y_n g_n(x_2) = 0$
$\vdots$
$y_1 g_1(x_m) + y_2 g_2(x_m) + \dots + y_n g_n(x_m) = 0$
is a homogeneous equation.
This is because it is a system of m equations in n unknowns. $(m < n)$

$\Leftrightarrow y_1 g_1 + \dots + y_n g_n$ is zero at $x_1, \dots, x_n$.

$\Rightarrow y_1 g_1 + \dots + y_n g_n$ is zero at any linear (K_0-linear) combination of $x_1, \dots, x_m$.

(If $x = \alpha_1 x_1 + \dots + \alpha_n x_m$ where $\alpha_i \in K_0$, then:
$(y_1 g_1 + \dots + y_n g_n)(\alpha_1 x_1 + \dots + \alpha_m x_m)$
$= y_1 g_1(\alpha_1 x_1 + \dots + \alpha_m x_m) + \dots + y_n g_n(\alpha_1 x_1 + \dots + \alpha_m x_m)$
$= (y_1 \alpha_1 g_1(x_1) + \dots + y_1 \alpha_m g_1(x_m)) + \dots + (y_n \alpha_1 g_n(x_1) + \dots + y_n \alpha_m g_n(x_m))$
$= \alpha_1 (y_1 g_1(x_1) + \dots + y_n g_n(x_1)) + \dots \alpha_m (y_1 g_n(x_1) + \dots + y_n g_n(x_m))$
$= 0$

But $\{x_1, \dots, x_m\}$ is a K_0-basis for K, so $(y_1 g_1 + \dots + y_n g_n)(x) = 0$ $\forall x \in K$.

$\Rightarrow y_1 g_1 + \dots + y_n g_n = 0$
which contradicts Dedekind's lemma.
$\Rightarrow m < n$ is not possible.

<u>case 2)</u> Suppose $m > n$

Then $\{x_1, \dots, x_n, x_{n+1}\}$ is linearly independent over K_0.
$\exists\, y_1, \dots, y_{n+1}$ not all zero such that

$y_1 g_1(x_1) + \dots + y_{n+1} g_1(x_{n+1}) = 0$
$y_1 g_2(x_1) + \dots + y_{n+1} g_2(x_{n+1}) = 0$
$\vdots$
$y_1 g_n(x_1) + \dots + y_{n+1} g_n(x_{n+1}) = 0$

Pick such a solution (which exists as $m > n$) with as few non-zero terms as possible, and renumber:

$y_1 g_1(x_1) + \dots + y_r g_1(x_r) = 0$
$\vdots$
$y_1 g_n(x_1) + \dots + y_r g_n(x_r) = 0$

all $y_i \neq 0$, and there is no solution with less than r terms.
Let $g \in G$ and apply to 10.8:

$$g(y_1)gg_1(x_1) + \dots + g(y_r)gg_1(x_r) = 0$$
$$\vdots$$
$$g(y_1)gg_n(x_1) + \dots + g(y_r)gg_n(x_r) = 0$$

As g varies over G, so does gg_i (10.8), (10.9)
so the above system is the same as:

$$g(y_1)g_1(x_1) + \dots + g(y_r)g_1(x_r) = 0$$
$$\vdots$$
$$g(y_1)g_n(x_1) + \dots + g(y_r)g_n(x_r) = 0$$

$$\Rightarrow \quad (g(y_1)y_1 - y_1g(y_1))g_1(x_1) + (g(y_1)y_2 - y_1g(y_2))g(x_2) + \dots = 0$$
$$\vdots$$
$$\underbrace{(g(y_1)y_1 - y_1g(y_1))}_{=0} g_n(x_1) + (g(y_1)y_2 - y_1g(y_2))g_n(x_2) + \dots = 0$$

So this is a shorter solution than 10.8, which is a contradiction unless all coefficients are zero

$$\Rightarrow \quad g(y_1)y_2 = y_1g(y_2)$$
$$g(y_1)y_3 = y_1g(y_3)$$
$$\vdots$$

$$\Rightarrow \quad g(y_1)y_i = y_ig(y_1)$$
$$\Rightarrow \quad g(y_iy_1^{-1}) = y_iy_1^{-1} \quad \forall g \in G$$
$$\Rightarrow \quad y_iy_1^{-1} \in K_0 \text{ and so } y_i = y_1z_i \quad (z_i \in K_0)$$

Back to 10.8:

$$y_1g_1(x_1) + \dots + y_rg_1(x_r) = 0$$

Take $g_1 = id$

$$y_1x_1 + \dots + y_rx_r = 0$$
$$\Rightarrow y_1x_1 + y_1z_2x_2 + \dots + y_1z_ry_r = 0$$
$$\Rightarrow x_1 + z_2x_2 + \dots + z_rx_r = 0$$
$$\Rightarrow \{x_1, \dots, x_r\} \text{ is linearly dependent } / K_0.$$

contradiction!

$$\Rightarrow m = n \quad \square$$

<u>Chapter 10</u> <u>21st February 13</u>

G finite group of automorphisms of K, K_0 = fixed field

$$[K : K_0] = |G|$$

<u>Chapter 11</u>

<u>Corollary 11.11</u>

$L:K$ finite normal sep extension. then:

$$|\Gamma(L:K)| = [L:K]$$

Definition

Let K be a subfield of L, M. Then a K-monomorphism is a field homomorphism $\varphi: L \longrightarrow M$ which is injective and $\varphi|_K = id$.

Example

$$\begin{tikzcd} L \arrow[r, "\varphi"] \arrow[d, dash] & L \arrow[d, dash] \\ M \arrow[r] \arrow[d, dash] & \varphi(M) \arrow[d, dash] \\ K \arrow[r, "id"'] & K \end{tikzcd}$$

What are $\mathbb{Q}$-monomorphisms $\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$?

id, $\varphi_1(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, $\varphi_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$

Theorem 11.3

Let $K \leq M \leq L$ and suppose $L:K$ is normal and finite. Then any K-monomorphism $\tau: M \longrightarrow L$ extends to a K-automorphism $\sigma: L \rightarrow L$.

$$\begin{tikzcd} L \arrow[r, dashed, "\sigma"] \arrow[d, dash] & L \arrow[d, dash] \\ M \arrow[r, "\tau"'] \arrow[d, dash] & \tau(M) \arrow[d, dash] \\ K \arrow[r, "id"'] & K \end{tikzcd}$$

$(\Leftrightarrow \sigma|_M = \tau)$

Proof

By 9.9, L = splitting field of some polynomial f over K.

$\Rightarrow L$ = splitting field of f over M, and over $\tau(M)$, so by Theorem 9.6, $\exists\ \sigma: L \rightarrow L$ such that:

$$\begin{tikzcd} L \arrow[r, dashed] \arrow[d, dash] & L \arrow[d, dash] \\ M \arrow[r, "\tau"] \arrow[r, phantom, shift right=3ex, "f \mapsto f"] \arrow[d, dash] & \tau(M) \arrow[d, dash] \\ K \arrow[r, "id"'] & K \end{tikzcd}$$

$\sigma|_M = \tau$
$\sigma|_K = \tau|_K = id$

Proposition 11.4

Suppose $L:K$ is a finite normal extension, and α, β are $\in L$ with the same minimal polynomial, say p over K. Then $\exists$ a K-automorphism σ of L such that $\sigma_p(\alpha) = \beta$.

