3202 Galois Theory Notes

Based on the 2012 spring lectures by Dr M L Roberts

The Author has made every effort to copy down all the content on the board during lectures. The Author accepts no responsibility what so ever for mistakes on the notes or changes to the syllabus for the current year. The Author highly recommends that reader attends all lectures, making his/her own notes and to use this document as a reference only.

GALOIS THEORY

Evariste Galois 1811-1832

i) Establishes a 1-1 correspondence between extensions of ~~groups~~ fields and groups

ii) Analyses the questions of solving polynomials equations in terms of roots ("radicals") and in particular shows that quintic equations cannot be solved in radicals.

iii) Solves some classical geometrical problems such as trisecting the angle and dublicating the cube using ruler and compasses.

i) Fields and Groups

The Fundemental Theorem of Galois Theory associates to a field extension $K \subset F$ (e.g $\mathbb{R} \subseteq \mathbb{C}$) a group G called the Galois group of the extension and under certain conditions gives a 1-1 correspondence between fields L such that $K \subseteq L \subseteq F$ and subgroups of G

$$\begin{tikzcd}
L_1 \arrow[r, leftrightarrow] \arrow[d, phantom, "\cap|"] & H_1 \arrow[d, phantom, "\cup|"] \\
L_2 \arrow[r, leftrightarrow] & H_2
\end{tikzcd}$$

Won't look at this in any detail now, but note 2 things,

a) G is the group of automorphisms of F which fix K
(An automorphism φ of algebraic structure is a bijective map which preserves the structure; fixing K means $\varphi(k) = k \ \forall k \in K$)
Looking at the automorphism group is often a way of getting information about a structure (not just in this context).

b) More generally this is an example of attaching a group to some other structure (In this case a field extension)
This also appears in many other contexts ~~eg~~
eg. (co)-homology
This attaches to a geometrical object (eg surface) a group and the group tells you something about the surface

ii) Solving Polynomial Equations

$at + b = 0$ $\qquad t = -b/a$

$at^2 + bt + c = 0$ $\qquad t = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

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

$y = t + a/3$ change variables

$y^3 + py + q = 0$

$y = U + V$

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

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

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

we have a solution if $U^3 + V^3 + q = 0$ and $3UV + p = 0$

$U^3 + V^3 = -q$ $\qquad 3UV = -p$

$u = U^3 \quad v = V^3 \qquad u + v = -q \qquad 27uv = -p^3$

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

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

$u = \dfrac{-q \pm \sqrt{q^2 + 4p^3/27}}{2} \qquad U = \sqrt[3]{u}$

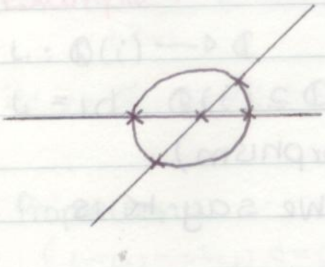
$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

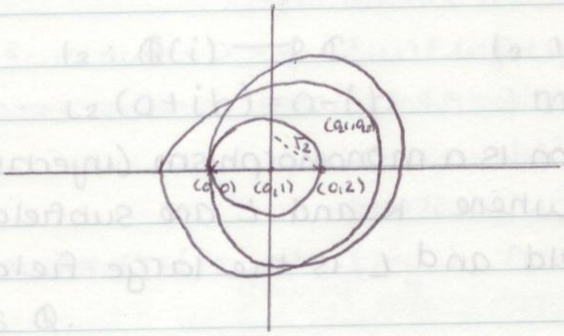
Similarly for quartic

Can all polynomial equations be solved in this way ie by radicals in particular, what about quintics?

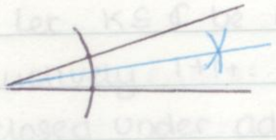
Galois Theory proves the answer is 'no'
Attach a field extension to the equation : show that the Galois group doesn't have a certain property : show that if equation is soluble by radicals, the field extension has the property (using the translation provided by the fundemental Theorem)

iii) Geometric problems.



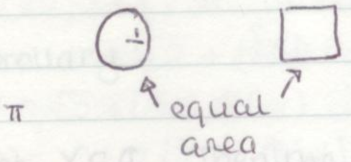


Q1)



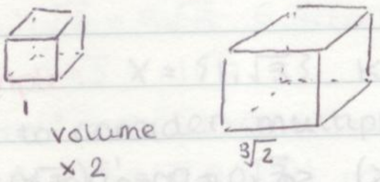
Bisect angle.
Can you trisect angle ?

Q2) Squaring the circle



ie is π constructable?

Q3) Duplicating the cube



ie is $\sqrt[3]{2}$ constructable?

using the idea of the degree of a field extension one can prove all these are impossible.

Handout 1.

Field Extensions

Definition:

A field extension is a monomorphism (injective, homomorphism) $\iota : K \longrightarrow L$, where K and L are subfields of $\mathbb{C}$. We say K is the small field and L is the large field.

Examples:

$$\left.\begin{aligned} \iota_1 &: \mathbb{Q} \longrightarrow \mathbb{R} \\ \iota_2 &: \mathbb{R} \longrightarrow \mathbb{C} \\ \iota_3 &: \mathbb{Q} \longrightarrow \mathbb{C} \end{aligned}\right\} \text{Inclusion maps.}$$

$f : \mathbb{Q} \longrightarrow P \qquad P = \{a+bi : a,b \in \mathbb{Q}\}. \quad (P = \mathbb{Q}(i))$

$a \longmapsto a \ (b=0)$

Need to check f is a monomorphism, ~~qu~~ trivial

Need to check $\mathbb{Q}$, P subfields of $\mathbb{C}$

$\mathbb{Q}$ obviously subfield

Need to check multiplicative inverse for P

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

We can usually identify K with its image $\iota(K)$, so ι is thought of as an inclusion map and K can be thought of as a subfield of L. We then use the notation $L : K$ (or $L|K$) for the extension and say that L is the extension of K.

