3202 Galois Theory Notes

Based on the spring 2013 lectures by Dr ML Roberts

To an unrequited love

15/1/13

Galois Theory

This includes
(a) establishes a 1-1 structure preserving correspondence between extensions of field and groups

(b) analyzes the solutions of polynomial equations $f(x)=0$ in terms of (a) in particular, showing that the quintic has no solutions "by radials".

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

In more detail
(a) Field extensions and groups.
The Fundamental Theorem of Galois Theory associates to a field ext^n $F \subseteq K$ (eg. $\mathbb{R} \subseteq \mathbb{C}$) a group G called the Galois group G of the ext^n. and (under certain conditions) a 1-1 correspondence between intermediate fields $F \subseteq M \subseteq K$ and subgroups of G.

This construction fits into two important general ideas in algebra.

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

information of the structure.

(ii) The more general idea of attaching a group to a structure is also important e.g. the homotopy group of a space.

(b) Solving polynomial equations

Quadratic : $ax^2 + bx + c = 0$.

Soln : $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

sq. root

The solution is given as an expression in the coefficients involving only $x, +, \div, -$ and $\sqrt{\ }$. This is called a "solution by radicals". The cubic and quatic can in fact be solved similarly.

eg: $t^3 + at^2 + bt + c = 0$.

Change variable to $y = t + a/3$.

Eqn. becomes $y^3 + py + q = 0$

(p, q expressions in a, b, c)

Write $y = U + V$.

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

$$U^3 + 2U^2V + V^3 + p(U+V) + q = 0.$$

$$[U^3 + V^3 + q] + (U+V)[3UV + p] = 0.$$

$$\left.\begin{aligned} U^3 + V^3 + q &= 0 \\ 3UV + p &= 0 \end{aligned}\right\} \qquad \left.\begin{aligned} u + v &= -q \\ 27uv &= -p^3 \end{aligned}\right\}$$

Write $u = U^3$, $v = V^3$, $\quad 3uv = -p$, $\quad 27u^3v^3 = -p^3$

$$u - \frac{p^3}{27u} = -q.$$

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

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

$$y = U + V$$

$$= \sqrt[3]{u} + \sqrt[3]{v}$$

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

Cardano's formula.

A quartic can be solved similarly (by reducing to a cubic), so a natural hypothesis is that all poly eq^n, can be slved by radicals". However, Galois theory shows that this is not true for quintic. The method (vaguely) is:

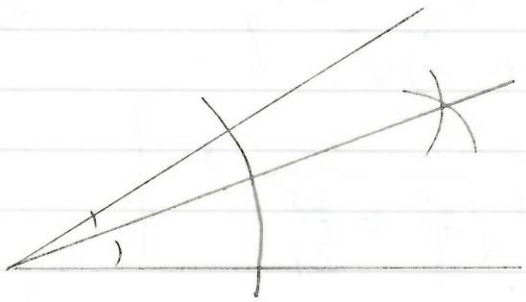
(i) attach a field ext^n $\mathbb{Q} \subseteq L$ to a polynomial $f(x) \in \mathbb{Q}_{[x]}$

(ii) if the equation $f(x) = 0$ is solvable by radicals then there is a chain fields $\mathbb{Q} \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq L$ with certain properties.

(iii) By the fundamental Th^m, this corresponds to a chain of subgroup of the Galois group G.

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

(c) <u>Geometric problems.</u>

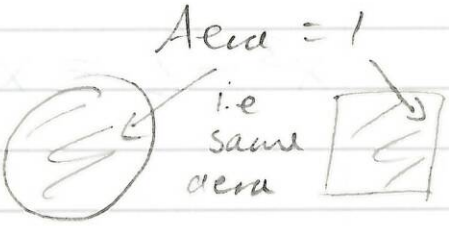


The question of which geometrical construction can be done by ruler + compasses goes back more than 2000 years to classical Greek mathematics

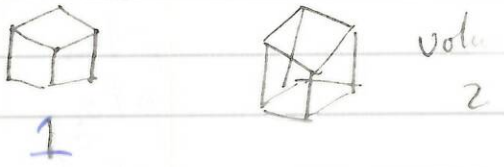
These famous unsolved questions were only answered in the 19th century.

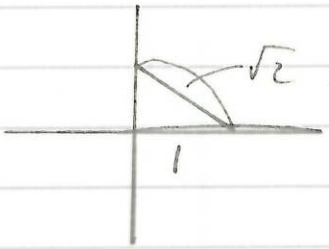
(i) trisecting an angle:

(ii) "squaring the circle" (i.e can you construct π)



(iii) duplicating the cube:





i.e can you construct $\sqrt[3]{2}$.

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

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

(a) Basic linear algebra: vector spaces, bases, dimension.

(b): Group theory e.g group, subgroup, Lagrange's theorem, permutation groups, normal subgroups statement of Sylow's theorem.

(c): some abstract algebra e.g ideals in rings, quotient rings.

(d): need to be O.K with quite complicated algebraic calculations.

Structure of course.
Set book : Stewart, Galois Theory (3rd ed)

— / —

$x^3 - 2 = x^3 - 2$ irr over $\mathbb{Z}[x]$ (no root in $\mathbb{Z}$ — particular to quadratic & cubic)

or Eisenstein (prime 2)

$f(x) = a_n x^n + \dots + a_1 x + a_0$

$p \nmid a_n$

$p \mid a_{n-1}, \dots, a_1, a_0$

$p^2 \nmid a_0$

$= x^3 - 2$ irr in $\mathbb{Q}[x]$
(Gauss' lemma)

$= (x - \alpha)(x^2 + \alpha x + \alpha^2)$

$(\alpha = \sqrt[3]{2}$ in $\mathbb{R}[x])$

$= (x - \alpha)(x - \alpha\omega)(x - \alpha\omega^2)$ in $\mathbb{C}[x]$
where $\omega = e^{2\pi i/3}$

$f(x) = x^3 - 2$, $\mathbb{Z}_3[x]$

$f(\bar{0}) = -\bar{2} = \bar{1}$
$f(\bar{1}) = -\bar{1} = \bar{2}$
$f(\bar{2}) = \bar{6} = \bar{0}$

$$f(x) = (x-\bar{2})(x^2+\bar{2}x+4)$$
$$= (x-\bar{2})(x^2+\bar{2}x+\bar{1})$$
$$= (x-\bar{2})(x-\bar{2})^2 = (x-\bar{2})^3$$

in $\mathbb{Z}_5$.

$$f(x) = x^3 - 2$$

$$0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8 = \bar{3}$$

$$3^3 = 27 = \bar{2}$$

So $f(3) = \bar{0}$

$$x^3 - 2 = (x-3)(x^2+3x+9)$$

irr in $\mathbb{Z}_5[x]$ because of no root.

$f(x) \in \mathbb{Z}[x]$, $f(x) = x^n + \dots$
If $\bar{f}(x) \in \mathbb{Z}_p[x]$ is irr so is $f(x) \in \mathbb{Z}[x]$.

3202 2012-2013 Handout 1: Chapters 1 - 3

A. Historical introduction, Chapter 1 and Chapter 2

Please read through this at home. Much of it should be revision. I will talk about some of Chapter 1 in class.

In Chapter 2, note particularly the formal definition of a polynomial in 2.1, the statement of the Fundamental Theorem of Algebra (Thm 2.4) - don't worry about the complex analysis proof of this - and Section 2.3.

B. Chapter 3 Factorization of polynomials

3.1 - 3.5

Sections 3.1 - 3.4 should all be revision. Look through it briefly and then read 3.5, which may or may not be revision. Then answer the following:

(i) Factorise $x^3 - 2$ into irreducibles (i) over $\mathbf{Z}$, (ii) over $\mathbf{Q}$, (iii) over $\mathbf{R}$, (iv) over $\mathbf{C}$, (v) over $\mathbf{Z}_3$, (v) over $\mathbf{Z}_5$.

(ii) Show that $2t^3 + t^2 + t + 1$ is irreducible over $\mathbf{Q}$ by considering it over a suitable $\mathbf{Z}_n$.

(iii) Determine whether or not the following are irreducible over $\mathbf{Q}$:

(a) $t^3 + 7t^2 - 8t + 1$,

(b) $t^4 - t^2 + 2t - 1$,

(c) $t^4 + t^3 + t^2 + t + 1$.

3.6 Zeroes of polynomials

This should be very familiar: read through it at home some time.

We will finish the chapter by looking at 3.17

Note: The references are to Ian Stewart, Galois Theory (3rd ed), Chapman and Hall, ISBN 1-58488-393-6)

17/01/12

If $f(t) \in \mathbb{Z}[t]$, $f(t) = a_n t^n + \dots + a_0$, a_n coprime to p, $\bar{f}(t)$ irr in $\mathbb{Z}_p[t] \Rightarrow f$ irr in $\mathbb{Z}[t]$. [$f = gh \Rightarrow \bar{f} = \bar{g}\bar{h}$]

(ii) $f(t) = 2t^3 + t^2 + t + 1$

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

$\bar{f}$ red $\Leftrightarrow$ $\bar{f}$ has root (since $\deg(\bar{f}) = 3$)

$\bar{f}(\bar{0}) = \bar{1} \neq 0$ No root
$\bar{f}(\bar{1}) = \bar{2} \neq 0$ $\bar{f}$ irr
$\bar{f}(\bar{2}) = \bar{2} \neq \bar{0}$ $\bar{f}$ irr.

a) $f(t) = t^3 + 7t - 8t + 1$.

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

Root could only be ± 1 $f(1) \neq 0$, $f(-1) \neq 0$ so irr.

b) $f(t) = t^4 - t^2 + 2t - 1$ over $\mathbb{Q}$.

± 1 not root so no linear terms:

$$\textcircled{1}: \quad t^4 - t^2 + 2t - 1 = (t^2 + At + B)(t^2 + Ct + D)$$
$$= t^4 + (A + C)t^3 + (B + D + AC)t^2 + (AD + BC)t + BD$$

$A + C = 0$
$B + D + AC = -1$
$AD + BC = 2$
$BD = -1$.

$B = 1$ or -1
$D = -1$ or 1

$\Downarrow$

$AC = -1$
$A = -C$
$-A + C = 2$
$A^2 = 1$
$A = \pm 1$

$A = -1$, $C = -1$.

$\Rightarrow (t^2 - t + 1)(t^2 + t - 1)$

OR:

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

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

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

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

Trick: $t = s + 1$, $f = \dfrac{(s+1)^5 - 1}{(s+1) - 1}$

$$\ldots = \frac{(s+1)^5 - 1}{s}$$

$$= \frac{s^5 + 5s^4 + 10s^3 + 10s^2 + 5s}{s}$$

$$= s^4 + 5s^3 + 10s^2 + 10s + 5. \quad = g(s).$$

Apply Eisenstein $p = 5$

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

$\Rightarrow$ · $g(s)$ irreducible.
$f(t)$ irreducible.

Note $p \mid {}^pC_r \quad (1 \leq r \leq p-1)$.

Form 3:15.

a) F $(t-1)^2$
b) T
c) F
d) F $t \mid t$
e) T
f) T
g) F eg $t^2 - 2 \in \mathbb{Q}[t]$
(h) T (Gauss' lemma)
i) F $t^2 - 2$.
j) T

Ch 4 : Field extensions.

e.g $f(t) = t^4 - 4t^2 + 5$.

roots ? $f(t) = (t^5 - 1)(t^2 + 1)$.

$\pm\sqrt{5}, \pm i$

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

$= P$ say.

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

Def^n 4.1 : A field extension is a field monomorphism $i : K \to L$, where K, L are subfields. (monomorphism - injective homomorphism)

$K \cong i(K)$ 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, K the small field.

$\mathbb{C}$

|

L

|

K

|

$\mathbb{Q}$

e.g: $\mathbb{R} : \mathbb{Q}$
$\mathbb{C} : \mathbb{R}$.

22/1/13

$L : K$

$\mathbb{C}$
∪|
L
∪|
K

$X \neq \{0\}, \emptyset$

Def^n 4.3: Let $X \subseteq \mathbb{C}$. Then the field generated by X is the intersection of all subfields of $\mathbb{C}$ containing X.

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

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 (i.e the result of a finite sequence of field ops).

Prop^n 4.4: Any subfield of $\mathbb{C}$ contains $\mathbb{Q}$

Proof: Let F be a subfield.

Then $1 \in F$, so $\forall n \in \mathbb{N}$, $n = 1 + 1 + \ldots + 1 \in F$ hence also $-n \in F$. Then $\forall m, n \neq 0 \in \mathbb{Z}$, $m/n \in F$, i.e $\mathbb{Q} \subseteq F$.

Cor^y 4.5 Let $X \subseteq \mathbb{C}$ $(X \neq \emptyset, \{0\})$ then the subfield generated by $X \supseteq \mathbb{Q}$ (contains).

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

e.g. What is $\mathbb{Q}(\sqrt{2})$?
If $a, b \in \mathbb{Q}$ then $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$

$\therefore$ If $M = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, then $M \subseteq \mathbb{Q}(\sqrt{2})$
M is closed under $+$, $\times$ and $-$ and contains 1 and 0.
If $a + b\sqrt{2} \neq 0$.
$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \neq 0$ (since $\sqrt{2}$ is irrational).

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

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

$\therefore M$ is a subfield of $\mathbb{C}$ containing $\sqrt{2}$.

$\therefore M = \mathbb{Q}(\sqrt{2})$.

Generally more complicated e.g

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

so the next chapter develops theory about $\mathbb{Q}(X)$.

Def^n 4.7 : Let $L : K$ be a field ext^n and $Y \subseteq L$. Then the subfield of L generated by $K \cup Y$ is written $K(Y)$.

Clearly $K(Y) \subseteq L$

$K(y)$ means $K(\{y\})$

$K(y_1, \ldots, y_n)$ means $K(\{y_1, \ldots, y_n\})$

e.g. $\mathbb{Q}(i, \sqrt{3}) = \{a + bi + c\sqrt{3} + di\sqrt{3} : a, b, c, d \in \mathbb{Q}\}$

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

—/—

4.3 Rational functions

$\frac{p(t)}{q(t)}$, p and q polynomials e.g $\frac{t}{t^2 - 1}$.

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

Add & multiply by

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

$$(a_i)(b_i) = c_i \quad , c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

This makes $K(t)$ into a ring. Usually write:

$(a_0, a_1, a_2, \ldots)$ as $a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n = p(t)$ say:

We can then think of $p(t)$ as a function $K \to K$.

$K[t]$ is an integral domain. [$pq = 0 \Rightarrow p = 0$ or $q = 0$].

Given any integral domain R, we can construct a field K containing K called the field of fractions of R. Elements of K are of the form rs^{-1} $(r, s \in R, s \neq 0)$

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

(a, b) $\qquad$ $(2,4) \sim (1,2)$

$2/4 = 1/2$.

E.g.

Consider $\sim$ on $R \times R^* = \{(r,s) : r \in R, s \in R^* = R - \{0\}\}$ by $(r,s) \sim (r',s')$ if $rs' = sr'$

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

Eg: $F\ [1,2] = \{(1,2), (2,4), (3,6), \ldots, (-4,-8) \ldots\}$

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 form $rs^{-1} = [r,1][s,1]^{-1}$
$= [r,1][1,s] = [r,s]$

F is the field of fractions of R.

Apply this to $K[t]$: we get the field of fractions

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

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

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

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

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

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

But this function $= 0$)

4.2 Simple extensions

Def^n 4.10: A field extension $L : K$ is simple if $\exists \alpha \in L$ s.t. $L = K(\alpha)$

eg. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is simple

Simple extensions may not be obviously simple

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

Let $\alpha = \sqrt{2} + \sqrt{3}$

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

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

$(\sqrt{3} + \sqrt{2})(\sqrt{3} - \sqrt{2}) = 1$

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

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

$\therefore \sqrt{3} \in \mathbb{Q}(\alpha)$

$\therefore \alpha - \sqrt{3} = \sqrt{2} \in \mathbb{Q}(\alpha)$

$\therefore \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$

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

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

$\therefore \mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ is in fact simple.

$= \mathbb{Q}(\alpha)$

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

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

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

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

$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \sqrt[6]{2}, \ldots) : \mathbb{Q}$ is not simple.