Proof

By 5.13, $\exists$ a K-isomorphism $\tau: K(\alpha) \rightarrow K(\beta)$. Regard τ as a K-monomorphism from $K(\alpha) \rightarrow L$. By 11.3, $\exists\ \sigma: L \rightarrow L$ K-automorphism such that $\sigma|_{K(\alpha)} = \tau$. Hence $\sigma(\alpha) = \tau(\alpha) = \beta$. □

Definition 11.5

Let $L:K$ be a finite extension. A normal closure of $L:K$ is an extension $N:K$ where $L \leq N$ such that:

1) $N:K$ is normal
2) If $L \leq M \leq N$ and $M:K$ is normal, then $M = N$.

Theorem 11.6

If $[L:K]$ is a finite extension inside $\mathbb{C}$, then $\exists$ a unique normal closure $N:K$, which is finite.

Proof

Let $x_1, \dots, x_r$ be a basis for L over K, let m_i be the minimal polynomial of x_i over K.

Let $f = m_1 \dots m_r \in K[t]$

Let $N =$ splitting field of f over K.

$N:K$ is normal and finite by Theorem 9.9. Suppose $L \subseteq M \subseteq N$, $M:K$ is normal. Then $x_i \in M$ with minimal polynomial m_i / K

$\Rightarrow$ by normality m_i splits in M.
$\Rightarrow$ f splits in M.

By the definition of splitting field, $M = N$
$\Rightarrow$ N is a normal closure of $L:K$

Suppose M, N both normal closures of $L:K$. Then f splits in both M and N, so both M and N contain the splitting field of f over K. By minimality, $N = M =$ splitting field.

Lemma 11.8

Suppose $K \subseteq L \subseteq \cancel{M}\, N \subseteq M$ where $L:K$ is finite and $N:K$ is the normal closure of $L:K$. Let $\tau : L \longrightarrow M$ be any K-monomorphism. Then $\tau(L) \subseteq N$.

$$\begin{tikzcd} M \arrow[d, dash] & & M \arrow[dd, dash] & \\ N \arrow[d, dash] & & & N \arrow[dl, dash] \\ L \arrow[d, dash] \arrow[rr, "\tau"] & & \tau(L) \arrow[d, dash] & \\ K \arrow[rr, "id"] & & K & \end{tikzcd}$$

Proof

Let $\alpha \in L$. Let $m \in K[t]$ be the minimal polynomial of α over K, so $m(\alpha) = 0$

$\Rightarrow$ $\tau(m(\alpha)) = 0$
$\Rightarrow$ $m(\tau(\alpha)) = 0$
$\Rightarrow$ $\tau(\alpha)$ is a root of m since $m(\tau(\alpha)) = 0$.

Since $N:K$ is normal and m irreducible over K and m has one root in α in N, m must split over N $\Leftrightarrow$ $\tau(\alpha) \in N$ $\square$

26th February 2013

Recall

Let $L:K$ be a finite extension. Then any K-monomorphism $L \to L$ is a K-automorphism of L.

Theorem 11.9

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

1) $L:K$ is normal

2) $\exists$ a finite normal extension $N:K$ such that $L \subseteq N$, such that every K-monomorphism $\tau : L \longrightarrow N$ is a K-automorphism of L ($\Leftrightarrow$ $\tau(L) \subseteq L$)

3) For every finite extension $M \supseteq L$, every K-monomorphism $\tau: L \longrightarrow L$ is a K-automorphism of L ($\tau(L) \subseteq L$)

Proof

$1 \Rightarrow 3$

Let $L:K$ be normal. Then the normal closure of $L:K$ is L. By 11.8, $\tau(L) \subseteq L$.

$3 \Rightarrow 2$

Let N be the normal closure of $L:K$. By (3), for any K-monomorphism $\tau: L \to N$, $\tau(L) \subseteq L$.

$2 \Rightarrow 1$

Let f be any irreducible polynomial over K, with one root α in L. $\alpha \in N$. Since $N:K$ is normal, any other root β of f lies in N. By 11.4, since $N:K$ is normal, $\exists$ a K-automorphism $\sigma: N \longrightarrow N$ such that $\sigma(\alpha) = \beta$. Then $\tau = \sigma_{|L}$

$\tau: L \to N$ is a K-monomorphism.
By (2) $\tau(L) \subseteq L \Rightarrow \beta = \tau(L) \subseteq L$
$\Rightarrow L:K$ is normal.

Theorem 11.10

Suppose $[L:K] = n$. Then there are precisely n K-monos $L \to N$, where N is the normal closure of $L:K$.

(and hence into any $M \supseteq L$ such that $M:K$ is normal).

Corollary 11.11

If $L:K$ is normal and $[L:K] = n$, then $|\Gamma(L:K)| = n$

Proof of corollary 11.1

By theorem, there are precisely n K-monomorphisms of L into $N = L$. As noted above, any K-monomorphism $L \to L$ is in fact a K-automorphism of L.
$\Leftrightarrow$ an element of $\Gamma(L:K)$.

Proof of theorem 11.10

We do induction of $[L:K]$.

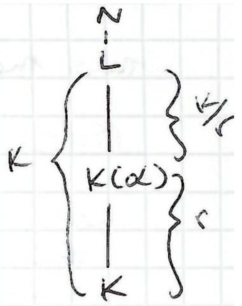
If $[L:K] = 1$, nothing to prove.

Suppose $[L:K] = k$ and the result holds for $1, \dots, k-1$.

Pick $\alpha \in L \setminus K$, and let $m \in K[t]$ be the minimal polynomial of α over K, with $\deg(m) = r$, $r > 1$.

$\Rightarrow [K[\alpha]:K] = r$

m splits in N, say with roots $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$.
(all distinct since separable)



Since m is an irreducible polynomial over K with roots α, α_i in N and $N:K$ normal, so by 11.4, $\exists$ a K-automorphism τ_i of N such that $\tau_i(\alpha) = \alpha_i$

$L:K(\alpha)$ is a finite extension of degree $s<k$ and N is the normal closure of $L:K(\alpha)$. By the induction hypothesis, there are exactly s $(= k/r)$ K-monomorphism $\rho_1, \dots, \rho_s : L \to N$.

Let $\varphi_{ij} = \tau_i \rho_j \quad L \longrightarrow N$. We claim that φ_{ij} $(1 \leq i \leq r,\ 1 \leq j \leq s)$ are precisely the K-monomorphisms $L \longrightarrow N$.

These clearly are K-monomorphisms $L \longrightarrow N$ and are all distinct. (missing from book)... suppose $\varphi_{ij} = \varphi_{kl}$
$\Leftrightarrow \tau_i \rho_j = \tau_k \rho_l$. Then $\tau_i \rho_j(\alpha) = \tau_i(\alpha) = \alpha_i$ and $\tau_k \rho_l(\alpha) = \tau_k(\alpha) = \alpha_k \Rightarrow \alpha_i = \alpha_k$. But the roots are all distinct, $\Rightarrow i = k$. So $\tau_i \rho_j = \tau_i \rho_l$. τ_i is bijective,
$\Rightarrow \rho_j = \rho_l \Rightarrow j = l$. $\Rightarrow$ all distinct!

There are $rs = k$ of these φ_{ij} - now need that any K-monomorphism $L \to N$ is one of the φ_{ij}.