*

Definition:

Let $X \subseteq \mathbb{C}$. Then the subfield of $\mathbb{C}$ generated by X is the intersection of all subfields of $\mathbb{C}$ that contain X.

This is equivalent to either of

1. The (unique) smallest subfield of $\mathbb{C}$ that contains X
2. The set of all elements ~~that~~ of $\mathbb{C}$ that can be obtained from elements of X by a finite sequence of field operations provided $X \neq \{0\}$ or $\emptyset$.

Example:

$\iota_1 : \mathbb{Q}(i) \longrightarrow \mathbb{C}$ $\qquad$ $\iota_2 : \mathbb{Q}(i) \longrightarrow \mathbb{C}$ $\qquad$ ι_2 is also a field

$\iota_1 = \mathrm{id}$ $\quad$ $\mathbb{Q}(i) \subseteq \mathbb{C}$. $\qquad$ $\iota_2(a+ib) = a - ib$ $\qquad$ monomorphism

Proposition:

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

Proof: Let $K \subseteq \mathbb{C}$ be a subfield. Then $0, 1 \in K$ by def^n.
So inductively $1+1+\ldots+1 = n \in K$ for every interger $n > 0$.
K is closed under addition, so $-n \in K \Rightarrow \mathbb{Z} \subseteq K$.
If $p, q \in \mathbb{Z}$ and $q \neq 0$, K closed under multiplication so $q^{-1} \in K$
so $pq^{-1} \in K \Rightarrow \mathbb{Q} \subseteq K$.

Corollary:

Let $X \subseteq \mathbb{C}$. Then the subfield of $\mathbb{C}$ generated by X contains $\mathbb{Q}$.

Notation: We denote the subfield of $\mathbb{C}$ generated by X by $\mathbb{Q}(X)$

Example: $X = \{1, \sqrt{3}\}$ $\quad$ $K \supseteq \mathbb{Q}$ $\quad$ $K = \{q + p\sqrt{3} \mid p, q \in \mathbb{Q}\}$
Need to consider multiplicative inverses

$$(q+p\sqrt{3})^{-1} = \frac{q-p\sqrt{3}}{q^2-3p^2}$$

$$\frac{(q+p\sqrt{3})(q-p\sqrt{3})}{q^2-p^2\sqrt{3}} = \frac{q^2-3p^2}{q^2-3p^2} = 1 \quad \text{subfield}$$

$K = \mathbb{Q}(\sqrt{3})$.

Definition:

If $L : K$ is a field extension and Y is a subset of L, then the subfield of $\mathbb{C}$ generated by $K \cup Y$ is written $K(Y)$ and is said to be obtained from K by adjoining Y.

Example: $K(\omega)$, $K = \mathbb{Q}$ $\quad$ $\omega = e^{2\pi i/3}$ $\quad$ $\omega^3 = 1$
$\alpha = p + q\omega + r\omega^2$
$L = K(Y)$

Want to show L is a subfield of $\mathbb{C}$

L closed - $\alpha = p+q\omega+r\omega^2$, $\beta = a+b\omega+c\omega^2$

$\alpha+\beta \in L$, $\alpha\beta \in L \Rightarrow L$ closed

$\forall \alpha \in L \ \exists \alpha^{-1} \in L$

Consider $p+q\omega$ instead

$(\omega^3=1, \omega^3-1=0, \underset{\neq 0}{(\omega-1)}(\omega^2+\omega+1)=0 \Rightarrow \omega^2+\omega+1=0 \Rightarrow \omega^2=-\omega-1)$

$$(p+q\omega)(p+q\omega^2) = p^2+pq\omega+pq\omega^2+q^2$$
$$= p-pq+q^2$$

$$\Rightarrow (p+q\omega)^{-1} = \frac{p+q\omega^2}{\underset{\neq 0}{p^2-pq+q^2}} = A+B\omega$$

OR $\mathbb{Q}(\omega) = \mathbb{Q}(-1/2-\sqrt{3}/2\, i) = \mathbb{Q}(\sqrt{-3})$ (since $1/2, 2 \in \mathbb{Q}$)

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

Rational Expressions

eg. $\dfrac{t^2+1}{t^3+1}$

If R is an intergral domain then there is a method of constructing a field of fractions of R ie. a monomorphism $\varphi : R \rightarrow Q$ such that $\forall q \in Q$ $q = \varphi(r)/\varphi(s)$ for some $r,s \in R$.

eg. $\mathbb{Z} \rightarrow \mathbb{Q} = \{a/b : a,b \in \mathbb{Z}\ b \neq 0\}$

In general, let $S = R \times R \setminus \{0\} = \{(a,b) : a,b \in R, b \neq 0\}$ and define $(a,b) \sim (a',b')$ if $ab' = a'b$

Let $\mathbb{Q} = \{[(a,b)]\}$ = set of equivalence classes

Define $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ etc.

$K[t] = \{a_0 + a_1 t + \dots + a_n t \mid a_n \in K\}$

$K(t)$ = field of fractions of $K[t]$

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

$K[t_1 \dots t_n]$ eg $t_1^2 + t_2^3 - t_1 t_2$ etc

$K(t_1 \dots t_n)$ field of fractions of $K[t_1 \dots t_n]$

Chapter 5: Simple extensions.

$f(t) = \frac{t^2}{t^2-1} \in \mathbb{Q}(t)$

$\forall \alpha \in \mathbb{Q},\ \alpha \neq 1, -1$ $f(\alpha)$ makes sense.

Simple Extensions

Definition:

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

eg. By def^n $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$ is simple

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

Let $\alpha = \sqrt{2} + \sqrt{3}$. What is $\mathbb{Q}(\alpha)$?

