3202 Galois Theory Notes

Based on the 2017 autumn lectures by Dr M L Roberts

The Author(s) has made every effort to copy down all the content on the board during lectures. The Author(s) accepts no responsibility for mistakes on the notes nor changes to the syllabus for the current year. The Author(s) highly recommends that the reader attends all lectures, making their own notes and to use this document as a reference only.

02-10-17 Galois Theory - Dr Mark Roberts

80% exam, 10% coursework, 10% groupwork project.

Set Textbook: Galois Theory - Ian Stewart (ed 3 or 4)
(most of chapters 1-15)

Galois Theory concepts.

a). Establishing a 1-to-1 correspondence between extensions of fields and groups

b). Analysing the solution of polynomial equations using this correspondence, in particular showing that the general quintic eqn. does not have a solution "by radicals".

c). Solving some classical geometric problems, such as "squaring the circle".

---

a). The Fundamental Theorem of Galois Theory associates to a field extension $\mathbb{F} \subseteq K$ a group G, called the Galois group of the extension, and (under certain conditions) a 1-1 correspondence between intermediate fields $\mathbb{F} \subseteq M \subseteq K$ and subgroups of G.

b). Solving polynomial equations

$ax+b=0 \qquad x = -b/a$

$ax^2+bx+c=0 \qquad x = \dfrac{-b \pm \sqrt{b^2-4ac}}{2a}$

$t^3+at^2+bt+c=0$

$y = t + a/3 \qquad y^3 = t^3 + 3t^2(\frac{a}{3}) + \dots$

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

$y = u+v$

$\Rightarrow (u+v)^3 + p(u+v) + q = 0$

$\Rightarrow u^3 + 3u^2v + 3uv^2 + v^3 + p(u+v) + q = 0$

$(u^3+v^3+q) + (3u^2v + 3uv^2 + p(u+v) = 0$

$(u^3+v^3+q) + (3uv(u+v) + p(u+v)) = 0$

$(u^3+v^3+q) + (u+v)(3uv+p) = 0$

We want to make $U^3 + V^3 + q = 0$

and $3UV + p = 0$

$$\begin{cases} U^3 + V^3 = -q \\ 3UV = -p \quad \Rightarrow \quad U^3V^3 = -p^3/27 \end{cases}$$

Let $U^3 = u$, $V^3 = v$

$$\Rightarrow \begin{cases} u + v = -q \\ uv = -p^3/27 \end{cases}$$

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

$$27u^2 + 27qu - p^3 = 0$$

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

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

(Cardano's formula) - Solution of cubic by radicals.

A quartic can be solved similarly.

We can use the Fundamental Theorem to show that the general quintic equation cannot be solved by radicals.

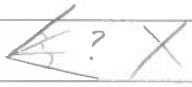
$x^2 + 1 = 0$ over $\mathbb{R}$

$\Rightarrow x = \pm i$

field extension.

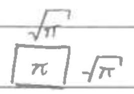
$\mathbb{R}, i \longrightarrow \mathbb{C} \Rightarrow \mathbb{C} : \mathbb{R}$

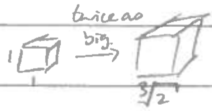
c). Geometric problems



not possible to trisect an angle with ruler and compass

Area $= \pi$





MATH 3202

02-10-17

What do you need to know?

a). Linear algebra (LI, bases, dimension,..) (MATH1201/2)

b). A bit of group theory (group, subgroup, Lagrange's Thm, statement of Sylow's Thms, permutations) (MATH 7202/1201/1202).

c). Abstract algebra (ideals, quotient rings)

d). Algebraic calculations (eg. calculations in groups)

06-10-17

Handout 1, part B

(i) $x^3 - 2$ is irreducible over $\mathbb{Z}$ and $\mathbb{Q}$

(since it is a cubic with no root, and then by Gauss irr over $\mathbb{Z} \Rightarrow$ irr over $\mathbb{Q}$)

$\mathbb{R}$: $x^3 - 2 = (x-\alpha)(\overset{\uparrow \text{ irr. (quadratic with no root)}}{x^2 + \alpha x + \alpha^2})$, $\alpha = \sqrt[3]{2}$

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

$\{\bar{0}, \bar{1}, \bar{2}\} = \mathbb{Z}_3$: $x^3 - \bar{2} = x^3 + \bar{1} = (x+\bar{1})^3$ since $3 = 0$

$\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \mathbb{Z}_5$: $f(x) = x^3 - \bar{2}$, $f(\bar{3}) = \bar{0}$ $\therefore$ $x - \bar{3}$ is a factor

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

$\uparrow$ irreducible (since no root)

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

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

$t^3 + 2t^2 - t + 1 \in \mathbb{Z}[t]$

$t^3 + t + \bar{1} \in \mathbb{Z}_2[t]$

If $f = gh$ in $\mathbb{Z}[t]$ then $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{Z}_n[t]$

If $\bar{f}$ is irreducible in $\mathbb{Z}_n[t]$, then f irreducible in $\mathbb{Z}[t]$

(need the leading coefficient to be coprime to n).

$2t^3 + t^2 + t + 1 = f(t) \in \mathbb{Z}[t]$

$\bar{f}(t) = 2t^3 + t^2 + t + 1 \in \mathbb{Z}_3[t]$

$\bar{f}(\bar{0}) = \bar{1}$ $\bar{f}(\bar{1}) = \bar{2}$ $\bar{f}(\bar{2}) = \bar{2}$ no root $\Rightarrow$ irreducible over $\mathbb{Z}_3$

$\therefore$ irreducible over $\mathbb{Z}$ $\therefore$ irreducible over $\mathbb{Q}$

(iii) ⓐ $t^3 + 7t^2 - 8t + 1 = f(t)$

$f(t) = t^3 + t^2 + \bar{1} \in \mathbb{Z}_2[t]$

$f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{1}$ ⇒ no root so irreducible over $\mathbb{Z}_2$

∴ irreducible over $\mathbb{Z}$ ∴ irreducible over $\mathbb{Q}$

Cubic so if red. has linear factor $t-a$, hence a root in $\mathbb{Q}$ which divides 1 ie. ± 1, $f(1) \neq 0$, $f(-1) \neq 0$

~~ⓑ $t^4 - t^2 + 2t - 1 = f(t)$~~

~~$f(t) = t^4 + t^2 + \bar{1} \in \mathbb{Z}_2[t]$~~

~~$f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{1}$ ⇒ no root so irreducible over $\mathbb{Z}_2$~~

~~∴ irreducible over $\mathbb{Z}$ ∴ irreducible over $\mathbb{Q}$.~~

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

~~$f(t) = t^4 + t^3 + t^2 + t + \bar{1} \in \mathbb{Z}_2[t]$~~

~~$f(\bar{0}) = \bar{1}$, $f(\bar{1}) = \bar{1}$ ⇒ no root so irreducible over $\mathbb{Z}_2$~~

~~∴ irreducible over $\mathbb{Z}$ ∴ irreducible over $\mathbb{Q}$.~~

ⓑ $f(t) = t^4 - t^2 + 2t - 1$

$f(1) \neq 0$, $f(0) \neq 0$, so no root, so no linear factor

Does not imply irreducible.

$t^4 - t^2 + 2t - 1 = (t^2 + at + b)(t^2 + ct + d)$

$$\Rightarrow \begin{cases} a + c = 0 \\ b + ac + d = -1 \\ ad + bc = 2 \\ bd = -1 \end{cases}$$

⇒ $b = 1, d = -1$ or $b = -1, d = 1$

$c = -a$

$ac = -1$ ⇒ $ac = -1$

so $-a^2 = -1$ ⇒ $a = 1$, $c = -1$

so $f(t) = (t^2 + t - 1)(t^2 - t + 1)$

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

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

MATH 3202

06-10-17

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

$t = s+1$

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

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

5 divides 5, 10, 10

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

$\therefore$ irreducible by Eisenstein's criterion with $p = 5$.

3.17 from book.

a - F, b - T, c - F, d - F, e - T, f - T, g - F, $\overset{\text{eg. } t^4 - 2}{\nearrow}$

h - T, i - F, j - T.

Chapter 4 - Field Extensions

Recall a field is a ring in which every non-zero element has an inverse.

Examples:

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$

This$\uparrow$ is clearly a ring. In fact if $x = a + bi \in \mathbb{Q}(i)$, $x \neq 0$, then x has an inverse.

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2} \in \mathbb{Q}(i)$$

So $\mathbb{Q}(i)$ is a field: in fact a subfield of $\mathbb{C}$.

If K, L are two fields, a field homomorphism is a map $\phi : K \mapsto L$

s.t. $\phi(a+b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a)\phi(b)$

$\phi(0) = 0$, $\phi(1) = 1$

[hence also $\phi(a-b) = \phi(a) - \phi(b)$, $\phi(a^{-1}) = \phi(a)^{-1}$]

ϕ is a field monomorphism if it is an injective homomorphism. (i.e. $\phi(a)=0 \Rightarrow a=0$).

The inclusion map is a field monomorphism eg. $\mathbb{R} \rightarrow \mathbb{C}$ $[\mathbb{R} \subseteq \mathbb{C}]$

ϕ is a field isomorphism if it is a bijective homomorphism

e.g. $\phi: \mathbb{Q}(i) \mapsto \mathbb{Q}(i)$ by $\phi(a+bi) = a-bi$
is a field isomorphism.

Def^n 4.1
A field extension is a field monomorphism $\phi: K \mapsto L$, K, L fields.

e.g. $i_1: \mathbb{Q} \mapsto \mathbb{R}$ inclusion map
$i_2: \mathbb{R} \mapsto \mathbb{C}$ " "
$i_3: \mathbb{Q}(i) \mapsto \mathbb{C}$ " "
$j: \mathbb{Q}(i) \mapsto \mathbb{C}$, $j(a+bi) = a-bi$

If $i: K \mapsto L$ is a field monomorphism, then
$i: K \mapsto i(K) \subseteq L$ is a field isomorphism, so $K \cong i(K)$

Usually we can identify isomorphic objects, so
$K \subseteq L$ and i is inclusion.

Nearly all the time a field extension will be
K a subfield of L. Then we write $L:K$.

So objects considered are basically extensions $L:K$
where K is a subfield of L.
Work inside $\mathbb{C}$ unless otherwise specified.

MATH 3202

06-10-17

Def^n 4.2

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

$$= \bigcap_{X \subseteq K \leq \mathbb{C}} K$$

Note that $\langle X \rangle$ is a subfield of $\mathbb{C}$.

$\langle X \rangle$ can also be described as:

1). $\langle X \rangle$ = unique smallest subfield of $\mathbb{C}$ containing X

2). $\langle X \rangle$ = set S of all elements obtained by combining elements of X using $+, \times, -, ^{-1}$.

e.g. $((x_1 + x_2)^{-1} + x_2)^{-1} - x_3$

(since $\langle X \rangle$ subfield, $S \subseteq \langle X \rangle$)

(need $X \neq \emptyset, \{0\}$)

Any subfield of $\mathbb{C}$ must contain $\mathbb{Q}$ (4.4).

Hence if $X \subseteq \mathbb{C}$, $\langle X \rangle \supseteq \mathbb{Q}$ (4.5).

If $K \subseteq L$, want fields containing K.

Def^n

Let $L:K$ be an extension and $Y \subseteq L$

Then the subfield of L generated by $K \cup Y$ is denoted $K(Y)$

$K(Y)$ is said to be obtained from K by adjoining Y.

Since every subfield of $\mathbb{C}$ contains $\mathbb{Q}$, we can write

$$\underset{\langle X \cup \mathbb{Q} \rangle}{\overset{\shortparallel}{\langle X \rangle}} = \mathbb{Q}(X)$$

If $Y = \{y\}$, write $K(y) = K(\{y\})$.

If $Y = \{y_1, \dots, y_n\}$, write $K(y_1, \dots, y_n) = K(\{y_1, \dots, y_n\})$.

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

– closed under inverses since $(a+b\sqrt{2})(a-b\sqrt{2}) = a^2-2b^2$

so $(a+b\sqrt{2})^{-1} = \underset{\overset{\cap}{\mathbb{Q}}}{\frac{a}{a^2-2b^2}} - \underset{\overset{\cap}{\mathbb{Q}}}{\frac{b}{a^2-2b^2}}\sqrt{2}$ $\quad (a^2-2b^2 \neq 0)$

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

In fact $K(\alpha) = \left\{\frac{f(\alpha)}{g(\alpha)} : f(t), g(t) \in K[t], g(\alpha) \neq 0\right\}$ $\forall \alpha$

Rational Functions $K(t)$

Intuitively $K(t)$ is the field of quotients of polynomials

eg $\frac{t^2+1}{t^3-1}$

If R is an integral domain, then we can construct a field Q called the field of fractions of R s.t.

1). $R \overset{\phi}{\hookrightarrow} Q$

2). every element of Q is of the form $\phi(r)^{-1}\phi(s)$, $r, s \in R$.

$\hookrightarrow$ = injective homomorphism
embedding

e.g. field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$

$(1,2) + (3,4) = (5,4)$ $\left[\text{i.e. } \frac{1}{2} + \frac{3}{4} = \frac{5}{4}\right]$

Let $S = R \times R - \{0\}$
$= \{(a,b) : a \in R, b \in R, b \neq 0\}$

X set

$\sim$ is an equivalence relation on R if

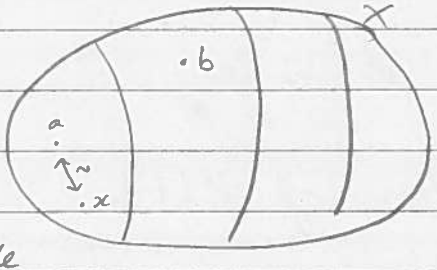
i). $a \sim a$ (reflexive)

ii). $a \sim b \Rightarrow b \sim a$ (symmetric)

iii). $a \sim b$ & $b \sim c \Rightarrow a \sim c$ (transitive)

06-10-17

An equivalence relation partitions X into equivalence classes.
Equivalence class of a: $[a] = \{x \in X : a \sim x\}$



Example

$\mathbb{Z}$ $a \sim b$ if $3 \mid b-a$

$[0] = \{\ldots, -3, 0, 3, \ldots\}^{=[3]}$, $[1] = \{\ldots, -2, 1, 4, \ldots\}$

$[2] = \{\ldots, -1, 2, 5, \ldots\}$

From above, $S = R \times R - \{0\} = \{(a,b) : a \in R, b \in R, b \neq 0\}$

Define an equivalence relation $\sim$ on S by
$(a,b) \sim (c,d)$ if $ad = bc$.

Let Q = set of equivalence classes
$[a,b]$ = equivalence class of (a,b)

Define
$$[a,b] \cdot [c,d] = [ac, bd]$$
$$[a,b] + [c,d] = [ad+bc, bd]$$
$$[0,1] = 0_Q$$
$$[1,1] = 1_Q$$

$\mathbb{Z}_3 = \{[0], [1], [2]\}$
$[a] + [b] = [a+b]$

Check well-defined and ring properties hold.
Also $[a,b]^{-1} = [b,a]$ if $a \neq 0$.
So Q is a field.
Define $\phi : R \mapsto Q$ by $\phi(r) = [r,1]$, then ϕ is an injective homomorphism.
If $x \in Q$, $x = [r,s] = [r,1][s,1]^{-1} = \phi(r)\phi(s)^{-1}$.

If we identify R and $\phi(R)$ then $R \leq Q$ and every element of Q is of the form rs^{-1} $(r, s \in R)$.

e.g. field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

$K(t)$ is the field of fractions of $K[t]$.

Formally, can define $K[t]$ as
$\{(a_0, a_1, a_2, \dots) : \exists N \text{ s.t. } \forall n \geq N, a_n = 0\}$

e.g. $2 + t^2 - t^3 \longleftrightarrow (2, 0, 1, -1, 0, 0, \dots)$.
in $\mathbb{Z}_2[t]$ then the functions t^2 and $t : \mathbb{Z}_2 \mapsto \mathbb{Z}_2$ are the same but polys are different.

Simple extensions

Def^n 4.10

An extension $L:K$ is called simple if $\exists \alpha \in L$ s.t. $L = K(\alpha)$.

e.g. $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ is simple by definition.
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ is in fact simple.
Take $\alpha = \sqrt{2} + \sqrt{3}$, then $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

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

$\alpha^2 = 5 + 2\sqrt{6} \in \mathbb{Q}(\alpha)$

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

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

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

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

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

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q} = \mathbb{Q}(\alpha) : \mathbb{Q}$ is simple.

$\mathbb{R} : \mathbb{Q}$ is <u>not</u> simple, $\mathbb{Q}(e, \pi) : \mathbb{Q}$ is <u>not</u> simple

MATH3202

09-10-17

$L:K$, K subfield of L

$L=K(\alpha)$ — simple field extension

Def 4.12

Two field extensions $i: K \mapsto \hat{K}$, $j: L \mapsto \hat{L}$ are isomorphic if there exist field isomorphisms $\mu: \hat{K} \mapsto \hat{L}$, $\lambda: K \mapsto L$ s.t. $j(\lambda(k)) = \mu(i(k))$ $\forall k \in K$.

i.e. the following diagram commutes

$$\begin{tikzcd}
i(k) & \hat{K} \arrow[r, "\mu", "\cong"'] & \hat{L} & \mu(i(k)) = j(\lambda(k)) \\
k & K \arrow[u, "i"] \arrow[r, "\cong", "\lambda"'] & L \arrow[u, "j"'] & \lambda(k)
\end{tikzcd}$$

Often we are interested in the situation where $K=L$ and $\lambda = id$; also where i and j are inclusions. Then the condition reduces to $\mu|_K = id$.

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

e.g. $\mu: \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$

$\mu(a+bi) \longrightarrow a-bi$

μ is a field isomorphism and $\mu|_{\mathbb{Q}} = id$

$$\begin{tikzcd}
\mathbb{Q}(i) \arrow[r, "\mu"] \arrow[d, dash] \arrow[dr, phantom, "\cong"] & \mathbb{Q}(i) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "id"'] & \mathbb{Q}
\end{tikzcd}$$

Chapter 5 - Simple Extensions

(Done slightly differently to the book)

Recall quotient rings.