Let $\tau : KL \longrightarrow N$ be a K-monomorphism.

$$m(\tau(\alpha)) = \tau(m(\alpha)) = \tau(0) = 0$$
$\Leftrightarrow \tau(\alpha) =$ a root of m.
$\Rightarrow \tau(\alpha) = \alpha_i$ for some $1 \leq i \leq r$.

$\tau_i^{-1} \tau$ is a K-monomorphism $L \longrightarrow N$ and $\tau_i^{-1}\tau(\alpha) = \tau_i^{-1}(\alpha_i) = \alpha$

$\Rightarrow \tau_i^{-1}\tau$ is a $K(\alpha)$-monomorphism $L \to N$.
$\Rightarrow \tau_i^{-1}\tau = \rho_j$ some $1 \leq j \leq s$.
$\Rightarrow \tau = \tau_i \rho_j = \varphi_{ij}$ $\square$

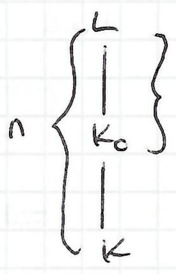
Theorem 11.12

Let $L:K$ be a finite normal extension of degree n with Galois Group ~~g~~ G.

Then $K =$ fixed field of G.

Proof

Let $K_0 =$ fixed field of G. $K_0 \supseteq K$ by definition



By Corollary, $|G| = n$
By Theorem 10.5, $[L:K_0] = |G| = n$

$\Rightarrow [K_0 : K] = 1$ by the Tower Law.
$\Rightarrow K_0 = K$ $\square$

Theorem 11.13

Suppose $K \subseteq L \subseteq ~~\mathcal{S}~~ M$ and, and $[M:K] < \infty$, Then the number of distinct K-monomorphisms $L \to M \leq [L:K]$

Proof

Let N = normal closure of M : K.
Then any K-monomorphism $L \to M$ is a K-monomorphism $L \to N$.

By 11.11, there are exactly $[L:K]$ K-monomorphisms $L \to N$, hence $\leq [L:K]$ K-monomorphisms $L \to M$.

Theorem 11.14

Let $L:K$ be a finite extension with Galois group G. If K is the fixed field of G, then $L:K$ is normal

Proof

By Theorem 10.5, $[L:K] = |G| = n$.
Hence, there are exactly n K-automorphisms of L.

Let N be the normal closure of $L:K$. By Theorem 11.10, there are precisely n K-monomorphisms $L \to N$, but the n elements of G are K-monos of $L \to N$. $\Rightarrow$ every K-monomorphism $L \to N$ is a K-automorphism of L. By 11.9, $L:K$ is normal $\square$

Exercise 11.7

b 1) True
c 2) True
d) False
e) False
f) False
g) True
h) True
i) False

Lemma 12.2

Let $L:K$ be a field extension, $K \subseteq M \subseteq L$, τ is a K-automorphism of L.

Then $\tau(M)^* = \tau M^* \tau^{-1}$

Proof

Let $g \in M^*$. Then for any $m \in M$.

$(\tau g \tau^{-1})(\tau(m)) = \tau g(m) = \tau(m)$
$\Rightarrow$ $\tau g \tau^{-1}$ fixes every element in $\tau(M)$

$\Rightarrow$ $\tau M^* \tau^{-1} \leq \tau(M)^*$

Suppose $g \in \tau(M)^*$.
Then $\forall m \in M$, $g(\tau(m)) = \tau(m)$
$\Rightarrow$ $(\tau^{-1} g \tau)(m) = m$

$$\Rightarrow \quad \tau^{-1} g \tau \in M^{*}$$
$$\Rightarrow \quad g \in \tau M^{*} \tau^{-1} \quad \forall g \in \tau(M^{*})$$
$$\Rightarrow \quad \tau(M^{*}) \subseteq \tau M^{*} \tau^{-1}$$
$$\Rightarrow \quad \tau(M^{*}) = \tau M^{*} \tau^{-1}! \qquad \square$$

28/2/13.

$$\begin{array}{ccc} L & \longleftrightarrow & \{id\} \\ | & & | \\ M = H^+ & \longleftrightarrow & H = M^* \\ | & & | \\ K & \longleftrightarrow & G \end{array}$$

(iv) ($\Rightarrow$) Suppose $M:K$ normal
Let $\tau \in G$ i.e. $\tau : L \to L$ is a K-aut. $\tau|_M : M \to L$ is a K-mono.

Since $M:K$ normal, by E, $\tau(M) \subseteq M$ and $\tau|_M : M \to M$ is a K-aut

By D

$$\tau M^* \tau^{-1} = \tau(M)^* = M^*$$

M^* is a normal subgroup of G.

($\Leftarrow$) Suppose $M^* \trianglelefteq G$ normal subgroup

Let $\sigma : M \to L$ be a K-mono. By F, σ extents to a K-aut of L say $\tau : L \to L$ i.e. $\tau|_M = \sigma$.

By D, $\tau(M)^* = \tau M^* \tau^{-1}$

and since M^* normal, $\tau M \tau^{-1} = M^*$

$$\tau(M)^* = M^*$$

Hence by previous part of th^m, $\tau(M) = M$ i.e $\sigma(M) = M$

Thus for any K-mono $\sigma : M \to L$ $\sigma(M) = M$

By E, $M:K$ is normal, so $M^* \trianglelefteq G$.

Define $\varphi : \Gamma(L:K) \longrightarrow \Gamma(M:K)$
by $\varphi(\tau) = \tau|_M$ (because $M:K$ is normal,
by E, $\tau(M) = M$ so $\varphi(\tau) : M \to M$)

By F, φ is surjective. [if $\sigma \in \Gamma(M:K)$,
σ can be regarded as a K-mono $M \to L$
by F this extends to a K-aut, say $\tau : L \to L$
i.e $\tau|_M = \sigma$]

φ is a group homomorphism. By 1st iso theorem

$$\frac{\Gamma(L:K)}{Ker(\varphi)} \cong Im\,\varphi = \Gamma(M:K)$$

$$\begin{aligned} Ker\,\varphi &= \{\tau \in \Gamma(L:K) : \varphi(\tau) = id\} \\ &= \{\tau \in \Gamma(L:K) : \tau|_M = id\} \\ &= M^* \end{aligned}$$

$$\frac{G}{M^*} \cong \Gamma(L:K)$$

Ex: Find Galois group of the splitting field of t^3-2 over $\mathbb{Q}$. Find all intermediate fields

① Let L = splitting field.

Roots of $t^3-2=0$ are $\alpha, \omega\alpha, \omega^2\alpha$.
where $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3}$

$$L = \mathbb{Q}(\alpha, \alpha\omega, \alpha\omega^2)$$

$$L = \mathbb{Q}(\alpha, \omega)$$

② Find $[L:K]$

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha,\omega) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & & \mathbb{Q}(\omega) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

α has min poly t^3-2 (irreducible by Eisenstein, prime 2) $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$

ω has min poly $\dfrac{t^3-1}{t-1} = t^2+t+1$

This is irreducible since $\omega \notin \mathbb{Q}$. $[\mathbb{Q}(\omega):\mathbb{Q}]=2$
Hence $[\mathbb{Q}(\alpha)(\omega):\mathbb{Q}(\alpha)] \leqslant 2$, i.e $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}] \leqslant 6$ by Tower law, 2 and 3 divide $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]$, so $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]=6$.