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

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

$\alpha^3 = (\sqrt{2}+\sqrt{3})(5+2\sqrt{6})$

$= 5\sqrt{2} + 5\sqrt{3} + 4\sqrt{3} + 6\sqrt{2}$

$= 11\sqrt{2} + 9\sqrt{3} \in \mathbb{Q}(\alpha)$

$11\alpha = 11\sqrt{2} + 11\sqrt{3}$

$11\alpha - \alpha^3 = 2\sqrt{3} \in \mathbb{Q}(\alpha)$

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

$\mathbb{Q}(\sqrt{2}+\sqrt{3})$ = smallest subfield containing $\mathbb{Q}, \sqrt{2}, \sqrt{3}$.

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

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

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

Q Are all extensions simple? No

eg $\mathbb{Q}(t_1, t_2) : \mathbb{Q}$ is not simple

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

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

Definition:

An isomorphism between two field extensions $i: K \to \hat{K}$ and $j: L \to \hat{L}$ is a pair λ, μ of isomorphisms $\lambda: K \to L$, $\mu: \hat{K} \to \hat{L}$ such that $\forall k \in K \quad j(\lambda(k)) = \mu(i(k))$

$$\begin{tikzcd}
i(k) \arrow[rrr] & & & \mu(i(k)) \\
& \hat{K} \arrow[r, "\cong", "\mu"'] \arrow[d] & \hat{L} \arrow[d] & j(\lambda(k)) \\
& K \arrow[r, "\cong", "\lambda"'] & L & \\
k \arrow[uuu] \arrow[rrr, mapsto] & & & \lambda(k) \arrow[uu]
\end{tikzcd}$$

"commutative diagram"

Identify K with $i(K)$ and L with $i(L)$

$$\begin{tikzcd}
\hat{K} \arrow[r, "\mu"] & \hat{L} \\
K \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\lambda"] & L \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

$\mu|_K = \lambda$

If we identify K and L

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

$\mu|_K = id$

eg. $\mu: \mathbb{Q}(i) \to \mathbb{Q}(i)$

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

$\mu|_{\mathbb{Q}} = id$

Chapter 5: Simple extensions.

Algebraic and Transcendental Extensions

There are two distinct types of simple extensions.

Definition:

Let K be a subfield of $\mathbb{C}$ and let $\alpha \in \mathbb{C}$. Then α is algebraic over K if there exists a non-zero polynomial over K such that $p(\alpha) = 0$. Otherwise, α is transcendental.

Note: We shorten algebraic over $\mathbb{Q}$ to algebraic and transcendental over $\mathbb{Q}$ to transcendental.

Example:

1. The number $\alpha = \sqrt{2}$ is algebraic (over $\mathbb{Q}$) because $\alpha^2 - 2 = 0$
2. The number $\alpha = \sqrt[3]{2}$ is algebraic because $\alpha^3 - 2 = 0$
3. π is transcendental (proof later)
4. $\alpha = \sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$ because $\alpha^2 - \pi = 0$
5. $\alpha = \sqrt{\pi}$ is transcendental over $\mathbb{Q}$

Suppose $p(\sqrt{\pi}) = 0$, $p(t) \neq 0$

$$p(\sqrt{\pi}) = \underbrace{a(\pi)}_{\text{even degree}} + \underbrace{\sqrt{\pi}\, b(\pi)}_{\text{odd degree}} = 0$$

$$a(\pi) = -\sqrt{\pi}\, b(\pi)$$

$$a^2(\pi) = \pi\, b^2(\pi)$$

$$a^2(\pi) - \pi^2 b^2(\pi) = 0$$

$\Rightarrow f(\pi) = 0$ for $f(t) = \underbrace{a^2(t)}_{\text{even}} - \underbrace{t^2 b(t)}_{\text{odd}} \neq 0$

$\Rightarrow$ π is algebraic, contradiction

Theorem:

$K(t)$, the field of rational expressions of $K[t]$ is a simple transcendental extension of $K \subseteq \mathbb{C}$.

Proof: $K(t):K$ is clearly a simple extension generated by t.
p, polynomial over K st $p(t)=0$
$p=0$ by $\det^n$ of $K(t)$, so it is transcendental.

The Minimal Polynomial

Definition:

A polynomial $f(t) = a_0 + a_1 t + \ldots + a_n t^n$ over a subfield K of $\mathbb{C}$ is monic if $a_n = 1$.

Clearly, every polynomial is a constant multiple of some monic polynomial and for a non-zero polynomial this monic polynomial is unique.

Suppose that $K(\alpha):K$ is a simple algebraic extension.
There is a polynomial p over K such that $p(\alpha)=0$. We may ~~assume~~ suppose that p is monic.
Therefore there exists at least one monic polynomial of smallest degree that has α as a zero.
We claim p is unique.
Suppose p, q are two such polynomials.
Then $p(\alpha) - q(\alpha) = 0$, so if $p \neq q$ then some constant multiple of $p-q$ is a monic polynomial with α as a zero, contrary to the definition.

Definition:

Let $L:K$ be a field extension and suppose that $\alpha \in L$ is algebraic over K. Then the minimal polynomial of α over K is the unique monic polynomial m over K of smallest degree such that $m(\alpha)=0$

Example: $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$
$m(t) = t^2+1$ m is monic
$m(i) = i^2+1 = 0$
are there are ~~pa~~ monic polynomials ~~st~~ of smaller degree st
i is a zero.
$t+r$, 1 are only options (if minimal polynomial $\Rightarrow i \in \mathbb{R}$)
$\Rightarrow$ minimal polynomial of i over $\mathbb{R}$ is $m(t) = t^2+1$.

Lemma:

If α is algebraic over $K \subseteq \mathbb{C}$ subfield, then m_α is irreducible over K. m_α divides every polynomical of which α is a zero.