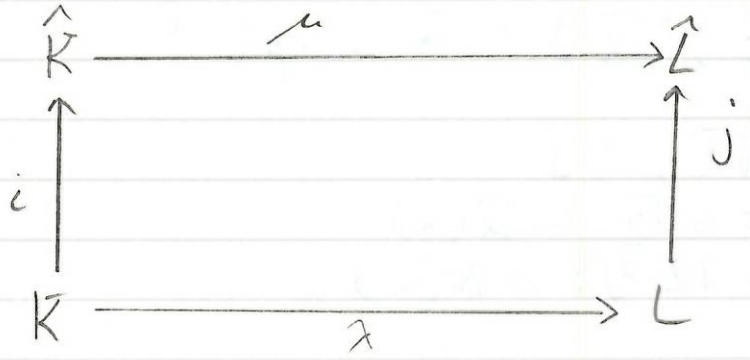
Suppose $= \mathbb{Q}(\alpha)$, α is some expression in $\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[n]{2}$. $= f(\sqrt[N]{2})$ for some $N = n!$

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

Def^n 4.12: Let $i : K \to \hat{K}$, $j : L \to \hat{L}$ be two field ext^{n}s. Then an isomorphism between these two field ext^{n}s is a pair (λ, μ) where

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

st...

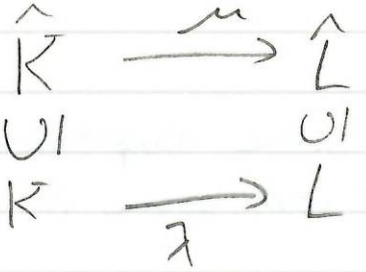


commutes.

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

i.e $\mu i = j\lambda$.

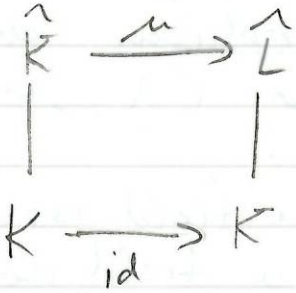
We can usually think of i, j as inclusions:



$\mu|_K$ means μ restricted to K.

st $\mu|_K = \lambda$. i.e $\mu(k) = \lambda(k), \forall k \in K$

Often also $K = L$ and $\lambda = id$.



$\mu|_K = id$

i.e μ fixes each element of K.

eg.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\ c\ } & \mathbb{C} \\ \cup & & \cup \\ \mathbb{R} & \xrightarrow{\ id\ } & \mathbb{R} \end{array}$$

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

Form 4.10:

a T
b T
c T
d F
e F $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$
f T
g T
h F
i F $\mathbb{Q}(\sqrt{2}, -\sqrt{2})$.

Chap 5: Simple extensions.

5.1:
Want to classify ext's $K(\alpha) : K$.

Def" 5.1: Let $K \subseteq \mathbb{C}$, $\alpha \in \mathbb{C}$. Then α is algebraic over K if $\exists\ p(t) \in K[t]$, $p \neq 0$ st $p(\alpha) = 0$. If α is not algebraic, it is called transcendental (over K)
e.g: 1) $\sqrt{2}$ is algebraic over $\mathbb{Q}$ $f(t) = t^2 - 2 \in \mathbb{Q}[t]$, $f(\sqrt{2}) = 0$

2) $\omega = e^{2\pi i/17}$ is algebraic / $\mathbb{Q}$ $f(t) = t^{17} - 1$

3) π is transcendal over $\mathbb{Q}$.

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

5) $\sqrt{\pi}$ is algebraic $\mathbb{Q}(\pi)$, $f(t) = t^2 - \pi \in \mathbb{Q}(\pi)[t]$

(field of rational functions)

Thm 5.3 : $K(t) : K$ is a transcendental field ext^n.

Proof: Suppose t alg / K
Then $\exists\ 0 \neq p(t) \in K[t]$ st $p(t) = 0$.
Contradicts def^n of $K(t)$
$\therefore$ t is transcendental.

24/1/13

5.2 Minimal polynomial.

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

$L : K$ and $\alpha \in L$ is algebraic over K then there exists $f(t) \in K[t]$ st $f(\alpha) = 0$.

e.g: $K : \mathbb{Q}$, $\alpha = i$

$$f(t) = t^2 + 1, \quad f(i) = 0.$$

$$g(t) = 4(t^4 - 1), \quad g(i) = 0.$$

There is a unique monic poly $m(t) \neq 0$ of least degree s.t $m(\alpha) = 0$.

[Pick poly f of least degree s.t $f(\alpha) = 0$
Divide by top coefficient to get monic poly in say $m = t^n + a_{n-1} t^{n-1} + \dots + a_0$.

If m' is another monic poly of degree n st $m'(\alpha) = 0$ say $m' = t^n + a_{n-1}' t^{n-1} + \dots + a_0'$.

$(m - m')$ is a polynomial of degree $< n$ st $(m - m')(\alpha) = 0$
$m - m' = 0$ i.e $m = m'$]

m is called the minimal polynomial of α.

Lemma 5.6 : Let α be alg over K, with min poly m. Then m is irreducible and $f(\alpha) = 0 \Rightarrow m | f$ (i.e. if $I = \{ f \in K[t],\ f(\alpha) = 0 \}$ then $I = m K[t]$ is a principal ideal with generator m).

Pf : Suppose $m = fg$. Then $m(\alpha) = f(\alpha) g(\alpha) = 0$, $f(\alpha) = 0$ or $g(\alpha) = 0$. If $f(\alpha) = 0$, by def^n m, $\partial f \geq \partial m$ $\partial g = 0$ and g is a unit. Similarly if $g(\alpha) = 0$. Thus m has no non-trivial factorisation i.e is irreducible.

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

$$0 = r(\alpha).$$

By def^n m, $r = 0$ i.e $f = mq$.

Ex : What is min poly of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$?

$$\alpha = \sqrt{2} + \sqrt{3}$$

$$\alpha^2 = 5 + 2\sqrt{6}$$

$$\alpha^2 - 5 = 2\sqrt{6}$$

$$(\alpha^2 - 5)^2 = 24$$

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$

So $f(t) = t^4 - 10t + 1$, $f(\alpha) = 0$.

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

$$f(t) = (t^2 + At + B)(t^2 + Ct + D)$$

$$t^4 - 10t^2 + 1 = t^4 + (A+C)t^3 + (B + AC + D)t^2 + (AD + BC)t + BD$$

$$\left.\begin{array}{l} A + C = 0 \\ B + D + AC = -10 \\ AD + BC = 0 \\ BD = 1 \end{array}\right\} \Rightarrow \begin{array}{l} B + D - A^2 = 10 \\ AD - AB = 0 \Rightarrow A(D-B) = 0 \\ BD = 1 \end{array}$$

$A = 0$, $B + D = -10$, $BD = 1$ impossible.

$B = D \longrightarrow B = D = 1 \Rightarrow 2 = A^2 - 10$, $A^2 = 12$.

$\hookrightarrow B = D = -1 \Rightarrow -2 = A^2 - 10$, $A^2 = 8$.

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

Quad factors would have to be $(t - \alpha_1)(t - \alpha_2)$ $= t^2 - (\alpha_1 + \alpha_2)t + \alpha_1\alpha_2$. α_1, α_2 are chosen from $\sqrt{2} + \sqrt{3}$, $\sqrt{2} - \sqrt{3}$, $-\sqrt{2} + \sqrt{3}$, $-\sqrt{2} - \sqrt{3}$, $\alpha_1 + \alpha_2 \in \mathbb{Z}$ $\alpha_1 = \alpha_2$. Then $\alpha_1\alpha_2 \in \mathbb{Z}$.

f is irreducible, so must be min poly of α.
A little later we'll see alternative method using degrees.

$S' = K[\epsilon]/(m)$ $\quad (m) = \{m(\epsilon)f(\epsilon) : f(\epsilon) \in K[\epsilon]\}$

R, $I \lhd R$ $\quad (i_1, i_2 \in I \Rightarrow i_1 - i_2 \in I$.
$i \in I, r \in R \Rightarrow ir \in I)$.

e.g $2\mathbb{Z} \lhd \mathbb{Z}$.

$R/I = \{I + r : r \in R\} = \{i + r : i \in I\}$.

$(I + r) + (I + s) = I + (r + s)$.

$(I + r)(I + s) = I + rs$.

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

$5\mathbb{Z} + r$

e.g $5\mathbb{Z} + 1 = \{\ldots, -9, -4, 1, 6, 11, 16\}$

$5\mathbb{Z} = \{\ldots, -5, 0, 5, \ldots\}$

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

Consider $K[\epsilon]/(m)$, $(m) = \{m(\epsilon)f(\epsilon) : f \in K[\epsilon]\}$

$= \{(m) + f(\epsilon) : \partial f < \partial m\}$

Let $f(\epsilon) \in K[\epsilon]$, $f = mq + r$ $\quad \partial r < \partial m$

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

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

Then $f - g \in (m)$.

i.e $f - g = ms$.

since $\partial(f-g) < \partial m$, $s = 0$ and $f = g$.

Thus every element of $K[t]/(m)$ can be written uniquely as $\underbrace{(m) + f(t)}_{\| \; f(t)}$ $(\partial f < \partial m)$

29/1/13

$$\frac{K[t]}{(m)} = \{ \bar{f} \quad : \partial f < n \}$$

$\bar{f}$: $f + (m)$

$$= \{ \overline{a_0 + a_1 t + \ldots + a_{n-1} t^{n-1}} \quad : a_i \in K \}$$

$n = \partial m$.

Thm 5.10: $K[t]/(m)$ is a field $\Leftrightarrow$ m irreducible over K.

Proof: ($\Rightarrow$) $m = fg$.

Then in $K[t]/(m)$, $\bar{m} = \bar{f}\bar{g}$ i.e $\bar{0} = \bar{f}\bar{g}$
Since $K[t]/(m)$ field, either $\bar{f} = \bar{0}$ or $\bar{g} = \bar{0}$.
i.e $f \in (m)$ or $g \in (m)$ hence g or f is a unit and factorisation is trivial ... m irreducible.

($\Leftarrow$) Let $\bar{f} \in K[t]/(m)$, $f \neq 0$. Then $m \nmid f$. Let $d = hcf(m, f)$ divides m and m irreducible so $d = 1$ or m, $d \neq m$ since $m \nmid f$: hence $d = 1$.

$\therefore \exists\, h, k \in K[t]$ s.t.

$$mh + fk = 1$$
$$\bar{m}\bar{h} + \bar{f}\bar{k} = \bar{1}$$
$$\bar{f}\bar{k} = \bar{1}$$

i.e. $\bar{f}$ has inverse $\bar{k}$.

□

e.g. $\frac{\mathbb{R}[t]}{(t^2+1)}$ is a field.

$$= \{ a\bar{t} + b : a, b \in \mathbb{R} \}.$$

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

$$= -1.$$

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

i.e $\mathbb{R}[t]/(t^2+1) = \mathbb{C}$.

Classifying simple extensions.

Thm 5.11 : (transcendental case)

Skip this.

Thm 5.12 : Let $K(\alpha) : K$ be a simple algebraic ext^n and let m be min poly of α over K. Then $K(\alpha) \overset{\varphi}{\cong} K[t]/(m)$ st $\varphi(t) = \alpha$, $\varphi|_K = \mathrm{Id}$.

$$\begin{array}{ccc} K[t]/(m) & \xrightarrow[t \to \alpha]{\cong \ \varphi} & K(\alpha) \\ | & & | \\ K & \xrightarrow[\mathrm{Id}]{} & K \end{array}$$

Proof: Define

$$\psi : K[t] \longrightarrow K(\alpha)$$

$$\text{by } \psi(f(t)) = f(\alpha)$$

ψ is a ring homo st $\psi|_K = id$

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

$$= (m(t))$$

By 1st isomorphism theorem ($\phi : R \to S$, $\bar{\phi} : R/\text{Ker}(\phi) \to S$). $\exists$ map

$$\varphi : K[t]/\text{Ker}(\psi) \longrightarrow K(\alpha)$$

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

$$\varphi : K[t]/(m) \to \varphi(\bar{f}(t)) = f(\alpha)$$

φ is injective.

$\text{Im}\,\varphi \cong K[t]/(m)$ is a field $\subseteq K(\alpha)$ and containing $\varphi(\bar{t}) = \alpha$ and K.

By def^n $K(\alpha)$, $\text{Im}\,\varphi = K(\alpha)$, φ is the required isomorphism.

□.

e.g $\mathbb{Q}(\sqrt{2})$

$\sqrt{2}$ has min poly t^2-2.

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

$$\{(t^2-2)+at+b\}$$

$$\{\overline{at+b}\}, \bar{t}^2=2.$$

Lemma 5.14: Let α be algebraic over K with min poly $m(t)$. Then $K(\alpha) = \{a_0+a_1\alpha+\dots+a_{n-1}\alpha^{n-1} : \alpha_i \in K\}$ (where $n=\partial m$). This expression is unique so $\{1, \alpha, \dots, \alpha^{n-1}\}$ forms a K-basis for $K(\alpha)$. In particular $[K(\alpha):K] = n$. (Ch 6)

Pf: $K(\alpha) \cong K[t]/(m)$

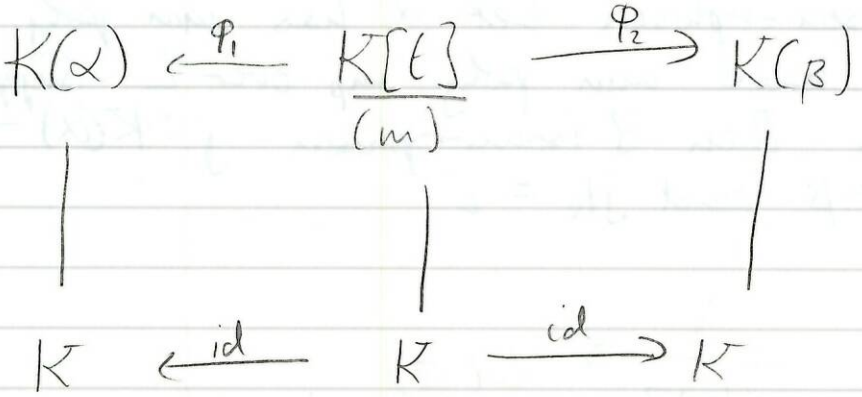
$$\{a_0+a_1\bar{t}+\dots+a_{n-1}\bar{t}^{n-1} : a_i \in K\}.$$

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

Corr 5.13. Suppose α and β have the same min poly over K. Then $K(\alpha) \cong K(\beta)$ where $\varphi(\alpha)=\beta$ and $\varphi|_K = id$.

$$\begin{array}{ccc} K(\alpha) & \xrightarrow[\alpha \mapsto \beta]{\varphi} & K(\beta) \\ | & & | \\ K & \xrightarrow[id.]{} & K \end{array}$$

Proof: By 5.12.



$\varphi : \varphi_2 \varphi_1^{-1} : K(\alpha) \longrightarrow K(\beta)$ is required isomorphism

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

Note $K(\alpha) \cong K(\beta)$ does not imply α, β have same min poly e.g. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}-1)$

min poly $\sqrt{2}$ is $t^2 - 2$

min poly $\sqrt{2}-1$ is $t^2 + 2t - 1$.

If $\exists$ isomorphism $\varphi : K(\alpha) \longrightarrow K(\beta)$ st $\varphi(\alpha) = \beta$ and $\varphi|_K = id$, then α and β have same min poly.

Def^n 5.15: Let $i : K \to L$ be a field monomorphism. Then there is a ring monomorphism.

$$\hat{i} : K[t] \longrightarrow L[t]$$

$$\hat{i}(a_n t^n + \ldots + a_0) = i(a_n) t^n + \ldots + i(a_0)$$

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

Usually write i for $\hat{i}$.

Th^m 5.16 : Let K, L be subfeilds of $\mathbb{C}$, $i: K \to L$ a field isomorphism. Let α has min poly m_α over K and β have min poly m_β over L. Suppose $i(m_\alpha) = m_\beta$. Then $\exists$ isomorphism $j: K(\alpha) \to L(\beta)$ st $j(\alpha) = \beta$ and $j|_K = i$

$$\begin{array}{ccc} K(\alpha) & \xrightarrow[\alpha \mapsto \beta]{j} & L(\beta) \\ | & & | \\ K & \xrightarrow[i]{} & L \end{array}$$

Proof :

$$\begin{array}{ccccccc} K(\alpha) & \xleftarrow{\varphi_1} & K[t]/(m_\alpha) & \xrightarrow{\Psi} & L[t]/(m_\beta) & \xrightarrow{\varphi_2} & L(\beta) \\ | & & \alpha \leftarrow \bar{t} \;| & & \bar{t} \longleftrightarrow \bar{t} & & \bar{t} \mapsto \beta \;| \\ K & \xrightarrow{id} & K & \xrightarrow{i} & L & \xrightarrow{id} & L \end{array}$$

φ_1, φ_2 exist by 5.12.

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

πi is surjective.