③ $|G| = 6$.

④ Find the elements of G. $\sigma : \mathbb{Q}(\alpha, \omega) \to \mathbb{Q}(\alpha,\omega)$
Any $\sigma \in G$ is determined by $\sigma(\alpha)$ and $\sigma(\omega)$. Also $\sigma(\alpha)$ must be a root of min poly of α, $t^2 - 2$, i.e $\sigma(\alpha) = \alpha$ or $\alpha\omega$ or $\alpha\omega^2$. $\sigma(\omega)$ must be a root of $t^2+t+1=0$ i.e $\sigma(\omega) = \omega$ or ω^2.

This it gives us 6 potenial elements of G

$$\sigma_1(\alpha) = \alpha, \quad \sigma_1(\omega) = \omega.$$
$$\sigma_2(\alpha) = \alpha\omega, \quad \sigma_2(\omega) = \omega$$
$$\sigma_3(\alpha) = \alpha\omega^2, \quad \sigma_3(\omega) = \omega$$
$$\sigma_4(\alpha) = \alpha, \quad \sigma_4(\omega) = \omega^2$$
$$\sigma_5(\alpha) = \alpha\omega, \quad \sigma_5(\omega) = \omega^2$$
$$\sigma_6(\alpha) = \alpha\omega^2, \quad \sigma_6(\omega) = \omega^2.$$

⑤ We dont know priori that there is a $\mathbb{Q}$-aut of L st e.g $\sigma_3(\alpha) = \alpha\omega^2$, $\sigma_3(\omega) = \omega$. We could prove existence of σ_3 by extenseoin theorems, but here since $|G| = 6$ and $\tau_1 \dots \tau_6$ are the only candiates, they make up G.

⑥ $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

Let $g = \sigma_2$, $\quad g(\alpha) = \alpha\omega$, $\quad g(\omega) = \omega$
$\quad\; h = \sigma_4$, $\quad h(\alpha) = \alpha$, $\quad h(\omega) = \omega^2$

$g^2(\alpha) = g(\alpha\omega) = g(\alpha)g(\omega) = \alpha\omega\omega = \alpha\omega^2$

$g^2(\omega) = g(\omega) = \omega$. $\quad g^2 = \sigma_3$.

$(gh)(\alpha) = g(\alpha) = \alpha\omega$.

$(gh)(\omega) = g(\omega^2) = \omega^2$

$gh = \sigma_5$

$g^2h = \sigma_6$.

$G = \{id, g, g^2, h, gh, g^2h\}$.

5th March

L = splitting field of t^3-2 over $\mathbb{Q}$.
$G = \mathrm{Gal}(L:\mathbb{Q})$

$L = \mathbb{Q}(\alpha, \omega)$, $\alpha = \sqrt[3]{2}$, $\omega = e^{\frac{2\pi i}{3}}$

$[L:\mathbb{Q}] = 6$
$\Rightarrow |G| = 6$

Find all possibilities for $g \in G$.

$G = \{g_1, g_2, \ldots, g_6\}$

$g(\alpha) = \alpha\omega \quad g(\omega) = \omega$
$h(\alpha) = \alpha \quad h(\omega) = \omega^2$

$\Rightarrow G = \{e, g, g^2, h, gh, g^2h\}$

$g^3 = e$
$h^2 = e$

$(hg)(\alpha) = h(g(\alpha)) = h(\alpha\omega) = h(\alpha)h(\omega) = \alpha\omega^2$
$(hg)(\omega) = h(\omega) = \omega^2$

$(g^2h)(\alpha) = g^2(\alpha) = g(g(\alpha)) = g(\alpha\omega) = g(\alpha)g(\omega) = \alpha\omega^2$
$(g^2h(\omega) = g^2(\omega^2) = g(g(\omega^2)) = g(\omega^2) = \omega^2$

$\Rightarrow \quad g^2h = hg$

$\Rightarrow \quad G = \langle g, h : g^2 = h^3 = e, \ hg = g^2h \rangle$

<u>Stage 7</u> : Find all subgroups of G.

Suppose $H \leq G$. Then by Lagrange's Theorem:

$|H| \mid |G| = 6$
$\Rightarrow \quad |H| = 1, 2, 3, 6.$

if $|H| = 1, \quad H = \{e\}$
$|H| = 6, \quad H = G$

if $|H| = 3$, since 3 is prime $H \cong C_3 \Rightarrow H = \langle K \rangle \ o(K) = 3.$

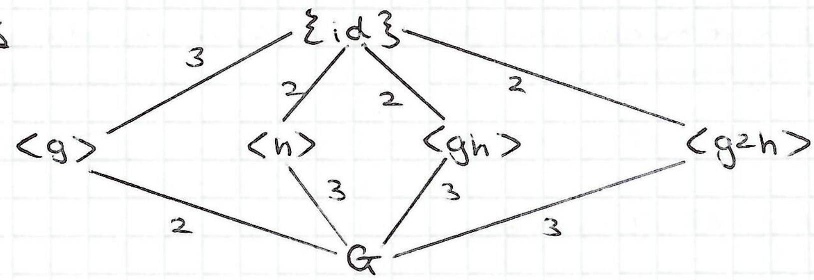
$G = \{e, \ g, \ g^2, \ h, \ hg, \ hg^2\}$
order: 1 3 3 2 2 2

$\Rightarrow \quad K = g$ or g^2.

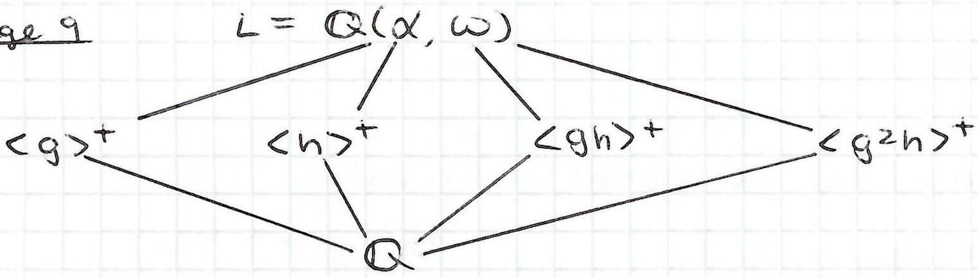
$H = \langle g \rangle = \langle e, g, g^2 \rangle = \langle g^2 \rangle$
$\Rightarrow$ only one subgroup of order 3 : $\langle g \rangle$.

if $|H| = 2$, 2 is prime $\Rightarrow H \cong C_2$.
$\Rightarrow \quad H = \langle h \rangle, \langle gh \rangle, \langle g^2h \rangle$.