Proof: suppose m_α is reducible, $m=fg$, $\partial f < \partial m$, $\partial g < \partial m$
assume f, g are monic
$m(\alpha)=0$, $f(\alpha)g(\alpha)=0$
$\Rightarrow f(\alpha)=0$ or $g(\alpha)=0$
contradiction to definition of m_α.
Let p be a polynomial over K st $p(\alpha)=0$
$\exists$ polynomials q, r st $p=qm+r$ $\partial r < \partial m$
$p(\alpha) = q(\alpha)m(\alpha)+r(\alpha) = 0 \Rightarrow r(\alpha)=0$
If $r \neq 0$, contradiction
$\Rightarrow r=0$, $\Rightarrow p=qm \Rightarrow m|p$.

Theorem

$K \subseteq \mathbb{C}$ subfield and m is irreducible, monic polynomial over K.
Then $\exists\, \alpha \in \mathbb{C}$ such that α is algebraic over K and m is minimal polynomial of α.

Proof: Let $\alpha \in \mathbb{C}$ such that $m(\alpha)=0 \Rightarrow m_\alpha | m$ but m monic irreducible $\Rightarrow m_\alpha = m$.

It turns out that finding the minimal polynomial of some α is a fundemental bit of calculation. This tells us ~~that~~ what to do: ~~to~~ find some polynomial f such that $f(\alpha)=0$ and check for irreducibility.

If f is irreducible then f is the minimal polynomial.
If not factorise to get ~~polyng~~ polynomial g of smaller degree such that $g(\alpha)=0$

Example: Minimal polynomial $\sqrt[3]{2}$ over $\mathbb{Q}$
$\alpha = \sqrt[3]{2}$
$\alpha^3 - 2 = 0$
$f(t) = t^3 - 2$, $f(\alpha) = 0$
f irreducible (eisenstiens prime 2) so f is minimal polynomial

Example: Minimal polynomial $\alpha = i + \sqrt{2}$ over $\mathbb{Q}$
$\alpha^2 = -1 + 2 + 2i\sqrt{2}$
$\alpha^2 - 1 = 2i\sqrt{2}$
$(\alpha^2 - 1)^2 = -8$
$\alpha^4 - 2\alpha^2 + 9 = 0$
If $f(t) = t^4 - 2t^2 + 9$, $f(\alpha) = 0$
Clearly no linear factors since roots are $\pm i \pm \sqrt{2}$
Quadradic factor would have to be of the form
$(t^{\cancel{2}} + (\cancel{3} \pm i \pm \sqrt{2}))(t^{\cancel{2}} - (\pm i \pm \sqrt{2}))$
Check this never $\in \mathbb{Q}[t]$ (look at coeffs of t and constants)
$\therefore$ f irreducible, so f minimal polynomial.

Recall:

R ring, $I \underset{\text{ideal}}{\underset{\uparrow}{\Delta}} R$

$r_1, r_2 \in I \Rightarrow r_1 - r_2 \in I$
$r_1 \in I, r \in R \Rightarrow r_1 r \in I$
eg. $6\mathbb{Z} \,\Delta\, \mathbb{Z}$

If $r \in R$ then $rR = \{rs : s \in R\} \,\Delta\, R$

The quotient ring R/I has elements which are cosets
$I + r = \{i + r : i \in I\}$
$(I+r) + (I+s) = I + (r+s)$
$(I+r)(I+s) = I + rs$

Why do these operations make sense?

$I+r = I+r'$ (eg $6\mathbb{Z}+1 = 6\mathbb{Z}+7$)

$\Leftrightarrow i'+r' = i+r$

$r' = i'-i+r$

$r'-r = i'-i \in I$

Hence $I+r = I+r'$, $I+s = I+s'$ then

$(r'+s')-(r+s) = (r'-r)+(s'-s) \in I$

$I+(r'+s') = I+(r+s)$ ∴ addition is well defined.

Similarly $r's'-rs = r's-r's+r's-rs$

$= r'(s'-s)+(r'-r)s \in I$

∴ $I+rs = I+r's'$ multiplication is well defined.

Check ring axioms.

The zero is $I+0 = I$.

Example: $\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 6\mathbb{Z}+1, 6\mathbb{Z}+2, 6\mathbb{Z}+3, 6\mathbb{Z}+4, 6\mathbb{Z}+5\}$

$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, 5\}$

$\bar{4} \times \bar{3} = (6\mathbb{Z}+4)(6\mathbb{Z}+3)$

$= 6\mathbb{Z}+12 = 6\mathbb{Z} = \bar{0}$

There is a ring homomorphism $\varphi : R \to R/I$ given by $\varphi(r) = I+r$

eg: $\varphi : \mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ sends a to $a \bmod 6$

$5 \mapsto \bar{5}$

$11 \mapsto \bar{5}$

$\operatorname{Ker} \varphi = I$.

It is useful to have a unique way of representing elements in R/I as $I+r$.

eg. for $\mathbb{Z}/6\mathbb{Z} = \{\tilde{0}, 1, 2, 3, 4, 5\}$.

Lemma:

Let $m \in K[t]$. Then each element of $K[t]/(m)$ ($(m) = mK[t]$) can be written uniquely as $(m)+f(t)$, where $\partial f < \partial m$

eg. $\mathbb{R}[t]/(t^2+1) = \{(t^2+1)+at+b : a,b \in \mathbb{R}\}$

$= \{\overline{at+b} : a,b \in \mathbb{R}\} \cong \mathbb{C}$

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

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

$= \overline{3t+1}$

Proof: Let $(m)+f(t)$ be any element of $K[t]/(m)$.

Write $f(t) = m(t)+q(t)+r(t) \quad \partial r < \partial m$

Then $(m)+f(t) = (m)+r(t)$, ie every coset is of required form.