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

$= (m_\alpha)$

$$\frac{K[t]}{(m_\alpha)} \overset{\Psi}{\cong} \frac{L[t]}{(m_\beta)}$$

Now $j = \varphi_2 \Psi \varphi_1^{-1}$

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

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

Then $u = \sum_{j\in J} \zeta_j y_j = \sum_{j\in J} \left(\sum_{i\in I_j} \alpha_{ij} x_i\right) y_j$

$$= \sum_{i,j} x_i y_j$$

LI: Suppose $\sum_{i,j} \alpha_{ij} x_i y_j = 0 \quad (\alpha_{ij} \in K)$

$$\sum_j \Big(\underbrace{\sum_i \alpha_{ij} x_i}_{\in L}\Big) y_j = 0$$

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

$\therefore [M:K] = |I \times J| = |I||J| = [L:K][M:L]$.

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

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

|

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

|

$\mathbb{Q}$.

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

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

Cor^y 6.6 Let $K_0, K_1, \ldots, K_n$ be fields with $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$.

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

Proof By induction.

Prop 6.7

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

(ii) If α is algebraic over K, then $[K(\alpha) : K] = 2m$, when m = min poly of α.

Proof: Claim $\{1, \alpha, \ldots, \alpha^n\}$ is LI/K. Suppose $\sum_{i=0}^{n} k_i \alpha_i = 0$ $(k_i \in K)$

Let $f(t) = \sum_{i=0}^{n} k_i t^i$: $f(t) \in K[t]$
and $f(\alpha) = 0$. Since α transecdental.
$f=0$ i.e all $k_i = 0$

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

For 5.9.

a) T $K \subseteq K[t]$.
b) F $\mathbb{C}$
c) F $\mathbb{C} \subseteq \mathbb{C}(t)$.
d) F $\mathbb{C}(s,t) : \mathbb{C}$ or $\mathbb{C} : \mathbb{Q}$ or $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots) : \mathbb{Q}$
e) F $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$ (*)
f) T $K(\alpha) \cong K(\beta)$
g) T
h) F e.g $t^2 - 1$
i) F

(*) $\varphi : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{3})$

$$(\varphi(\sqrt{2}))^2 = \varphi((\sqrt{2})^2)$$
$$= \varphi(2)$$
$$= 2$$

$$\varphi(\sqrt{2}) = a + b\sqrt{3} \qquad (a + b\sqrt{3})^2 = 2.$$
$$a, b \in \mathbb{Q}.$$

$$a^2 + 3b^2 + 2ab\sqrt{3} = 2$$
$$2ab = 0$$
$$a = 0 \text{ or } b = 0$$
$$3b^2 = 2 \text{ or } a^2 = 2.$$

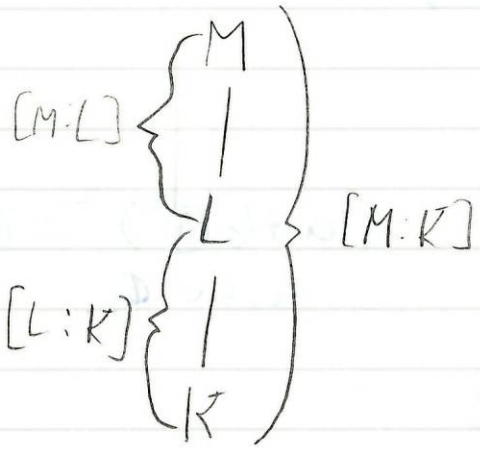
Ch 6:

Thm 6.1: If $L:K$ is a field ext^n, then L can be regarded as a vector space over K.

Def 6.2: The degree of a field extension $L:K$ is the dimension of L as a vector space over K, denoted $[L:K]$.

6.2 The Tower law.

Thm 6.4 Let K, L, M be fields with $K \leq L \leq M$ Then $[M:K] = [M:L][L:K]$.



Proof: Let $(x_i)_{i \in I}$ be a basis for L over K and $(y_j)_{j \in J}$ be a basis for M over L; $[L:K] = |I|$, $[M:L] = |J|$.

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

Spanning: Let $m \in M$. Since $(y_j)_{j \in J}$ spans M over L so $\exists (_j \in L$ st $m = \Sigma_{j \in J} (_j y_j$

(ii) lemma 5.14 $\partial_m = n$.

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

—/—

Calculating degrees of exentenseon comes down to finding minimal poly + tower law.

e.g $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}$.

$\mathbb{Q}(\sqrt{2})(\sqrt{3})(\sqrt{5})$

| 2 since min poly of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{2}, \sqrt{3}$ is $t^2 - 5$.

$\mathbb{Q}(\sqrt{2})(\sqrt{3})$

| 2 since min poly of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{3})$ is $t^2 - 3$.

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

| 2 since min poly $\sqrt{2}$ over $\mathbb{Q} = t^2 - 2$

$\mathbb{Q}$.

deg $= 2 \times 2 \times 2 = 8$.

e.g $\mathbb{Q}(\sqrt{2})(-\sqrt{2})$

| 1

$(-\sqrt{2})$ satisfies t^2-2 over $\mathbb{Q}(\sqrt{2})$ but not irredue $(t-\sqrt{2})(t+\sqrt{2})$

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

| 2

$\mathbb{Q}$.

31/1/13.

Def^n 6.9 An extension $L:K$ is finite if its degree is finite.

We have seen that if α is algebraic over K, then $K(\alpha):K$ is finite.

Def^n 6:10 : $L:K$ is algebraic if every element of L is algebraic over K

Lemma 6.11: The following are equivalent
(i) $L:K$ is algebraic and finite generated (i.e $\exists \alpha_1 \dots \alpha_n \in L$ st $L = K(\alpha_1, \dots, \alpha_n)$)

(ii) $L:K$ is finite.

—/—

To say $K(\alpha):K$ is simple algebraic could mean
(i) α alg over K
or (i) every element of $K(\alpha)$ is alg/K.

This result means these are equivalent.

—/—

Proof of lemma: ($\Leftarrow$) Suppose $L:K$ is finite, i.e $[L:K] = m < \infty$. Let $\ell_1, \dots, \ell_m$ be a K-basis for L then $L : K(\ell_1, \dots, \ell_m)$ so L is finitely generated over K.

Let $x \in L$. Then set $\{1, x, \dots, x^n\}$ is a set of $m+1$ elements in a vector space of dimension m over K, so linear dep say:

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

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

($\Rightarrow$) Suppose $L.K$ is algebraic and L fin gen $/K$
say $L = K(\alpha_1, \ldots, \alpha_n)$. Consider tower:

$$L = K(\alpha_1, \ldots, \alpha_n)$$
$$\vdots$$
$$K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2)$$
$$|$$
$$K(\alpha_1)$$
$$|$$
$$K$$

α_1 alg $/K$ so by 5.14, $[K(\alpha) : K] < \infty$

α_2 alg $/K$, so alg $/K(\alpha_1)$
so by 5.14
$[K(\alpha_1)(\alpha_2) : K(\alpha_1)] < \infty$
$\parallel$
$K(\alpha_1, \alpha_2)$

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

—/—

6.17

a $[L_1 : K] = [L_2 : K] \Rightarrow L_1 \cong L_2$ False e.g
$\mathbb{Q}(\sqrt{2}) : \mathbb{Q} \cong \mathbb{Q}(\sqrt{3}) : \mathbb{Q}$
both of degree 2.

b $L_1 : K \cong L_2 : K \Rightarrow [L_1 : K] = [L_2 : K]$ True.

c False

d $[K(t) : K] = \infty$ - True.

e $\mathbb{C} : \mathbb{R}$ alg $[\mathbb{C} : \mathbb{R}] = 2 < \infty$ by 6.11 alg
or $\alpha = a + bi$, $(\alpha - a)^2 = -b^2$
$\alpha^2 - 2a\alpha + (a^2 + b^2) = 0$

$f(x) = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x]$

$f(x) = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x]$

and $f(\alpha) = 0$.

f $[K:\mathbb{R}] < \infty$, Flase $\mathbb{R}(\epsilon):\mathbb{R}$.

g Every alg ext^n of $\mathbb{Q}$ is finite (Ex 1, Q 3).

h V_k vector space $\dim_k V < \infty \Rightarrow \exists\, L:K$ s.t $V_k \cong L_k$ as vector space.

$\Updownarrow$

$\dim_k V = \dim_k L$

Can you find an ext^n $L:K$ of degree n?

Chap 7: Skip - not examinable.

Chap 8: Do only 8.5 and 8.6.

8.5

Def^n 8.1: Let $L:K$ be a field extension. A K-automorphism of L is a bijective field hom^m $\alpha: L \to L$ st $\alpha|_K = id$.

$$\begin{array}{ccc} L & \xrightarrow{\alpha} & L \\ | & & | \\ K & \xrightarrow{id} & K \end{array}$$

(We say α fixes K)
i.e $\alpha(k) = k \ \forall k \in K$

e.g $c : \mathbb{C} \to \mathbb{C}$ by:

$$c(a+ib) = a - ib$$

Then c is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

c is bijective.
$c(z_1 z_2) = c(z_1)\, c(z_2)$
$c(z_1 - z_2) = c(z_1) - c(z_2)$
For $z \in \mathbb{R}$, $c(z) = z$

Th^{m} 8.2 / Def^{n} 8.3

The set of all K-auts of L forms a group under composition of maps. This is called the Galois group of the ext^{n} $L:K$, denoted $\Gamma(L:K)$ or $\mathrm{Gal}(L:K)$.

5/2/13.

$f: L \to L$ st $f|_K = id$, f hom, f bij

$L : K$ $\quad \Gamma(L:K)$ = group of K-auts of L under composition.

Galois group of $L:K$.

e.g: i) What is $\Gamma(\mathbb{C}:\mathbb{R})$?

Let $\sigma : \mathbb{C} \to \mathbb{C}$ be an $\mathbb{R}$-automorphism.

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

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1.$$

$$\sigma(i) = \pm 1 \quad \text{(but not both)}$$

If $\sigma(i) = i$, then $\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i)$
$= a + bi$
i.e $\sigma = id$.

id is an $\mathbb{R}$-aut of $\mathbb{C}$.

If $\sigma(i) = -i$ then $\sigma(a+bi) = a - bi$, i.e $\sigma(z) = \bar{z}$. Write $c(z) = \bar{z}$, $c : \mathbb{C} \to \mathbb{C}$ satisfies $c(zw) = c(z)c(w)$, $c(z+w) = c(z) + c(w)$. and $c(a) = a \quad \forall a \in \mathbb{R}$, i.e. c is an $\mathbb{R}$-aut of $\mathbb{C}$.

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

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

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

Let $\sigma \in \Gamma$

$\sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(2) = 2$.

$\sigma(\alpha) \in \mathbb{Q}(\alpha) \subseteq \mathbb{R} \quad \therefore \sigma(\alpha) = \alpha$.

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

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

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

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

f is determined by $f(\sqrt{2})$, $f(\sqrt{3})$.

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

Similarly $f(\sqrt{3}) = \pm\sqrt{3}$. This gives us 4 potential elements of Γ.

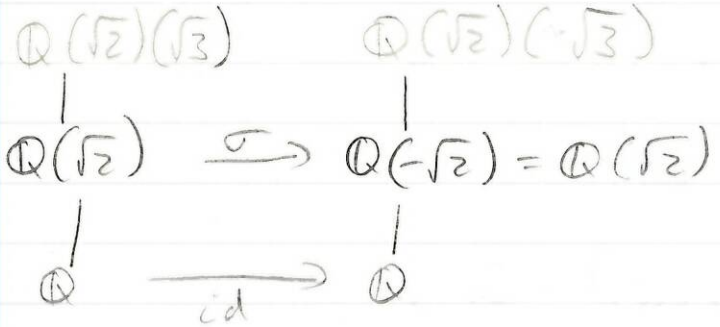
$id \quad \sqrt{2} \mapsto \sqrt{2}, \quad \sqrt{3} \mapsto \sqrt{3}$

$f_1 \quad \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3} \mapsto \sqrt{3}$

$f_2 \quad \sqrt{2} \mapsto \sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3}$

$f_3 \quad \sqrt{2} \mapsto -\sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3}$.

Need to check these are all $\mathbb{Q}$-aut of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$



Silly example:
$\mathbb{Q}(\sqrt{2}, -\sqrt{2})$: $\mathbb{Q}$
$\sqrt{2} \mapsto \pm\sqrt{2}$
$-\sqrt{2} \mapsto \pm\sqrt{2}$
but $f(\sqrt{2}) = \sqrt{2}$
$f(-\sqrt{2}) = \sqrt{2}$.

$\sqrt{2}$ and $-\sqrt{2}$ have same min poly $t^2 - 2$ over $\mathbb{Q}$.
By 5.13 $\exists\ \sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$
$\sqrt{2} \longrightarrow -\sqrt{2}$
$\sigma|_{\mathbb{Q}} = id$.

$\sqrt{3}$ has min poly $t^2 - 3$ over $\mathbb{Q}(\sqrt{2})$
[because $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: check if
$\sqrt{3} = a + b\sqrt{2}$
$3 = a^2 + 2b^2 + 2ab\sqrt{2}$
$\sqrt{2} \in \mathbb{Q}$, so $ab = 0$
$a = 0 \Rightarrow 3 = 2b^2 \Rightarrow \sqrt{\frac{3}{2}} \in \mathbb{Q}$, impossible
$b = 0 \Rightarrow 3 = a^2 \Rightarrow \sqrt{3} \in \mathbb{Q}$ impossible]

$\sqrt{3}$ has min poly $t^2 - 3 = \sigma(t^2 - 3)$ over $\mathbb{Q}(\sqrt{2})$

By Th^m 5.16, $\exists\ f_1 : \mathbb{Q}(\sqrt{2})(\sqrt{3})$
$\to \mathbb{Q}(\sqrt{2})(\sqrt{3})$ st $f_1(\sqrt{3}) = \sqrt{3}$
and $f_1|_{\mathbb{Q}(\sqrt{2})} = id$

$f_1 : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$f_1(\sqrt{3}) = \sqrt{3}$

$f_1|_{\mathbb{Q}(\sqrt{2})} = \sigma$

$f_1(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$.

$f_1|_{\mathbb{Q}} = \sigma|_{\mathbb{Q}} = id$.

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

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

$f_1 \circ f_2 = f_3$, so $f_3 \in \Gamma$.

$\therefore \Gamma = \{id, f_1, f_2, f_3\}$

$f_1^2 = f_2^2 = f_3^2 = id$.

$\Gamma = C_2 \times C_2$.

$= [id, f_1] \times [id, f_2]$.

8.6.

field ext^n	Group
$L : K$	$\Gamma(L:K)$

$f(L:K) = f$ $\longleftrightarrow$ G_Γ

$= \{$set of fields M st $K \subseteq M \subseteq L$ (intermediate fields)$\}$

$= \{$set of subgroups H of $G = \Gamma(L:K)\}$.

If $M \in f$, then $M^* = \{\sigma \in \Gamma : \sigma(m) = m \ \forall_{m \in M}\}$

$M^* \subseteq \Gamma$.

$M^* = \Gamma(L:M)$, $M^* \in G$.

If $H \in \mathcal{G}$, $H \subseteq G$.

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

$K \subseteq H^+ \subseteq L$. In fact $H^+ \subseteq L$ [let $x, y \in H^+$ so $h(x) = x \quad \forall h \in H$, $h(y) = y \quad \forall h \in H$

Then $h(x+y) = h(x) + h(y)$
$= x + y \quad \forall h \in H$.

so $x + y \in H^+$. Similarly $xy \in H^+$, $xy^{-1} \in H^+$, $x - y \in H^+$]

i.e $H^+ \in \mathcal{f}$.

fidd ext^n	Groups
$L : K$	$\Gamma(L:K)$
M	M^*
H^+	H

$* : \mathcal{f} \to \mathcal{G}$.

$+ : \mathcal{G} \to \mathcal{f}$.

Suppose $M_1 \subseteq M_2$ then $M_1^* \supseteq M_2^*$.

[let $g \in M_2^*$: then $g(x) = x \quad \forall x \in M_2$. Since $M_1 \subseteq M_2$ so $g(x) = x \quad \forall x \in M_1$, , i.e. $g \in M_1^*$]

Suppose $H_1 \subseteq H_2$: then $H_1^+ \supseteq H_2^+$

(H^+ is called the fixed field of H).

We have $M \subseteq M^{*+}$ $(\forall M \subseteq F)$ and $H \subseteq H^{+*}$

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

[let $x \in M$, $g \in M^*$. By def^n M^*, $g(x) = x$
$\forall g \in M^*$. By def^n $+$, $x = (M^*)^+$]

Under some circumstances (normality + seperability)

$M = M^{*+}$, $H = H^{+*}$ i.e $*$ and $+$ are mutual inverses. In this case $\mathcal{G}_+$ is just $\mathcal{G}$ upside-down
This is the Galois correspondence.