<u>Stage 8</u>



<u>Stage 9</u>



$\langle g \rangle^+ = \{x \in L : g(x) = x\}$

$\Rightarrow \quad x = \beta_0 + \beta_1 \alpha + \beta_2 \alpha^2 + \beta_3 \omega + \beta_4 \alpha\omega + \beta_5 \alpha^2 \omega \quad (\beta_i \in \mathbb{Q})$
$\Rightarrow g(x) = \beta_0 - \beta_4 \alpha - \beta_2 \alpha^2 + \beta_5 \alpha^2 + \beta_3 \omega + (\beta_1 - \beta_4)\alpha\omega - \beta_2 \alpha^2 \omega.$

$x = g(x) \Leftrightarrow \beta_1 = \beta_4 \quad \beta_2 = -\beta_2 + \beta_5, \quad \beta_4 = \beta_1 - \beta_4, \quad \beta_5 = -\beta_2$

$\beta_1 = \beta_4 = 0$
$\beta_2 = 0$

$\Rightarrow \langle g \rangle^\dagger = \{\beta_0 + \beta_3 : \beta_0, \beta_3 \in \mathbb{Q}\} = \mathbb{Q}(\omega)$

This is quite a tedious way of doing this. there is a quicker way, which is:

Clearly $\omega \in \langle g \rangle^\dagger$
$\Rightarrow \mathbb{Q}(\omega) \subseteq \langle g \rangle^\dagger$
$\Rightarrow \mathbb{Q}(\omega) = \mathbb{Q}$ or $\langle g \rangle^\dagger$

since $\omega \notin \mathbb{Q}$, $\mathbb{Q}(\omega) = \langle g \rangle^\dagger$

Similarly, $\langle h \rangle^\dagger = \mathbb{Q}(\alpha)$

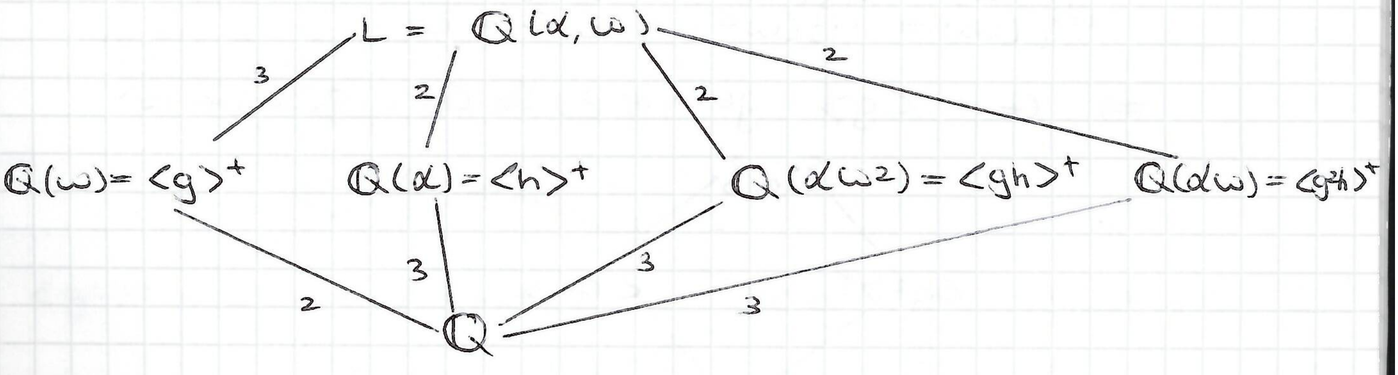
what about $\langle gh \rangle^\dagger$? Note that for any $x \in L$, $x + gh(x)$ is fixed by gh:

$$gh(x + gh(x)) = gh(x) + (gh)^2(x) = gh(x) + x$$

Try $\alpha + gh(\alpha) = \alpha + \alpha\omega = \alpha(1+\omega) = -\omega^2\alpha$
$\Rightarrow \alpha\omega^2 \in \langle gh \rangle^\dagger$
$\Rightarrow \mathbb{Q}(\alpha\omega^2) \subseteq \langle gh \rangle^\dagger$

$\alpha\omega^2 \notin \mathbb{Q} \Rightarrow \mathbb{Q}(\alpha\omega^2) = \langle gh \rangle^\dagger$

Going like this also gives $\mathbb{Q}(\alpha\omega) = \cancel{\mathbb{Q}} \langle g^2 h \rangle$



<u>Normality</u>

The only normal subgroup is $\langle g \rangle$ $\quad (\langle g \rangle \lhd G)$
$\Rightarrow \mathbb{Q}(\omega) : \mathbb{Q}$ is normal.

$\Rightarrow \Gamma(\mathbb{Q}(\omega) : \mathbb{Q}) \cong G/\langle g \rangle = S_3 / C_3 \cong C_2.$

<u>Example</u>

Let L = splitting field of $t^7 - 1$ over $\mathbb{Q}$

$\omega = e^{\frac{2\pi i}{7}}$

1) $L = \mathbb{Q}(\omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6)$ $\qquad \omega = e^{\frac{2\pi i}{7}}$

~~$[L : \mathbb{Q}] = 7$ as $t^7 - 1$ has degree 7.~~

~~$[\mathbb{Q}(\omega) : \mathbb{Q}] = 7$~~
~~$[\mathbb{Q}(\omega, \omega^2) : \mathbb{Q}] =$~~

But $\omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6$ all have the same minimal polynomial.

$\Rightarrow \quad L = \mathbb{Q}(\omega)$
$\Rightarrow \quad [L : \mathbb{Q}] = \cancel{7}\, 6$ (by the degree of $\cancel{7}^{\,6}$)

2) ~~3)~~ $|G| = [L : \mathbb{Q}] = \cancel{7}\, 6$
$\Rightarrow |G| = \cancel{7}\, 6$

$G = \{g_1, g_2, g_3, \dots, g_{\cancel{7}}\}$

$m(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$
(by Eisenstein's criterion - $s = t+1$)

5) $g \in G = \Gamma(L : \mathbb{Q})$ is determined by

$g(\omega) = \omega$ or ω^2 or ... or ω^6
$\Rightarrow$ 6 possibilities of g.
$\Rightarrow |G| = 6$

$G = \{g_1, g_2, \dots, g_6\}$ where $g_i(\omega) = \omega^i$

$g_3(\omega) = \omega^3$
$g_3^2(\omega) = g_3(\omega^3) = \omega^9 = \omega^2$
$g_3^3(\omega) = g_3(\omega^2) = \omega^6$
$g_3^4(\omega) = g_3(\omega^6) = \omega^{18} = \omega^4$
$g_3^5(\omega) = g_3(\omega^4) = \cancel{g}\, \omega^{12} = \omega^5$
$g_3^6(\omega) = g_3(\omega^5) = \omega^{15} = \omega$

$\Rightarrow \quad G = \langle g_{\cancel{3}} : g^6 = e \rangle \cong C_6 \qquad g(\omega) = \omega^3$

$$\begin{tikzcd}[column sep=small] & \{id\} \arrow[dl, dash] \arrow[dr, dash] & \\ \langle g^2 \rangle^* \arrow[dr, dash] & & \langle g^3 \rangle \arrow[dl, dash] \\ & G & \end{tikzcd}$$

$$\begin{tikzcd}[column sep=small] & \{id\} \arrow[dl, dash] \arrow[dr, dash] & \\ \langle g^2 \rangle^{\dagger} \arrow[dr, dash] & & \langle g^3 \rangle^{\dagger} \arrow[dl, dash] \\ & G & \end{tikzcd}$$

$g(\omega) = \omega^3$
$g^3(\omega) = \omega^6 = \omega^{-1}$

$$g^3(\omega + g^3(\omega)) = g^3(\omega) + g^6(\omega) = g^3 + \omega$$

$$\Rightarrow \omega + \omega^6 \subseteq \langle g^3 \rangle^+$$

<u>Explanation</u>

α automorphism of order m.
$y = x + \alpha(x) + \alpha^2(x) + \dots + \alpha^{m-1}(x)$