If R is a ring and $I \trianglelefteq R$ (ie. I is an ideal of R) then the elements of the quotient ring R/I are the cosets $I+r = \{i+r : i \in I\}$ with operations defined by $(I+r)+(I+s) = I+(r+s)$

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

Need to check that these operations are well-defined, and that they make R/I into a ring with 1, $I+1$, and 0, $I+0$.

e.g. multiplication is well-defined.

$$I+r = I+r' \quad , \quad I+s = I+s'$$

$$\Rightarrow r'-r \in I \quad , \quad s'-s \in I$$

$$(r'-r)s' = r's' - rs' \in I \quad , \quad (s'-s)r = s'r - sr \in I$$

Adding: $r's' - rs' + s'r - sr \in I$

$$\Rightarrow r's' - rs \in I$$

i.e. $I + rs = I + r's'$.

[Roughly speaking $(I+r')(I+s') = (I+r)(I+s)$

$$I + r'I + Is' + r's' = I + rI + sI + rs$$

$$I + r's' = I + rs \,]$$

Often write $\bar{r} = I + r$.

eg. $R = \mathbb{Z}$, $I = 3\mathbb{Z}$, $3\mathbb{Z} \trianglelefteq \mathbb{Z}$

Elements of $\mathbb{Z}/3\mathbb{Z}$ are

$$3\mathbb{Z}+0 = 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}+3$$

$$3\mathbb{Z}+1 = \{\dots, -5, -2, 1, 4, 7, \dots\} = 3\mathbb{Z}+4$$

$$3\mathbb{Z}+2 = \{\dots, -4, -1, 2, 5, 8, \dots\} \qquad \text{etc}$$

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

09-10-17

$\bar{2} + \bar{2} = (3\mathbb{Z}+2) + (3\mathbb{Z}+2)$

$= 3\mathbb{Z}+4 = 3\mathbb{Z}+1 = \bar{1}$

There is a canonical surjective ring homomorphism
$\pi : R \mapsto R/I$, $\pi(r) = I + r = \bar{r}$

e.g. $\pi : \mathbb{Z} \mapsto \mathbb{Z}/3\mathbb{Z}$
sends each integer to itself (mod 3)
$\pi(2) = \bar{2}$, $\pi(5) = \bar{2}$

One way of thinking about R/I is that it is the ring obtained from R by making everything in I zero.
e.g. $\mathbb{Z}/3\mathbb{Z}$ is obtained by making 3 zero.

e.g. $\dfrac{\mathbb{R}[x]}{(x^2+1)}$ $\quad (x^2+1) = \{(x^2+1)f(x) : f(x) \in \mathbb{R}[x]\} \trianglelefteq \mathbb{R}[x]$

$$\frac{R[x]}{(x^2+1)} \cong \mathbb{C}$$

Cosets of (x^2+1) are $(x^2+1) + f(x)$
$f(x) = (x^2+1)q(x) + ax+b$
$(x^2+1) + f(x) = (x^2+1) + ax+b$
Distinct cosets are $(x^2+1) + ax+b = \overline{ax+b}$
$\overline{ax+b} + \overline{cx+d} = \overline{(a+c)x + (b+d)}$
$\overline{ax+b} \cdot \overline{cx+d} = \overline{acx^2 + (bc+ad)x + bd}$
$= \overline{ac(x^2+1)} + \overline{(bc+ad)x + bd - ac}$
$= bd - ac + (bc+ad)x$
$(ai+b)(ci+d) = (bd-ac) + (bc+ad)i$

MATH 3202

13-10-17

$I \trianglelefteq R \qquad R/_I = \{I + r\} = (\bar{r})$

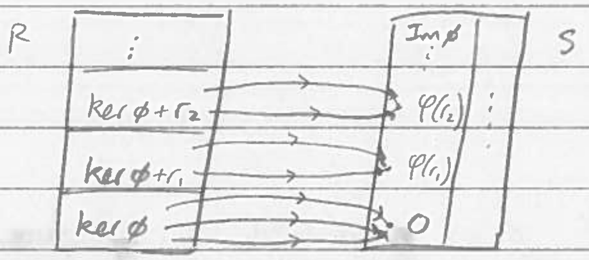
$\pi : R \mapsto R/_I$

$\pi(r) = \bar{r}$

1st Isomorphism Theorem

Let $\phi : R \mapsto S$ be a ring homomorphism.

Then $\dfrac{R}{\mathrm{Ker}\,\phi} \cong \mathrm{Im}\,\phi$



$\ker\phi = \{r \in R : \phi(r) = 0\} \trianglelefteq R$

$\mathrm{Im}\,\phi = \{\phi(r) : r \in R\}$ subring of S.

Proof

Define $\bar{\phi} : \dfrac{R}{\ker\phi} \mapsto S$ by $\bar{\phi}(\ker\phi + r) = \phi(r)$

$\bar{\phi}$ is well defined, since $\ker\phi + r = \ker\phi + r'$

$\Rightarrow r' - r \in \ker\phi \Rightarrow \phi(r' - r) = 0$

$\Rightarrow \phi(r') - \phi(r) = 0 \Rightarrow \phi(r') = \phi(r)$

$\bar{\phi}$ is a ring homomorphism

$\bar{\phi}$ is injective $(\bar{\phi}(\ker\phi + r) = 0 \Rightarrow \phi(r) = 0 \Rightarrow r \in \ker\phi$

$\Rightarrow \ker\phi + r = \ker\phi)$

If $\bar{\phi} : \dfrac{R}{\ker\phi} \mapsto \mathrm{Im}\,\phi$ then $\bar{\phi}$ is also surjective.

$\therefore$ $\bar{\phi}$ is an isomorphism. $\square$

e.g. $\phi : \mathbb{R}[t] \mapsto \mathbb{C}$ by $\phi(t) = i$, $\phi(a) = a \; \forall a \in \mathbb{R}$

$\ker\phi = \{f(t) \in \mathbb{R}[t] : f(i) = 0\}$

$f(t) = (t^2+1)g(t) + at + b$

$f(i) = ai + b$

So $f(i) = 0 \Rightarrow a = b = 0$

So $\ker\phi = \{(t^2+1)g(t) : g(t) \in \mathbb{R}[t]\} = (t^2+1)$

$\therefore \dfrac{\mathbb{R}[t]}{t^2+1} \cong \operatorname{Im}\phi = \mathbb{C}.$

If K is a field, $f(t) \in K[t]$ we can form $\dfrac{K[t]}{(f)}$.

Theorem 5.10

$K[t]/(f)$ is a field iff f is irreducible.

Proof

[$\Rightarrow$] If $f = gh \Rightarrow \bar{f} = \bar{g}\bar{h}$ in $K[t]/(f)$

$\Rightarrow \bar{0} = \bar{g}\bar{h} \Rightarrow \bar{g} = \bar{0}$ or $\bar{h} = \bar{0}$

$\Rightarrow g \in (f)$ or $h \in (f)$

$\Rightarrow g = fu$ or $h = fu$ $(u \in K^*)$

$\therefore$ f has no non trivial factorisations, so is irreducible.

[$\Leftarrow$]

Suppose f is irreducible and $\bar{0} \neq \bar{g} \in K[t]/(f)$.

$\Rightarrow g \notin (f)$ so $f \nmid g$

Since f irreducible, this means $hcf(f,g) = 1$.

By h,k-lemma, $\exists h,k \in K[t]$ st. $fh + gk = 1$

In $K[t]/(f)$ $\bar{f}\bar{h} + \bar{g}\bar{k} = 1 \Rightarrow \bar{g}\bar{k} = 1$

i.e. $\bar{k} = \bar{g}^{-1}$. Thus $K[t]/(f)$ is a field. □

Example

$\mathbb{R}[t]/(t^2+1)$, $t+1$

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

13-10-17

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

$\Rightarrow \; 1 = (t^2+1)\cdot\frac{1}{2} + (t+1)\frac{1}{2}(1-t)$

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

$\Rightarrow \; \overline{t+1}^{\,-1} = \overline{\tfrac{1}{2}(1-t)}$

so $(i+1)^{-1} = \frac{1}{2}(1-i)$

∂ = degree

Elements of $K[t]/(f)$ can be written uniquely as $g(t)$ where $\partial g < \partial f$.
This is because any $h(t) \in K[t]$ can be written uniquely as $h(t) = f(t)q(t) + g(t)$ where $\partial g < \partial f$.
i.e. if $\partial f = n$, $\dfrac{K[t]}{(f)} = \{a_0 + a_1\bar{t} + \dots + a_{n-1}\bar{t}^{\,n-1} : a_i \in K\}$

e.g. $\dfrac{\mathbb{R}[t]}{(t^2+1)} = \{a + b\bar{t} : a, b \in \mathbb{R}\}$.

Def 5.1
Let $K \leq \mathbb{C}$ subfield, $\alpha \in \mathbb{C}$.
Then α is <u>algebraic over K</u> if there exists a non-zero polynomial $f(t) \in K[t]$ s.t. $f(\alpha) = 0$.
Otherwise α is <u>transcendental over K</u>
[Abbreviate algebraic over $\mathbb{Q}$ to algebraic.]

<u>Examples</u>

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

π is transcendental over $\mathbb{Q}$ (analytic proof).

$\sum_{i=1}^{\infty} 10^{-i!} = 1.\underset{1}{1}\underset{2}{1}000\underset{6}{1}0\ldots0\underset{24}{1}$ etc. is transcendental over $\mathbb{Q}$.

$\sqrt{\pi}$ is also transcendental over $\mathbb{Q}$, but $\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$, take $f(t) = t^2 - \pi \in \mathbb{Q}(\pi)[t]$.

If α is transcendental over K, then $K(\alpha) \cong K(t)$, rational function field, by an isomorphism ϕ s.t. $\phi(\alpha) = t$, $\phi(k) = k \ \forall k \in K$ (Thm 5.3)

Let α be algebraic over K. Then there is a unique monic polynomial $m(t) \in K[t]$ of least degree s.t. $m(\alpha) = 0$. We call m the minimal polynomial of α over K. If $f(\alpha) = 0$ then $m \mid f$. m is irreducible.

Example

Minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $m(t) = t^3 - 2$. [$m(\sqrt[3]{2}) = 0$ and m is irreducible so it is minimal poly.]

What is the minimal polynomial of $\omega = e^{2\pi i/7}$?

$f(t) = t^7 - 1$, $f(\omega) = 0$ not minimal poly. since reducible.

$f(t) = (t-1)(t^6 + t^5 + t^4 + t^3 + t^2 + t + 1) = (t-1)m(t)$

$\omega - 1 \neq 0 \ \therefore m(\omega) = 0$

m is irreducible: let $t = s+1$ and use Eisenstein with $p = 7$.

Exercise

Find minimal poly of $\alpha = \sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

$$(\alpha^2 - 5)^2 - 24 = ((5 + 2\sqrt{6}) - 5)^2 - 24$$
$$= (2\sqrt{6})^2 - 24 = 0$$

$= \alpha^4 - 10\alpha^2 + 25 - 24 = \alpha^4 - 10\alpha^2 + 1$, $f(t) = t^4 - 10t^2 + 1$

Now to prove $f(t)$ is irreducible. Can work over $\mathbb{Z}$ by Gauss.

No roots since, $f(\pm 1) \neq 0$.

Suppose $f(t) = (t^2 + at + b)(t^2 + ct + d) = t^4 - 10t^2 + 1$

$bd = 1$, $\underline{b = d = 1}$, or $b = d = -1$

$t^4 - 10t^2 + 1 = (t^2 + at + 1)(t^2 + ct + 1)$

coeff of t^3: $a + c = 0$

$\Rightarrow t^4 - 10t^2 + 1 = (t^2 + at + 1)(t^2 - at + 1)$

13-10-17

coeff of t^2 : $-10 = 1 - a^2 + 1 \Rightarrow a^2 = 12$ not possible.

$b = d = -1$ similarly not possible

$\therefore f(t)$ irreducible

$\therefore$ min poly of α is $f(t)$.

Classifying simple extensions

Thm 5.12

Let $K(\alpha) : K$ be a simple extension with α algebraic over K and m min. poly. of α over K.

Then $\exists$ an isomorphism

$\phi : K[t]/(m) \mapsto K(\alpha)$ s.t.

$\phi(\bar{t}) = \alpha$ and $\phi|_K = id$, i.e. there is an isomorphism of extensions $K[t]/(m) : K \cong K(\alpha) : K$

$$\begin{tikzcd} K[t]/(m) \arrow[r, mapsto, "\phi"] & K(\alpha) \\ \bar{t} \arrow[r, mapsto] & \alpha \\ K \arrow[uu, dash, "i"] \arrow[r, mapsto, "id"'] & K \arrow[uu, dash] \end{tikzcd}$$

$i(k) = \bar{k}$

Proof

Define $\psi : K[t] \mapsto K(\alpha)$ defined by $\psi(f(t)) = f(\alpha)$

ψ is clearly a ring homomorphism.

By 1st Isomorphism Thm, there is an isomorphism

$\phi : \dfrac{K[t]}{\ker \psi} \mapsto \operatorname{Im} \psi$.

$\ker \psi = \{ f(t) : f(\alpha) = 0 \} = (m)$

$\therefore \phi : \dfrac{K[t]}{(m)} \overset{\cong}{\mapsto} \operatorname{Im} \psi \leq K(\alpha)$

$\operatorname{Im} \psi \cong \dfrac{K[t]}{(m)}$ which is a field. $\operatorname{Im} \psi$ is a subfield of $K(\alpha)$

$\operatorname{Im} \psi$ contains $\alpha = \psi(t)$ and $K = \psi(K)$. By def^n $\operatorname{Im} \psi = K(\alpha)$.

$\therefore \phi : \dfrac{K[t]}{(m)} \overset{\cong}{\mapsto} K(\alpha)$. check $\phi|_K = id$. □

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

Corollary 5.13

Suppose $K(\alpha):K$ and $K(\beta):K$ are simple algebraic extensions ~~and~~ s.t. α and β have the same minimal polynomial m over K.
Then the extensions $K(\alpha):K$ and $K(\beta):K$ are isomorphic by an isomorphism $\phi : K(\alpha) \longmapsto K(\beta)$ s.t. $\phi(\alpha) = \beta$ and $\phi|_K = id$.

Proof

$$\begin{tikzcd}
K(\beta) & K[t]/(m) \arrow[l, "\phi_2"] \arrow[l, "\beta \leftarrow \bar{t}"'] \arrow[r, "\phi_1"] \arrow[r, "\bar{t} \mapsto \alpha"'] & K(\alpha) \\
K \arrow[u, dash] & K \arrow[u, dash] \arrow[l, "id"'] \arrow[r, "id"'] & K \arrow[u, dash]
\end{tikzcd}$$

$\phi = \phi_2 \, \phi_1^{-1} : K(\alpha) \longmapsto K(\beta)$
is the required isomorphism. □

This means that algebraically, all the roots of an irreducible polynomial are irreducible.
e.g. $t^3 - 2 = 0$ has roots $\sqrt[3]{2}$, $\sqrt[3]{2}\,\omega$, $\sqrt[3]{2}\,\omega^2$
$(\omega = e^{2\pi i/3})$

$\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q} \cong \mathbb{Q}(\sqrt[3]{2}\,\omega) : \mathbb{Q}$

"all we know" about $\sqrt[3]{2}$ and $\sqrt[3]{2}\,\omega$ is that they cube to 2.

MATH3202

13-10-17

Thm 5.14

If α is algebraic over K with minimum polynomial m of degree n, then

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

so as a vector space over K, $K(\alpha)$ has a basis $\{1, \alpha, \dots, \alpha^{n-1}\}$ and $\dim_K(K(\alpha)) = n$.

Proof

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

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

If $i : K \mapsto L$ is a field monomorphism
then $\hat{i} : K[t] \mapsto L[t]$ by $\hat{i}(a_0 + a_1 t + \dots + a_n t^n) = i(a_0) + i(a_1)t + \dots + i(a_n)t^n$
is a ring monomorphism.

eg. $i : \mathbb{C} \mapsto \mathbb{C}$ by $i(a+ib) = a - ib$
Then $\hat{i}(1 + it + (1-i)t^2) = 1 - it + (1+i)t^2$
If i is an isomorphism, so is $\hat{i}$. Write i instead of $\hat{i}$.

Thm 5.16

Let $K, L \leq \mathbb{C}$, $\alpha, \beta \in \mathbb{C}$, $i : K \mapsto L$ field isomorphism.
Suppose $m_\beta = i(m_\alpha)$. Then $\exists$ a field isomorphism
$j : K(\alpha) \mapsto L(\beta)$ s.t. $j(\alpha) = \beta$ and $j|_K = i$

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

Proof

$$\begin{tikzcd}
K(\alpha) \arrow[dd, dash] & K[t]/(m_\alpha) \arrow[l, "\phi_1"'] \arrow[r, "\phi"] \arrow[dd, dash] & L[t]/(m_\beta) \arrow[r, "\phi_2"'] \arrow[dd, dash] & L(\beta) \arrow[dd, dash] \\
\alpha & \bar{t} \arrow[l, mapsto] & \bar{t} \arrow[r, mapsto] & \beta \\
K & K \arrow[l, "id"'] \arrow[r, "i"'] & L \arrow[r, "id"'] & L
\end{tikzcd}$$

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

ϕ is surjective

$\ker\phi = \{f(t) \in K[t] : i(f) \in (m_\beta)\} = (m_\alpha)$

$\therefore \dfrac{K[t]}{\ker\phi} \cong \operatorname{Im}\phi \qquad \dfrac{K[t]}{(m_\alpha)} \cong \dfrac{L[t]}{(m_\beta)}$

$j = \phi_2\phi\phi_1^{-1}$ is the required isomorphism.

$\square$

MATH 3202

13-10-17

α, β same minimal poly $\Rightarrow K(\alpha):K \cong K(\beta):K$
Converse is not true.