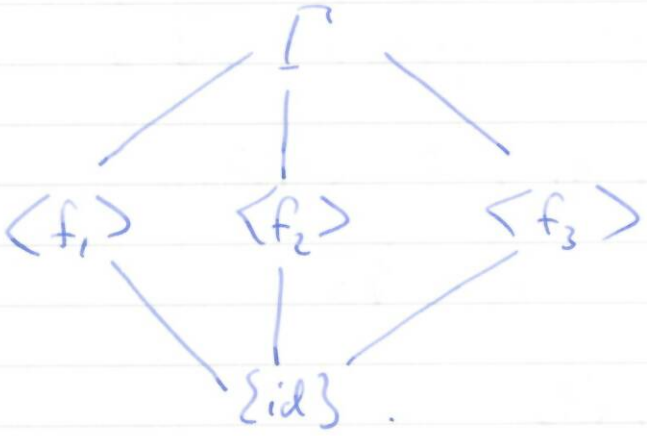
e.g $\mathbb{Q}(\sqrt{2}, \sqrt{3})$: $\mathbb{Q}$ is a separable normal ext^n, so Galois correspondence holds

$$\Gamma = \{id, f_1, f_2, f_3\} \cong C_2 \times C_2 .$$

$f_1(\sqrt{2}) = -\sqrt{2}$, $f_1(\sqrt{3}) = \sqrt{3}$
$f_2(\sqrt{2}) = \sqrt{2}$, $f_2(\sqrt{3}) = -\sqrt{3}$
$f_3(\sqrt{2}) = -\sqrt{2}$, $f_3(\sqrt{3}) = -\sqrt{3}$

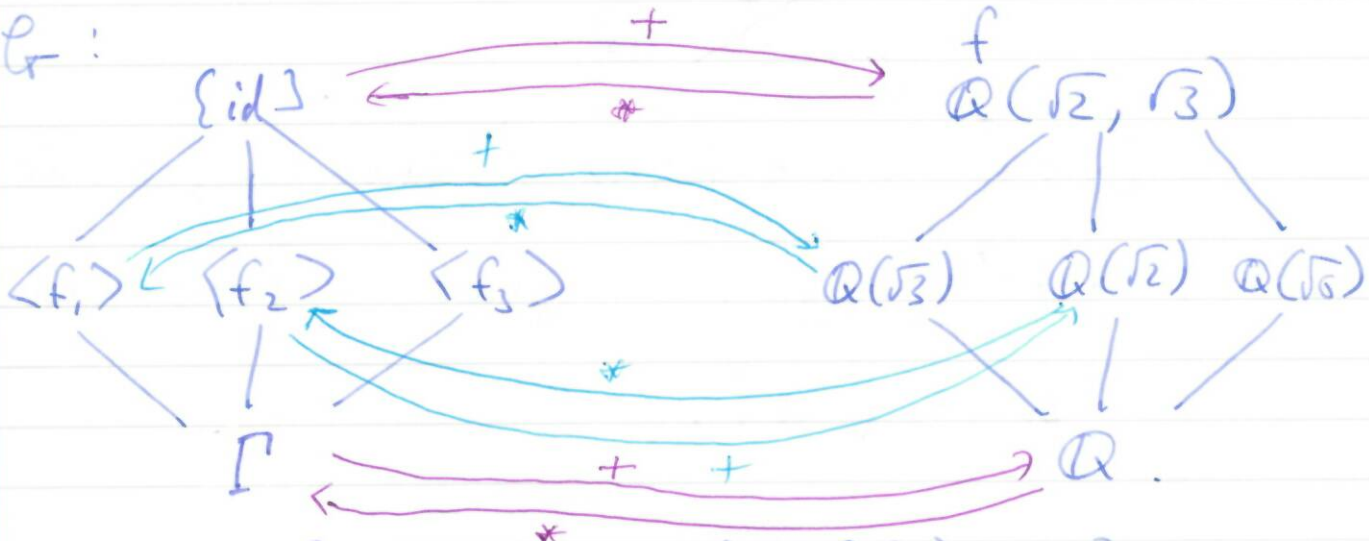
There are exactly 3 proper subgroups:
$\langle f_1 \rangle = \{id, f_1\}$, $\langle f_2 \rangle = \{id, f_2\}$
$\langle f_3 \rangle = \{id, f_3\}$.

Γ (upside down).



f: Obvious intermediate fields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$. Quite long calculation shows there aren't any others.

Γ:



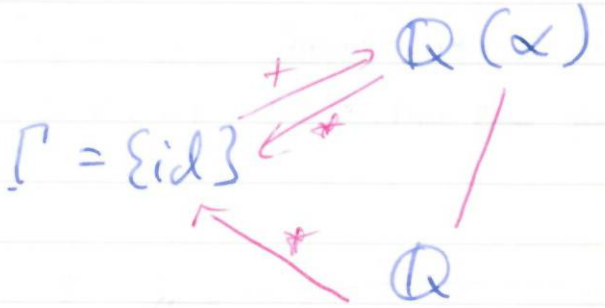
$$\langle f_1\rangle^+ = \{ x \in \mathbb{Q}(\sqrt{2},\sqrt{3}) : f_1(x) = x \}$$

$$x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$
$$f_1(x) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$
$$f_1(x) = x \iff b = -b \;,\; d = -d$$
$$\iff b = 0 \;,\; d = 0$$
$$\iff x = a + c\sqrt{3}$$
$$\langle f_1\rangle^+ = \mathbb{Q}(\sqrt{3}).$$

$$\mathbb{Q}(\sqrt{3})^* = \{g \in \Gamma : g(x) = x \ \forall x \in \mathbb{Q}(\sqrt{3})\}$$
$$= \{g \in \Gamma : g(\sqrt{3}) = \sqrt{3}\}$$
$$= \{id, f_1\} = \langle f_1 \rangle.$$

(2) $\mathbb{Q}(\alpha) : \mathbb{Q} \qquad \alpha = \sqrt[3]{2}$

Not normal $\Gamma = \{id\}$



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

— / —

Chapter 9.

Def^n 9:1 : Let $K \leq \mathbb{C}$, $f(t) \in K[t]$. f splits over K if f factorises into linear factor in $K[t]$:

$$f(t) = k(t-\alpha_1)(t-\alpha_2)\ldots(t-\alpha_n)$$

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 poly $f \in \mathbb{C}[t]$ splits
(Fundamental Th^m of algebra)

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

$= (t - \sqrt{5})(t + \sqrt{5})$

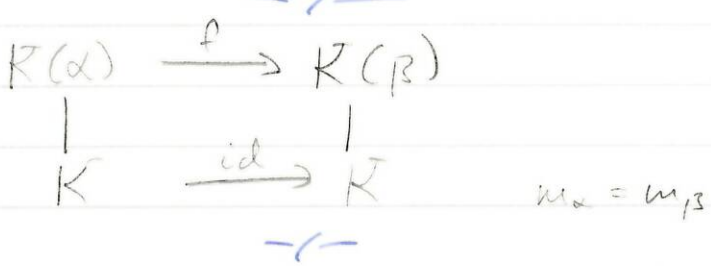
Def^n 9.3 A field $\Sigma \subseteq \mathbb{C}$ is a splitting field for the polynomial $f(t) \in K[t]$ if $K \subseteq \Sigma$ and
i) f splits over Σ
ii) if $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ', then $\Sigma = \Sigma'$

In fact if f has roots $\sigma_1, \ldots, \sigma_n$ in $\mathbb{C}$ then

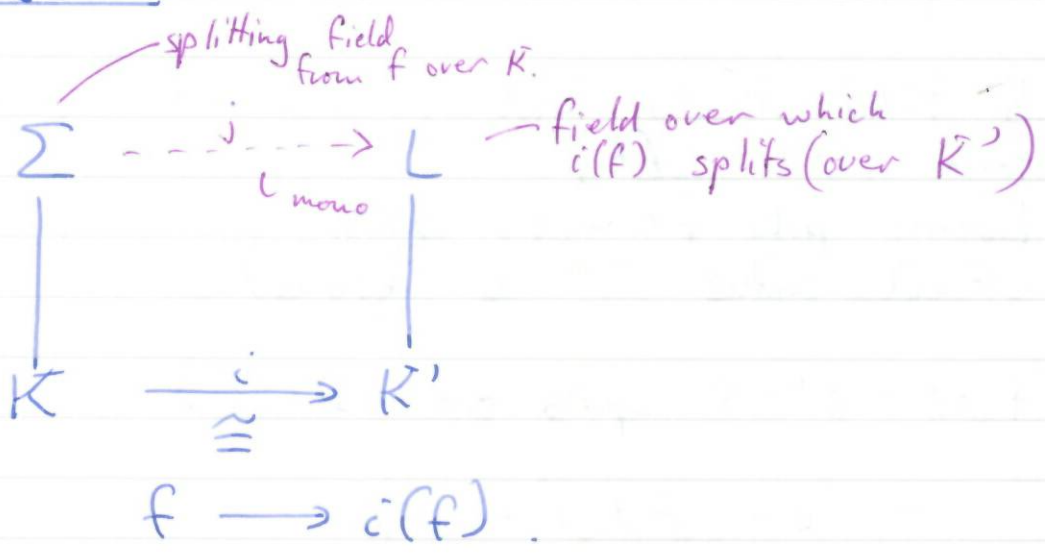
$\Sigma = K(\sigma_1, \sigma_2, \ldots, \sigma_n)$

Thm 9.4: Let $K \subseteq \mathbb{C}$, $f \in K[t]$. Then there exist a unique splitting field Σ for f over K, and $[\Sigma : K] < \infty$.

Pf: $\Sigma = K(\sigma_1, \ldots, \sigma_n)$ is the unique splitting field. Since Σ is fin gen and algebraic over K, so by 6.11, $[\Sigma : K] < \infty$.



Lemma 9.5.

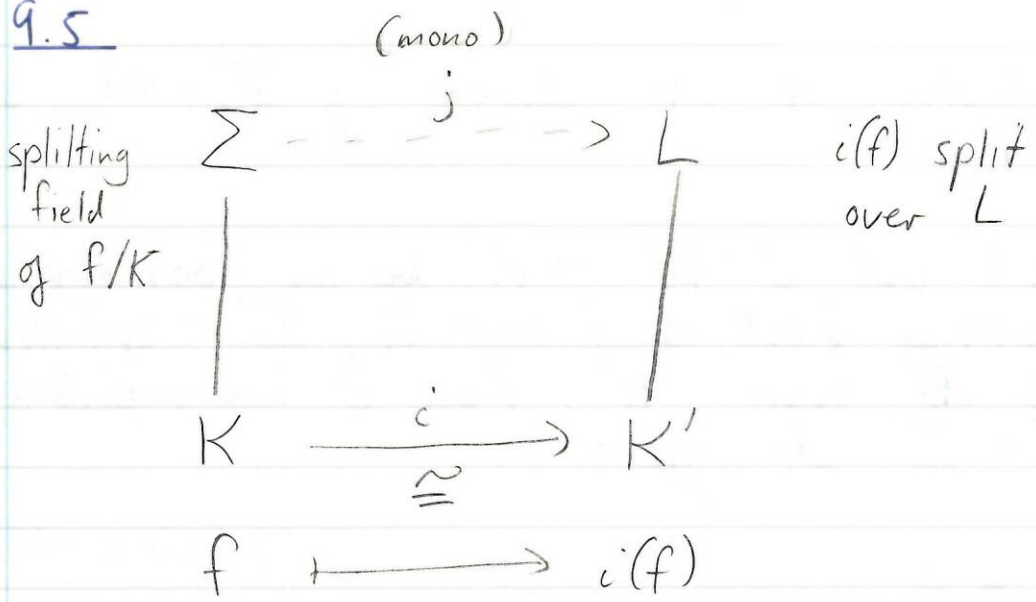


Let $K, K' \subseteq \mathbb{C}$, $i : K \to K'$ a field isomorphism.
Let $f \in K[t]$ with splitting field Σ, and let $L \supseteq K'$ be such that $i(f)$ splits over L.

Then $\exists$ field mono $j : \Sigma \to L$ st $j|_K = i$

7/2/13

9.5



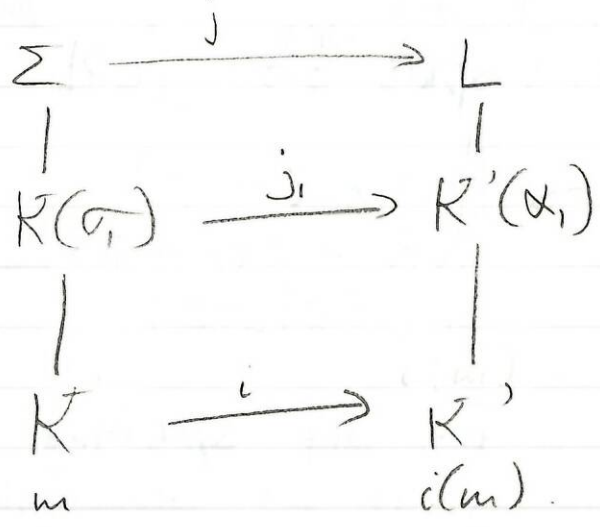
Pf: Let

$$f(t) = k(t-\sigma_1)\dots(t-\sigma_n)$$

when $\sigma_i \in \Sigma$

Let m be minimal poly of σ_i over K: m is irreducible and $m \mid f \Rightarrow i(m) \mid i(f)$. Since $i(f)$ splits L, so $i(m)$ splits over L say $i(m) = (t-\alpha_1)\dots(t-\alpha_r)$ $(\alpha_i \in L)$

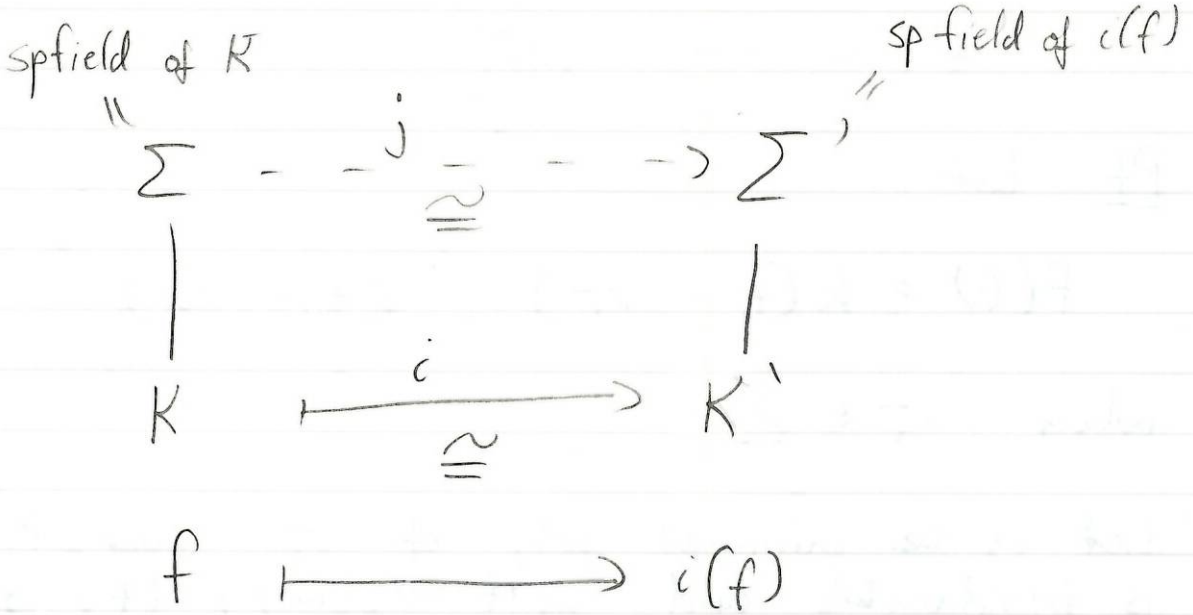
By 5.16 since min poly of σ_1 over $K = m(t)$ and min poly of α_1 over $K_1 = i(m)(t)$, $\exists$ iso $j_1 : (K(\sigma_1)) \to K'(\sigma_1)$ st $j_1(\sigma_1) = \alpha_1$, $j_1|_K = i$
Σ = splitting field of $f(t)/t-\sigma_1$ over $K(\sigma_1)$



$i(f(\epsilon)/\epsilon - \sigma_1)$ splits over $K(\alpha_1)$

By induction of $\deg f$, $\exists$ unique $j: \Sigma \to L$ st $j|_{K(\sigma_1)} = j_1$

Thm 9.6 Let $i: K \to K'$ be an isomorphism Σ = splitting field of f over K, Σ' = splitting field of $i(f)$ over K'. Then $\exists$ isomorphism $j: \Sigma \to \Sigma'$ st $j|_K = i$



Proof: By 9.5, $\exists$ monomorphism $j: \Sigma \to \Sigma'$ s.t. $j|_K = i$. Now $j(\Sigma) \subseteq \Sigma'$ and $i(f)$ splits over $j(\Sigma)$

[$f = k(t-\sigma_1)\dots(t-\sigma_n)$ in $\Sigma[t]$:
$i(f) = j(f) = j(k)(t - j(\sigma_1))\dots(t - j(\sigma_n))$
in $j(\Sigma)[t]$]

By def^n splitting field, $j(\Sigma) = \Sigma'$. Hence j is an isomorphism.