Suppose $(m)+f(t) = (m)+g(t)$ where $\partial f, \partial g < \partial m$

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

$\underbrace{f(t)-g(t)}_{\deg < \partial m} = m(t)s(t) \quad \Rightarrow s(t)=0$

$\Rightarrow f(t) = g(t)$.

Theorem:

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

Proof: $\Leftarrow$ Suppose m is irreducible. Let $0 \neq (m)+f \in K[t]/(m)$

Them ~~m/~~ $m \nmid f$. Since m is irreducible, this means m and f are coprime.

By Thm 3.9 (book) $\exists\, r(t), s(t) \in K[t]$ st $m(t)r(t)+f(t)s(t) = 1$

Then $((m)+f)((m)+s) = (m)+fs = (m)+1$

ie $\bar{f}\bar{s} = \bar{1}$

$\Rightarrow$ suppose $m(t) = f(t)g(t)$

Then $\bar{0} = (m)+m = ((m)+f)((m)+g) = \bar{f}\bar{g}$

Since $K[t]/(m)$ is a field, $\bar{f} = \bar{0}$ or $\bar{g} = \bar{0}$

ie $f(t) \in (m)$ or $g(t) \in (m)$

$\therefore$ Factorisation $m = fg$ is trivial

Classifying simple extensions

Theorem:

Any simple transcendental extension $K(\alpha):K$ is isomorphic to $K(t):K$ with an isomorphism $\phi: K(t) \rightarrow K(\alpha)$ such that

$\varphi(t) = \alpha$ and $\varphi|_K = id$.

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

Proof: define $\varphi(f(t)/g(t)) = f(\alpha)/g(\alpha)$
This is well defined [since α is transendental, $g(\alpha) \neq 0$] and is a ring homomorphism and $\varphi(k) = k$, $\forall k \in K$.
$\varphi(f(t)/g(t)) = 0 \Rightarrow f(\alpha)/g(\alpha) = 0 \Rightarrow f(\alpha) = 0 \Rightarrow f = 0$
So $\ker\varphi = \{0\}$ and φ is injective.
φ is also surjective (since any element of $K(\alpha)$) is of the form $f(\alpha)/g(\alpha)$), $\varphi(t) = \alpha$.
This φ is in the required form.

Theorem:

Let $K(\alpha):K$ be a simple algebraic extension. Let $m(t)$ be minimal polynomial of α over K. Then $\exists$ an isomorphism $\varphi: K[t]/(m) \rightarrow K(\alpha)$ st $\varphi(\bar{t}) = \alpha$ and $\varphi|_K = id$.

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

eg.
$$\begin{tikzcd}
\mathbb{R}[t]/(t^2+1) \arrow[r, "\varphi", "\varphi(\overline{at+b}) = ai+b"'] \arrow[d, dash] & \mathbb{R}(i) = \mathbb{C} \arrow[d, dash] \\
\mathbb{R} \arrow[r, "id"'] & \mathbb{R}
\end{tikzcd}$$

Proof: Define $\varphi: K[t]/(m) \rightarrow K(\alpha)$ by $\varphi(\bar{f}) = f(\alpha)$
This is well defined: if $\bar{f} = \bar{g}$ ie $(m)+f = (m)+g$, then $g-f \in (m)$ say $g(t) - f(t) = m(t)r(t)$: Then $g(\alpha) - f(\alpha) = m(\alpha)r(\alpha) = 0$ so $f(\alpha) = g(\alpha)$.
clearly ring homomorphism and is injective
(if $\varphi(f) = 0$, the $f(\alpha) = 0$, so f is multiple of m, so $\bar{f} = \bar{0}$).
Then $\mathrm{Im}\varphi$ is a subfield of $K(\alpha)$ (since $K[t]/(m)$ is a field) and it contains K and $\alpha = \varphi(\bar{t})$

By definition $K(\alpha) = \mathrm{Im}\,\varphi$.
ie φ is an isomorphism with required properties.

Since every element of $K[t]$ is [illegible] uniquely of the form $(m) + f(t)$ $\partial f < \partial m (= n)$ ie. ~~any~~ $a_0 + a_1 t + \dots + a_{n-1} t^{n-1}$ any element of $K(\alpha)$ is uniquely of the form $a_0 + a_1 \alpha + \dots + a_{n-1} \alpha^{n-1}$.

[c.f $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, we showed this directly by showing $(a+b\sqrt{2})^{-1}$ is of the form $x + y\sqrt{2}$, but it now follows immediately from the result]

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

Corollary:

Suppose α and β have the same minimum polynomial over K
Then $\exists$ an isomorphism $\varphi : K(\alpha) \longrightarrow K(\beta)$ st $\varphi_K = \mathrm{id}$ and $\varphi(\alpha) = \beta$.

$$\begin{tikzcd}
K(\alpha) \arrow[r, "\overset{\varphi}{\cong}", "\varphi(\alpha)=\beta"'] & K(\beta) \\
K \arrow[u, dash] \arrow[r, "\mathrm{id}"] & K \arrow[u, dash]
\end{tikzcd}$$

eg. $\alpha = \sqrt[3]{2}$ $\beta = \sqrt[3]{2}\,\omega$ $\omega = e^{2\pi i/3}$
α and β both have the minimal polynomial $t^3 - 2$
$\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$
$\alpha \mapsto \beta$
$q \mapsto q$

Lemma:

Let α be algebraic over K, with minimal polynomial m of degree n.
Then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a K-basis for $K(\alpha)$
ie every element of $K(\alpha)$ can be written uniquely as
$k_0 + k_1\alpha + \dots + k_{n-1}\alpha^{n-1}$ $(k_i \in K)$

Proof: Restatement of previous lemma.