Chapter 6 - Degree of an extension

If $L:K$ is a field extension, L forms a vector space over K.

Def 6.2
The degree of an extension $L:K$ is the dimension of L as a vector space over K.
Write $[L:K]$ for degree.

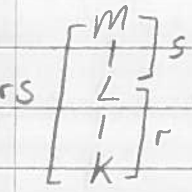
eg. $[\mathbb{C}:\mathbb{R}] = 2$, since $\mathbb{C}$ has $\mathbb{R}$-basis $\{1, i\}$

In fact we have already seen that $[K(\alpha):K] = \partial m$ if α is algebraic over K with minimum polynomial $m(t) \in K[t]$.

If $\partial m = n$ then $K(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}\}$ with basis $\{1, \alpha, \dots, \alpha^{n-1}\}$.

If α is transcendental over K, $[K(\alpha):K] = \infty$, since $1, \alpha, \alpha^2, \dots$ are independent (6.7).

The Tower Law
Thm 6.4 (Short Tower Law)
Suppose $K \leq L \leq M \leq \mathbb{C}$. Then $[M:K] = [M:L][L:K]$.



Proof

Suppose $[L:K]$ and $[M:L]$ are finite, say $[L:K] = r$, $[M,L] = s$.

Let $\{x_1, \dots, x_r\}$ be a K-basis for L.

Let $\{y_1, \dots, y_s\}$ be an L-basis for M.

Claim: $\{x_i y_j : 1 \le i \le r,\ 1 \le j \le s\}$ is a K-basis for M.

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

$$\text{So } \sum_{j=1}^{s} \underbrace{\left(\sum_{i=1}^{r} \alpha_{ij} x_i \right)}_{\in L} y_j = 0$$

Since $\{y_1, \dots, y_s\}$ is LI over L, all $\sum_{i=1}^{r} \alpha_{ij} x_i = 0$.

Since $\{x_1, \dots, x_r\}$ is LI over K, all $\alpha_{ij} = 0$.

Spanning: Let $m \in M$. $\{y_1, \dots, y_s\}$ spans M over L

so $\exists\ \beta_j \in L$ st. $m = \sum_{j=1}^{s} \beta_j y_j$

Since $\{x_1, \dots, x_r\}$ spans L over K,

$\exists\ \alpha_{ij} \in K$ st. $\beta_j = \sum_{i=1}^{r} \alpha_{ij} x_i$

$$\text{Then } m = \sum_{j=1}^{s} \beta_j y_j = \sum_{j=1}^{s} \left(\sum_{i=1}^{r} \alpha_{ij} x_i \right) y_j = \sum_{i,j} \alpha_{ij} x_i y_j$$

$\therefore$ Claim is true.

? Hence $[M:K] = |\{x_i y_j : 1 \le i \le r,\ 1 \le j \le s\}|$ modulus?

$= rs = [L:K][M:L]$ □

Example

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

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash, "?\ 2 \text{ since min poly is } t^2-3 \text{ over } \mathbb{Q}(\sqrt{2})"] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2 \text{ since min poly is } t^2-2"] \\
\mathbb{Q}
\end{tikzcd}$$

Looks like $[\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ since $\sqrt{3}$ satisfies $t^2 - 3 \in \mathbb{Q}(\sqrt{2})[t]$. Need to check t^2-3 is irreducible over $\mathbb{Q}(\sqrt{2})$. If not, $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ which is impossible. $\therefore$ true

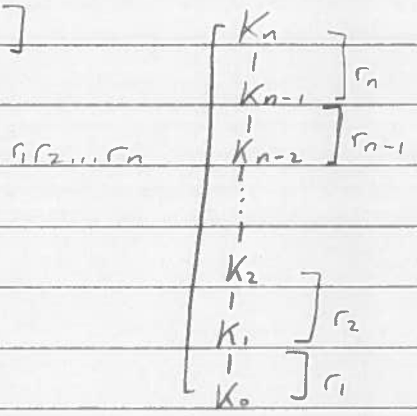
By Tower Law $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4$.

13-10-17

We already knew this since
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$
and $\sqrt{2}+\sqrt{3}$ has min poly t^4-10t^2+1.
so $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$.

Corollary 6.6

Let $K_0 \leq K_1 \leq \dots \leq K_n \leq \mathbb{C}$.
Then $[K_n:K_0]=[K_1:K_0][K_2:K_1]\dots[K_n:K_{n-1}]$



Proof
Induction using 6.5. □

MATH 3202

16-10-17

Defs

- An extension $L:K$ is simple if $\exists \alpha \in L$ s.t. $L = K(\alpha)$.
- α is algebraic over K if there exists a non-zero polynomial $f(t) \in K[t]$ s.t. $f(\alpha) = 0$
- $K(\alpha):K$ is a simple algebraic extension if α is algebraic over K

Def 6.9

$L:K$ is finite if $[L:K]$ is finite.

Def 6.10

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

Def

$L:K$ is finitely generated if $\exists \alpha_1, \dots, \alpha_n \in L$ s.t. $L = K(\alpha_1, \dots, \alpha_n)$.

Lemma 6.11

Let $L:K$ be an extension, then the following are equivalent:

i). $L:K$ is finite

ii). $L:K$ is finitely generated and algebraic

iii). $\exists \alpha_1, \dots, \alpha_n \in L$ algebraic over K s.t. $L = K(\alpha_1, \dots, \alpha_n)$.

Proof

(i)$\Rightarrow$(ii)

Let $x_1, \dots, x_n$ be a K-basis for L. Then $L = K(x_1, \dots, x_n)$, so L is finitely generated. $\to$ $([L:K] = n)$

Let $x \in L$. Consider $1, x, \dots, x^n$. These must be linearly dependent over K ($n+1$ elements in a vector space of dimension n)

$\therefore$ $\exists \alpha_i \in K$, not all zero s.t.

$$\alpha_0 + \alpha_1 x + \dots + \alpha_n x^n = 0$$

Let $f(t) = \alpha_0 + \alpha_1 t + \dots + \alpha_n t^n \in K[t]$

$f \neq 0$ and $f(x) = 0$, so x is algebraic over K.

(ii) $\Rightarrow$ (iii)

Automatic

(iii) $\Rightarrow$ (i).

Consider the tower of fields:

$$\begin{tikzcd}
K(\alpha_1, \dots, \alpha_n) = L \arrow[d, dotted, dash, "< \infty"] \\
K(\alpha_1, \alpha_2) \arrow[d, dash, "< \infty"] \\
K(\alpha_1) \arrow[d, dash, "< \infty"] \\
K
\end{tikzcd}$$

α_1 is algebraic over K $\Rightarrow [K(\alpha_1) : K] = \partial m_{\alpha_1} < \infty$.

α_2 is algebraic over K so α_2 is alg $/ K(\alpha_1)$

so $\left[\underset{\overset{\shortparallel}{K(\alpha_1, \alpha_2)}}{K(\alpha_1)(\alpha_2)} : K(\alpha_1)\right] < \infty$

etc.

$\therefore$ by the Tower Law $[L, K] = [K(\alpha_1) : K][K(\alpha_1, \alpha_2) : K(\alpha_1)] \dots [L : K(\alpha_1, \dots, \alpha_n)]$
$< \infty$.

□

e.g. $\mathbb{Q}(\sqrt[5]{5}, \sqrt[7]{7})$ is algebraic and finitely generated

$\therefore [\mathbb{Q}(\sqrt[5]{5}, \sqrt[7]{7}) : \mathbb{Q}] < \infty$

and $\sqrt[5]{5} + \sqrt[7]{7}$ is algebraic over $\mathbb{Q}$.

MATH 3202

20-10-17

Def 8.1

Let $L:K$ be a field extension ($\subseteq \mathbb{C}$).

A k-automorphism of L is a field automorphism $\alpha: L \to L$ s.t. $\alpha|_K = id$, ie $\alpha(k)=k \ \forall k \in K$.

[field automorphism = bijective field homomorphism $L \to L$]

Thus a K-aut of L is an automorphism of the extension $L:K$,

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

Theorem 8.2

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

Proof

Let α, β be K-auts of L.

So α, β are field homs $\Rightarrow$ $\alpha \circ \beta$ is a field hom.

α, β bijective $\Rightarrow$ $\alpha \circ \beta$ bijective

$(\alpha \circ \beta)(k) = \alpha(\beta(k)) = \alpha(k) = k \quad \forall k \in K.$

$\therefore$ $\alpha \circ \beta$ is a K-aut of L.

α^{-1} is defined, since α bijective, and is bijective

$\alpha(\alpha^{-1}(l+m)) = l+m = \alpha(\alpha^{-1}(l)) + \alpha(\alpha^{-1}(m)) = \alpha(\alpha^{-1}(m) + \alpha^{-1}(l))$

$\Rightarrow \alpha^{-1}(l+m) = \alpha^{-1}(l) + \alpha^{-1}(m).$

Similarly $\alpha^{-1}(lm) = \alpha^{-1}(l)\alpha^{-1}(m).$

$k = \alpha^{-1}(\alpha(k)) = \alpha^{-1}(k)$

$\therefore$ α^{-1} is a K-aut of L.

id is a K-aut of L.

Composition of maps is associative

$\therefore$ it is a group. □

Def 8.3 The Galois Group

The Galois Group of $L:K$, deoted $\Gamma(L:K)$ or $Gal(L:K)$, is the group of K-auts of L under composition.

Examples

1). $\mathbb{C}:\mathbb{R}$

Let $\phi \in Gal(\mathbb{C}:\mathbb{R})$

$\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$

$\phi(i) = \pm i$

$\phi(i)$ determines ϕ, since $\phi(a+bi) = \phi(a) + \phi(b)\phi(i)$

$= a + b\phi(i)$

This gives 2 potential elements of $\Gamma(\mathbb{C}:\mathbb{R})$:

$\alpha_1 : a+bi \longmapsto a+bi$

$\alpha_2 : a+bi \longmapsto a-bi$

$\alpha_1 = id \in \Gamma$

$\alpha_2 =$ complex conjugation , $\alpha_2(c) = \bar{c}$, $\overline{cd} = \bar{c}\bar{d}$, $\overline{c+d} = \bar{c} + \bar{d}$

$\Rightarrow \alpha_2$ is a field hom.

$\Rightarrow \Gamma = \{id, \alpha_2\} \cong C_2 \qquad [\alpha_2^2 = id]$

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

Any $\phi \in \Gamma$ is determined by $\phi(\sqrt{2})$ and $\phi(\sqrt{3})$.

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

Similarly $\phi(\sqrt{2}) = \pm\sqrt{2}$.

The only possible elements of Γ are

$\alpha_1 : \sqrt{2} \longmapsto \sqrt{2}, \sqrt{3} \longmapsto \sqrt{3}$

$\alpha_2 : \sqrt{2} \longmapsto -\sqrt{2}, \sqrt{3} \longmapsto \sqrt{3}$

$\alpha_3 : \sqrt{2} \longmapsto \sqrt{2}, \sqrt{3} \longmapsto -\sqrt{3}$

$\alpha_4 : \sqrt{2} \longmapsto -\sqrt{2}, \sqrt{3} \longmapsto -\sqrt{3}$.

$\alpha_1 = id \in \Gamma$

α_2 :

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[r, phantom, "="] & \mathbb{Q}(\sqrt{3})(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3})(-\sqrt{2}) \arrow[d, dash] \arrow[r, phantom, "="] & \mathbb{Q}(\sqrt{2},\sqrt{3}) \\
& \mathbb{Q}(\sqrt{3}) \arrow[r, "id"] & \mathbb{Q}(\sqrt{3}) &
\end{tikzcd}$$

MATH 3203

20-10-17

Corollary 5.13

α and β have same min poly over $\mathbb{K}$

Then $\exists$ field isomorphism $\phi : K(\alpha) \longrightarrow K(\beta)$

s.t. $\phi(\alpha) = \beta$, $\phi|_K = id$

$$\begin{tikzcd}
K(\alpha) \arrow[rr, "\cong", "\phi"'] \arrow[dd, dash] & & K(\beta) \arrow[dd, dash] \\
& \alpha \mapsto \beta & \\
K \arrow[rr, "id"'] & & K
\end{tikzcd}$$

$\sqrt{2}$ and $-\sqrt{2}$ both have min poly $t^2 - 2$ over $\mathbb{Q}\sqrt{3}$

By 5.13 $\exists\, \phi : \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3})$ s.t. $\phi(\sqrt{2}) = -\sqrt{2}$

and $\phi|_{\mathbb{Q}(\sqrt{3})} = id$, so $\phi(\sqrt{3}) = \sqrt{3}$.

$\therefore\ \alpha_2 = \phi \in \Gamma$.

$\alpha_3 \in \Gamma$ similarly.

$\alpha_4 = \alpha_2 \alpha_3 \in \Gamma$

$\therefore\ \Gamma = \{id, \alpha_2, \alpha_3, \alpha_2\alpha_3\} = \langle \alpha_2, \alpha_3 \mid \alpha_2^2 = \alpha_3^2 = id, \alpha_2\alpha_3 = \alpha_3\alpha_2 \rangle$

$\cong C_2 \times C_2$

3). $\Gamma(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{id\}$

Let $\phi \in \Gamma$, then $\phi(\sqrt[3]{2})^3 = \phi(2) = 2$

$\Rightarrow \phi(\sqrt[3]{2}) = \sqrt[3]{2}$ since the other two roots of $t^3 - 2$ are complex and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

$\therefore\ \phi = id$.

The Galois Correspondence

Let $L : K$ be a field extension, $\Gamma = \Gamma(L : K)$

Let F be the set of intermediate fields $= \{M : K \overbrace{\le M \le}^{\text{subfield}} L\}$

Let $\mathcal{G}$ be the set of subgroups of $\Gamma = \{H : H \underbrace{\le}_{\text{subgroup}} \Gamma\}$

We set up maps $\dagger : \mathcal{G} \to F$, $* : F \to \mathcal{G}$

which, under certain circumstances are mutual inverses.

This is called the Galois correspondence.

i). If $M \in \mathcal{F}$, $M^* = \{g \in \Gamma : g(m) = m \ \forall m \in M\}$

i.e. M^* is the set of elements of Γ which fix each element of M.

$M^* \subseteq \Gamma$: in fact $M^* \leq \Gamma$ (subgroup)

⌈ $g, h \in M^*$, then $\forall m \in M$, $(gh)(m) = g(h(m)) = g(m) = m$ ⌉

$\therefore gh \in M^*$

$\forall m \in M$, $g(m) = m$ so $g^{-1}(m) = m$ i.e. $g^{-1} \in M^*$

⌊ $id \in M^*$ ⌋

$\therefore M^* \in \mathcal{G}$

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

i.e. H^+ is the set of elements of L fixed by everything in H.

Since K is fixed by Γ, $K \subseteq H^+$ and by definition $H^+ \subseteq L$.

In fact $H^+ \leq L$.

⌈ $x, y \in H^+$. Then $\forall h \in H$, ⌉

$h(x+y) = h(x) + h(y) = x + y$, so $x+y \in H^+$

⌊ Similarly $xy \in H^+$ ⌋

H^+ is called the fixed field of H

$H \in \mathcal{G}$, $H^+ = \{x \in L : h(x) = x \ \forall h \in H\}$

= elements of L fixed by H

$M \subseteq \mathcal{F}$, $M^* = \{g \in \Gamma : g(m) = m \ \forall m \in M\}$

= elements of Γ fixing all of M

$M \subseteq M^{*+} \leftarrow$ "M is fixed by everything that fixes M."

⌈ $m \in M$ and $g \in M^*$, then $g(m) = m$ by defn of M^* ⌉

⌊ $\therefore g(m) = m \ \forall g \in M^*$ $\therefore m \in (M^*)^+ = M^{*+}$ ⌋

$H \subseteq H^{+*} \leftarrow$ "H fixes everything that is fixed by H."

⌈ $h \in H$, then $\forall x \in H^+$, $h(x) = x$ by defn of H^+ ⌉

⌊ $\therefore h \in (H^+)^* = H^{+*}$ ⌋

20-10-17

Under some circumstances, in fact $M = M^{*+}$, $H = H^{+*}$.
In this case $*+ = id$, $+* = id$, i.e. $*$, $+$ are mutually inverse maps.
i.e. they establish a 1-1 correspondence between $\mathcal{F}$ and $\mathcal{G}$.
In fact, this is an order-reversing (in terms of inclusion) correspondence: $H_1 \subseteq H_2 \in \mathcal{G} \Rightarrow H_1^+ \supseteq H_2^+$

$$M_1 \subseteq M_2 \in \mathcal{F} \Rightarrow M_1^* \supseteq M_2^*$$

$H_1 \subseteq H_2$. Let $x \in H_2^+$.
Then $g(x) = x \ \forall g \in H_2$, but $H_1 \subseteq H_2$, so $g(x) = x \ \forall g \in H_1$, $x \in H_1^+$

Example
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$
$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$
$\mathbb{Q}(\sqrt{2}\ \sqrt{3})$ has $\mathbb{Q}$-basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$
$\Gamma = \Gamma(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \alpha, \beta, \alpha\beta\}$
$= \langle \alpha, \beta ; \alpha^2 = \beta^2 = id,\ \alpha\beta = \beta\alpha \rangle$

$\alpha(\sqrt{2}) = -\sqrt{2}$, $\beta(\sqrt{3}) = \sqrt{3}$
$\beta(\sqrt{2}) = \sqrt{2}$, $\alpha(\sqrt{3}) = -\sqrt{3}$.
$|\Gamma| = 4$. By Lagrange's Thm, if $H \leq \Gamma$, $|H| = 1, 2$ or 4.
If $|H| = 2$, $H = \langle g \rangle$, $o(g) = 2$.
This gives 3 subgroups
$\langle \alpha \rangle = \{id, \alpha\}$, $\langle \beta \rangle = \{id, \beta\}$, $\langle \alpha\beta \rangle = \{id, \alpha\beta\}$.

$$\mathcal{G} = \begin{tikzcd} & \Gamma \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle\alpha\rangle \arrow[dr, dash] & \langle\beta\rangle \arrow[d, dash] & \langle\alpha\beta\rangle \arrow[dl, dash] \\ & \{e\} & \end{tikzcd}$$

Let $M \in \mathcal{F}$ i.e. $\mathbb{Q} \leq M \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
By Tower Law $[M : \mathbb{Q}] \mid 4$.
$[M : \mathbb{Q}] = 1 \Rightarrow M = \mathbb{Q}$
$[M : \mathbb{Q}] = 4 \Rightarrow M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$\begin{tikzcd} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[d, dash] \arrow[dd, phantom, bend left=60, "4"] \\ M \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$

Suppose $[M : \mathbb{Q}] = 2$. Let $x \in M \setminus \mathbb{Q}$, then $\overbrace{\mathbb{Q} \underset{\substack{\neq \\ \deg > 1}}{<} \mathbb{Q}(x)}^{\text{degree 2}} \leq M$. $\therefore M = \mathbb{Q}(x)$.