Normality:

Def" 9.8: A field ext" $L:K$ is *normal* if every *irreducible* poly over K with one root in L splits over L.

e.g $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ is normal but this is not evident.

e.g $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ is *not* normal: let $f(t) = t^3 - 2$, $f(t) \in \mathbb{Q}[t]$. f irreducible. f has one root in $\mathbb{Q}(\sqrt[3]{2})$ namely $\sqrt[3]{2}$ f doesn't split over $\mathbb{Q}(\sqrt[3]{2})$, because the other 2 roots are not real.

Theorem 9.9: $L:K$ is normal and finite if and only if L is the splitting field of some poly $f(t) \in K[t]$ over K.

Proof: ($\Rightarrow$) Suppose $L:K$ normal and finite. By 6.11, $\exists \alpha_1, \ldots, \alpha_n$ algebraic over K st $L = K(\alpha_1, \ldots, \alpha_n)$. Let m_i = min poly α_i over K. Let $f = m_1 \ldots m_n$.

Then L = 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 root of $f(\alpha_1, \ldots, \alpha_n)$ so L = splitting field of f over K]

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

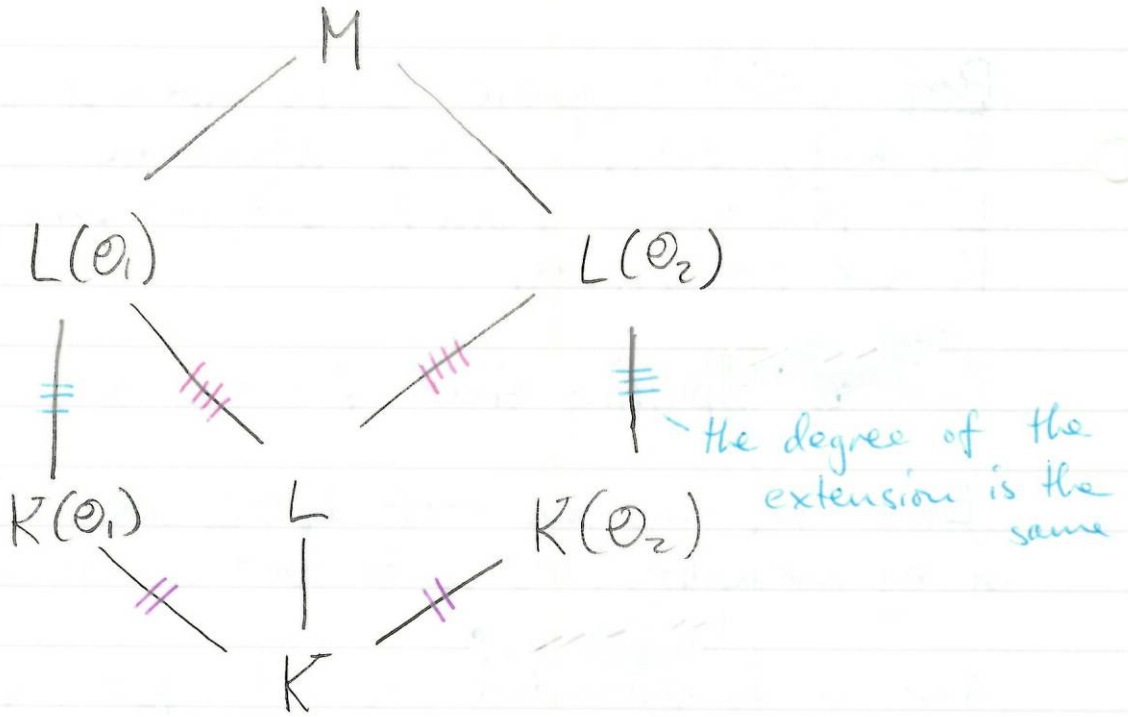
$L:K$ is finite [fin gen algebraic]

Let $f(t) \in K[t]$ be an irreducible poly 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 2 roots of f in M, we aim to prove

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



θ_1, θ_2 are roots of the same irr poly f/K so by 5.13:

$$K(\theta_1) : K \cong K(\theta_2) : K .$$

and by 6.7:

$$[K(\theta_1) : K] = 2f = [K(\theta_2) : K]$$

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

$K(\theta_1) \cong K(\theta_2)$ $\quad (g \mapsto g)$

so by 9.6.

$$L(\theta_1) : K(\theta_1) \cong L(\theta_2) : K(\theta_2)$$

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

By Tower law

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

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

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

Then if $\theta_1 \in L$, degree is 1 and so $\theta_2 \in L$.

Hence $L : K$ normal.

19/2/13

Ch 9 Separability.

If $K \subseteq \mathbb{C}$ then any irreducible polynomial over K is separable. i.e. has no repeated roots, i.e. an irreducible polynomial of degree n has n distinct roots.

[Proof uses idea of Df, the derivative of f]

Lemma 9.13 $K[\epsilon]$ not $\Sigma[\epsilon]$.

Ch 10

Aiming at result: If H is a finite group of automorphism of a field L, then

(1) $[L : H^+] = |H|$, where $H^+ = \{x \in L : h(x) = x \ \forall h \in H\}$.

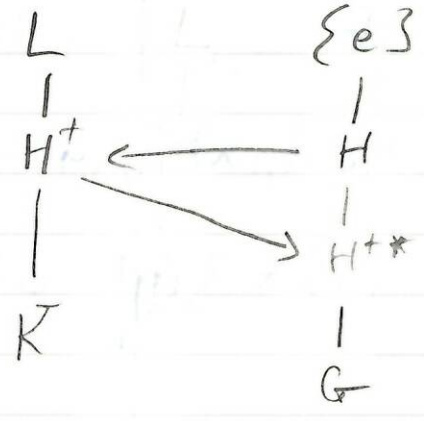
In Ch 11, we show that if $L:K$ is a finite normal (separable) ext^n then $|K^*| = [L:K]$ (2)

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

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

$$|H^{+*}| \overset{\text{by 2}}{=} [L : H^+] \overset{\text{by 1}}{=} |H|$$

Since $H \subseteq H^{+*}$, $H = H^{+*}$



e.g $\mathbb{C}$

$H = \{id, c\}$ $\quad c(a+bi) = a - bi$

$|H| = 2$

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

$= \mathbb{R}$

<u>lemma 10.1</u> If $\lambda_1, \ldots, \lambda_n : K \to L$ are distinct monomorphisms then $\lambda_1, \ldots, \lambda_n$ are linear independant over L.

← function, not a monomorphism.

[if $a_1, \ldots, a_n \in L$ then $a_1\lambda_1 + \ldots + a_n\lambda_n : K \to L$ by $(a_1\lambda_1 + \ldots + a_n\lambda_n)(k) = a_1\lambda_1(k) + \ldots + a_n\lambda_n(k)$: then $a_1\lambda_1 + \ldots + a_n\lambda_n = 0 \Rightarrow$ all $a_i = 0$]

Suppose length 3 shortest say:

$$2\lambda_1 + 3\lambda_2 - 4\lambda_3 = 0.$$

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

For any y $\quad 2\lambda_1(xy) + 3\lambda_2(xy) - 4\lambda_3(xy) = 0. \qquad (2)$

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

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

$(3)-(4)$: $2(\lambda_1(y)-\lambda_3(y))\lambda_1(x)$

$+3(\lambda_2(y)-\lambda_3(y))\lambda_2(x)=0.$

$2(\lambda_1(y)-\lambda_3(y))\lambda_1+3(\lambda_2(y)-\lambda_3(y))\lambda_2=0$

(5)

Pick y st $\lambda_1(y)\neq\lambda_3(y)$

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

You can't have a relation of length 1

$a_1\lambda_1=0.$

$\Rightarrow a_1\lambda_1(1)=0$

$\Rightarrow a_1.1=0.$

$\Rightarrow a_1=0$

10.3 : $\left.\begin{aligned} x+2y+z&=0\\ x-y+z&=0\end{aligned}\right\}$

10.4 : $G=\{g_1,\dots,g_n\}$ eg $G_3=\{e,x,x^2\}$

$G=\{gg_1,\dots,gg_n\}$

$\alpha=\sqrt[4]{3}$

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

$x\in K\Rightarrow x=q_0+q_1x+q_2$

$\alpha = \sqrt[4]{3}$

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

$\varphi : K \to K$

$\varphi(\alpha) = \alpha i$ $\quad x \in K \Rightarrow x \in q_0 + q_1\alpha + q_2\alpha^2 + q_3\alpha^3 + q_4 i + q_5 \alpha i + q_6 \alpha^2 i + q_7 \alpha^3 i$

$\varphi(i) = -i$

$G = \{id, \varphi\}$ $\quad \varphi(x) = q_0 + q_1 i\alpha - q_2\alpha^2 - q_3 i\alpha^3 - q_4 i + q_5\alpha + q_6 i\alpha^2 - q_7\alpha^3$

$[K : K_0] = |G|$

$x = \varphi(x) \iff q_1 = q_5,\ q_2 = -q_2$

$q_3 = -q_7,\ q_4 = -q_4$

So $q_5 = q_1$, $q_7 = -q_3$

$q_1 = q_5$

$q_2 = 0$

$q_7 = -q_3$

$q_4 = 0$

$K^\circ = \{ q_0 + q_1\alpha + q_2\alpha^3 + \dots + q_1 \alpha i + q_6 \alpha^2 + q_3 i\alpha^3 \}$

$= \{ q_0 + q_1(\alpha + \alpha_1) + q_3(\alpha^3 - i\alpha^3) + q_3 i\alpha^2 : q_0, q_1, q_3, q_6 \in \mathbb{Q} \}$

$[K^\circ : \mathbb{Q}] = 4$

$[K : K^\circ] = 8/4 = 2 = |G|.$

Thm^{n} 10.5: Let G be a finite group of automorphisms of a field K and $K_0 = \{x \in K : g(x) = x \ \forall g \in G\}$ be the fixed field. Then:

$$[K : K^0] = |G|.$$

Pf: Let $G = \{g_1, g_2, \ldots, g_n\}$, so $|G| = n$

Let $\{x_1, \ldots, x_{n+1}\}$ be a K_0-basis for K so $[K : K_0] = m$.

Must prove $m = n$.

① Suppose $m < n$.

Then $\exists\, y_1, \ldots, y_m \in K$, not all zero such that:

$$\left.\begin{aligned} y_1 g_1(x_1) + y_2 g_2(x_1) + \ldots + y_n g_n(x_1) &= 0 \\ y_1 g_1(x_2) + g_2 g_2(x_2) + \ldots + y_n g_n(x_2) &= 0 \\ &\vdots \\ y_1 g_1(x_m) + y_2 g_2(x_m) + \ldots + y_n g_n(x_m) &= 0 \end{aligned}\right\}.$$

because this is a homogenous system of m eqn in n unknowns ($m < n$) i.e. $y_1 g_1 + \ldots + y_n g_n$ is n unknowns ($m < n$) i.e. $y_1 g_1 + \ldots + y_n g_n$ is zero at $x_1, x_2, \ldots, x_n$

Hence $y_1 g_1 + \ldots + y_n g_n$ is zero at any K_0-linear combination of $x_1, \ldots, x_m$.

[If $x = \alpha_1 x_1 + \ldots + \alpha_n x_n$ $(\alpha_i \in K)$

then $(y_1 g_1 + \ldots + y_n g_n)(\alpha_1 x_1 + \ldots + \alpha_m x_m)$

$= y_1 g_1 (\alpha_1 x_1 + \ldots + \alpha_m x_m)$
$+ \ldots + y_n g_n (\alpha_1 x_1 + \ldots + \alpha_m x_m)$

$= (y_1 \alpha_1 g_1(x_1) + \ldots + y_1 \alpha_m g_1(x_m)) + \ldots$

$+ (y_n \alpha_1 g_n(x_1) + \ldots + y_n \alpha_m y_n(x_m))$

$= \alpha_1 (y_1 g_1(x_1) + \ldots + y_n g_n(x_1)) + \ldots$

$= 0$]

But $\{x_1, \ldots, x_n\}$ is a K-basis for K so $(y_1 g_1 + \ldots + y_n g_n)(x) = 0$ for all $x \in K$.

i.e $y_1 g_1 + \ldots + y_n g_n = 0$

Contradicting Dedekind's lemma.

2) Suppose $n < m$

Then $\{x_1, \ldots, x_n, x_{n+1}\}$ is LI over K_0
$\exists\, y_1, \ldots, y_{n+1}$ not all zero st:

$$\left.\begin{aligned} y_1 g_1(x_1) + \ldots + y_{n+1} g_1(x_{n+1}) &= 0 \\ y_1 g_2(x_1) + \ldots + y_{n+1} g_2(x_{n+1}) &= 0 \\ &\vdots \\ y_1 g_n(x_1) + \ldots + y_{n+1} g_n(x_{n+1}) &= 0 \end{aligned}\right\}$$

Pick such a solution with as few non-zero terms as possible and re-number to get:

$$\left.\begin{aligned} y_1 g_1(x_1) + \dots + y_r g_1(x_r) &= 0 \\ &\vdots \\ y_1 g_n(x_1) + \dots + y_r g_n(x_r) &= 0 \end{aligned}\right\} \text{(10.8)}, \quad \text{all } y_i \neq 0$$

(No sol^n with $< r$ terms)

Let $g \in G$: apply to 10.8.

$$\left.\begin{aligned} g(y_1)\overbrace{g g_1}^{g_3}(x_1) + \dots + g(y_r)\overbrace{g g_1}^{g_3}(x_r) &= 0 \\ g(y_1) g g_n(x_1) + \dots + g(y_r) g g_n(x_r) &= 0 \end{aligned}\right\}$$

$g g_1 = g_3$, As g_i varies over G, so does $g g_i$

So this is the same as:

$$\left.\begin{aligned} g_1(y_1) g_1(x_1) + \dots + g(y_r) g_1(x_r) &= 0 \\ &\vdots \\ g(y_1) g_n(x_1) + \dots + g(y_r) g_n(x_r) &= 0 \end{aligned}\right\} \text{(10.9)}$$

$g(y_1) \times (10.8) - y_1 \times (10.9)$

$$\left.\begin{aligned} (g(y_1) - y_1 g(y_1)) g_1(x_1) + (g(y_1) y_2 - y_1 g(y_2)) g_1(x_2) + \dots &= 0 \\ (g(y_1) y_1 - y_1 g(y_1)) g_n(x) + (g(y_1) y_2 - y_1 g(y_2)) g_n + \dots &= 0. \end{aligned}\right\}$$

($y_1 g(y_1) - y_1 g(y_1) = 0$)

This is a shorter sol^n than 10.8. a contradiction unless all co-eff are zero i.e.

$$\begin{aligned} g(y_1)\,y_2 &= y_1\,g(y_2) \\ g(y_1)\,y_3 &= y_1\,g(y_2) \\ &\vdots \end{aligned}$$

i.e $g(y_1)\,y_i = y_1\,g(y_i)$

$$g(y_i y_1^{-1}) = y_i y_1^{-1} \quad \forall\, g \in G.$$

$y_i y^{-1} \in K_0$.

$$y_i = y_1 z_i \qquad (z_i \in K_0)$$

10.8; $y_1 g(x_1) + \ldots + y_r g_1(x_r) = 0$.

Take $g = id$.

$$y_1 x_1 + \ldots + y_r x_r = 0.$$

$$y_1 x_1 + y_1 z_2 x_2 + \ldots + y_1 z_r x_r = 0.$$

$$x_1 + z_2 x_2 + \ldots + z_r x_r = 0.$$

i.e $\{x_1, \ldots, x_r\}$ lin dep / K_0.