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

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

$\omega = e^{2\pi i/3}$

$\omega^3 = 1$

$\omega^3 - 1 = 0$

$(\omega - 1)(\omega^2 + \omega + 1) = 0$

so min poly $t^2 + t + 1$

$\mathbb{Q}(\omega) = \{a + b\omega : a, b \in \mathbb{Q}\}$ ← unique

$= \{a + b\omega + c\omega^2 : a, b, c \in \mathbb{Q}\}$.

Definition:

Let $i : K \to L$ be a field $\overset{\text{mono}}{\text{isomorphism}}$. Then there exists an $\overset{\text{mono}}{\text{isomorphism}}$ $\hat{i} : K[t] \to L[t]$ given by $\hat{i}(a_0 + a_1 t + \dots + a_n t^n) = i(a_0) + i(a_1)t + \dots + i(a_n)t^n$

Usually write i instead of $\hat{i}$

Theorem:

Suppose $K, L \in \mathbb{C}$, $i : K \to L$ is an isomorphism. Let $K(\alpha) : K$ and $L(\beta) : L$ be simple algebraic extensions ~~and~~ st $\hat{i}(m_\alpha) = m_\beta$, where m_α and m_β are the minimal polynomials of α and β respectively. Then $\exists$ an isomorphism $j : K(\alpha) \to L(\beta)$ st $j(\alpha) = \beta$ and $j|_K = i$

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

Proof: $$\begin{tikzcd}
K[t] \arrow[r, "\hat{i}"] \arrow[rr, bend right, "\phi"'] & L[t] \arrow[r, "\pi"] & L[t]/(m_\beta)
\end{tikzcd}$$

ϕ is a surjective homomorphism

$\operatorname{Ker}\phi = \{f(t) \in K[t] : \phi(f) = 0\}$

$= \{f(t) \in K[t] : \cancel{\phi}\,\pi(i(f)) = 0\}$

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

$= \{f(t) \in K[t] : f = m_\alpha(t) s(t)\} = (m_\alpha) \cancel{\}}$

1st isomorphism theorem: $K[t]/\ker\varphi \cong \operatorname{Im}\varphi$

$K[t]/(m_\alpha) \underset{\psi}{\cong} L[t]/(m_\beta)$ $\qquad \psi(\bar{t}) = \bar{t}$

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

$$\begin{tikzcd}
K(\alpha) & K[t]/(m_\alpha) \arrow[l, "\delta"', "\alpha \leftarrow \bar{t}"] \arrow[r, "\psi", "\bar{t} \mapsto t"'] & L[t]/(m_\beta) \arrow[r, "\varepsilon", "\bar{t} \mapsto \beta"'] & L(\beta) \\
K \arrow[u, dash] \arrow[r, "id"] & K \arrow[u, dash] \arrow[r, "i"] & L \arrow[u, dash] \arrow[r, "id"] & L \arrow[u, dash]
\end{tikzcd}$$

Let $j = \varepsilon\psi\delta^{-1} : K(\alpha) \rightarrow \overset{L}{\cancel{K}}(\beta)$

$j(\alpha) = \varepsilon\psi\delta^{-1}(\alpha) = \varepsilon\psi(\bar{t}) = \varepsilon(\bar{t}) = \beta$

$j|_K = id\, i\, id = i$

j is required isomorphism

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

$i(a+b\sqrt{2}) = a - b\sqrt{2}$

Consider $\alpha = \sqrt{3}$, $\beta = \sqrt{3}$

$m_\alpha = t^2 - 3$ $\quad m_\beta = t^2 - 3$

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

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

ie $\exists$ an isomorphism $j : \mathbb{Q}(\sqrt{2},\sqrt{3}) \hookrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3})$ st $j(\sqrt{3}) = -\sqrt{3}$

$j(\sqrt{2}) = -\sqrt{2}$

j is in fact an element of the Galois group of $\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})$

DEGREE!

Theorem:

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

Proof: We have addition on L : $l_1 + l_2$

If $\lambda \in K$, $l \in L$ then $\lambda l \in L$ using field multiplication.

Easy check that normal vector space rules apply.

To get a vector space we just 'forget' some of the structure.

Definition :

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

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

$\mathbb{Q}(\sqrt{2})$ has a basis over $\mathbb{Q} = \{1, \sqrt{2}\}$ so $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Theorem : (Short Tower Law)

If K, L, M are subfields of $\mathbb{C}$ and $K \subseteq L \subseteq M$ then

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

Proof : Let $[M : L] = d$, $[L : K] = e$

ie $\{x_1, \ldots, x_d\}$ basis for M ~~over M~~ as a vector space over L

$\{y_1, \ldots, y_e\}$ basis for L as a vector space over K

Want to show $\{x_i y_j\}_{\substack{1 \le i \le d \\ 1 \le j \le e}}$ is a basis for M as a vector space over K.

Need to prove Linear independence and spanning.

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

$$\sum_j \underbrace{\left(\sum_i k_{ij} x_i\right)}_{\in L} \underbrace{y_j}_{LI} = 0$$

$$\Rightarrow \sum_i \underbrace{k_{ij}}_{\in M} \underbrace{x_i}_{LI} = 0$$

$$\Rightarrow k_{ij} = 0$$

Span: $x \in M$ can be written $x = \sum_j \lambda_j y_j$ $\lambda_j \in L$

But $\lambda_j = \sum_i \lambda_{ij} x_i$ $\lambda_{ij} \in K$.

$$\Rightarrow x = \sum_{i,j} \lambda_{ij} x_i y_j$$

Example : $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$

have already shown that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Want to show $\{1, i\}$ is a basis for $\mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}(\sqrt{2})$.