Since $[\mathbb{Q}(x):\mathbb{Q}]=2$, min poly of x over $\mathbb{Q}$ is a quadratic.

w.l.o.g $x^2 \in \mathbb{Q}$.

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

$$x^2 = a^2 + 2b^2 + 3c^2 + 6d^2 + \sqrt{2}(2ab + 6cd) + \sqrt{3}(2ac + 4bd) + \sqrt{6}(2ad + 2bc)$$

$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ LI over $\mathbb{Q}$

$x^2 \in \mathbb{Q}$

$\Rightarrow 2ab + 6cd = 0, \quad 2ac + 4bd = 0, \quad 2ad + 2bc = 0$

$$\Rightarrow \begin{cases} ab = -3cd \\ ac = -2bd \\ ad = -bc \end{cases}$$

$$\Rightarrow \left.\begin{cases} abc = -3c^2d \\ abc = -2b^2d \end{cases}\right\} \Rightarrow 3c^2d = 2b^2d \quad \text{so } d(3c^2 - 2b^2) = 0$$
$$\quad ad = -bc$$

$\Rightarrow \quad d = 0 \quad$ or $\quad 3c^2 - 2b^2 = 0$

$\qquad\qquad\qquad\qquad\qquad \Rightarrow b = c = 0 \Rightarrow M = \mathbb{Q}(\sqrt{6})$

$\Downarrow$

$bc = 0 \Rightarrow b = 0$ or $c = 0 \Rightarrow M = \mathbb{Q}(\sqrt{3})$ or $M = \mathbb{Q}(\sqrt{2})$.

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

$$\begin{tikzcd} & \{e\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[rrr, bend left, "+"] & & & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[lll, bend left, "*"] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle\alpha\rangle \arrow[dr, dash] \arrow[rrr, bend left, "+"] & \langle\beta\rangle \arrow[d, dash] & \langle\alpha\beta\rangle \arrow[dl, dash] & \mathbb{Q}(\sqrt{3}) \arrow[lll, bend left, "*"] \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\ & \Gamma \arrow[rrr, bend left, "+"] & & & \mathbb{Q} \arrow[lll, bend left, "*"] & \end{tikzcd}$$

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

$x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$

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

MATH 3202

20-10-17

$$\begin{aligned} x = \alpha(x) &\iff b = 0 \text{ and } d = 0 \\ &\iff x = a + c\sqrt{3} \\ &\iff x \in \mathbb{Q}(\sqrt{3}) \end{aligned}$$

$\Rightarrow \alpha^{+} = \mathbb{Q}(\sqrt{3})$

$$\begin{aligned} \mathbb{Q}(\sqrt{3})^{*} &= \{g \in \Gamma : g(x) = x \ \forall x \in \mathbb{Q}(\sqrt{3})\} \\ &= \{g \in \Gamma : g(\sqrt{3}) = \sqrt{3}\} \\ &= \{id, \alpha\} = \langle \alpha \rangle \end{aligned}$$

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

$\mathbb{Q}(\sqrt{2}, \sqrt{3})^{*} = \{g \in \Gamma : g(x) = x \ \forall x \in \mathbb{Q}(\sqrt{2}, \sqrt{3})\} = \{e\}$

Example where Galois correspondence fails

$\Gamma(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{id\}$

$$\begin{tikzcd}
 & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, shift left, "*"] \arrow[dd, dash] & \\
\mathcal{G} & \{id\} \arrow[ur, shift left, "+"] & & \mathcal{F} \\
 & & \mathbb{Q} \arrow[ul, "*"] &
\end{tikzcd}$$

$\mathbb{Q}^{*+} = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q} \qquad *+ \neq id.$

Chapter 9 - Normality and Seperability

Def 9.1

A polynomial $f(t) \in K[t]$ splits if it factorises into linear factors

$f(t) = k(t - \alpha_1) \dots (t - \alpha_n) \quad \alpha_i \in K, \ k \in K.$

Roots of f are then $\alpha_1, \dots, \alpha_n$.

If $K \leq L$ then it makes sense to regard f as a polynomial in $L[t]$, so we can say a polynomial $f \in K[t]$ splits over L if it splits when regarded as a polynomial in $L[t]$.

e.g. if $K \leq \mathbb{C}$, every polynomial in $K[t]$ splits over $\mathbb{C}$ (Fundamental Thm of Algebra : proved in MATH 2101).

Example

$(t^2-2)(t^2-3) \in \mathbb{Q}[t]$

splits over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Def

A subfield Σ of $\mathbb{C}$ is a splitting field for $f(t) \in K[t]$ if $K \leq \Sigma$ and

i). f splits over Σ

ii). if $K \leq \Sigma' \leq \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

(If f has roots $\sigma_1, \dots, \sigma_n \in \mathbb{C}$ then $\Sigma = K(\sigma_1, \dots, \sigma_n)$.)

Theorem 9.4

Let $K \leq \mathbb{C}$, $f(t) \in K[t]$. Then $\exists!$ splitting field Σ for f over K and $[\Sigma : K] < \infty$.

Proof

$\Sigma = K(\sigma_1, \dots, \sigma_n)$

Each σ_i is algebraic over K (since they are roots of f), so by 6.11, $[K(\sigma_1, \dots, \sigma_n) : K] < \infty$.

$$\begin{tikzcd}
K(\sigma_1, \dots, \sigma_n) = \Sigma \arrow[d, dash, dashed] \\
K(\sigma_1, \sigma_2) \arrow[d, dash] \\
K(\sigma_1) \arrow[d, dash] \\
K
\end{tikzcd}$$

□

Lemma 9.5

Suppose $i : K \to K'$ is an isomorphism of fields

Let $f \in K[t]$ with splitting field Σ.

Let $L \geq K'$ s.t. $i(f) \in K[t]$ splits in L.

Then $\exists$ a field monomorphism $j : \Sigma \to L$ s.t. $j|_K = i$.

$$\begin{tikzcd}
 & & L \arrow[d, dash] & i(f) \text{ splits in } L \arrow[l] \\
\text{splitting field of } f \arrow[r, dash] & \Sigma \arrow[r, "j"] \arrow[dd, dash] & j(\Sigma) \arrow[dd, dash] & \\
 & & & \\
 & K \arrow[r, "i", "\cong"'] & K' & \\
 & f \arrow[r, mapsto] & i(f) &
\end{tikzcd}$$

MATH 3202

20-10-17

Proof

Induction on ∂f.

Over Σ

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

Let m = min poly of σ_1 over K

m divides f

$i(m)$ divides $i(f)$

$i(f)$ splits over L, so $i(m)$ splits over L.

$i(m) = (t-\alpha_1)\dots(t-\alpha_r)$

Since $i(m)$ irreducible, $i(m)$ is the min poly of α_1

Apply 5.16:

$$\begin{tikzcd}
\Sigma \arrow[r, "j"'] & L \\
K(\sigma_1) \arrow[u, dash] \arrow[r, "\overset{j_1}{\cong}", "\sigma_1 \mapsto \alpha_1"'] & K'(\alpha_1) \arrow[u, dash] \\
K \arrow[u, dash] \arrow[r, "i", "\cong"'] & K' \arrow[u, dash]
\end{tikzcd}$$

m = min poly of σ_1 $i(m)$ = min poly of α_1

Let $g(t) = f(t) / (t-\sigma_1) \in K(\sigma_1)[t]$

$j_1 : K(\sigma_1) \longrightarrow K'(\alpha_1)$ is an isomorphism

$j_1(g)$ splits over L

By inductive hypothesis, $\exists$ field monomorphism

$j : \Sigma \longrightarrow L$ s.t. $j|_{K(\sigma_1)} = j_1$, then $j|_K = j_1|_K = i$.

□

Theorem 9.6

Let $f \in K[t]$, and let Σ = splitting field of f over K.

Let $i : K \longrightarrow K'$ be a field isomorphism and let

Σ' = splitting field of $i(f)$ over K'.

Then $\exists$ field isomorphism $j : \Sigma \longrightarrow \Sigma'$ st. $j|_K = i$.

Proof

$$\begin{tikzcd}
 & \Sigma' \\
\Sigma \arrow[r, "j"'] & j(\Sigma) \arrow[u, dash] \\
K \arrow[u, dash] \arrow[r, "i"'] & K' \arrow[u, dash] \\
f \arrow[r, mapsto] & i(f)
\end{tikzcd}$$

By lemma,
$\exists$ field monomorphism
$j : \Sigma \longrightarrow \Sigma'$ s.t. $j|_K = i$.
But $i(f)$ splits over $j(\Sigma)$.
By definition of the splitting field, $j(\Sigma) = \Sigma'$.
Therefore j is a field isomorphism

23-10-17

Normality

Def 9.8
An extension $L : K$ is called normal if every irreducible polynomial $f \in K[t]$ with one root in L splits in L

["irreducible" is crucial part def"
In definition of splitting field, irreducibility of the polynomial is not required.]

Example
Let $\alpha = \sqrt[3]{2}$.
Then $\mathbb{Q}(\alpha) : \mathbb{Q}$ is not normal.
Let $f(t) = t^3 - 2$. f is irreducible over $\mathbb{Q}$
(e.g. by Eisenstein $p = 2$)
f has one root (α) in $\mathbb{Q}(\alpha)$, but f does not split in $\mathbb{Q}(\alpha)$ since the other two roots
($\alpha\omega$, $\alpha\omega$, where $\omega = e^{2\pi i/3}$) are not real but $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

Normality is almost always proved for specific extensions using the next theorem.

Theorem 9.9
Let $L : K$ be a field extension. Then $L : K$ is normal and finite $\Leftrightarrow$ L is the splitting field of some polynomial over K.

MATH 3202

23-10-17

e.g $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$ is normal, since it $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field of $(t^2-2)(t^2-3)$ over $\mathbb{Q}$.

Proof

[$\Rightarrow$] Suppose $L:K$ is normal and finite.
Let $[L:K]=n$. Let $\{x_1,\dots,x_n\}$ be a K-basis for L.
Let m_i = min. poly. of x_i over K.
Since $L:K$ normal, m_i splits over L.
Let $m = m_1 \cdots m_n$
Claim: L is splitting field of m over K.
$m = m_1 \cdots m_n$ splits over L.
Also L is generated over K by the roots of m, since $L = K(x_1,\dots,x_n)$.

[$\Leftarrow$] Suppose L is the splitting field of $g \in K[t]$.
We have already seen that $L:K$ is finite.
WTS: If f is irreducible over K with one root in L, then all its roots lie in L.
In fact, we will prove something more general:
If θ_1, θ_2 are two roots of f, then $[L(\theta_1):L] = [L(\theta_2):L]$
$(\theta_1 \in L \Rightarrow L(\theta_1) = L \Rightarrow [L(\theta_1):L] = 1$
$\Rightarrow [L(\theta_2):L] = 1 \Rightarrow L(\theta_2) = L \Rightarrow \theta_2 \in L)$.
So let M = splitting field for f over L and consider the following diagram

$$\begin{tikzcd}
 & M \arrow[dl, dash] \arrow[dd, dash] \arrow[dr, dash] & \\
L(\theta_1) \arrow[dd, dash, "\equiv"'] & & L(\theta_2) \arrow[dd, dash, "\equiv"] \\
 & L \arrow[ul, dash, "\times"] \arrow[ur, dash, "\times"'] \arrow[dd, dash] & \\
K(\theta_1) & & K(\theta_2) \\
 & K \arrow[ul, dash, "\ast"] \arrow[ur, dash, "\ast"'] &
\end{tikzcd}$$

θ_1 and θ_2 are both roots of f, which is irreducible, so f is the min. poly. of θ_1 and θ_2.
Hence there is a K-isomorphism $j: K(\theta_1) \to K(\theta_2)$ s.t. $j(\theta_1) = \theta_2$

$$\begin{tikzcd}
K(\theta_1) \arrow[r, dashed, "j"] & K(\theta_2) \\
K \arrow[u, dash] \arrow[r, "id"] & K \arrow[u, dash]
\end{tikzcd}$$

(5.12)

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

L is splitting field of g over K, i.e. if roots of g are $\sigma_1,\dots,\sigma_n$ then $L = K(\sigma_1,\dots,\sigma_n)$.

Then $L(\theta_1) = K(\sigma_1,\dots,\sigma_n)(\theta_1) = K(\theta_1)(\sigma_1,\dots,\sigma_n)$

So $L(\theta_1)$ is splitting field of g over $K(\theta_1)$

Similarly $L(\theta_2)$ is splitting field of g over $K(\theta_2)$

$$\begin{tikzcd}
\text{splitting field of } g \text{ over } K(\theta_1) = L(\theta_1) \arrow[r, dashed, "\cong"', "\phi"] \arrow[d, dash] & L(\theta_2) = \text{splitting field of } g \text{ over } K(\theta_2) \arrow[d, dash] \\
K(\theta_1) \arrow[r, "\cong", "j"'] & K(\theta_2) \\
g \arrow[r, mapsto] & g
\end{tikzcd}$$

By 9.6, $\exists$ isomorphism $\phi: L(\theta_1) \to L(\theta_2)$ s.t. $\phi|_{K(\theta_1)} = j$

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

By Tower Law, $[L(\theta_1):K] = [L(\theta_1):K(\theta_1)][K(\theta_1):K]$

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

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

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

e.g. if $\omega = e^{2\pi i/7}$ then $\mathbb{Q}(\omega):\mathbb{Q}$ is normal since $\mathbb{Q}(\omega)$ is the splitting field of t^7-1 over $\mathbb{Q}$

(Roots of t^7-1 are $1,\omega,\dots,\omega^6$, so splitting field is $\mathbb{Q}(1,\omega,\dots,\omega^6) = \mathbb{Q}(\omega)$).

<u>Separability</u>

<u>Def</u> 9.10

An irreducible poly $f \in K[t]$ is <u>seperable</u> if it has no repeated roots (in a splitting field).

⌈If $K \subseteq \mathbb{C}$ then in fact every irreducible polynomial over K is seperable. In a more general context seperability is not automatic.⌋

23-10-17 e.g. $L = \mathbb{F}_p(t)$ (p odd prime) ← rational function field over $\mathbb{F}_p$
$K = \mathbb{F}_p(t^p) \leq L$
Let $f(x) = x^p - t^p \in K[x]$
f is irreducible over K.
However, over L, $f(x) = (x-t)^p$
(since all $\binom{p}{r}$ $(r=1,\dots,p-1)$ are divisible by p)
So f has one root repeated p times.

27-10-17 Splitting Field $\Leftrightarrow$ Normal & finite. (Last time)

Let $K \leq \mathbb{C}$ and f an irreducible polynomial over K.
Then f does not have repeated roots.

Proof

Note that if $f, g \in K[t]$ are coprime in $K[t]$, then they are still coprime in $\mathbb{C}[t]$. [Since f, g coprime $\exists\, h, k \in K[t]$ s.t. $fh + gk = 1$. Now suppose $p \in \mathbb{C}[t]$ st. $p | f$ and $p | g$. Then $p | fh + gk = 1$ so p is a unit, ie. f, g are coprime in $\mathbb{C}[t]$.]
Now suppose f is irreducible in $K[t]$ with repeated root $\alpha \in \mathbb{C}$. $f(t) = (t-\alpha)^2 g(t)$ for some $g \in \mathbb{C}[t]$.

$$f'(t) = 2(t-\alpha)g(t) + (t-\alpha)^2 g'(t)$$
$$= (t-\alpha)[2g(t) + (t-\alpha)g'(t)]$$

$\therefore$ $t - \alpha$ is a common factor of f and f' in $\mathbb{C}[t]$
$\Rightarrow f$ and f' not coprime in $\mathbb{C}[t]$
$\therefore f$ and f' not coprime in $K[t]$
But f is irreducible and $\partial f' < \partial f$, so
$hcf(f, f') | f \Rightarrow hcf(f, f') = 1$ or f
$hcf(f, f') = 1 \Rightarrow f, f'$ coprime ⨳
$hcf(f, f') = f \Rightarrow f | f'$ so $f' = 0$ ie. $\partial f = 0$ ⨳
$\therefore f$ has no repeated roots. □

↖ uses fact that $\leq \mathbb{C}$ so char 0 [e.g. in char p : $f(t) = t^p - 1$, $f'(t) = 0$]

Chapter 10

We are now aiming at the Fundamental Theorem, which is that for $L:K$ a finite normal extension, $+$ and $*$ are mutual inverses.