21/2/13

Ch 10

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

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

Ch 11

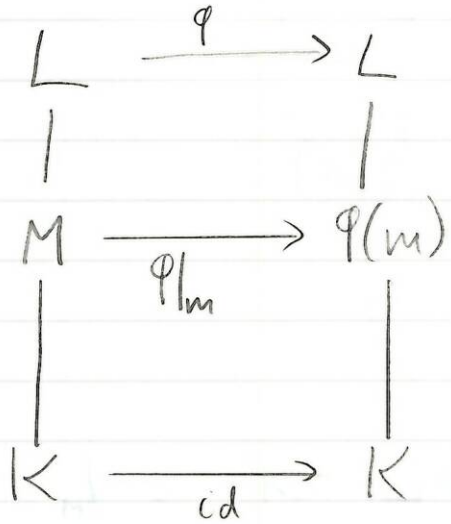
Cor^n 1.11: $L : K$ finite normal sep ext^n then

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

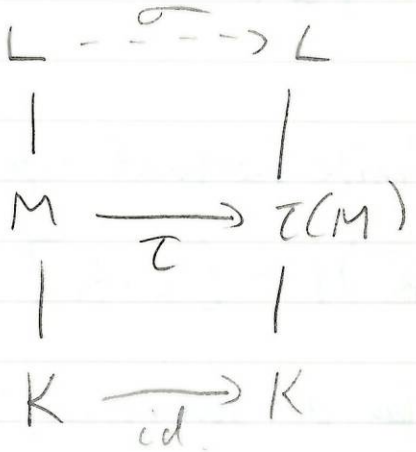
Def 11.1 Let K be a subfield of L, M. Then a K-monomorphism is a field homo^m $\varphi : L \to M$ which is injective and $\varphi|_K = id$

e.g: What are $\mathbb{Q}$-monos $\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$?

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

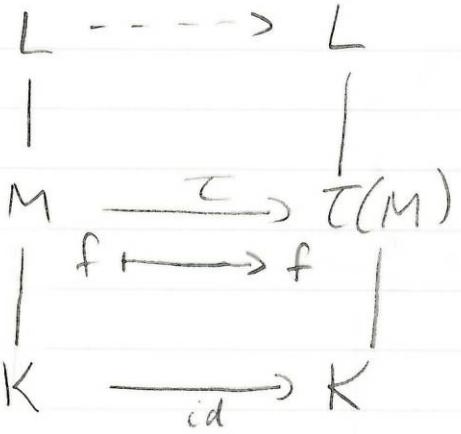


Thm 11.3 Let $K \subseteq M \subseteq L$ and suppose $L:K$ is finite normal. Then any K-monomorphism $\tau: M \to L$ extends to a K-automorphism $\sigma: L \to L$ (i.e $\sigma|_M = \tau$).



Pf: By 9.9, L = splitting of some poly f over K.

Hence L = splitting field of f over M, and over $\tau(M)$.



By 9.6 $\exists\ \sigma: L \to L$ s.t. $\sigma|_M = \tau$, $\sigma|_K = \tau|_K = id$.

Prop 11.4: Suppose $L:K$ is a finite normal-extension and $\alpha, \beta \in L$ with same min poly p over K. Then $\exists$ K-aut σ of L st $\sigma(\alpha) = \beta$

Pf: By 5:13, $\exists$ K-isomorphism $\tau : K(\alpha) \to K(\beta)$. Regard τ as a K-mono $K(\alpha) \to L$. By 11.3 $\exists$ $\sigma : L \to L$, K-aut st $\sigma|_{K(\alpha)} = \tau$. Hence $\sigma(\alpha) = \tau(\alpha) = \beta$.

Def 11.5: Let $L:K$ be a finite extension. A normal closure of $L:K$ is an extension $N:K$ where $L \subseteq N$ st

(i) $N:K$ is normal
(ii) If $L \subseteq M \subseteq N$ and $M:K$ is normal then $M = N$.

Thm 11.6: If $L:K$ is a finite ext^n inside $\mathbb{C}$, then there exist a unique normal closure $N:K$, which is finite.

Pf: Let $x_1, \ldots, x_n$ be a basis for L over K, let m_i be a min poly of x_i over K. Let $f = m_1 \ldots m_r \in K[t]$.

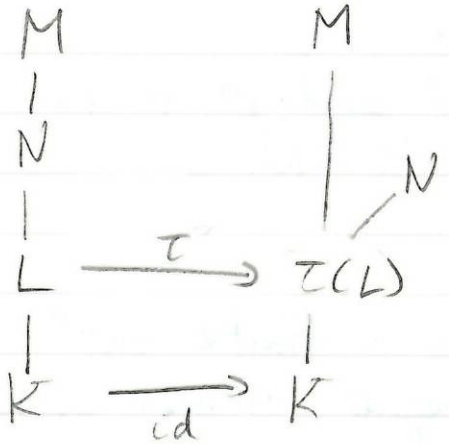
Let N = splitting field of f over $N:K$ is normal and finite (thm 9.9)

Suppose $L \subseteq M \subseteq N$, $M:K$ normal. Then $x_i \in M$ with min poly m_i over K so by normality, m_i splits

in M. Hence f splits in M, so by def" splitting field, $M = N$. Hence N is a normal closure of $L:K$.

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

Lemma 11.8: Suppose $K \subseteq L \subseteq M$ where $L:K$ is finite and $N:K$ is the normal closure of $L:K$. Let $\tau: L \to M$ be any K-mono. Then $\tau(L) \subseteq N$.



Pf: Let $\alpha \in L$. Let $m \in K[t]$ be a min poly of α over K, so $m(\alpha) = 0$.

$$\tau(m(\alpha)) = 0$$

$$m(\tau(\alpha)) = 0.$$

i.e $\tau(\alpha)$ is a root of m. Since $N:K$ normal and m irreducible over K and m has one root α in N, must split over N i.e $\tau(\alpha) \in N$

26/2/13.

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

Th^m 11.9: Let $L:K$ be finite
Then the following are equivalent.
(1) $L:K$ is normal
(2) $\exists$ finite normal extension $N:K$ st $N \supseteq L$ st every K-mono $\tau: L \to N$ is a K-aut of L. (i.e. $\tau(L) \subseteq L$)
(3) For every finite ext^n $M \supseteq L$, every K-mono $\tau: L \to L$ is a K-aut of L (i.e $\tau(L) \subseteq L$)

Pf (1) $\Rightarrow$ (3) Let $L:K$ be normal. Then normal closure of $L:K$ is L. By 11.8 $\tau(L) \subseteq L$

(3) $\Rightarrow$ (2) Let N = normal closure of $L:K$.
By (3) for any K-mono $\tau: L \to N$, $\tau(L) \subseteq L$

(2) $\Rightarrow$ (1) Let f be any irr poly 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, $\exists$ K-aut $\sigma: N \to N$ st $\sigma(\alpha) = \beta$. Then let $\tau = \sigma|_L$

$\tau: L \to N$ is a k-mono.

By (2), $\tau(L) \subseteq L$ i.e. $\beta = \tau(\alpha) \in L$

$\therefore$ $L:K$ normal.

Thm 11.10 : Let $[L:K] = n$. Then there are precisely n K-monos $L \to N$, where N is normal closure of $L:K$ (and hence into any $M \supseteq L$ st $M:L$ is normal)

Cor^y 1.11. If $L:K$ is normal and $[L:K] = n$ then $|\Gamma(L:K)| = n$.

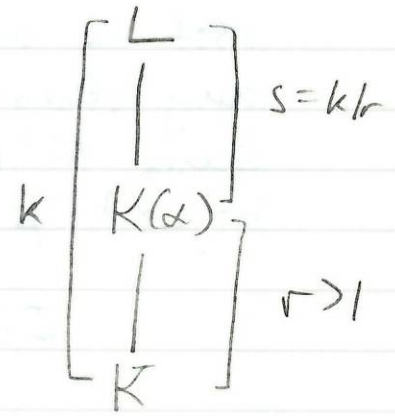
Pf Cor^y, By theorem, there are precisely n K-monos of L into $N = L$. As noted above, any K-mono $L \to L$ is in fact a K-auto of L, i.e. element of $\Gamma(L:K)$.

Pf of theorem.
Induction on $[L:K] = n$

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

Suppose $[L:K] = k$. Pick $\alpha \in L \setminus K$ and let $m \in K[t]$ be min poly of α over K with $\deg m = r$ (say) $r > 1$.

$[K(\alpha):K] = r$
m splits in N,
say with roots
$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$.
(all distinct since separable)



Since m is irr poly over K, with roots α, α_i in N and $N:K$ normal so by 11.4, $\exists$ k-aut τ_i of N st $\tau_i(\alpha) = \alpha_i$.

$L : K(\alpha)$ is a finite ext^n of degree $s < k$ and N is normal closure of $L : K(\alpha)$. By the inductive hypothesis, there are exactly s $K(\alpha)$-monos $e_1 \ldots e_s : L \to N$. Let $\varphi_{ij} = \tau_i e_j : L \to N$

We claim the φ_{ij} $(1 \leq i \leq r,\ 1 \leq j \leq s)$ are precisely the K-monos $L \to N$. These clearly are K-monos $L \to N$ and are all distinct (suppose $\varphi_{ij} = \varphi_{ke}$ i.e. $\tau_i e_j = \tau_k e_c$ then
$\tau_i e_j(\alpha) = \tau_i(\alpha) = \alpha_i$.
$\tau_k e_c(\alpha) = \tau_k(\alpha) = \alpha_k$.

$\therefore \alpha_i = \alpha_k$ so $i = k$ $\quad \tau_i e_j = \tau_i e_c$

τ_i is bijective

$$e_j = e_c$$

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

Let $\tau : L \to N$ be a K-mono $m(\tau(\alpha)) = \tau(m(\alpha)) = \tau(0) = 0$. i.e. $\tau(\alpha)$ is a root of m.

$\therefore \tau(\alpha) = \alpha_i$ for some $1 \leq i \leq r$.

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

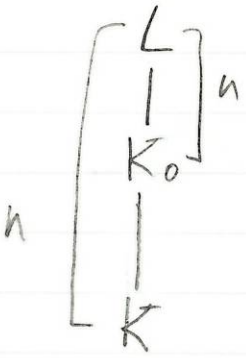
$\therefore \tau_i^{-1}\tau$ is a $K(\alpha)$-mono $L \to N$ $\therefore \tau_i^{-1}\tau = e_j$ for

some $1 \le j \le s$.

$\therefore \tau = \tau_i e_j = \varphi_{ij}$.

Th^m 11.R. Let $L:K$ be a finite normal ext^n of degree n with Galois group G. Then K = fixed field of G.

Pf: Let K_0 = fixed field of G. $K_0 \supseteq K$.



By Cor^y 11, $|G| = n$

By 10.5, $[L:K_0]$

$\therefore$ By Tower law
$[K:K_0] = 1$
i.e $K = K_0$.

Th^m 11.13: Suppose $K \subseteq L \subseteq M$ and $[M:K] < \infty$. Then the number of distinct K-mono $L \to M$ is $\le [L:K]$.

Proof: Let N = normal closure of $M:K$.

Then any K-mono $L \to M$ is a K-mono $L \to N$

By 11.11, there are exactly $[L:K]$ K-monos $L \to N$: hence $\le [L:K]$ k-monos $L \to M$.

Thm 11.14 : Let $L:K$ be a finite extension with Galois group. If K = fixed field of G, then $L:K$ is normal.

Proof : By Thm 10.5, $[L:K] = |G| = n$ (say)
Hence there are exactly n K-autos of L.

Let N be normal closure of $L:K$. By Thm 11.10 there are precisely n K-monos $L \to N$ but the n elements of G are K-monos $L \to N$. Hence every K-mono $L \to N$ is a K-auto of L. By 11.9, $L:K$ is normal.

11.7

a) F
b) T
c) T
d) F : $\mathbb{Q}(\sqrt[3]{2})$
|
$\mathbb{Q}$
e) T
f) F
g) T
h) T
i) F

Lemma 12.2: Let $L:K$ be a fixed ext^n, $K \subseteq M \subseteq L$, τ a K-aut of L.

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

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

$$(\tau g \tau^{-1})(\tau(m)) = \tau g(m)$$
$$= \tau(m)$$

i.e $\tau g \tau^{-1}$ fixes every element in $\tau(M)$.

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

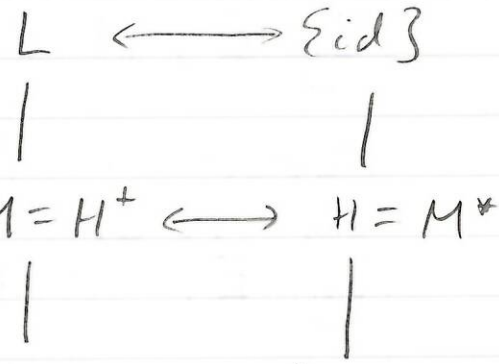
Suppose $g \in \tau(M)^*$. Then $\forall m \in M$, $g(\tau(m)) = \tau(m)$
$(\tau^{-1} g \tau)(m) = m$.

i.e $\tau^{-1} g \tau \in M^*$

$$g \in \tau M^* \tau^{-1}.$$

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

28/2/13.



(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

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

$$\ker\varphi = \{ \tau \in \Gamma(L:K) : \varphi(\tau) = id \}$$

$$= \{ \tau \in \Gamma(L:K) : \tau|_M = id \}$$

$$= M^*$$

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

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

① Let L = splitting field.

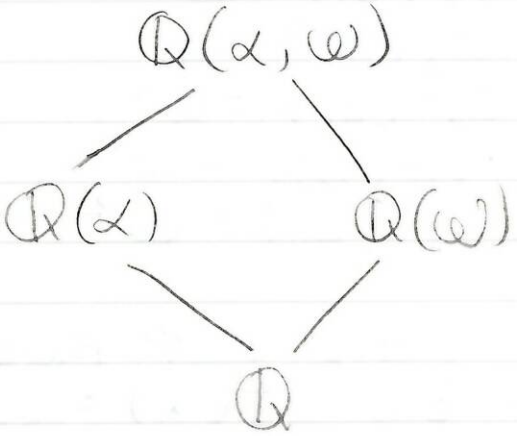
Roots of $t^3-2=0$ are $\alpha, \omega\alpha, \omega^2\alpha$.

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 $[L:K]$



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

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

This is irreducible since $\omega \notin \mathbb{Q}$. $[\mathbb{Q}(\omega):\mathbb{Q}]=2$

Hence $[\mathbb{Q}(\alpha)(\omega):\mathbb{Q}(\alpha)] \leq 2$, i.e $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}] \leq 6$ 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 potential elements of G

$$\begin{aligned}
&\sigma_1(\alpha) = \alpha \quad , \sigma_1(\omega) = \omega. \\
&\sigma_2(\alpha) = \alpha\omega \, , \sigma_2(\omega) = \omega \\
&\sigma_3(\alpha) = \alpha\omega^2, \sigma_3(\omega) = \omega \\
&\sigma_4(\alpha) = \alpha \quad , \sigma_4(\omega) = \omega^2 \\
&\sigma_5(\alpha) = \alpha\omega \, , \sigma_5(\omega) = \omega^2 \\
&\sigma_6(\alpha) = \alpha\omega^2, \sigma_6(\omega) = \omega^2.
\end{aligned}$$

⑤ We don't 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 extension theorems, but here since $|G| = 6$ and $\tau_1 \ldots \tau_6$ are the only candidates, they make up G.

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

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

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

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

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

$gh = \sigma_5$
$g^2h = \sigma_6$.

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

5/3/13.

L = splitting field of $t^3 - 2$ over $\mathbb{Q}$

$G = Gal(L : \mathbb{Q})$

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

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

Found all 6 possibilites for $g \in G$.

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

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

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

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

$g^3 = e$, $h^3 = e$.

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

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

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

$= \alpha\omega \cdot \omega = \alpha\omega^2$

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

so $hg = g^2h$.

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

7) Find all subgroups of G.

Suppose $H \subseteq G$. By Lagrange's th^m:

$|H|$ divides $|G| = 6$ so $|H| = 1, 2, 3$ or 6.