$\alpha(y) = y$
$\Rightarrow y \in \langle \alpha \rangle^+$

<u>Back to example</u>

$\mathbb{Q}(\omega + \omega^6) \subseteq \langle g^3 \rangle^+$

If $\omega + \omega^6 \in \mathbb{Q}$, $\omega^6 + \omega - q = 0$

The minimal polynomial of ω is $m(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1$.
$t^6 + t - q$ is not a multiple of m, contradiction.

$$\Rightarrow \langle g^3 \rangle^+ = \mathbb{Q}(\omega + \omega^6)$$

$g(\omega) = \omega^3$
$g^2(\omega) = \omega^2$

$$\Rightarrow g^2(\omega + g^2(\omega) + g^4(\omega)) = \omega + g^2(\omega) + g^4(\omega)$$

$\beta = \omega + \omega^2 + \omega^4$
$\beta \in \langle g^3 \rangle^+$

$\mathbb{Q}(\beta) \subseteq \langle g^2 \rangle^+$
$\mathbb{Q}(\beta) \neq \mathbb{Q}$
$\Rightarrow \langle g^2 \rangle^+ = \mathbb{Q}(\beta)$

$$\begin{tikzcd}
 & \mathbb{Q}(\omega) \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\langle g^2 \rangle^+ = \mathbb{Q}(\omega + \omega^2 + \omega^4) \arrow[dr, dash, "2"'] & & \langle g^3 \rangle^+ = \mathbb{Q}(\omega + \omega^6) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$\beta = \omega + \omega^2 + \omega^4$
$\beta^2 = \omega^2 + \omega^4 + \omega + 2\omega^3 + 2\omega^5 + 2\omega^6$

$\Rightarrow \beta + \beta^2 = 2(\omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6)$
$= -2$

$\Rightarrow \beta^2 + \beta + 2 = 0$
$\Rightarrow \beta = \dfrac{-1 \pm \sqrt{-7}}{2}$

$$\begin{array}{ccl} \vdots & \vdots & \\ | & | & \text{cyclic} \\ \mathbb{Q}(\sqrt[r]{p})(\sqrt[n]{s}) & b & \\ | & | & \text{cyclic} \\ \mathbb{Q}(\sqrt[r]{p}) & a & \\ | & | & \text{cyclic} \\ \mathbb{Q} & G & \end{array}$$

Solvable Groups

Definition

A group G is soluble if there exists a chain of subgroups of G:

$$\{e\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

Such that $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is an abelian group.

Example

1) Any abelian group is soluble.

$$\{e\} = G_0 \trianglelefteq G_1 = G$$
$$G_1/G_0 \cong G \text{ is abelian.}$$

2) D_{2n} is soluble.

$$D_{2n} = \langle g, h : g^n = h^2 = e, hg = g^{n-1}h \}$$
$$= \{ g^i h^j : 0 \leq i \leq n, 0 \leq j < 2 \}.$$

Let $G_1 = \langle g \rangle = \{e, g_1, g_2, \ldots, g^{n-1}\}$

consider $\{e\} = G_0 \leq G_1 \leq G_2 = G$

$G_1/G_0 \cong G_1 \cong C_n$ is abelian.

$G_1 \trianglelefteq G_2$. $G_2/G_1 = D_{2n}/C_1 \cong C_2$: abelian

$\Rightarrow D_{2n}$ is soluble $\square$

we will see that S_4 is soluble, and that S_5 is not soluble. (This is in the book).

Theorem

Let G be a group, H a subgroup of G, $H \leq G$ and $N \trianglelefteq G$.

i) if G is soluble $\Rightarrow$ H is soluble.

ii) G is soluble $\Rightarrow$ G/N soluble.

iii) N soluble, G/N soluble $\Rightarrow$ G soluble.

(this is called "closure under extensions")

3rd March 2013

Proof of 14.4

(i) G soluble, $H \leq G \Rightarrow H$ soluble

$$\{e\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$$
$$G_i \trianglelefteq G_{i+1}, \; G_{i+1}/G_i \text{ is abelian.}$$

Let $H_i = G_i \cap H$, $H_i \le H$. $\{e\} = H_0 \le H_1 \le \dots \le H_n = H$

Let $g \in H_{i+1}$, $h \in H_i$

(Recall. $N \le G$, N is normal if $\forall g \in G$, $g^{-1}Ng \subseteq N$)

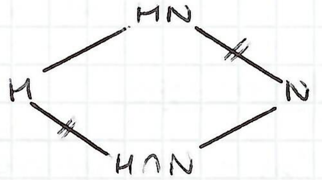
$g^{-1}hg \in G_i$ (because $h \in G_i$, $g \in G_{i+1}$ and $G_i \trianglelefteq G_{i+1}$)
$g^{-1}hg \in H$ (because $g, h \in H$)
$\Rightarrow$ $g^{-1}hg \in H \cap G_i = H_i$
$\Rightarrow$ $H_i \trianglelefteq H_{i+1}$.

Recall

1) $\varphi : G \longrightarrow H$ be a homomorphism. Then:

$$\frac{G}{\ker\varphi} \cong \operatorname{Im}\varphi$$

2) $H \le G$, $N \trianglelefteq G$

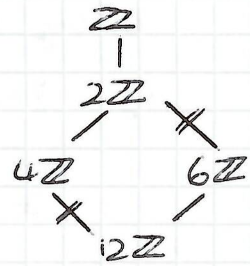


Then $HN = \{hn : h \in H, n \in N\} \le G$
$N \trianglelefteq HN$, $H \cap N \trianglelefteq H$ and:

$$\frac{HN}{H} \cong \frac{H}{H \cap N}$$

Example

$G = (\mathbb{Z}, +)$
$H = 4\mathbb{Z}$
$N = 6\mathbb{Z}$



Group is abelian, so all subgroups are normal.

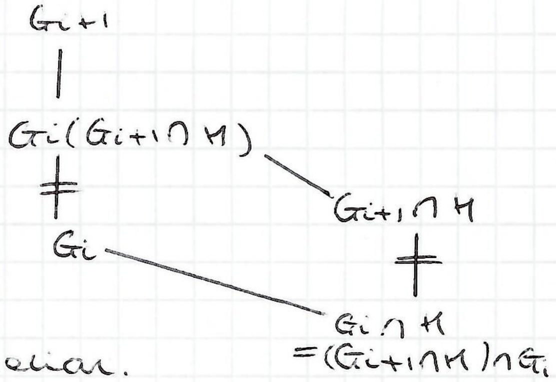
$H \cap N = 4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$
$HN = 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$

$$\frac{2\mathbb{Z}}{6\mathbb{Z}} \cong \frac{4\mathbb{Z}}{12\mathbb{Z}}$$

$\Leftrightarrow$ $\{\bar{0}, \bar{1}, \bar{2}\} \cong \{\bar{0}, \bar{4}, \bar{8}\}$

Back to proof

$$\frac{H_{i+1}}{H} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{(G_{i+1} \cap H) \cap G_i}$$



$$\Rightarrow \frac{G_{i+1} \cap H}{(G_{i+1} \cap H) \cap G_i} \cong \frac{G_i(G_{i+1} \cap H)}{G_i}$$

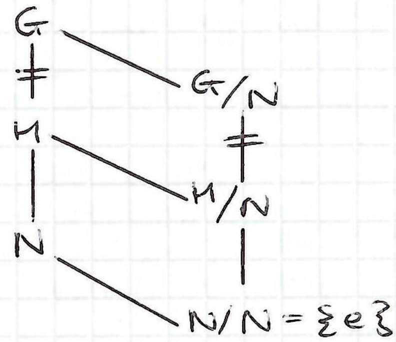
$$\le \frac{G_{i+1}}{G_i}$$

G_{i+1}/G_i is abelian $\Rightarrow$ subgroups are abelian.
$\Rightarrow$ H_{i+1}/H_i is abelian.
$\Rightarrow$ H is soluble.