$\Gamma = \Gamma(L:K)$ = group of all K-auts of L

$H \leq \Gamma$, H^+ = fixed field of $H = \{x \in L : h(x) = x \ \forall h \in L\}$

If $M \leq L$, $M^* = \{g \in \Gamma : g(m) = m \ \forall m \in M\}$

We saw that $H < H^{+*}$

Need to prove $H = H^{+*}$

Since these are finite sets, it is enough to show $|H| = |H^{+*}|$

In Chapter 10, we show that $|H^+|$ is the "right size"

$$\begin{tikzcd}
\{e\} \arrow[d, dash, "\text{size } |H|"'] & & L \arrow[d, dash, "\text{degree } {[L:H^+]}"] \\
H \arrow[d, dash] & & H^+ \arrow[d, dash] \\
\Gamma & & K
\end{tikzcd}$$

i.e. $|H| = [L:H^+]$ ①

In Chapter 11, we show that $|M^*|$ is the "right size"

$$\begin{tikzcd}
\{e\} \arrow[d, dash, "\text{size } |M^*|"'] & & L \arrow[d, dash, "\text{degree } {[L:M]}"] \\
M^* \arrow[d, dash] & & M \arrow[d, dash] \\
\Gamma & & K
\end{tikzcd}$$

i.e. $|M^*| = [L, M]$ ②

Putting these together: $|H^{+*}| \underset{\substack{\uparrow \\ \text{by ②}}}{=} [L:H^+] \underset{\substack{\uparrow \\ \text{by ①}}}{=} |H|$

MATH 3202

27-10-17

injective homomorphisms

Field Monomorphisms

This chapter is about field monomorphisms.

We need to put them in the more general context of maps $L \to L$.

Note that a field homomorphism is in fact a monomorphism.

Let $\phi: K \to L$ be a field homomorphism,

then $\operatorname{Ker}\phi \triangleleft K$.

Since K is a field, $\operatorname{Ker}\phi = \{0\}$ or K.

$\operatorname{Ker}\phi \neq K$ since $\phi(1)=1$

$\Rightarrow \operatorname{Ker}\phi = \{0\} \Rightarrow \phi$ is injective $\Rightarrow \phi$ is a field monomorphism.

Given any two fields K, L, Let $Map(K,L)$ be the set of all functions $K \to L$.

We can make $Map(K,L)$ into a vector space over L:

$(f+g)(x) = f(x)+g(x)$

$(cf)(x) = c \cdot f(x)$ (for $c \in L$)

Easy to check vector space axions.

It thus makes sense to talk about maps $K \to L$ being linearly independent over L:

$f_1, \dots, f_n$ are LI over L if

$c_1 f_1 + \dots + c_n f_n = 0$ $(c_i \in L) \Rightarrow$ all $c_i = 0$.

This means $(c_1 f_1 + \dots + c_n f_n)(x) = 0$

$\Rightarrow c_1 f_1(x) + \dots + c_n f_n(x) = 0$ $\forall x \in K$.

Now look at $Map(K,K)$ and suppose $K_0 \leq K$,

then K is a vector space over K_0, and we can define

$Hom_{K_0}(K,K) = \{ f: K \to K \mid f$ is K_0-linear$\}$

e.g. $\mathbb{R} \leq \mathbb{C}$, $\mathbb{C}$ is a 2-dim vector space over $\mathbb{R}$ with basis $\{1, i\}$.

$Hom_{\mathbb{R}}(\mathbb{C},\mathbb{C}) = \{ f: \mathbb{C} \to \mathbb{C} \mid f$ is $\mathbb{R}$-linear$\}$

e.g. $f(1) = 1+i$, $f(i) = 2$

$\Rightarrow f(a+bi) = af(1) + bf(i) = a(1+i) + b \cdot 2 = (a+2b) + ai$

This has matrix $\begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix}$

$f\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix} = \begin{pmatrix}a+2b\\ a\end{pmatrix}$

As a vector space over $\mathbb{R}$,
$Hom_{\mathbb{R}}(\mathbb{C}, \mathbb{C})$ is 4-dimensional
In terms of matrices, the basis is
$\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right\}$

In terms of maps, the basis is $\{\delta_{11}, \delta_{12}, \delta_{21}, \delta_{22}\}$
$\delta_{11}(1) = 1$, $\delta_{12}(1) = i$, $\delta_{21}(1) = 0$, $\delta_{22}(1) = 0$,
$\delta_{11}(i) = 0$, $\delta_{12}(i) = 0$, $\delta_{21}(i) = 1$, $\delta_{22}(i) = i$.

We can also look at $Hom_{\mathbb{R}}(\mathbb{C}, \mathbb{C})$ as a vector space over $\mathbb{C}$.
This is 2-dim: a basis is $\{\delta_{11}, \delta_{21}\}$.

In general, if $[K : K_0] = m$, then $\dim_K(Hom_{K_0}(K, K)) = m$.
Let $\{x_1, \dots, x_m\}$ be a K_0-basis for K.
Define δ_i $(1 \leq i \leq m)$ in $Hom_{K_0}(K, K)$ by $\delta_i(x_i) = 1$, $\delta_i(x_j) = 0$ $(j \neq i)$
Then $\{\delta_1, \dots, \delta_m\}$ is a basis for $Hom_{K_0}(K, K)$ over K.

LI:

Suppose $c_1\delta_1 + \dots + c_m\delta_m = 0$ $(c_i \in K)$
$\Rightarrow (c_1\delta_1 + \dots + c_m\delta_m)(x_i) = 0 \quad \forall x_i$
$\Rightarrow c_1\delta_1(x_i) + \dots + c_i\delta_i(x_i) + \dots + c_m\delta_m(x_i) = 0$
$\Rightarrow c_i \cdot 1 = 0 \Rightarrow c_i = 0 \Rightarrow c_i = 0 \ \forall i$

Spanning:

Let $f \in Hom_{K_0}(K, K)$ and let $f(x_i) = c_i \in K$.
Then $f = c_1\delta_1 + \dots + c_m\delta_m$ since $f(x_i) = c_1\delta_1(x_i) + \dots + c_i\delta_i(x_i) + \dots + c_m\delta_m(x_i)$
$\Rightarrow f(x_i) = 0 + \dots + c_1 \cdot 1 + \dots + 0 = c_i$.

MATH 3202

27-10-17

Lemma 10.1 (Dedekind's Lemma)
Let K, L be fields and $\lambda_1, \dots, \lambda_n$ be distinct field monomorphisms $K \to L$. Then $\{\lambda_1, \dots, \lambda_n\}$ is LI over L.

Proof
We need to prove that if $c_1\lambda_1 + \dots + c_n\lambda_n = 0$ $(c_i \in L)$ then all $c_i = 0$.
Suppose not. Pick a shortest possible relation of dependence.
By re-numbering, we obtain $c_1\lambda_1 + \dots + c_r\lambda_r = 0$ (all $c_i \neq 0$) and there is no relation involving $< r$ terms.
$r \neq 1$ since $c_1\lambda_1 = 0 \Rightarrow c_1\lambda_1(1) = 0 \Rightarrow c_1 \cdot 1 = 0 \Rightarrow c_1 = 0$.
We now get a contradiction by producing a shorter relation of dependence.

$(c_1\lambda_1 + \dots + c_r\lambda_r)(x) = 0 \quad \forall x \in K$

$\Rightarrow c_1\lambda_1(x) + \dots + c_r\lambda_r(x) = 0$ ①

For any $y \in K$, $c_1\lambda_1(xy) + \dots + c_r\lambda_r(xy) = 0$

$\Rightarrow c_1\lambda_1(x)\lambda_1(y) + \dots + c_r\lambda_r(x)\lambda_r(y) = 0$ ②

② $- \lambda_r(y)$①:

$$c_1\lambda_1(x)(\lambda_1(y) - \lambda_r(y)) + \dots + c_r\lambda_r(x)(\lambda_r(y) - \lambda_r(y)) = 0 \quad \forall x \in K$$

$$\Rightarrow c_1\lambda_1(x)(\lambda_1(y) - \lambda_r(y)) + \dots + c_{r-1}\lambda_{r-1}(x)(\lambda_{r-1}(y) - \lambda_r(y)) = 0$$

$$\Rightarrow c_1(\lambda_1(y) - \lambda_r(y))\lambda_1(x) + \dots + c_{r-1}(\lambda_{r-1}(y) - \lambda_r(y))\lambda_{r-1}(x) = 0$$ ③

Pick y s.t. $\lambda_1(y) \neq \lambda_r(y)$ since λ_1, λ_r are distinct.
Then ③ is a shorter relation of dependence (non trivial since $c_1(\lambda_1(y) - \lambda_r(y)) \neq 0$).
Contradiction ※.

□

Theorem 10.5

Let G be a finite group of automorphisms of a field K and let K_0 be the fixed field of G

i.e. $K_0 = \{x \in K : g(x) = x \quad \forall g \in G\}$

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

Proof

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

Suppose $[K : K_0] = m < n$.

Then $g_1, \dots, g_n$ are n distinct K_0-linear monomorphisms $K \to K$ and hence LI over K. (Dedekind's Lemma)

But $\dim_K(\mathrm{Hom}_{K_0}(K,K)) = m < n$, a contradiction.

$\therefore [K : K_0] \geq n$

Suppose $[K : K_0] > n$.

Then there are $n+1$ elements of K LI over K_0, say $x_1, \dots, x_{n+1}$.

Consider the system of equations

$$\begin{pmatrix} g_1(x_1) & \dots & g_1(x_{n+1}) \\ g_2(x_1) & \dots & g_2(x_{n+1}) \\ \vdots & & \vdots \\ g_n(x_1) & \dots & g_n(x_{n+1}) \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \\ 0 \end{pmatrix}$$

This is a system of homogeneous linear equations: n equations in $n+1$ unknowns, hence with a non-trivial solution.

Pick a solution with as few non-zero terms as possible,

say $\begin{pmatrix} g_1(x_1) & \dots & g_1(x_r) \\ \vdots & & \vdots \\ g_n(x_1) & \dots & g_n(x_r) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ ① (after renumbering).

All $y_i \neq 0$ and there is no non-trivial solution with $< r$ terms.

[$r \neq 1$, since then $\begin{pmatrix} g_1(x_1) \\ \vdots \\ g_n(x_1) \end{pmatrix} (y_1) = 0$ so $g_i(x_1) y_1 = 0$

so $g_i(x_1) = 0$

take $g_i = e$ so $x_1 = e(x_1) = 0$.]

27-10-17

Let $g \in G$: apply g to ①.

$$\begin{pmatrix} gg_1(x_1) & \cdots & gg_1(x_r) \\ \vdots & & \vdots \\ gg_n(x_1) & \cdots & gg_n(x_r) \end{pmatrix} \begin{pmatrix} g(y_1) \\ \vdots \\ g(y_r) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

As j varies, gg_j varies over all elements of G.
[e.g. $G = C_3 = \langle x \mid x^3 = e \rangle$, $x \cdot e = x$, $x \cdot x = x^2$, $x \cdot x^2 = e$]
So $gg_1, \dots, gg_n$ are just $g_1, \dots, g_n$ re-ordered.
By permuting rows we get

$$\begin{pmatrix} g_1(x_1) & \cdots & g_1(x_r) \\ \vdots & & \vdots \\ g_n(x_1) & \cdots & g_n(x_r) \end{pmatrix} \begin{pmatrix} g(y_1) \\ \vdots \\ g(y_r) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad ②$$

Multiply ① by $g(y_1)$ to get

$$\begin{pmatrix} g_1(x_1) & \cdots & g_1(x_r) \\ \vdots & & \vdots \\ g_n(x_1) & \cdots & g_n(x_r) \end{pmatrix} \begin{pmatrix} y_1 g(y_1) \\ \vdots \\ y_r g(y_1) \end{pmatrix} = \begin{pmatrix} 0 \\ \\ 0 \end{pmatrix} \quad ③$$

Multiply ② by y_1 to get

$$\begin{pmatrix} g_1(x_1) & \cdots & g_1(x_r) \\ \vdots & & \vdots \\ g_n(x_1) & \cdots & g_n(x_r) \end{pmatrix} \begin{pmatrix} y_1 g(y_1) \\ \vdots \\ y_1 g(y_r) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad ④$$

Take ④ − ③ to get

$$\begin{pmatrix} g_1(x_1) & \cdots & g_1(x_r) \\ \vdots & & \vdots \\ g_n(x_1) & \cdots & g_n(x_r) \end{pmatrix} \begin{pmatrix} 0 \\ y_2 g(y_1) - y_1 g(y_2) \\ \vdots \\ y_r g(y_1) - y_1 g(y_r) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

This is a solution with $< r$ non-zero terms,
so by definition this must be the trivial solution,
i.e. $y_j g(y_1) - y_1 g(y_j) = 0 \ \forall j = 2, .., r$.

$y_j g(y_1) = y_1 g(y_j)$

$\Rightarrow y_j y_1^{-1} = g(y_j) g(y_1)^{-1}$
$= g(y_j y_1^{-1})$

This holds $\forall g \in G$ so $y_j y_1^{-1} \in K_0$,
say $y_j y_1^{-1} = k_j \in K_0$
$\Rightarrow y_j = y_1 k_j \quad (j = 2, \dots, r)$.
Let $k_1 = 1$ then $y_j = y_1 k_j \quad (j = 1, \dots, r)$.
One of the g_i is e, say $g_1 = e$.

$$\begin{pmatrix} e(x_1) & \cdots & e(x_r) \\ \vdots & & \vdots \\ g_n(x_1) & \cdots & g_n(x_r) \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad ①$$

First equation says $x_1 y_1 + \dots + x_r y_r = 0$
$\Rightarrow x_1 y_1 k_1 + \dots + x_r y_1 k_r = 0$
$\Rightarrow y_1 (x_1 k_1 + \dots + x_r k_r) = 0$
$y_1 \neq 0 \Rightarrow x_1 k_1 + \dots + x_r k_r = 0$
Since $k_1 = 1 \neq 0$ and all $k_j \in K_0$
so this says $\{x_1, \dots, x_r\}$ is linearly dependent over K_0,
a contradiction. ✻.
□

Apply 10.5 to $\Gamma = \Gamma(L:K)$,
$H \leq \Gamma$ to get $|H| = [L : H^+]$

$$\begin{tikzcd} \{e\} \arrow[d, dash, "|H|"'] & L \arrow[d, dash, "{[L:H^+]}"] \\ H \arrow[d, dash] & H^+ \arrow[d, dash] \\ \Gamma & K \end{tikzcd}$$

$|H| = [L : H^+]$

MATH 3203

30-10-17

Th^m 10.5

Let G be a finite group of auts of L, and let K_0 be fixed field. Then $|G| = [K : K_0]$

eg. Let $K = \mathbb{R}(t)$, $\phi : K \to K$ by $\phi(t) = 1/t$

$[$eg $\phi(t^2 - t \,/\, t^2+1) = ((1/t)^2 - (1/t)) / ((1/t)^2 + 1) = (1-t)/(1+t^2)\,]$

What is K_0, the field fixed by $\langle\phi\rangle$?

$\phi^2 = id$, so $\langle\phi\rangle = \{e, \phi\}$

By Theorem, $[K : K_0] = |\langle\phi\rangle| = 2$

Let $\alpha = t + \phi(t)$, then $\phi(\alpha) = \phi(t) + \phi^2(t) = \phi(t) + t = \alpha$

$\therefore\ \alpha \in K_0$, so $\mathbb{R}(\alpha) \subseteq K_0$

$$\begin{tikzcd}[row sep=small] K = \mathbb{R}(t) \arrow[d, dash] \\ K_0 \arrow[d, dash] \\ \mathbb{R}(\alpha) \end{tikzcd} \qquad \leq 2 \text{ (from } K \text{ to } \mathbb{R}(\alpha)), \quad 2 \text{ (from } K \text{ to } K_0)$$

$\mathbb{R}(t) = \mathbb{R}(\alpha)(t)$

$\alpha = t + \frac{1}{t}$, $\alpha t = t^2 + 1$

so $t^2 - \alpha t + 1 = 0$

$f(x) = x^2 - \alpha x + 1 \in \mathbb{R}(\alpha)[x]$

$f(t) = 0$

$\therefore\ [\mathbb{R}(t) : \mathbb{R}(\alpha)] \leq 2$

By tower law $[K : \mathbb{R}(\alpha)] = 2$, $[K_0 : \mathbb{R}(\alpha)] = 1$, $K_0 = \mathbb{R}(\alpha)$

Thus if f is a rational polynomial unchanged under $t \mapsto 1/t$, f is a rational function in $(t + \frac{1}{t})$

Chapter 11

Key result is 11.11

If $L : K$ is normal and finite $(\subseteq \mathbb{C})$ then $|\Gamma(L:K)| = [L:K]$.

This applies to the following situation:

$$\begin{tikzcd}[row sep=small] {[L:M]}\ L \arrow[d, dash] & \{e\}\ \ |M^*| \arrow[d, dash] \\ M \arrow[r, "*"] \arrow[d, dash] & M^* = \Gamma(L:M) \arrow[d, dash] \\ K & \Gamma \end{tikzcd}$$

Def 11.1

Let $K \leq L$, $K \leq M$. Then a K-monomorphism $M \to L$ is a field monomorphism $\phi : M \to L$ s.t. $\phi|_K = id$.

e.g. $\phi : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{C}$ by $\phi(\sqrt[4]{2}) = \sqrt[4]{2}\, i$ is a $\mathbb{Q}$ monomorphism.

If $K \leq M \leq L$ then any K-aut of L, $\phi : L \to L$ restricts to a K-monomorphism $M \to L$.

$$\begin{tikzcd}
L \arrow[r, "\phi"] & L \\
M \arrow[u, dash] \arrow[r, dashed, "\phi|_M"] & \phi(M) \arrow[u, dash] \\
K \arrow[u, dash] \arrow[r, "id"] & K \arrow[u, dash]
\end{tikzcd}$$

Next result is about when this can be reversed:

Theorem 11.3

Let $K \leq M \leq L$ and let $L : K$ be normal and finite.
If $\tau : M \to L$ is a K-monomorphism then
$\exists$ a K-automorphism $\phi : L \to L$ st. $\phi|_M = \tau$

$$\begin{tikzcd}
 & L \arrow[r, dashed, "\phi"] & L \\
\text{normal \& finite} & M \arrow[u, dash] \arrow[r, "\tau"] & \tau(M) \arrow[u, dash] \\
 & K \arrow[u, dash] \arrow[r, "id"] & K \arrow[u, dash]
\end{tikzcd}$$

i.e. τ extends to an automorphism of L.