$|H| = 3$. Since 3 prime, $H \cong C_3$

i.e $H = \langle h \rangle$, $o(h) = 2$.

	e	g	g^2	h	gh	g^2h
ord:	1	3	3	2	2	2

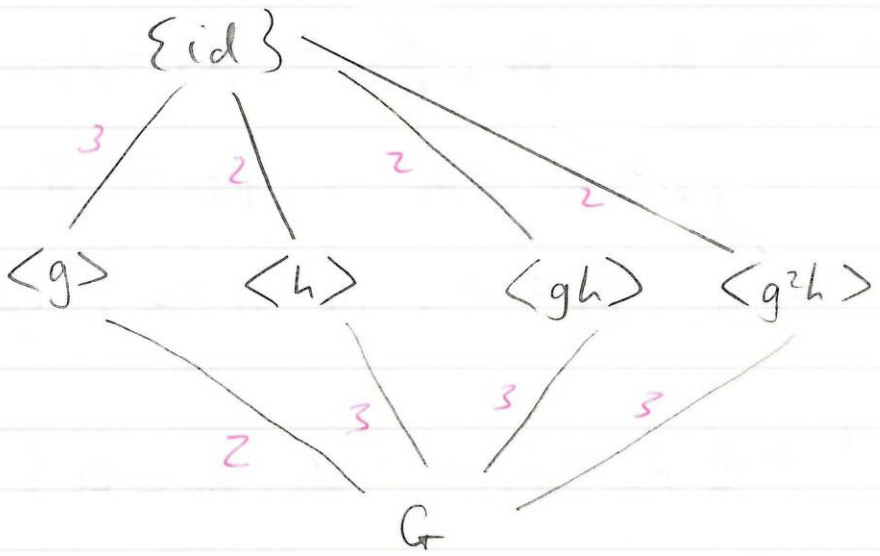
$x = g$ or g^2

$H = \langle g \rangle = \{e, g, g^2\} = \langle g^2 \rangle$

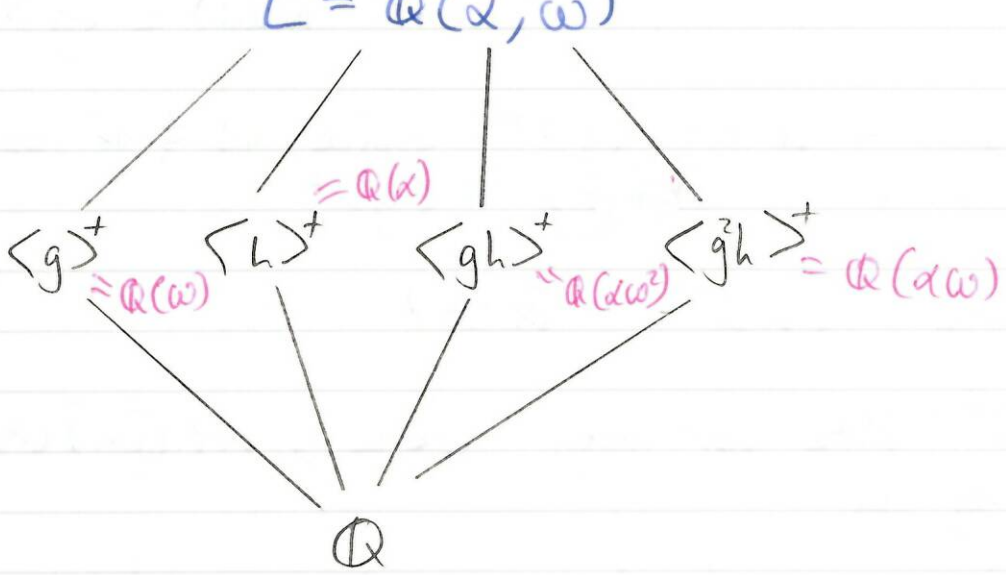
If $|H| = 2$,

$H = \langle h \rangle$ or $\langle gh \rangle$ or $\langle g^2h \rangle$.

8)



9)



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

$$g(\alpha^2) = g(\alpha)^2 = (\alpha\omega)^2 = \alpha^2\omega^2$$
$$= \alpha^2(-1-\omega)$$
$$= -\alpha^2 - \alpha^2\omega.$$

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

$$g(x) = \beta_0 - \beta_4\alpha - \beta_2\alpha^2 - \beta_5\alpha^2 + \beta_2\omega + \beta_1\alpha\omega$$
$$- \beta_4\alpha\omega - \beta_2\alpha^2\omega.$$

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

$\beta_4 = \beta_1 - \beta_4 , \ \beta_5 = -\beta_2 .$

$\Rightarrow \beta_1 = \beta_4 = 0 , \ \beta_2 = \beta_3 = 0 , \ 2\beta_4 = \beta_1$

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

or (quicker). Clearly $\omega \in \langle g \rangle^+$

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

$\therefore \mathbb{Q}(\omega) = \mathbb{Q}$ or $\langle g \rangle^+$ Since $\omega \notin \mathbb{Q}$, so $\mathbb{Q}(\omega) \neq \mathbb{Q}$ $\therefore \mathbb{Q}(\omega) = \langle g \rangle^+$

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

$\langle gh \rangle^+$. Note 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 $\alpha + (gh)(\alpha) = \alpha + \alpha\omega = \alpha(1+\omega) = -\omega^2\alpha .$

$\therefore \alpha\omega^2 \langle gh \rangle^+ \therefore \mathbb{Q}(\alpha\omega^2) \subseteq \langle gh \rangle^+$

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

$\langle g \rangle \triangleleft G$.

$\mathbb{Q}(\omega) : \mathbb{Q}$ is normal

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

L = splitting field of $t^7 - 1$ over $\mathbb{Q}$, $\omega = e^{\frac{2\pi i}{7}}$

Find $\Gamma(L : \mathbb{Q})$, & all subgroups and all intermediate fields.

① $L = \mathbb{Q}(1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6) = \mathbb{Q}(\omega)$

② $[L : \mathbb{Q}] = 6$, $t^7 - 1 = (t-1)\underbrace{(t^6 + t^5 + \dots + 1)}_{m(t)}$

③ $g \in G = \Gamma(L : \mathbb{Q})$ is determined by $g(\omega)$

$g(\omega) = \omega$ or ω^2 or $\dots$ ω^6.

$|G| = 6$.

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

$g_3(\omega) = \omega^5$.

$g_3^2(\omega) = g_3(\omega^3)$

$= (g_3(\omega))^3$

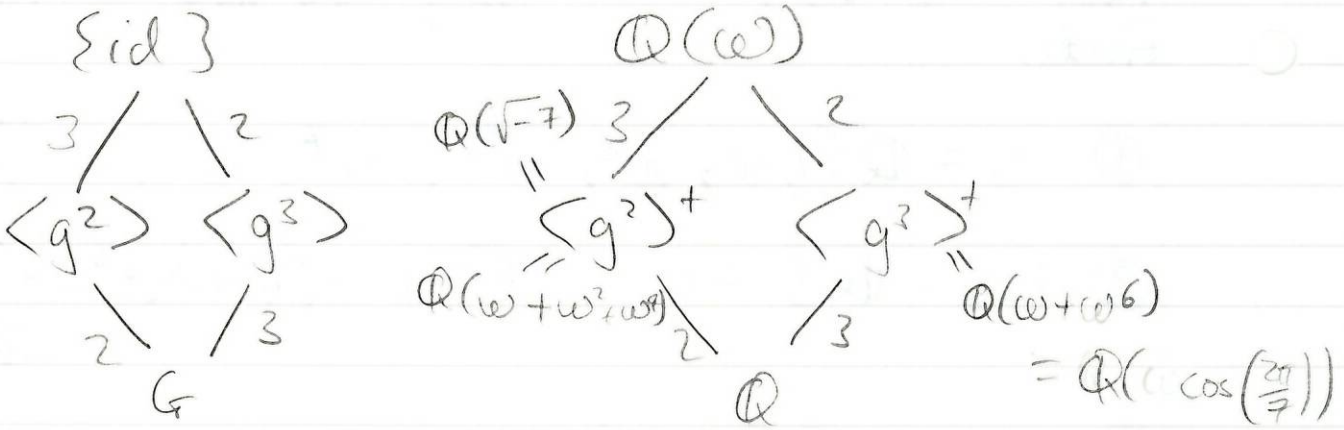
$= (\omega^5)^3 = \omega^{15} = \omega^2$

$g_3^3(\omega) = g_3(\omega^2) = (\omega^3)^2 = \omega^6$

$o(g_3) = 6 \quad g = g_3$.

$G = \langle g : g^6 = e \rangle \cong C_6$, $g(\omega) = \omega^3$

$\langle g^2 \rangle$, $\langle g^3 \rangle$ - subgroups.



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

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

$? \in \langle g^3 \rangle^+$

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

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

-/-

α aut of order m.

$y = x + \alpha(x) + \alpha^2(x) + \alpha^{m-1}(x)$

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

-/-

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

If $\omega + \omega^6 \in \mathbb{Q}$

$$\omega^6 + \omega - q = 0.$$

min poly of ω is

$$m(t) = t^6 + t^5 + \dots + t + 1.$$

$t^6 + t - q$ is not multiple of $m(t)$ -X.

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

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

$\beta = \omega + \omega^2 + \omega^4$

$\beta \in \langle g^2 \rangle^+$

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

$\mathbb{Q}(\beta) \neq \mathbb{Q}$.

$\beta = \omega + \omega^2 + \omega^4$

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

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

$= -2$.

$$\beta^2 + \beta - 2 = 0.$$

so $\beta = \frac{1 \pm \sqrt{1-8}}{2} = \frac{-1 \pm \sqrt{-7}}{2}$.

Soluble group.

Def^n : A group is soluble if there exists a finite chain of subgroup of G.

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \dots \leq G_n = G.$$

st $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian.

e.g any abelian group is soluble, G abelian.

$$\{e\} = G_0 \leq G_1 = G.$$

G_1/G is abelian.

D_{2n} is soluble $D_{2n} = \langle g, h : g^n = h^2 = e, hg = g^{n-1}h \rangle$.

$$= \{g^i h^j : 0 \leq i \leq n, 0 \leq j \leq 2\}.$$

Let $G_1 = \langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$.

Consider

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

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

$G_1 \trianglelefteq G_2$.

$G_2 / G_1 = D_{2n} / C_n \cong C_2$

abelian.

S_4 is soluble and S_5 is not soluble.

Thm: Let G be a group, $H \leq G$, $N \trianglelefteq G$.

(i) G soluble $\Rightarrow G/N$ soluble.

(ii) N soluble and G/N soluble $\Rightarrow G$ soluble.

(this is called "closure under extension").

7/3/13

G <u>soluble</u> if $\exists G_i \leq G$

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

$$G_i \trianglelefteq G_{i+1}$$

G_{i+1}/G_i abelian.

— / —

<u>Proof of 14.4</u>. (i) G soluble, $H \subseteq G \Rightarrow H$ soluble.

$$\{e\} = G_0 \subseteq G_1 \dots \subseteq G_n = G.$$

$G_i \trianglelefteq G_{i+1}$, G_{i+1}/G abelian.

Let $H_i = G_i \cap H$ $\quad H_i \subseteq H$

$$\{e\} = H_0 \subseteq H_1 \subseteq \dots \subseteq H_n = H.$$

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

$g^{-1}hg \in G_i$ (because $h \in G_i$, $g \in G_{i+1}$ and $G_i \trianglelefteq G_{i+1}$)

$N \subseteq G$
N is normal if $\forall g \in G$ $g^{-1}Ng \subseteq N$.

$g^{-1}hg \in H$ (because $g, h \in H$)

$g^{-1}hg \in H \cap G_i := H_i$

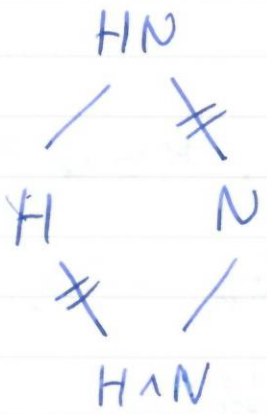
Thus $g^{-1}H_i g \subseteq H_i$ i.e. $H_i \trianglelefteq H_{i+1}$.

Recall the isomorphism theorems.

① $\varphi : G \to H$. gp hom^n.

Then $G/\ker\varphi \cong \operatorname{Im}\varphi$.

② $H \leq G$, $N \trianglelefteq G$.



The $HN = \{hn : h \in H, n \in N\} \subseteq G$.

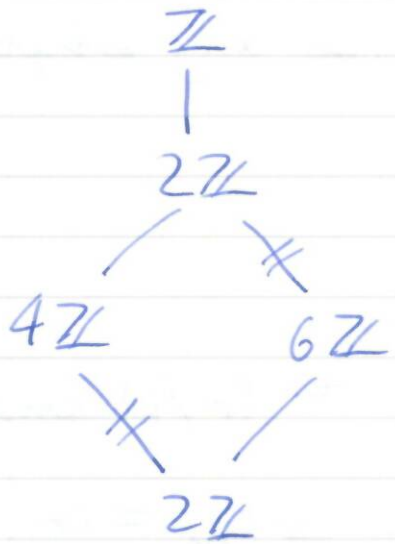
$N \trianglelefteq HN$, $H \wedge N \trianglelefteq H$.

and $HN/H \cong H/H\wedge N$.

e.g. $G = \mathbb{Z}$, $H = 4\mathbb{Z}$, $N = 6\mathbb{Z}$.

$H \wedge N = 4\mathbb{Z} \wedge 6\mathbb{Z} = 12\mathbb{Z}$.

$HN = 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$.



$2\mathbb{Z}/6\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$.

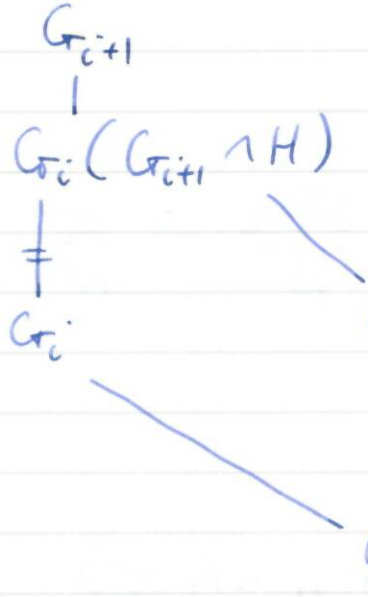
i.e $\{\bar{0}, \bar{2}, \bar{4}\} \cong \{\bar{0}, \bar{4}, \bar{8}\}$.

— / —

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

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

$G_i \trianglelefteq G_{i+1}$



Isomorphism thm:

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

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

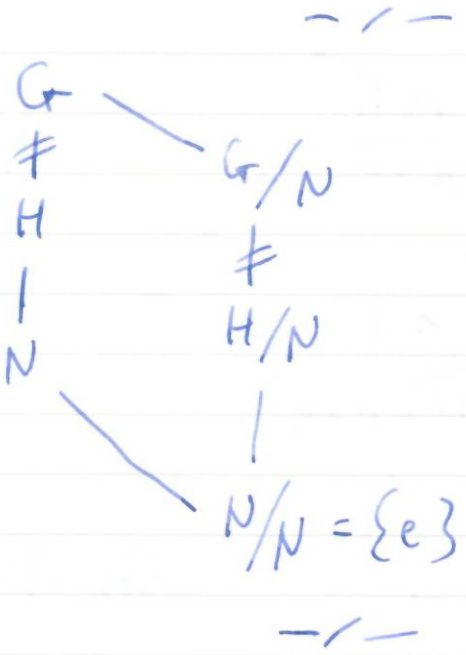
G_{i+1}/G_i is abelian, so any subgroup is abelian

H_{i+1}/H_i is abelian.

H is soluble.

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

$\{e\} = G_0 \subseteq G_1 \subseteq \dots \subseteq G_n = G$ $\quad G_{i+1}/G$ abelian



$$\frac{N}{N} \leq \frac{NG_1}{N} \subseteq \frac{NG_2}{N} \subseteq \dots \subseteq \frac{NG_n}{N} = \frac{G}{N}$$

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

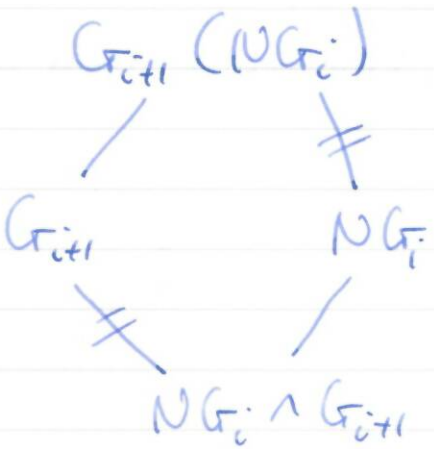
$$\frac{NG_{i+1}/N}{NG_i/N} \cong \frac{NG_{i+1}}{NG_i} = \frac{G_{i+1}(NG_i)}{NG_i}$$

$$\ldots = \frac{G_{i+1}(NG_i)}{NG_i} \cong \frac{G_{i+1}}{G_{i+1} \cap NG_i} \cong \ldots$$

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

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

G/N is soluble.



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

Suppose S_5 is soluble.

$A_5 \lhd S_5$ would also be soluble.

But A_5 is <u>simple</u>, i.e it has no normal subgroups (other than $\{e\}$ and itself) (Pf. Thm 14.7, not examinable).

If

$$\{e\} = G_1 \subseteq \ldots \subseteq G_{n-1} \subseteq G_n = G = A_5$$

$G_{n-1} \trianglelefteq G$, so $G_{n-1} = \{e\}$.

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

A_5 not abelian. contradiction, A_5 is <u>not</u> soluble.

—/—

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

(Cauchy's Thm follows from Sylow).

12/3/13.

$\sqrt[3]{2+\sqrt{3}}$

$\mathbb{Q}(\sqrt{3})(\sqrt[3]{2+\sqrt{3}})$ $\quad (\sqrt[3]{2+\sqrt{3}})^3 \in \mathbb{Q}(\sqrt{3})$

$\mathbb{Q}(\sqrt{3})$ $\quad (\sqrt{3})^2 \in \mathbb{Q}$.