Span: $\mathbb{Q}(i, \sqrt{2}) = a + bi + c\sqrt{2} + di\sqrt{2}$

$$= \underbrace{(a + c\sqrt{2})}_{\in \mathbb{Q}(\sqrt{2})} + \underbrace{(b + d\sqrt{2})}_{\in \mathbb{Q}(\sqrt{2})} i$$

$LI: a+c\sqrt{2}+(b+d\sqrt{2})i=0$

$\Rightarrow a+c\sqrt{2}=0, \quad b+d\sqrt{2}=0$

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

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

$$\begin{tikzcd} \mathbb{Q}(\sqrt{2},i) \arrow[d, dash, "\{1,i\}"] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "\{1,\sqrt{2}\}"] \\ \mathbb{Q} \end{tikzcd}$$

$$\{1\times 1, 1\times\sqrt{2}, i\times 1, i\times\sqrt{2}\} = \{1, \sqrt{2}, i, i\sqrt{2}\}$$

Note: The tower law is analagous to Legrange's theorem
$|G/M| = |G/N||N/M|$

Corollary:

If $K_0 \subseteq K_1 \subseteq \dots \subseteq K_n$ are subfields of $\mathbb{C}$, then
$[K_n:K_0] = [K_n:K_{n-1}][K_{n-1}:K_{n-2}]\dots[K_1:K_0]$

Proof: Induction on n.

Proposition:

Let $K(\alpha):K$ be a simple extension. If it is transcendental, then $[K(\alpha):K]=\infty$. If it is algebraic, then $[K(\alpha):K]=\partial m_\alpha$

Proof: If $K(\alpha):K$ is transcendental
claim: The set $\{1,\alpha,\dots,\alpha^n\}$ is LI over K for any $n\in\mathbb{N}$
Proof of claim: Assume $\{1,\alpha,\dots,\alpha^n\}$ is not LI over K.
ie $\exists\ k_i\in K$ (not all $k_i=0$) st $k_0+k_1\alpha+\dots+k_n\alpha^n=0$
$\Rightarrow \alpha$ is root of $k_0+k_1t+\dots+k_nt \neq 0$
contradiction.
So $\{1,\alpha,\dots,\alpha^n\}$ lies in $K(\alpha)$ and is LI $\forall n\in\mathbb{N}$.
Since n arbitrary, this means we can find an arbitrary large set in $K(\alpha)$ which is LI.
$\Rightarrow [K(\alpha):K] > n\ \forall n\in\mathbb{N}$
$\Rightarrow [K(\alpha):K]=\infty$

If $K(\alpha):K$ is algebraic, then by Lemma 5.14 $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K where n is the degree of m_α over K. So $[K(\alpha):K] = \partial m_\alpha$.

Example: Find $[\mathbb{Q}(i+\sqrt{3}):\mathbb{Q}]$

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

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

$\alpha^2 - 2 = 2i\sqrt{3}$

$(\alpha^2-2)^2 = -12$

$\alpha^4 - 4\alpha^2 + 16 = 0$

Let $f(t) = t^4 - 4t^2 + 16$

f monic, $f(\alpha)=0$ Need to show f is irreducible over $\mathbb{Q}$.

~~Let $y=t^2$ $y^2-4y+16=0$~~

~~$t^2 = y = 4 \pm \sqrt{16-4\cdot 16}$~~

roots of $f(t)$ are $\pm\sqrt{3} \pm i \in \mathbb{Q}$ so no linear factors in $\mathbb{Q}$

Quadratic factors would have to be of the form

$(t - (\pm\sqrt{3}\pm i))(t-(\pm\sqrt{3}\pm i))$ this is not possible in $\mathbb{Q}[t]$.

$\Rightarrow f(t)$ irreducible.

$f(t) = m_\alpha$

$\partial f = 4 \Rightarrow [\mathbb{Q}(i+\sqrt{2}):\mathbb{Q}] = 4$

Alternative method:

Claim: $\mathbb{Q}(i+\sqrt{3}) = \mathbb{Q}(i,\sqrt{3})$ check

$(i+\sqrt{3})^{-1} = \frac{1}{i+\sqrt{3}} \times \frac{i-\sqrt{3}}{i-\sqrt{3}} = \frac{i-\sqrt{3}}{-1-3} = \frac{1}{4}(\sqrt{3}-i)$?

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

$m = t^2+1$ min polynomial for i over $\mathbb{Q}$

$\Rightarrow [\mathbb{Q}(i):\mathbb{Q}] = 2$

$p = t^2 - 3$ is min polynomial for $\sqrt{3}$ over $\mathbb{Q}(i)$ $(\mathbb{Q}(i,\sqrt{3}) = \mathbb{Q}(i)(\sqrt{3}))$

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

$\Rightarrow [\mathbb{Q}(i,\sqrt{3}):\mathbb{Q}] = 2\times 2 = 4$.

Definition:

An extension is called finite if it has finite degree.

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

eg. Any finite extension $L:K$ is algebraic. ~~Let~~
Let $\alpha \in L$ and let $[L:K] < \infty$.
Then the set $\{1, \alpha, \dots, \alpha^n\}$ is a set of size $n+1$ in a vector space ~~[illegible]~~ $K(\alpha)$ of degree $\leq n$ over K.
Then the set is linearly dependent over K~~(α)~~
ie $\exists k_i \in K$ (not all 0) st $\sum_{i=0}^{n} k_i \alpha^i = 0$
$f(t) = \sum_{i=0}^{n} k_i t^i$ $f \neq 0$ $f(\alpha) = 0$ $\Rightarrow \alpha$ algebraic over K.