2) $N \trianglelefteq G$, G soluble $\Rightarrow$ G/N soluble.

$\{e\} = G_0 \leq G_1 \leq \dots \leq G_n \leq G$

G_{i+1}/G_i abelian.



$$\frac{N}{N} \leq \frac{NG_1}{N} \leq \dots \leq \frac{NG_n}{N} = \frac{G}{N}$$

Each $\frac{NG_i}{N} \trianglelefteq \frac{NG_{i+1}}{N}$

$$\frac{NG_{i+1}/N}{NG_i/N} \cong \frac{NG_{i+1}}{NG_i} = \frac{G_{i+1}(NG_i)}{NG_i}$$

$$\cong \frac{G_{i+1}}{G_{i+1} \cap NG_i} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap NG_i)/G_i)}$$

is a quotient of G_{i+1}/G_i, so abelian.

$\Rightarrow$ G/N is soluble.

Proposition

S_n is not soluble for $n \geq 5$. Suppose S_5 is soluble.

$A_5 \triangleleft S_5$ would also be soluble.

But A_5 is simple $\Leftrightarrow$ it has no normal subgroups (other than $\{e\}$ and itself.

(Proof 14.7: not examinable)

if $\{e\} = G_0 \leq G_1 \leq \dots \leq G_{n-1} \leq G_n = G = A_5$

$G_{n-1} \trianglelefteq G \Rightarrow G_{n-1}$

$G = G_n / G_{n-1} = G_n/\{e\} = G_n = A_5$ abelian.

A_5 not abelian. This is a contradiction $\Rightarrow$ A_5 is not soluble.

Cauchy's Theorem

If $p \mid |G|$ then $\exists$ an element of order p in G.

Proof

Follows from Sylow's theorem.

SOLUTION BY RADICALS

12th March 2013

consider ~~$\mathbb{Q}(\sqrt{3})$~~ $\sqrt[3]{}$

Definition (INSIDE $\mathbb{C}$ all the time)

$L:K$ is radical if there exist $\alpha_1, \dots, \alpha_m \in L$, $n_1, \dots, n_m \in \mathbb{N}$ such that

$\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_n)$ and $L = K(\alpha_1, \dots, \alpha_n)$

$$\begin{array}{rc} & K(\alpha_1, \dots, \alpha_m) \\ & | \\ & K(\alpha_1, \dots, \alpha_{n-1}) \\ & \vdots \\ & K(\alpha_1, \alpha_2) \\ \alpha_2^{n_2} \in \mathbb{Q}(\alpha_1) & | \\ & K(\alpha_1) \\ \alpha_1^{n_1} \in K & | \\ & K \end{array}$$

Definition

Let f be a polynomial over K, with splitting field Σ. Then f is soluble by radicals if $\exists$ a field $M \supseteq \Sigma$ such that $M:K$ is radical.

The aim of this section (and the theorem we are heading for) is:

Theorem 15.3

Let $K \subseteq L \subseteq M$, with $M:K$ radical. Then $Gal(L:K)$ is soluble.

Main Lemma (15.7)

Let $L:K$ be a normal radical extension, then $\Gamma(L:K)$ is soluble.

Theorem 15.4

Let $L:K$ be radical, $M:K$ is normal closure. Then $M:K$ is radical.

Proof

Let $L = K(\alpha_1, \dots, \alpha_m)$, then $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$. Let f_i = the minimal polynomial of α_i over K, $f = f_1 \dots f_m$. M = splitting field of f over K.

Let roots of f_i be $\alpha_i = \beta_{i1}, \dots, \beta_{i,t_i}$.
Then $M = K(\beta_{11}, \dots, \beta_{1t_1}, \beta_{21}, \dots, \beta_{2t_2}, \dots)$

Claim this is a radical sequence for M.

Since α_i and β_{ij} have the same minimal polynomial f_i over K, $\exists$ an isomorphism $\sigma: K(\alpha_i) \to K(\beta_{ij})$ such that $\sigma|_K = id$, $\sigma(\alpha_i) = \beta_{ij}$.

Since $M:K$ is normal, by 11.4, σ extends to a K-automorphism of M, τ.

$\tau: M \to M$, $\tau|_K = id$ $\tau(\alpha_i) = \beta_{ij}$

$\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$
$\tau(\alpha_i)^{n_i} \in K(\tau(\alpha_1), \dots, \tau(\alpha_{i-1}))$

$\beta_{ij}^{n_i} \in K(\tau(\alpha_1), \ldots, \tau(\alpha_{i-1}))$

α_1 has minimal polynomial f_1 $\Rightarrow$ $\tau(\alpha_1)$ is a root of f_1.
$\Rightarrow$ $\tau(\alpha_1) = \beta_{1k}$, for some k.

Similarly for $\tau(\alpha_2), \ldots, \tau(\alpha_{i-1})$

$\beta_{ij}^{n_i} \in K(\beta_{11}, \ldots, \beta_{1,t_1}, \beta_{2,1}, \ldots, \beta_{i-1,t_{i-1}})$

$\Rightarrow$ $M:K$ is radical $\square$

<u>Lemma 15.5</u>

L = splitting field of $t^p - 1$ over K (p prime). Then $\Gamma(L:K)$ is abelian.

<u>Proof</u>

$\omega = e^{2\pi i/p}$. Then $L = K(\omega)$ and roots of $t^p - 1$ are powers of ω.

Any $g \in \Gamma(L:K)$ is determined by $g(\omega)$, and send ω to ω^i for some i.

$(gh)(\omega) = g(\omega^j) = \omega^{ij}$
$(hg)(\omega) = h(\omega^i) = \omega^{ij}$
$\Rightarrow gh = hg$
$\Rightarrow \Gamma$ is abelian. $\square$

<u>Lemma 15.6</u>

Let K be a subfield of $\mathbb{C}$ over which $t^n - 1$ splits.

Let L = splitting field of $t^n - a$ over K where $a \in K$.
Then $\Gamma(L:K)$ is abelian.

<u>Proof</u>

Let α be a zero of $t^n - a$ in L. Then other roots are

~~$\varepsilon\alpha$, $\varepsilon\alpha$ where~~

$\varepsilon\alpha$ where ε is a root of $t^n - 1$.

Since $\varepsilon \in K$, $L = K(\alpha)$.

Any $g \in \Gamma(L:K)$ is determined by $g(\alpha)$, and $g(\alpha) = \varepsilon\alpha$, for some $\varepsilon \in K$, $\varepsilon^n = 1$.