$\mathbb{Q}$

Inside $\mathbb{C}$.

Def 15.1 $L:K$ is radical if there exist $\alpha_1, \dots, \alpha_m \in L$, $n_1, \dots, n_m \in \mathbb{N}$ st $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$ and $L = K(\alpha_1, \dots, \alpha_m)$.

$L = K(\alpha_1, \dots, \alpha_m)$, $\alpha_m^{n_m} \in K(\alpha_1, \dots, \alpha_{m-1})$

$K(\alpha_1, \dots, \alpha_{m-1})$

$\vdots$

$K(\alpha_1, \alpha_2)$ $\quad \alpha_2^{n_2} \in K(\alpha_1)$

$K(\alpha_1)$ $\quad \alpha_1^{n_1} \in K$

K

Def 15.2 : Let f be a poly over K, with splitting field Σ. Then f is *soluble by radicals* if $\exists$ a field $M \supseteq \Sigma$ st $M:K$ is radical.

Th^m 15.3 : Let $K \subseteq L \subseteq M$, with $M:K$ radical Then $Gal(L:K)$ is soluble.

Main Lemma (15.7) Let $M:K$ be a normal radical extension. Then $\Gamma(L:K)$ is soluble

—/—

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

$L = K(\alpha_1, \ldots, \alpha_m)$

ab
ab
Gal gp is abelian

$K(\alpha_1)$
|
K.

$\alpha_1^{n_1} \in K$

—/—

lemma 15.6 Let $L:K$ be radical, $M:K$ is normal closure. Then $M:K$ is radical.

Pf: $L = K(\alpha_1, \ldots, \alpha_m)$

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

Let f_i = min poly of α_i over K

$f = f_1 \dots f_m$, M = splitting field of f over K.

Let roots of f_i be $\alpha_i = \beta_{i,1}, \dots, \beta_{i,\epsilon_i}$

then $M = K(\beta_{1,1}, \dots, \beta_{1,\epsilon_1}, \beta_{2,1}, \dots \beta_{1,\epsilon_2}, \dots$

$\beta_{m1}, \dots, \beta_{m,\epsilon_m})$

Claim this is a radical sequence for M. Since α_i and β_{ij} have same min poly f_i over K, so by 5.13, $\exists$ iso $\sigma : K(\alpha_i) \longrightarrow K(\beta_{ij})$ st $\sigma|_K = id$, $\sigma(\alpha_i) = \beta_{ij}$.

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

$\tau : M \to M$, $\tau|_K = id$, $\tau(\alpha_1) = \beta_{ij}$

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

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

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

α_1 has min poly f_1 st $\tau(\alpha_1)$ is a root of f_1 i.e. $\tau(\alpha_i) =$ some β_{ik} similarly for $\tau(\alpha), \dots, \tau(\alpha_{i-1})$.

$$\beta_{ij}^{n_i} \in K(\beta_{11}, \dots, \beta_{1,\epsilon_1}, \beta_{2,1} \dots \beta_{2,\epsilon_2}, \dots, \beta_{i-1,1} \dots \beta_{i-1,\epsilon_{i-1}})$$

$\therefore M : K$ is radical.

Lemma 15.5. L = splitting field of $\epsilon^p - 1$ over K (p prime). Then $\Gamma(L:K)$ is abelian.

Pf: $\omega = e^{2\pi i/p}$. Then $L = K(\omega)$ and roots of $\epsilon^p - 1$ are powers of ω. Any $g \in \Gamma(L:K)$ is determined by $g(\omega)$ and send ω to ω^i for some i.

Let $g, h \in \Gamma(L:K)$, say $g(\omega) = \omega^i$, $h(\omega) = \omega^j$.

$$(gh)(\omega) = g(\omega^j) = \omega^{ij}$$

$$(hg)(\omega) = h(\omega^i) = \omega^{ij}$$

$\therefore gh = hg$ i.e. Γ is abelian.

Lemma 15.6: Let K be a subfield of $\mathbb{C}$ over which $\epsilon^n - 1$ splits. Let L = splitting field of $\epsilon^n - a$ over K, where $a \in K$. Then $\Gamma(L:K)$ is abelian.

Pf: Let α be a zero of $\epsilon^n - a$ in L. Then other roots are $\varepsilon\alpha$ where ε is a root of $\epsilon^n - 1$ since $\varepsilon \in K$, $L = K(\alpha)$.

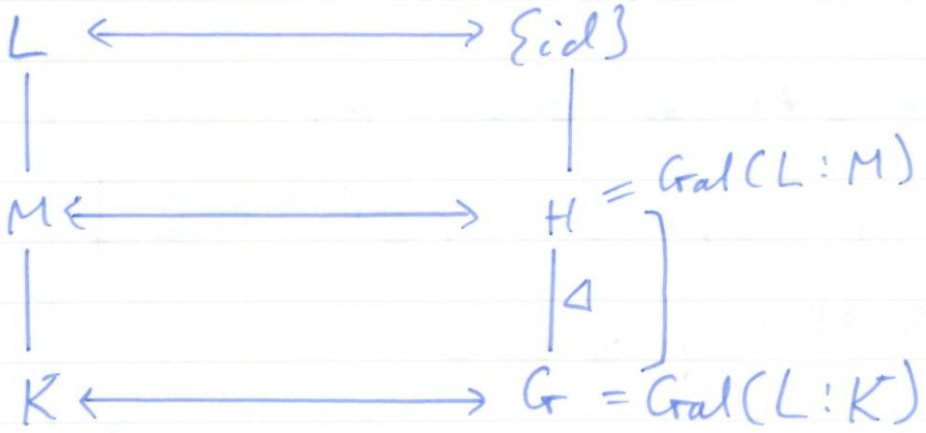
Any $g \in \Gamma(L:K)$ is determined by $g(\alpha)$ and $g(\alpha) = \varepsilon\alpha$ for some $\varepsilon \in K$, $\varepsilon^n = 1$. Let $g, h \in \Gamma(L:K)$, say $g(\alpha) = \varepsilon\alpha$, $h(\alpha) = \eta\alpha$. Then

$$(gh)(\alpha) = g(\eta\alpha) = \eta g(\alpha) = \eta\varepsilon\alpha$$

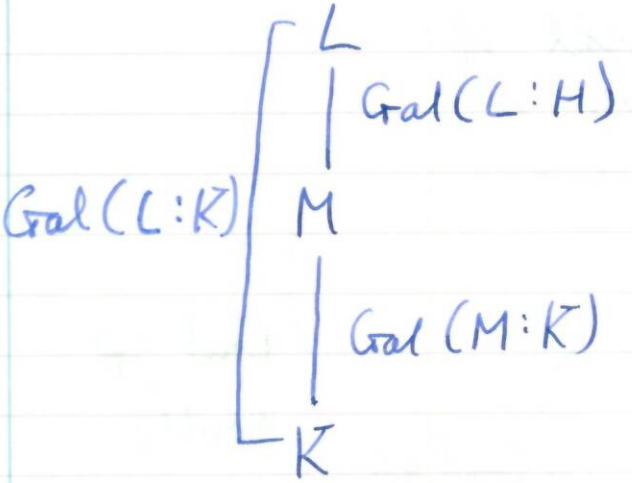
$$(hg)(\alpha) = h(\varepsilon\alpha) = \varepsilon h(\alpha) = \varepsilon\eta\alpha.$$

$gh = hg$ $\quad \therefore \Gamma$ abelian.

— / —



$\mathrm{Gal}(M:K) \cong G/H.$



If $\mathrm{Gal}(L:M)$ is soluble and $\mathrm{Gal}(M:K)$ is soluble then $\mathrm{Gal}(L:K)$ is soluble.

$$\mathrm{Gal}(M:K) \cong \frac{\mathrm{Gal}(L:K) = G}{\mathrm{Gal}(L:M) = N}$$

like G/N

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

Pf of 15.7. $L:K$ normal and radical $\Rightarrow$ $\Gamma(L:K)$ soluble. Let $L:K(\alpha_1,\ldots,\alpha_n)$, $\alpha_j^{n_j}\in K(\alpha_1,\ldots,\alpha_{j-1})$. WLOG, all n_j prime: in particular let $n_1=p$(prime) so $\alpha_1^p\in K$. Proof by induction on n [$\alpha_1\notin K$: let min poly of α_1 over K by f. $\therefore$ f splits in L, because $L:K$ normal. Let β be another root of $f\neq\alpha_1$. Let $\epsilon=\alpha_1/\beta$. Then $\epsilon^p=\alpha_1^p/\beta^p=1$.

Then $\epsilon\neq 1$, so $o(\epsilon)=p$.

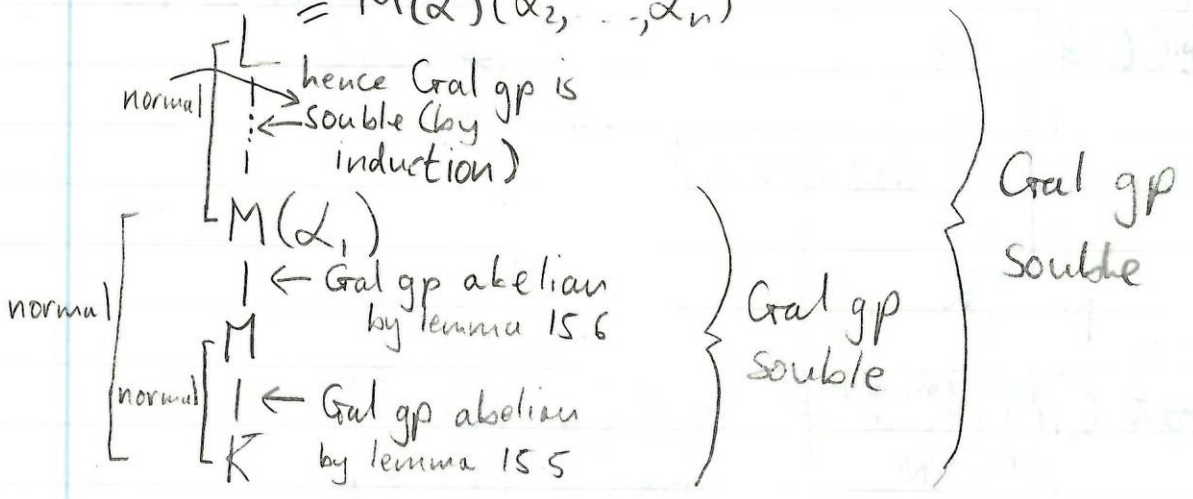
$\therefore 1,\epsilon,\epsilon^2,\ldots,\epsilon^{p-1}\in L$]

$\Rightarrow \epsilon^p-1$ splits in L.

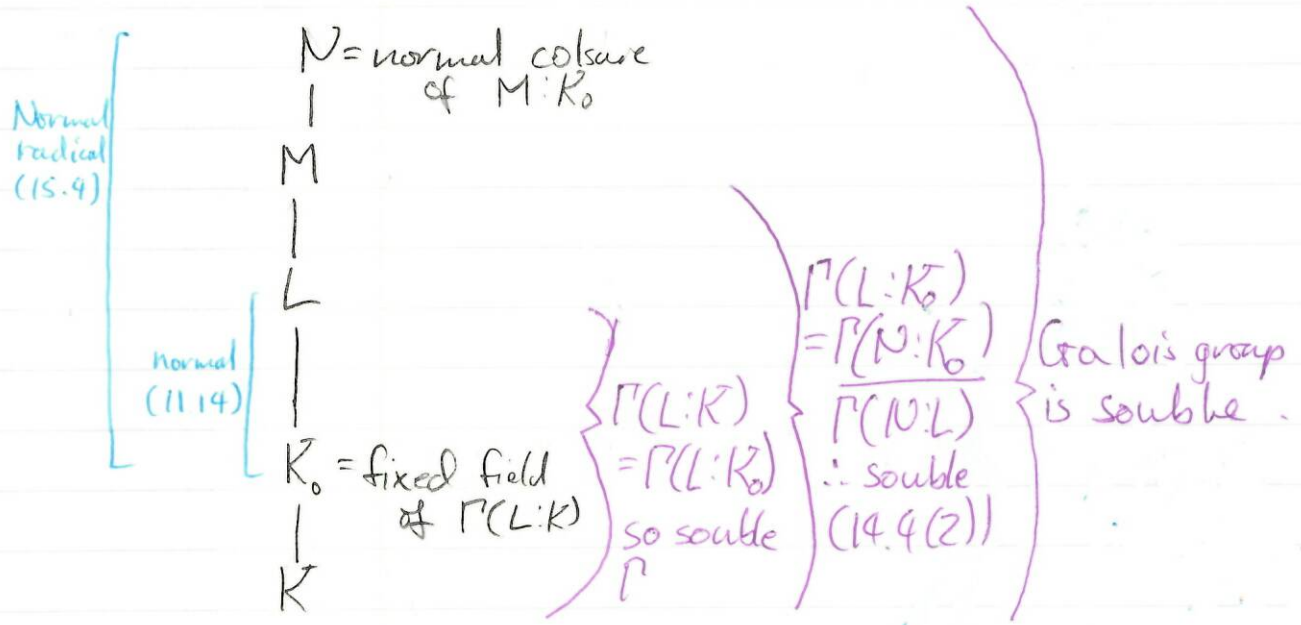
Let $M=$ splitting field of ϵ^p-1 over K. Then $M\subseteq L$. $M=K(\epsilon)$. Now consider:

$M(\alpha_1)=$ splitting field of $\epsilon^p-\alpha_1^p$ over K.

$=M(\alpha)(\alpha_2,\ldots,\alpha_n)$



Thm 15.3 $K \subseteq L \subseteq M$, $M:K$ radical $\Rightarrow \Gamma(L:K)$ is soluble.



14/3/13

$M : K$ radical, $K \subseteq L \subseteq M$; $\Rightarrow Gal(L:K)$ soluble.

Def 1.58: Let $f \in K[t]$ with splitting field Σ. Galois group of f over K is $Gal(\Sigma : K)$.

Thm 15.9: If $f \in K[t]$ is soluble by radicals then the Galois group of f over K is soluble.

We can think of $Gal(f)$ as a group of permutations of the root of f.

Let $f \in K[t]$, splitting field Σ, $\Sigma = K(\alpha_1, \ldots, \alpha_n)$ where α_i are root of f.

If $\sigma \in Gal(f) = Gal(\Sigma : K)$, then σ is determine by $\sigma(\alpha_1) \ldots \sigma(\alpha_r)$ 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 $\sigma \mapsto \pi$ gives an isomorphism

$$Gal(f) \longrightarrow G \subseteq S_r.$$

Thm 15.10: Let p be a prime, and f an irreducible ploy of degree p over $\mathbb{Q}$. Suppose f has exactly 2 non-real roots. Then

$$Gal(f) \cong S_p.$$

Proof: Think of $Gal(f) = Gal(\Sigma : \mathbb{Q})$ as a group of permutation of the roots. $\overset{\text{"}}{=} G$

There are p distinct roots.

$G \cong$ subgroup of S_p.

If α is one root, then $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \Sigma$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \partial f = p$. By Tower law $p \mid [\Sigma : \mathbb{Q}]$ so $p \mid |G|$.

Hence $\exists$ element of order p in G. (Cauchy's theorem or consequence of Sylow Th^{m})

Hence G contains a p-cycle. Also complex conjugation c gives a $\mathbb{Q}$-aut $\mathbb{C} \to \mathbb{C}$. Since $\Sigma : \mathbb{Q}$ normal $c|_\Sigma \in Gal(\Sigma : \mathbb{Q})$

This switches the 2 complex roots and fixes the next, so G contains a 2-cycle WLOG, 2-cycle is $(1\,2) = t$

Some power of p cycle will send 1 to 2 by re-ordering the other roots, we can take the p-cycle $(1\,2\,3 \ldots p) = \sigma \in G$.

Now $\sigma t \sigma^{-1} = (2\,3) \in G$

$$\sigma t \sigma^{-1}(2) = \sigma t(1) = \sigma(2) = 3$$
$$\sigma t \sigma^{-1}(3) = \sigma t(2) = \sigma(1) = 2$$
$$\sigma t \sigma^{-1}(1) = \sigma t(p) = \sigma(p) = 1.$$

Similary $\sigma^2 \tau \sigma^{-2} = (34) \in G$.

All adjacent transpositions lie in G, Any permutation is a product of adjacent transposition (1201) so $G = S_p$.

Thm 15.11. Let $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$. Then f is not soluble by radicals over $\mathbb{Q}$.

Pf: f is irreducible (Eisenstein $p = 3$) f has exactly 3 real roots (sketch the curve). By 15.10, $\mathrm{Gal}(f) \cong S_5$.

S_5 is not souble (because A_5 is not souble, because A_5 has no normal subgroups).

By 15.9, f is not souble by radical

— / —