Proof

Since L is normal and finite, L is splitting field of some polynomial $f(t) \in K[t]$.
Note: $\tau(f) = f$.
$\therefore$ L is splitting field of f over M.
L " " " " $\tau(f) = f$ over $\tau(M)$.
By 9.6 $\exists$ an automorphism $\phi : L \to L$ st. $\phi|_M = \tau$
Then $\phi|_K = \phi|_M|_K = \tau|_K = id$, i.e. ϕ is the required K-automorphism of L.
□

MATH 3202

30-10-17

Prop 11.4

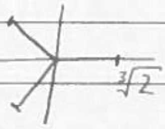
Let $L:K$ be finite normal and $\alpha, \beta \in L$ with same min poly over K. Then $\exists$ K-automorphism ϕ of L s.t. $\phi(\alpha) = \beta$.

Proof

By 5.13, $\exists$ K-isomorphism $\tau : K(\alpha) \to K(\beta)^{\subseteq L}$ s.t. $\tau(\alpha) = \beta$. We can regard τ as a K-monomorphism $K(\alpha) \to L$. Hence by 11.3, $\exists$ K-automorphism $\phi : L \to L$ s.t. $\phi|_{K(\alpha)} = \tau$ and hence $\phi(\alpha) = \beta$. □

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

e.g. $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}$, where $\omega = e^{2\pi i/3}$, is the splitting field of $t^3 - 2$



$\omega = e^{2\pi i/3}$
$= -\frac{1}{2} + \frac{\sqrt{3}}{2} i$

Then $\sqrt[3]{2}$ and $\sqrt[3]{2}\,\omega$ have the same minimal polynomial $t^3 - 2$, so $\exists$ $\mathbb{Q}$-automorphism $\phi : \mathbb{Q}(\sqrt[3]{2}, \omega) \to \mathbb{Q}(\sqrt[3]{2})$ s.t. $\phi(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$

$\nwarrow$ element of the Galois group $\Gamma(\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q})$.

03-11-17

Normal Closures

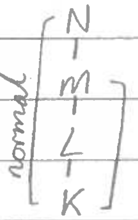
Def 11.5

Let $L:K$ be a finite extension. A normal closure of $L:K$ is an extension N of L st.

i). $N:K$ is normal

ii). if $L \leq M \leq N$ and $M:K$ is normal, then $M=N$

Inside $\mathbb{C}$, any extension $L:K$ has a unique normal closure.



Example

normal closure of $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \omega)$ $(\omega = e^{2\pi i/3})$

(systematic way of fining the normal closure is to put roots until we reach something normal).

Theorem 11.6

If $L:K$ is a finite extension in $\mathbb{C}$, then $\exists !$ normal closure N and $[N:K] < \infty$.

Proof

Let $x_1, \dots, x_n$ be a K-basis for L.

Let m_i = minimum polynomial of x_i over K and $f = m_1 \dots m_n \in K[t]$

Let N = splitting field of f over K.

Since each $x_i \in N$, $L \leq N$ (L generated by x_i's)

By 9.9, $N:K$ is normal and finite (splitting fields are always normal).

Minimality:

Suppose $L \leq P \leq N$ and $P:K$ is normal.

Each m_i has a root (x_i) in $L \leq P$, thus m_i is an irreducible polynomial with one root in P so splits over P.

$\therefore f$ splits over P, by def^n of N as splitting field,

$P = N$.

MATH 3202

03-11-17

Uniqueness:

Suppose $M:K$ is also a normal closure of $L:K$.

$L \leq M$ so all $x_i \in M$.

Hence all roots of f lie in M, i.e. $N \leq M$.

By minimality $N = M$. □

Lemma 11·8

Suppose $L:K$ is finite, $N:K$ is normal closure and $N \leq M$. Let $\tau : L \to M$ be a K-monomorphism. Then $\tau(L) \leq N$

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

"A K-monomorphism for L can't get outside the normal closure."

e.g. suppose $\tau : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}$ is a $\mathbb{Q}$-monomorphism, then $\tau(\mathbb{Q}(\sqrt[3]{2})) \leq \mathbb{Q}(\sqrt[3]{2}, \omega)$.

Proof

Let $\alpha \in L$ with min. poly. m over K, $m(\alpha) = 0$.

$\tau(m(\alpha)) = \tau(0) = 0$, $m(\tau(\alpha)) = 0$ since τ is a field homomorphism.

[e.g. $m(t) = t^3 - 3t + 1$, $\alpha^3 - 3\alpha + 1 = 0$

$\tau(\alpha^3 - 3\alpha + 1) = \tau(0) = 0$

$\tau(\alpha)^3 - 3\tau(\alpha) + 1 = 0$ so $\tau(\alpha)$ is a root of m

any K-mono sends an element to a root of its min. poly.]

So $\tau(\alpha)$ is a root of m.

m is irreducible over K with one root α in N, so by normality m splits over N, i.e. $\tau(\alpha) \in N$.

□

$$\begin{tikzcd}
N \arrow[d, dash] \\
L \arrow[d, dash] \\
K
\end{tikzcd} \Bigg] \text{normal}$$

Theorem 11·9

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

(i) $L:K$ is normal

(ii) $\exists$ a finite normal extension N of K containing L s.t. every K-mono $\tau : L \to N$ is a K-auto. of L

(iii) $\forall$ extension M of K containing L, every K-mono. $\tau : L \to M$ is a K-aut of L $(\tau(L) \subseteq L)$.

Proof

First note that any K-mono. $L \to L$ is infact a K-aut. of L since $L \cong \tau(L)$, so $[\tau(L):K] = [L:K]$

$$\begin{tikzcd} L \arrow[d, dash, "1"] \arrow[dd, dash, bend right, "n"'] \\ \tau(L) \arrow[d, dash, "n"] \\ K \end{tikzcd}$$

By Tower Law $[L:\tau(L)] = 1$, i.e. $\tau(L) = L$, so τ is also surjective and hence a K-aut of L.

(i) $\Rightarrow$ (iii)

Since $L:K$ is normal, L is normal closure. By 11·8 any K-mono. $L \to M$ satisfies $\tau(L) \subseteq L$.

(iii) $\Rightarrow$ (ii)

Take N = normal closure of $L:K$.

(ii) $\Rightarrow$ (i)

Suppose f is an irreducible poly. over K with one root α in L. Let β be another root of f. Since $N:K$ is normal, $\beta \in N$.

By 11·4, $\exists$ K-aut τ of N s.t. $\tau(\alpha) = \beta$.

$\tau|_L$ is a K-mono $L \to N$. By (ii), $\tau(L) \subseteq L$, so $\beta = \tau(\alpha) \in L$ $\therefore$ $L:K$ is normal.

$\square$

MATH 3202

03-11-17

Main Result

Theorem 11·10

Let $L:K$ be a finite extension of degree n. Then there are precisely n K-monomorphisms from L into the normal closure N of $L:K$ (and hence into any normal extension $M:K$ where $M \geq L$).

Corollary 11·11

Let $L:K$ be finite and normal with $[L:K]=n$. Then there are precisely n K-aut.s of L, i.e.

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

Proof (of thm 11.10)

(By induction on $[L:K]$).

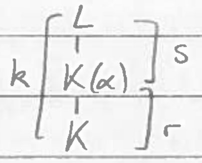
Case $[L:K]=1$ is trivial, $K=L=N$.

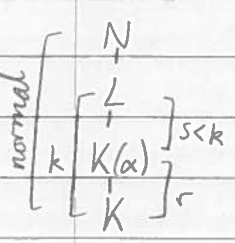
Suppose $[L:K]=k>1$.

Let $\alpha \in L \setminus K$ with min. poly. m of degree $[K(\alpha):K]=r>1$.

Let $s=k/r<k$.

N also is normal closure of $L:K(\alpha)$.





Hence by inductive hypothesis, there are exactly s $K(\alpha)$-monos. $L \to N$, say $\rho_1, \dots, \rho_s$.

Let m have (distinct) roots $\alpha = \alpha_1 \dots \alpha_r$. Since $N:K$ is normal, all $\alpha_i \in N$. By 11·4, $\exists$ K-auts τ_i of N st. $\tau_i(\alpha) = \alpha_i$ $(i=1,\dots,r)$.

Let $\phi_{ij} = \tau_i \rho_j : L \to N$. The ϕ_{ij}'s are K-monos.

□

Theorem 11·13

Let $K \leq L \leq M$, $M:K$ finite. Then the number of K-monos. $L \to M$ is $\leq n = [L:K]$.

Proof

Let N be the normal closure of $M:K$. Then any K-mono. $L \to M$ is also a K-mono. $L \to N$.
By 11·10, there are precisely n of these and hence there are $\leq n$ K-monos. $L \to M$.

$\square$

Theorem 11·14

Let $L:K$ be finite, $G = \Gamma(L:K)$. If K is the fixed field of G, then $L:K$ is normal.

Proof

Let $[L:K] = n$. By 10·5, $|G| = [L:K]$, thus there are precisely n K-auts of L.
Let N be an extension of K containing L and $\tau : L \to N$ a K-mono. By 11·13, there are at most n K-monos $L \to N$, but G provides n K-monos. $L \to N$.
$\therefore$ τ is one of the elements of G, i.e. $\tau(L) \subseteq L$.
By 11·9, $L:K$ is normal.

$\square$

[Stapled papers handout]

Lemma 12·2

Let $K \leq M \leq L$, $\tau : L \to L$ a K-automorphism.
Then $\tau(M)^* = \tau M^* \tau^{-1}$.

Proof

Let $g \in M^*$ and $m \in M$, $g(m) = m$ $\forall m \in M$.
$(\tau g \tau^{-1})(\tau(m)) = \tau g(m) = \tau(m)$
i.e. $\tau g \tau^{-1}$ fixes $\tau(m)$ $\forall m \in M$
$\tau g \tau^{-1} \in \tau(M)^*$ $\quad \therefore \tau M^* \tau^{-1} \subseteq \tau(M)^*$.
Let $g \in \tau(M^*)$.

$$\begin{tikzcd} m \arrow[r, "\tau"] \arrow[loop below, "g"] & \tau(m) \end{tikzcd}$$

$g\tau(m) = \tau(m)$ $\forall m \in M$

03-11-17

$\Rightarrow \tau^{-1} g \tau(m) = m \quad \forall m \in M$

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

$\Rightarrow g \in \tau M^* \tau^{-1} \quad \Rightarrow \quad \tau(M)^* \subseteq \tau M^* \tau^{-1}$

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

Example

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

Find $\Gamma(K, \mathbb{Q}) = G$ and hence find all intermediate fields.

$K = \mathbb{Q}(1, \omega, \dots, \omega^6)$, $\omega = e^{2\pi i/7}$ $= \mathbb{Q}(\omega)$.

ω satisfies $t^7 - 1 = (t-1)\underbrace{(t^6 + \dots + 1)}_{m(t)}$

$m(\omega) = 0$ and m is irreducible ($t = s+1$ and use Eisenstein, $p = 7$).

$[\mathbb{Q}(\omega), \mathbb{Q}] = \partial m = 6 \quad \therefore |G| = 6.$

Any element g of G is determined by $g(\omega)$ and $g(\omega)$ must be a root of $m(t)$, i.e. $g_i(\omega) = \omega^i$ for $i = 1, \dots, 6$.

Since $|G| = 6$ and these g_i are the only possible elements of G, they are all in G.

So $G = \{g_1, \dots, g_6\}$ (any group of order 6 is C_6 or D_6)

$$\left.\begin{aligned} g_2(\omega) &= \omega^2 \\ g_2^2(\omega) &= \omega^4 \\ g_2^3(\omega) &= \omega^6 \end{aligned}\right\} \Rightarrow g_2^3 = id.$$

$$\left.\begin{aligned} g_3(\omega) &= \omega^3 \\ g_3^2(\omega) &= g_3(\omega^3) = \omega^9 = \omega^2 \end{aligned}\right\} ord(g_3) = 6$$

(Quicker way: take something and show it gives us everything)

$\therefore G = < g_3 ; g_3^6 = e > \cong C_6$

Write $g = g_3$, $g(\omega) = \omega^3$

$$\begin{tikzcd} & \{e\} \arrow[dl, no head] \arrow[dr, no head] & \\ <g^2> = \{e, g^2, g^4\} \arrow[dr, no head] & & <g^3> = \{e, g^3\} \arrow[dl, no head] \\ & G & \end{tikzcd}$$

$$\begin{tikzcd} & \mathbb{Q}(\omega) \arrow[dl, no head] \arrow[dr, no head] & \\ <g^2>^+ \arrow[dr, no head] & & <g^3>^+ \arrow[dl, no head] \\ & \mathbb{Q} & \end{tikzcd}$$

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

? $\alpha = \omega + g^2(\omega) + g^4(\omega) \in <g^2>^+$, $\alpha = \omega + \omega^2 + \omega^4$

$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq <g^2>^+ \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}$ or $\mathbb{Q}(\alpha) = <g^2>^+$

$\omega + \omega^2 + \omega^4 \in \mathbb{Q}$

$\omega^4 + \omega^2 + \omega - q = 0$

Contradiction since min poly of ω is of degree 6.

$\therefore \ <g^2>^{+} = \mathbb{Q}(\alpha)$

Similarly $<g^3>^{+} = \mathbb{Q}(\beta)$, $\beta = \omega + \omega^6$

$$\begin{tikzcd}
 & \mathbb{Q}(\omega) \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\omega+\omega^2+\omega^4) \arrow[d, equal] \arrow[dr, dash, "2"'] & & \mathbb{Q}(\omega+\omega^6) = \mathbb{Q}(\cos(2\pi/7)) \arrow[dl, dash, "3"] \\
\mathbb{Q}(\sqrt{x}) & \mathbb{Q} &
\end{tikzcd}$$

$\mathbb{Q}(\sqrt{x})$ for some x (didn't have time to compute).

13-11-17

$f(t) = t^3 - 2$ over $\mathbb{Q}$

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

(L is the splitting field of $f(t)$ over $\mathbb{Q}$).

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

(min poly: $t^3 - 2$, irred by Eisenstein with $p=2$)

ω satisfies $t^3 - 1 = (t-1)(t^2+t+1)$

t^2+t+1 is irreducible since $\omega \notin \mathbb{R}$. (cyclotomic polys are irreducible).

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

$\Rightarrow [\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6.$

3). $G = \Gamma(L : \mathbb{Q})$, $|G| = 6 = [L : \mathbb{Q}]$

4). $\sigma_1 = e \in G$

$\sigma_2(\sqrt[3]{2}) = 2^{1/3}\omega \in L$, $\sigma_2(\omega) = \omega \in L$

$\sigma_3(\sqrt[3]{2}) = 2^{1/3} \in L$, $\sigma_3(\omega) = \omega^2 \in L$

$\sigma_4(\sqrt[3]{2}) = 2^{1/3}\omega \in L$, $\sigma_4(\omega) = \omega^2 \in L$

$\sigma_5(\sqrt[3]{2}) = 2^{1/3}\omega^2 \in L$, $\sigma_5(\omega) = \omega \in L$

$\sigma_6(\sqrt[3]{2}) = 2^{1/3}\omega^2 \in L$, $\sigma_6(\omega) = \omega^2 \in L$

$g \in G$

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

$g(\omega) = \omega$ or ω^2

5). $G = \{\sigma_1, \dots, \sigma_6\}$

MATH 3202

13-11-17

6). $\sigma_2{}^2(\sqrt[3]{2}) = \sigma_2(\sqrt[3]{2}\omega) = \sqrt[3]{2}\omega^2$

$\sigma_2{}^2(\omega) = \omega$

$\therefore \sigma_2{}^2 = \sigma_5$

$\sigma_2{}^3(\sqrt[3]{2}) = \sigma_2(\sqrt[3]{2}\omega^2) = \sqrt[3]{2} \Rightarrow \sigma_2{}^3 = \sigma_1$

$\sigma_3{}^2(\sqrt[3]{2}) = \sqrt[3]{2}$, $\sigma_3{}^2(\omega) = \omega$ $\therefore \sigma_3{}^2 = \sigma_1$

$\sigma_4{}^2(\sqrt[3]{2}) = \sigma_4(\sqrt[3]{2}\omega) = \sqrt[3]{2}\omega^3 = \sqrt[3]{2}$

$\sigma_4{}^2(\omega) = \omega^4 = \omega$

$\therefore \sigma_4{}^2 = \sigma_1$

$\sigma_5{}^2(\sqrt[3]{2}) = \sigma_5(\sqrt[3]{2}\omega^2) = \sqrt[3]{2}\omega^4 = \sqrt[3]{2}\omega$

$\sigma_5{}^2(\omega) = \omega$

$\therefore \sigma_5{}^2 = \sigma_2$

$(\sigma_2\sigma_3)(\sqrt[3]{2}) = \sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\omega$

$(\sigma_2\sigma_3)(\omega) = \sigma_2(\omega^2) = \omega^2$

$\therefore \sigma_2\sigma_3 = \sigma_4$

$(\sigma_2{}^2\sigma_3)(\sqrt[3]{2}) = \sigma_2{}^2(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2 = \sigma_3\sigma_2(\sqrt[3]{2})$

$(\sigma_2{}^2\sigma_3)(\omega) = \sigma_2{}^2(\omega^2) = \omega^2 = \sigma_3\sigma_2(\omega)$

$\therefore \sigma_2{}^2\sigma_3 = \sigma_6$

$\Rightarrow G = \{\sigma_1, \sigma_2, \sigma_2{}^2, \sigma_3, \sigma_2\sigma_3, \sigma_2{}^2\sigma_3\}$

$= \langle \sigma_2, \sigma_3 \mid \sigma_2{}^3 = \sigma_3{}^2 = e, \sigma_3\sigma_2 = \sigma_2{}^2\sigma_3 \rangle \cong D_6$ or S_3

$= \langle g, h \mid g^3 = h^2 = e, hg = g^2h \rangle$

17-11-17

7). ord $\sigma_1 = 1$

ord $\sigma_2 = 3$

ord $\sigma_3 = 2$

ord $\sigma_2{}^2 = 3$

ord $\sigma_2\sigma_3 = 2$

ord $\sigma_2{}^2\sigma_3 = 2$

$(\sigma_2\sigma_3)^2 = (\sigma_2\sigma_3)(\sigma_2\sigma_3) = \sigma_2\sigma_2{}^2\sigma_3\sigma_3 = ee = e$

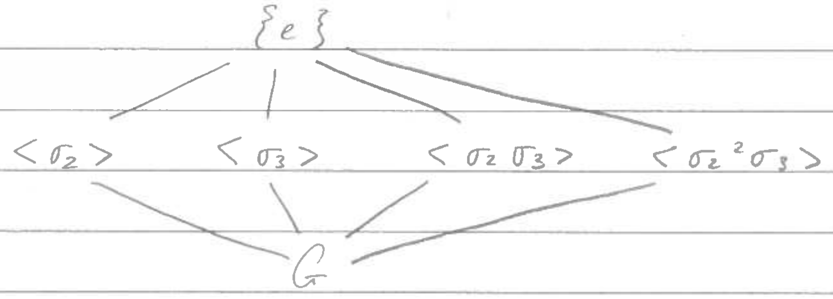
$(\sigma_2{}^2\sigma_3)^2 = \sigma_2{}^2\sigma_3\sigma_2{}^2\sigma_3 = \sigma^2\sigma_3\sigma_3\sigma_2 = \sigma^2 e \sigma = e$

Non trivial subgroups are of order 2 or 6 since $2|6$ and $3|6$ $(|G| = 6)$

$\Rightarrow C_2 \leq G$, $C_3 \leq G$

$H_1 = \langle\sigma_2\rangle = \langle\sigma_2{}^2\rangle$, $H_2 = \langle\sigma_3\rangle$, $H_3 \langle\sigma_2\sigma_3\rangle$, $H_4 = \langle\sigma_2{}^2\sigma_3\rangle$

8).