Let $g, h \in \Gamma(L:K)$, say $g(\alpha) = \varepsilon\alpha$

$h(\alpha) = \eta\alpha$. Then

$(gh)(\alpha) = g(\eta\alpha) = \eta\varepsilon\alpha$
$(hg)(\alpha) = h(\varepsilon\alpha) = \eta\varepsilon\alpha$
$\Rightarrow gh = hg$
$\Rightarrow \Gamma$ is abelian. $\square$

$$\begin{tikzcd} L \arrow[d, dash] \arrow[rr, leftrightarrow] & & \{id\} \arrow[d, dash] \\ M \arrow[d, dash] & & H = Gal(L:M) \arrow[d, dash, "\triangle"] \\ K \arrow[rr, leftrightarrow] & & G = Gal(L:K) \end{tikzcd}$$

$$Gal(M:K) \cong G/H$$

So $Gal(M:K) \cong \dfrac{Gal(L:K)}{Gal(L:M)}$

$$Gal(L:K) \left[\begin{array}{ll} L & \\ | & Gal(L:M) \\ M & \\ | & Gal(M:K) \\ K & \end{array} \right.$$

So if $Gal(L:M)$ is soluble and $Gal(M:K)$ is soluble, then $Gal(L:K)$ is soluble.

(This is because N normal and soluble, G/N soluble $\Rightarrow$ G soluble).

Proof of 15.7

($L:K$ normal and radical $\Rightarrow$ $Gal(L:K)$ soluble)

Let $L = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_j^{n_j} \in K(\alpha_1, \dots, \alpha_{j-1})$.

without loss of generality, n_j is prime: in particular let $n_1 = p$ (prime), so $\alpha_1^p \in K$.

Proof by induction on n.

$\alpha_1 \notin K$: Let the minimal polynomial of α_1 over K be f.

f splits in L (because $L:K$ is normal). Let β be another root of f $\neq \alpha_1$. Let $\varepsilon = \alpha_1 / \beta$.

Then $\varepsilon^p = \dfrac{\alpha_1^p}{\beta^p} = 1$

$$\begin{aligned} \varepsilon \neq 1 &\Rightarrow o(\varepsilon) = p \\ &\Rightarrow 1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1} \in L. \\ &\Rightarrow t^p - 1 \text{ splits in } L. \end{aligned}$$

Let M be the splitting field of $t^p - 1$ over K.
Then $M \subseteq L$.
$M = K(\varepsilon)$

Now consider the tower of fields:

L — GALOIS GROUP Soluble (by induction) — Soluble

normal radical

$M(\alpha_1)$ — GALOIS GROUP abelian by Lemma 15.6

normal

M — GALOIS GROUP abelian by Lemma 15.5 — Galois group soluble.

normal

K

whole Galois Group is Soluble.

$M : K$ is normal, because it is a splitting field of $t^p - 1$ over K.

$M(\alpha_1)$ is the splitting field of $t^p - \alpha_1^p$ over K.

$\Rightarrow M(\alpha_1) : K$ is normal.

$\Rightarrow \Gamma(L : K)$ is soluble. $\square$

<u>Proof of Theorem 15.3</u>

($K \subseteq L \subseteq M$, $M : K$ radical $\Rightarrow \Gamma(L : K)$ is soluble)

consider the chain of fields:

N = normal closure of $M : K_0$

M

L

K_0 = fixed field of $\Gamma(L : K)$

K

normal radical (15.4)

normal (11.14)

Galois group is soluble.

Galois Group is Soluble as $\Gamma(L : K_0) = \dfrac{\Gamma(N : K_0)}{\Gamma(N : L)}$ ($\cancel{1}$14.4(2))

$\Rightarrow \Gamma(L : K) = \Gamma(L : K_0)$ by definitions of K_0 of the Galois group.

$\Rightarrow \Gamma(L : K)$ is Soluble $\square$

<u>Definition</u> <u>14th March 2013</u>

Let $f \in K[t]$ with splitting field Σ. Then the Galois Group of Σ over K is $Gal(\Sigma : K)$

<u>Theorem 15.9</u>

If $f \in K[t]$ is soluble by ~~polynomials~~ radicals, then the Galois group of f over K is soluble.

<u>Proof</u>

we can think of Gal(f) as a group of the permutations of f.

Let $f \in K[t]$, splitting field Σ.

$\Sigma = K(\alpha_1, \dots, \alpha_r)$, where α_i are roots of f.

If $\sigma \in Gal(f) = Gal(\Sigma : K)$, then σ is determined by $\sigma(\alpha_1), \dots, \sigma(\alpha_r)$
and each $\sigma(\alpha_i) = \alpha_j$ for some j.

If we define $\sigma(\alpha_i) = \alpha_{\pi(i)}$, then $\pi \in S_r$.

The map $\sigma \longmapsto \pi$ gives an isomorphism

$$Gal(f) \longrightarrow G \leq S_r \quad \square$$

Theorem 15.10

Let p be prime, and f an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose f has exactly 2 non-real roots. Then $Gal(f) \cong S_p$.

Proof

Think of $Gal(f) = Gal(\Sigma : \mathbb{Q}) = G$ as a group of permutations of the roots. There are p distinct roots.

$G \cong$ subgroup of S_p.

If α is one root, then $\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq \Sigma$

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(f) = p.$$

By the Tower Law, $p \mid [\Sigma : \mathbb{Q}] \Rightarrow p \mid |G|$.

Hence, $\exists$ an element of order p in G (by Cauchy's Theorem, or as a consequence of Sylow's Theorem).

Hence G contains a p-cycle. Also, complex conjugation, c, gives a $\mathbb{Q}$-automorphism $\mathbb{C} \longrightarrow \mathbb{C}$. Since $\Sigma : \mathbb{Q}$ is normal $c|_\Sigma \in Gal(\Sigma : \mathbb{Q})$.

This switches the 2 complex roots and fixes the rest
$\Rightarrow$ G contains a 2-cycle.

WLOG: 2-cycle is $(1\ 2)$

Some power of the p cycle will send 1 to 2. By reordering the other roots we can take the p-cycle $(1\ 2\ 3 \dots p) \in G$.

Let $t = (1\ 2)$
$\sigma = (1\ 2\ 3 \dots p)$

Now $\sigma t \sigma^{-1} = (2\ \ 3)$

$$\sigma t \sigma^{-1}(2) = \sigma t(1) = \sigma(2) = 3$$
$$\sigma t \sigma^{-1}(3) = \sigma t(2) = \sigma(1) = 2$$
$$\sigma t \sigma^{-1}(1) = \sigma t(p) = \sigma(p) = 1 \quad \text{fixes } 1$$

Similarly $\sigma^2 t \sigma^{-2} = (3, 4) \in G$

All adjacent transpositions live in G.
Any permutation is a product of adjacent transpositions.
$\Rightarrow G = S_p \quad \square$

Theorem 15.11

Let $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$. Then f is not soluble by radicals over $\mathbb{Q}$.

Proof

f is irreducible (Eisenstein's with $p = 3$)
f has exactly 3 real roots (sketch the curve and formalise using the intermediate value theorem)

By 15.10, $Gal(f) \cong S_5$.

S_5 is not soluble, because A_5 is not soluble, and A_5 is a subgroup of S_5, as A_5 has no normal subgroups.

By 15.9, f is not soluble by radicals $\square$