$\{e\}$
$\langle \sigma_2 \rangle$
$\langle \sigma_3 \rangle$
$\langle \sigma_2 \sigma_3 \rangle$
$\langle \sigma_2^2 \sigma_3 \rangle$
G

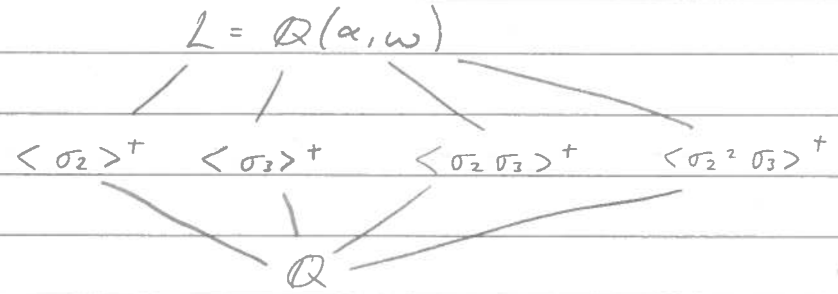
$\langle \sigma_2 \rangle \triangleleft G$

$\sigma_3^{-1} \sigma_2 \sigma_3 = \sigma_3 \sigma_2 \sigma_3 = \sigma_2^2 \sigma_3 \sigma_3 = \sigma_2^2 \in \langle \sigma_2 \rangle$

$\langle \sigma_3 \rangle$ is not normal in G

$\sigma_2^{-1} \sigma_3 \sigma_2 = \sigma_2^2 \sigma_3 \sigma_2 = \sigma_2^2 \sigma_2^2 \sigma_3 = \sigma_2 \sigma_3 \notin \langle \sigma_3 \rangle$

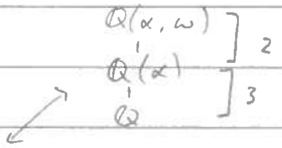
9).


$L = \mathbb{Q}(\alpha, \omega)$
$\langle \sigma_2 \rangle^+$
$\langle \sigma_3 \rangle^+$
$\langle \sigma_2 \sigma_3 \rangle^+$
$\langle \sigma_2^2 \sigma_3 \rangle^+$
$\mathbb{Q}$

$\sigma_2(\alpha) = \alpha\omega$, $\sigma_2(\omega) = \omega$ $\qquad \alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3}$

$\sigma_3(\alpha) = \alpha$, $\sigma_3(\omega) = \omega^2$

$\langle h \rangle^+ = \{ x \in \mathbb{Q}(\alpha, \omega) : \beta(x) = x \ \forall \beta \in \langle h \rangle \}$
$\qquad = \{ x \in \mathbb{Q}(\alpha, \omega) : h(x) = x \}$



$\langle \sigma_2 \rangle^+ = \{ x \in \mathbb{Q}(\alpha, \omega) ; \sigma_2(x) = x \} = \mathbb{Q}(\omega)$

Method 1: $\mathbb{Q}(\alpha, \omega)$ has basis $\{1, \alpha, \alpha^2, \omega, \alpha\omega, \alpha^2\omega\}$ over $\mathbb{Q}$

$x \in \mathbb{Q}(\alpha, \omega) \Rightarrow x = a_1 + a_2\alpha + a_3\alpha^2 + a_4\omega + a_5\alpha\omega + a_6\alpha^2\omega$

$\sigma_2(x) = a_1 + a_2\alpha\omega + a_3\alpha\omega^2 + a_4\omega + a_5(\alpha\omega)\omega + a_6(\alpha\omega)^2\omega$

$= a_1 + a_2\alpha\omega + a_3\alpha^2(-1-\omega) + a_4\omega + a_5\alpha(-1-\omega) + a_6\alpha^2$

$= a_1 - a_5\alpha + (a_6 - a_3)\alpha^2 + a_4\omega + (a_2 - a_5)\alpha\omega - a_3\alpha^2\omega$

$x \in \langle \sigma_2 \rangle^+ \iff a_2 = -a_5$, $a_6 - a_3 = a_3$, $a_5 = a_2 - a_5$, $a_6 = -a_3$

$\iff a_2 = a_3 = a_5 = a_6 = 0$

$\iff x = a_1 + a_4\omega$

$\Rightarrow \langle \sigma_2 \rangle^+ = \{ a_1 + a_4\omega \mid a_1, a_4 \in \mathbb{Q} \} = \mathbb{Q}(\omega)$

MATH 3202

17-11-17

Method 2: $\sigma_2(\omega)=\omega$ so $\omega \in \langle\sigma_2\rangle^+$

$\Rightarrow \mathbb{Q} \subseteq \mathbb{Q}(\omega) \subseteq \langle\sigma_2\rangle^+$

$\Rightarrow \mathbb{Q}(\omega) = \mathbb{Q}$ or $\mathbb{Q}(\omega) = \langle\sigma_2\rangle^+$

$\Downarrow$

$\omega \in \mathbb{Q}$ ※

$\therefore \langle\sigma_2\rangle^+ = \mathbb{Q}(\omega)$

$\langle\sigma_3\rangle^+ = \{x \in \mathbb{Q}(\alpha,\omega) : \sigma_3(x)=x\}$

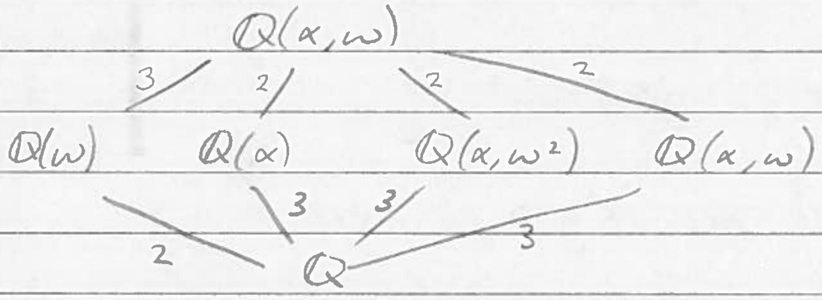
$= \mathbb{Q}(\alpha)$

$\langle\sigma_2\sigma_3\rangle^+ = \mathbb{Q}(\alpha\omega^2)$

$(\sigma_2\sigma_3)(\alpha\omega) = \sigma_2(\sigma_3(\alpha\omega)) = \sigma_2(\alpha\omega^2) = \alpha\omega\omega^2 = \alpha$

$(\sigma_2\sigma_3)(\alpha\omega^2) = \sigma_2(\sigma_3(\alpha\omega^2)) = \sigma_2(\alpha\omega) = \alpha\omega^2$

$\langle\sigma_2^2\sigma_3\rangle^+ = \mathbb{Q}(\alpha\omega)$


$\mathbb{Q}(\alpha,\omega)$
3
2
2
2
$\mathbb{Q}(\omega)$
$\mathbb{Q}(\alpha)$
$\mathbb{Q}(\alpha,\omega^2)$
$\mathbb{Q}(\alpha,\omega)$
2
3
3
3
$\mathbb{Q}$

? $\langle\sigma_2\rangle$ is the only normal subgroup

Example

$L=$ splitting field of $t^{13}-1$ over $\mathbb{Q}$

$\omega = e^{2\pi i/13}$

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

min poly of $\omega = m(t) = \dfrac{t^{13}-1}{t-1} = t^{12}+t^{11}+\dots+t+1$

m irreducible by putting $t=s+1$ then using Eisenstein $p=13$.

$[L,\mathbb{Q}]=12$, $G=\Gamma(L,\mathbb{Q})$, $|G|=12$.

$g \in G$ is determined by $g(\omega)$ and
$g(\omega)$ must be a root of m, i.e. $g(\omega) = \omega^i$
for some $1 \leq i \leq 12$.
Since $G = 12$ and these are the only possible 12
elements, these are all in G
$G = \{g_i : 1 \leq i \leq 12\}$ $\quad g_i(\omega) = \omega^i$.

$g_2(\omega) = \omega^2$
$g_2^2(\omega) = g_2(g_2(\omega)) = g_2(\omega^2) = g_2(\omega)^2 = (\omega^2)^2 = \omega^4$
$g_2^3(\omega) = \omega^8$
$g_2^4(\omega) = \omega^{16} = \omega^3$
$g_2^5(\omega) = \omega^6$
$g_2^6(\omega) = \omega^{12}$
Hence none of $g_2, \dots, g^6 = e$
$\therefore o(g_2) > 6 \Rightarrow o(g_2) = 12$
$g = g_2$
$G = \langle g ; g^{12} = e \rangle \quad g(\omega) = \omega^2$

Subgroups of G are $\langle g^i \rangle$, $i | 12$
$|\langle g^i \rangle| = 12/i$

$$\begin{tikzcd}
& \{e\} \arrow[dl, dash, "2"'] \arrow[dr, dash, "3"] & \\
\langle g^6 \rangle \arrow[d, dash, "2"'] \arrow[dr, dash] & & \langle g^4 \rangle \arrow[dl, dash, "2"] \\
\langle g^3 \rangle \arrow[dr, dash, "3"'] & \langle g^2 \rangle \arrow[d, dash, "2"] & \\
& G &
\end{tikzcd}$$

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

MATH 3202

17-11-17

$\langle g^3\rangle^+$, $g^3(\omega)=\omega^8$

$\alpha = \omega + g^3(\omega) + g^6(\omega) + g^9(\omega)$

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

$\alpha = \omega + \omega^8 + \omega^{12} + \omega^5$

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

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

$\Rightarrow$ ω satisfies $t^{12}+t^8+t^5+t-k=0$

contradicts min poly $= m(t)$.

$\therefore \langle g^3\rangle^+ = \mathbb{Q}(\alpha)$

$\langle g^6\rangle^+$, $g^6(\omega)=\omega^{12}$

$\beta = \omega + \omega^{12} \in \langle g^6\rangle^+$

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

$g^3(\beta) = g^3(\omega+\omega^{12}) = \omega^8+\omega^5 \neq \beta$

$\beta \notin \langle g^3\rangle^+$

similarly $\beta \notin \langle g^2\rangle^+$

$\therefore \langle g^6\rangle^+ = \mathbb{Q}(\beta)$

$\langle g^2\rangle^+$, $g^2(\omega)=\omega^4$

$\gamma = \omega + g^2(\omega) + g^4(\omega) + g^6(\omega) + g^8(\omega) + g^{10}(\omega)$

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

$\gamma = \omega + \omega^4 + \omega^3 + \omega^{12} + \omega^9 + \omega^{10}$

$\gamma \notin \mathbb{Q}$

$\therefore \mathbb{Q}(\gamma) = \langle g^2\rangle^+$

$$\gamma = \omega + \omega^3 + \cancel{\omega^4} + \omega^9 + \omega^{10} + \omega^{12}$$

$$\begin{aligned}\gamma^2 = {} & \omega^2 + \omega^6 + \omega^8 + \omega^5 + \omega^7 + \omega^{11} \\ & + 2(\cancel{\omega^4} + \omega^5 + \omega^{10} + \omega^{11} + \cancel{1}) \\ & + 2(\omega^7 + \omega^{12} + \cancel{1} + \cancel{\omega^2}) \\ & + 2(\cancel{1} + \omega + \omega^3) \\ & + 2(\omega^6 + \omega^8) + 2\cancel{\omega^9}\end{aligned}$$

$$\begin{aligned}\gamma^2 + \gamma &= 6 + 3\omega + 3\omega^2 + 3\omega^3 + 3\omega^4 + \dots + 3\omega^{12} \\ &= 3 + 3(1 + \omega + \dots + \omega^{12}) \\ &= 3\end{aligned}$$

$$\Rightarrow \gamma^2 + \gamma - 3 = 0$$

$$\gamma = \frac{-1 \pm \sqrt{1+12}}{2}$$

$$\Rightarrow \mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{13})$$

Soluble Groups Chapter 14

$$\begin{tikzcd}
L \arrow[r, leftrightarrow] \arrow[d, dash] & \{e\} \arrow[d, dash] \arrow[r, phantom, "\text{] cyclic}"] & {} \\
M \arrow[r, leftrightarrow] \arrow[d, dash] & H \arrow[d, dash] \arrow[r, phantom, "\text{] cyclic}"] & {} \\
K \arrow[r, leftrightarrow] & G &
\end{tikzcd}$$

normal

$$\Gamma(M:K) \cong \Gamma(L:K) / \Gamma(L:M)$$

G/H abelian

H abelian

Def 14.1

A group G is soluble if it has a finite chain of subgroups $\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G$ such that $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian.

$$\begin{tikzcd}
G_n = G \arrow[d, dotted, dash] \\
G_2 \arrow[d, dash] \arrow[r, phantom, "\text{] } G_2/G_1 \text{ abelian.}"] & {} \\
G_1 \arrow[d, dash] \\
\{e\} = G
\end{tikzcd}$$

MATH 3202

17-11-17

Examples

(i) an abelian group is soluble if G is abelian

$\{e\} = G_0 \leq G_1 = G$ and $G_1/G_0 = G$ is abelian

(ii) D_{2n} is soluble

$D_{2n} = \langle x, y : x^n = y^2 = e, \ yx = x^{-1}y \rangle$

$G_1 = \langle x \rangle = \{e, x, \dots, x^{n-1}\} \trianglelefteq D_{2n}$

$\{e\} \leq G_1 \leq D_{2n} = G$

$G_1 \cong C_n$ abelian

$G/G_1 \cong C_2$ abelian.

(iii) S_4 is soluble

$\{e\} \leq V \leq A_4 \leq S_4$

$V = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$

$|S_4| = 24$, $|A_4| = 12$, $|V| = 4$, $|\{e\}| = 1$

$|S_4/A_4| = 2$, $|A_4/V| = 3$, $|V/\{e\}| = 4$

$V \cong C_2 \times C_2$ abelian

$V \trianglelefteq A_4$, $A_4/V \cong C_3$

$A_4 \trianglelefteq S_4$, $S_4/A_4 \cong C_2$

(iv) S_5 is not soluble.

Theorem 14.4

The property of being soluble is closed under subgroups, quotient groups and extensions, i.e.

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

(ii) G soluble, $N \trianglelefteq G \Rightarrow G/N$ soluble

(iii) $N \trianglelefteq G$, N and G/N both soluble $\Rightarrow G$ soluble

$(0 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 0)$

Proof

(i) Suppose $\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G$ s.t. $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian.

$\{e\} = H_0 \leq H_1 = G_1 \cap H \leq \dots \leq H_n = G_n \cap H.$

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

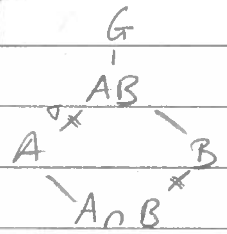
(let $g \in G_{i+1} \cap H$, then $g^{-1}H_i g \leq g^{-1}G_i g \leq G_i$ since $g \in G_{i+1}$ & $G_i \trianglelefteq G_{i+1}$.

Also, $g^{-1}H_i g \leq g^{-1}Hg \leq H$ since $g \in H$

$\therefore g^{-1}H_i g \leq G_i \cap H = H_i$)

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

[



$A \trianglelefteq G$, $B \leq G$

$$\frac{AB}{A} \cong \frac{B}{A \cap B}$$

]

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

$\frac{G_{i+1}}{G_i}$ is abelian, so $\frac{H_{i+1}}{H_i}$ is abelian.

$\therefore H$ soluble.

(ii) Suppose $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$ s.t. $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian. Suppose $N \trianglelefteq G$.

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

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

($g \in G_{i+1}$, $g^{-1}G_i N g = g^{-1}G_i g g^{-1} N g \leq G_i N$

$n \in N$, $n^{-1} g_i n' n = g_i \underbrace{g_i^{-1} n^{-1} g_i} \underbrace{n' n} \in G_i N$

By 3rd Isom Thm $\frac{G_i N}{N} \trianglelefteq \frac{G_{i+1} N}{N}$

$$\frac{G_{i+1}N/N}{G_i N/N} \cong \frac{G_{i+1}N}{G_i N} = \frac{G_{i+1}(G_i N)}{G_i N} \cong \frac{G_{i+1}}{G_i N \cap G_{i+1}} \cong \frac{G_{i+1}/G_i}{(G_i N \cap G_{i+1})/G_i}$$ abelian

$$\begin{tikzcd}
G \arrow[r] \arrow[d, dash] & G/N \arrow[d, dash] \\
B \arrow[r] \arrow[d, dash, "\ddagger" description] & B/N \arrow[d, dash, "\ddagger" description] \\
A \arrow[r] \arrow[d, dash] & A/N \arrow[d, dash] \\
N \arrow[r] & \{e\}
\end{tikzcd}$$

quotient of abelian group is abelian $\Rightarrow \frac{G_{i+1}N/N}{G_i N/N}$ is abelian

$\therefore G/N$ soluble.

17-11-17

(iii) N and G/N soluble.

$\{e\} = N_0 \leq N_1 \leq \dots \leq N_n = N$

$N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i abelian

$\{e\} = \frac{G_0}{N} \leq \frac{G_1}{N} \leq \dots \leq \frac{G_m}{N} = \frac{G}{N}$

$G_i/N \trianglelefteq G_{i+1}/N$ and $\frac{G_{i+1}/N}{G_i/N}$ abelian.

$\{e\} = N_0 \leq N_1 \leq \dots \leq N_n = N \leq G_1 \leq \dots \leq G_m = G$

each $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i abelian.

since $\frac{G_i}{N} \trianglelefteq \frac{G_{i+1}}{N} \Rightarrow G_i \trianglelefteq G_{i+1}$

and $\frac{G_{i+1}}{G_i} \cong \frac{G_{i+1}/N}{G_i/N}$ which is abelian

$\therefore$ G soluble.

□

20-11-17

Def

A group G is simple if there are no normal subgroups (apart from $\{e\}$ and G).

Result

If $n \geq 5$ then A_n is a simple group.

Proof

Omitted - see book if desired.

Result

If G is both simple and soluble, then $G \cong C_p$ for some prime p.

Proof

Let G be simple and soluble. Then we have

$\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G$, $G_{n-1} \trianglelefteq G$, G/G_{n-1} abelian.

Since G is simple, $G_{n-1} = \{e\}$,
so G is abelian.
Let $e \neq g \in G$, then $\langle g \rangle \trianglelefteq G$ and $\langle g \rangle \neq \langle e \rangle$
By simplicity $\langle g \rangle = G$, i.e. G is cyclic.
If G is not of prime order, then it has a non-trivial subgroup which is not normal.
$\therefore G \cong C_p$. □

Hence if G is not C_p and it is simple, it can't be soluble.
In particular A_n $(n \geqslant 5)$ is not soluble.
It follows that S_n is not soluble $(n \geqslant 5)$.

Fact

S_n is generated by $\tau = (1\,2)$, $\sigma (1 \dots n)$
Let $H = \langle \tau, \sigma \rangle$

$$(\sigma\tau\sigma^{-1})(1) = \sigma\tau(n) = \sigma(n) = 1$$
$$(\sigma\tau\sigma^{-1})(2) = \sigma\tau(1) = \sigma(2) = 3$$
$$(\sigma\tau\sigma^{-1})(3) = \sigma\tau(2) = \sigma(1) = 2$$
$$(\sigma\tau\sigma^{-1})(4) = \sigma\tau(3) = \sigma(3) = 4$$
$$\sigma\tau\sigma^{-1} = (2\ 3) \in H.$$

Continuing, all adjacent transpositions lie in H.
$\therefore H = S_n$

Cauchy's Thm

Let p be a prime, and suppose $p \mid |G|$. Then G contains an element of order p.

Proof

Apply Sylow's Theorem to get a subgroup H of G of order p^a $(a \geqslant 1)$.
All elements of H have order p^r $(r \geqslant 1)$ (not trivial elements)
Say $o(g) = p^r$, then $o(g^{p^{r-1}}) = p$.
□

MATH 3202

20-11-17

numbering different to book!

Solutions by radicals - Chapter 15

Idea: a polynomial equation $f(x) = 0$, $f(t) \in K[t]$ is soluble by radicals if you can express the roots in terms of the coefficients of f, using the basic field operations of $+, -, \times, \div$ and n^{th} roots.

e.g. $ax^2 + bx + c = 0$ is soluble by radicals since the roots are $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

We saw a similar but more complicated expression for the solution to a cubic, and the same can be done for a quartic.
What about quintics?

Def 15.1

An extension $L:K$ is called radical if $\exists \alpha_1, \ldots, \alpha_n \in L$ s.t. $L = K(\alpha_1, \ldots, \alpha_n)$ and for $i = 1, \ldots, n$ $\exists n_i \geq 1$ s.t. $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$.

i.e. $\alpha_1^{n_1} \in K$, $\alpha_2^{n_2} \in K(\alpha_1)$, $\alpha_3^{n_3} \in K(\alpha_1, \alpha_2)$, ...

$$\begin{tikzcd} L = K(\alpha_1, \ldots, \alpha_n) \arrow[d, dash, dotted] & \\ K(\alpha_1, \alpha_2) \arrow[d, dash] & \alpha_2^{n_2} \in K(\alpha_1) \\ K(\alpha_1) \arrow[d, dash] & \alpha_1^{n_1} \in K \\ K & \end{tikzcd}$$

e.g. $\sqrt[3]{2+\sqrt{3}} \cdot \sqrt[4]{7} + 2$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{2+\sqrt{3}})$

$\subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{2+\sqrt{3}}, \sqrt[4]{7})$

$\alpha \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{2+\sqrt{3}}, \sqrt[4]{7})$

Def 15.2

Let $f(t) \in K[t]$, $K \leq \mathbb{C}$. Then f is soluble by radicals if there exists M st. $M \supseteq \Sigma$, the splitting field of f over K and $M:K$ is radical.

i.e. all the roots of f lie in some radical extension of K.

Main result :

Theorem 15.3
If $K \leq L \leq M \leq \mathbb{C}$ and $M:K$ is radical, then $\Gamma(L:K)$ is soluble.

Proof : in a sequence of Lemmas.

Lemma 15.4
Suppose $L:K$ is radical and M is normal closure of L over K. Then $M:K$ is radical (inside $\mathbb{C}$).

Proof
Let $L = K(\alpha_1, \dots, \alpha_n)$, $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.
Let f_i = min poly of α_i over K, then M = splitting field of $f_1 \cdots f_n$ over K.
Let roots of f_i be $\alpha_i = \beta_{i1}, \beta_{i2}, \dots, \beta_{ir_i}$.
$M = K(\beta_{11}, \beta_{12}, \dots, \beta_{1r_1}, \beta_{21}, \dots, \beta_{2r_2}, \dots, \beta_{n1}, \dots, \beta_{nr_n})$ $(*)$
$K(\alpha_i) \cong K(\beta_{ij})$ since they have the same min poly f_i
By 11.4, $\exists \tau : M \to M$ s.t. τ is a K-aut and $\tau(\alpha_i) = \beta_{ij}$.
Now $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$
$\tau(\alpha_i)^{n_i} \in K(\tau(\alpha_1), \dots, \tau(\alpha_{i-1}))$.
Since τ is a K-aut of M, each $\tau(\alpha_k)$ is a root of f_k,
i.e. $\tau(\alpha_k) = \beta_{kt}$ for some t
$\beta_{ij}^{n_i} \in K(\beta_{1*}, \dots, \beta_{i-1,*}) \subseteq K(\beta_{11}, \dots, \beta_{1r_1}, \dots, \beta_{i-1,1}, \dots, \beta_{i-1,r_{i-1}})$
i.e. $(*)$ gives a radical sequence for M.

MATH 3202

24-11-17

Lemma 15.5

Let $K \leq \mathbb{C}$, $L =$ splitting field of $t^p - 1$ over $\overset{\leq K?}{\mathbb{Q}}$, p prime.
Then $\Gamma(L:K)$ is abelian.

Proof

Let $\omega = e^{2\pi i/p}$. Then $L = K(\omega)$ and any element g of $\Gamma(L:K)$ is determined by $g(\omega)$ and $g(\omega) = \omega^i$ for some i.
Let $g_i(\omega) = \omega^i$.
$(g_i g_j)(\omega) = g_i(\omega^j) = g_i(\omega)^j = \omega^{ij} = (g_j g_i)(\omega)$
Hence $g_i g_j = g_j g_i$, so $\Gamma(L:K)$ is abelian.
$\square$

Lemma 15.6

Let $K \leq \mathbb{C}$ and suppose $e^{2\pi i/n} \in K$.
Let $a \in K$ and let $L =$ splitting field of $t^n - a$ over K.
Then $\Gamma(L:K)$ is abelian.

Proof

Let α be any root of $t^n - a$ in L.
Then the other roots of $t^n - a$ are $\alpha\omega^i$ where $\omega = e^{2\pi i/n}$.
Since $\omega \in K$, $L = K(\alpha, \alpha\omega, \dots) = K(\alpha)$.
Any element g of $\Gamma(L:K)$ is determined by $g(\alpha)$ and $g(\alpha) = \alpha\omega^i$ for some i.
Let $g_i(\alpha) = \alpha\omega^i$
$(g_i g_j)(\alpha) = g_i(\alpha\omega^j) = g_i(\alpha)\, g_i(\omega)^j = \alpha\omega^i\omega^j = \alpha\omega^{i+j}$
Similarly $(g_j g_i)(\alpha) = \alpha\omega^{i+j}$
$\therefore g_i g_j = g_j g_i$
So $\Gamma(L:K)$ is abelian.
$\square$

Lemma 15.7

Let $L:K$ be a normal radical extension (in $\mathbb{C}$).
Then $\Gamma(L:K)$ is soluble.

Proof

We have $L = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$

W.l.o.g., all n_i are prime.

~~Write $n_1 = p$~~ In particular $\exists\, p$ prime st $\alpha_1^p \in K$.

Prove result by induction on n.

Let f be minimal poly of α_1 over K.

f has one root α_1 in L, so since L is normal, f splits in L.

$\partial f > 1$; let β be another root of f.

Then $(\alpha_1/\beta)^p = \alpha_1^p/\beta^p = 1$

[Both α_1 and β satisfy $f(t)$, which divides $t^p - (\alpha_1^p) \in K[t]$.]

$\alpha_1/\beta \neq 1$ and $(\alpha_1/\beta)^p = 1$

$\therefore$ α_1/β is a complex p^{th} root of unity.

$\therefore$ all p^{th} roots of unity are contained in L,

i.e. $t^p - 1$ splits in L.

Let $M = K(\omega)$ where $\omega = e^{2\pi i/p}$, M is the splitting field of $t^p - 1$ over K. Let $\alpha_1^p = a \in K$.

$$\begin{tikzcd}
L \arrow[d, dash] \\
M(\alpha_1) \arrow[d, dash, "\text{abelian (15.6)}"] \\
M = K(\omega) \arrow[d, dash, "\text{abelian (15.5) and normal } (t^p-1 \text{ splitting field})"] \\
K
\end{tikzcd}$$

normal since splitting field of $t^p - a$ over K

By Fundamental Theorem, $\Gamma(M:K) \cong \Gamma(M(\alpha_1):K) / \Gamma(M(\alpha_1):M)$

$$\begin{tikzcd}
L \arrow[d, dash] & \{e\} \arrow[d, dash] \\
M \arrow[d, dash, "\text{normal}"] & H \arrow[d, dash, "\triangleleft"] \\
K & G
\end{tikzcd}$$

$\Gamma(M:K)$ abelian so soluble; $\Gamma(M(\alpha_1):M)$ abelian so soluble

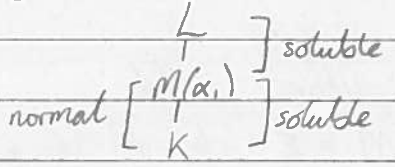
$\therefore$ $\Gamma(M(\alpha_1):K)$ is soluble $(14.4(3))$

$L : M(\alpha_1)$ is normal radical and $L = M(\alpha_1)(\alpha_2, \dots, \alpha_n)$ so

MATH 3202

24-11-17

by induction $\Gamma(L:M(\alpha_1))$ is soluble.



$$\underset{\text{soluble}}{\underset{\uparrow}{\Gamma(M(\alpha_1):K)}} \cong \Gamma(L:K) / \underset{\text{soluble}}{\underset{\uparrow}{\Gamma(L:M(\alpha_1))}}$$

$\therefore \Gamma(L:K)$ is soluble (14.4 (3))

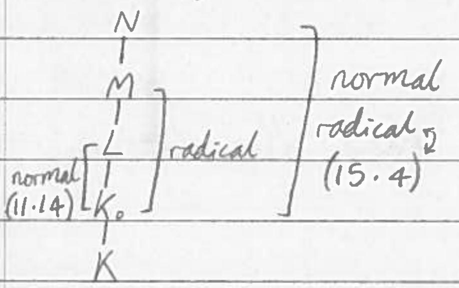
□

Thm 15.3

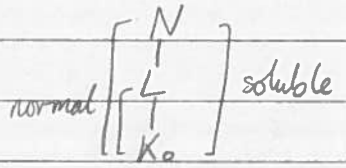
Suppose $K \leq L \leq M$ where $M:K$ is radical (in $\mathbb{C}$). Then $\Gamma(L:K)$ is soluble.

Proof

Let K_0 = fixed field of $\Gamma(L:K)$, and $N:K_0$ normal closure of $M:K_0$.



$N:K_0$ is radical and normal, so $\Gamma(N:K_0)$ is soluble (15.7)



By fundamental thm,

$$\Gamma(L:K_0) \cong \underset{\text{soluble.}}{\underset{\uparrow}{\Gamma(N:K_0)}} / \Gamma(N:L)$$

By 14.4 (2), $\Gamma(L:K_0)$ is soluble.

Finally $\Gamma(L:K) = \Gamma(L:K_0)$.

□

01-12-17

A quintic not soluble by radicals

1). Let $K \leq \mathbb{C}$, $f(t) \in K[t]$, Σ = splitting field
f is soluble by radicals if $\exists M \geq \Sigma$ s.t. $M:K$ is radical.
i.e. $M = K(\alpha_1, \dots, \alpha_p)$ where for each i, $\exists n_i$
s.t. $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$.

2). We proved that if $M:K$ is radical and
$K \leq L \leq M$ then $\Gamma(L:K)$ is soluble.
[G soluble if $\exists G_i \leq G$ s.t. $\{e\} \leq G_0 \leq G_1 \leq \dots \leq G_n = G$
s.t. $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelian]

$$\begin{tikzcd}
K(\alpha_1, \dots, \alpha_p) = L \arrow[d, dash, dotted] & \text{] abelian} \\
K(\alpha_1, \alpha_2) \arrow[d, dash] & \text{] abelian} \\
K(\alpha_1) \arrow[d, dash] & \text{] abelian} \\
K &
\end{tikzcd}$$

3). If f is soluble by radicals, then the Galois group is soluble.

4). S_5 not soluble

5). Hence if f has Galois group S_5, then f is not soluble by radicals.

Suppose $f \in K[t]$ is of degree n with roots $\sigma_1, \dots, \sigma_n$
and splitting field $\Sigma = K(\sigma_1, \dots, \sigma_n)$ and suppose
f is irreducible so the σ_i are distinct.

Let $G = \Gamma(\Sigma : K)$. Then any $g \in G$ is determined
by $g(\sigma_i)$ $(i = 1, \dots, n)$.
$g(\sigma_i)$ is a root of f, so $g(\sigma_i) = \sigma_j$ for some j.

01-12-17

$\therefore$ g induces a permutation of the roots.
We can regard G as a subgroup of S_n.

e.g. $f(t) = (t^2-2)(t^2-3)$ over $\mathbb{Q}$
$\sigma_1 = \sqrt{2}$, $\sigma_2 = -\sqrt{2}$, $\sigma_3 = \sqrt{3}$, $\sigma_4 = -\sqrt{3}$
$G = \{id, g, h, gh\}$
$g(\sqrt{2}) = \sqrt{2}$, $g(\sqrt{3}) = -\sqrt{3}$
$h(\sqrt{2}) = -\sqrt{2}$, $h(\sqrt{3}) = \sqrt{3}$
$g(\sigma_1) = \sigma_1$, $g(\sigma_2) = \sigma_2$, $g(\sigma_3) = \sigma_4$, $g(\sigma_4) = \sigma_3$
$\Rightarrow g \longleftrightarrow (3\ 4)$
$h \longleftrightarrow (1\ 2)$ similarly
$gh \longleftrightarrow (3\ 4)(1\ 2)$
$\therefore G \cong \{e, (3\ 4), (1\ 2), (3\ 4)(1\ 2)\}$

Let f be an irreducible quintic over $\mathbb{Q}$ with exactly 2 non-real roots σ_1, σ_2 which are conjugates. ($\sigma_3, \sigma_4, \sigma_5$ real roots)
Let Σ = splitting field, $G = \Gamma(\Sigma : K) \leq S_5$
Complex conjugation $c: \mathbb{C} \to \mathbb{C}$ is a $\mathbb{Q}$-aut.
Since $\Sigma : K$ is normal, $c|_\Sigma : \Sigma \to \Sigma$,
ie. $h = c|_\Sigma \in G$.
h switches the two complex roots and fixes the real roots, $h = (1\ 2) \in G$.
$[\mathbb{Q}(\sigma_1) : \mathbb{Q}] = 5$, so $5 \mid [\Sigma : K]$ by the tower law
$\Rightarrow 5 \mid |G| = [\Sigma, K]$.
By Cauchy's Theorem, G contains an element of order 5, ie a 5-cycle. W.l.o.g., this is $g = (1\ 2\ 3\ 4\ 5)$
$\therefore G \leq S_5$, $h = (1, 2)$, $g = (1\ 2\ 3\ 4\ 5) \in G$.
But $(1\ 2)$ and $(1\ 2\ 3\ 4\ 5)$ generate all of S_5
$\therefore G = S_5$
$\therefore f$ is not soluble by radicals

e.g. $f(x) = x^5 - 6x + 3$