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

Any simple algebraic extension is algebraic

eg. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \dots)$
Claim i) $L:\mathbb{Q}$ algebraic
ii) $[L:\mathbb{Q}] = \infty$

i) Let $\alpha \in L$. Then $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \dots, \sqrt[n]{2})$ for some n.

eg
$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}) \arrow[d, dash, "\leq 4 \quad t^4 - 2"] \\
\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \arrow[d, dash, "\leq 3 \quad t^3 - 2"] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

By tower law
$[\mathbb{Q}(\sqrt{2}, \dots, \sqrt[n]{2}) : \mathbb{Q}] \leq n! < \infty$
α is algebraic over $\mathbb{Q}$.

ii)
$$\begin{tikzcd}
L \arrow[d, dash] \\
\mathbb{Q}(\sqrt[n]{2}) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

$[L:\mathbb{Q}] = [L : \mathbb{Q}(\sqrt[n]{2})][\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]$
$\geq 1 \times n = n \quad \forall n \in \mathbb{N}$.
$\Rightarrow [L:\mathbb{Q}] = \infty$

Lemma:

$[L:K] < \infty \iff L:K$ algebraic and $L:K$ is finitely generated.

Proof: $\Rightarrow$ We already saw $L:K$ algebraic
Let $x_1 \dots x_n$ be K-basis for L then $L = K(x_1 \dots x_n)$ so L is finitely generated over K.
$\Leftarrow$ Suppose $L:K$ algebraic and finitely generated.

Say $L = K(\alpha_1, \dots, \alpha_r)$
Then $[L:K] = [K(\alpha_1 \dots \alpha_r) : K(\alpha_1, \dots, \alpha_{r-1})] \times \dots \times [K(\alpha_1) : K]$
Since $L:K$ is algebraic each $[K(\alpha_1, \dots \alpha_{r-1})(\alpha_r) : K(\alpha_1 \dots \alpha_{r-1})]$
$< \infty$
By tower law $[L:K] < \infty$.

Polynomials and Extensions

Definition:

Let $L:K$ be a field extension, $(L \subseteq \mathbb{C})$.
A K-automorphism of L is a field automorphism $\alpha : L \to L$
s.t $\alpha(k) = k \quad \forall k \in K$
(we say α fixes K).

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

(ie it is an automorphism of the extension)

Theorem:

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

Proof: Suppose α, β are K-auts of L
Then $\alpha \circ \beta : L \to L$ which is again a field homomorphism and bijective and $\forall k \in K \quad (\alpha \circ \beta)(k) = \alpha(\beta(k)) = \alpha(k) = k$
ie $\alpha \circ \beta$ is a K-aut of L.
$id : L \to L$ by $id(x) = x \quad \forall x \in L$
id is clearly a K-aut of L.
Composition of maps is associative.
If α is a K-aut of L, since α is bijective there is an inverse map $\alpha^{-1} : L \to L$. α^{-1} is again a field homorphism
eg. $\alpha(\alpha^{-1}(x) + \alpha^{-1}(y)) = \alpha(\alpha^{-1}(x)) + \alpha(\alpha^{-1}(y))$
$\qquad = x + y$
so $\alpha^{-1}(x+y) = \alpha^{-1}(x) + \alpha^{-1}(y)$.

Also ~~then~~ $\forall x \in K$ $\alpha(x) = x$ so $\alpha^{-1}(x) = x$.
ie α^{-1} is a K-aut of L.

Definition:

The Galois Group $\Gamma(L:K)$ of the extension $L:K$ is the group of K-automorphisms of L.

Example: $\Gamma(\mathbb{C}:\mathbb{R})$

Let $\alpha: \mathbb{C} \to$ ~~$\mathbb{R}$~~ $\mathbb{C}$ be an $\mathbb{R}$-aut of $\mathbb{C}$.

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

$\alpha(i) = \pm i$

There are only two possible $\mathbb{R}$-auts of $\mathbb{C}$:

α_1 where $\alpha_1(i) = i$ and α_2 where $\alpha_2(i) = -i$

$\alpha_1(a+bi) = \alpha_1(a) + \alpha_1(b)\alpha_1(i)$

$\qquad = a + bi$

ie $\alpha_1 = id$

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

$\alpha_2(a+bi) = a + b\alpha_2(i)$

$\qquad = a - bi$

Is this an $\mathbb{R}$-aut of $\mathbb{C}$?

Yes, complex conjugation is a field automorphism.

$\overline{zw} = \bar{z}\bar{w}$, $\overline{z+w} = \bar{z} + \bar{w}$ $\bar{r} = r$ $\forall r \in \mathbb{R}$.

$\alpha_2 \in \Gamma(\mathbb{C}:\mathbb{R})$

$\Gamma(\mathbb{C}:\mathbb{R}) = \{id, \alpha_2\} \cong C_2$.

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

Let $\alpha: \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ be a $\mathbb{Q}$-aut

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

$\therefore$ $\alpha(\sqrt[3]{2})$ is a cube root of 2 inside $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

$\therefore$ $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$

$\alpha(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$

ie $\alpha = id$

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

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

If $\alpha \in G$, then $\alpha(\sqrt{2}) = \pm\sqrt{2}$, $\alpha(\sqrt{3}) = \pm\sqrt{3}$.

$\alpha(\sqrt{2})$ and $\alpha(\sqrt{3})$ determine α completely.

This gives 4 possible elements of G.

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

$\alpha_1 : \sqrt{2} \mapsto \sqrt{2} \quad \sqrt{3} \mapsto -\sqrt{3}$

$\alpha_2 : \sqrt{2} \mapsto -\sqrt{2} \quad \sqrt{3} \mapsto \sqrt{3}$

$\alpha_3 : \sqrt{2} \mapsto -\sqrt{2} \quad \sqrt{3} \mapsto -\sqrt{3}$

Are these all in G?

eg α_3 $\sqrt{2}$ and $-\sqrt{2}$ have the same min polynomial $t^2 - 2$ over $\mathbb{Q}$.

By 5.18 $\exists\, \phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(-\sqrt{2})$ st $\phi(\sqrt{2}) = -\sqrt{2}$ and $\phi|_{\mathbb{Q}} = id$.

$\sqrt{3}$ and $-\sqrt{3}$ have the same min poly $t^2 - 3$ over $\mathbb{Q}(\sqrt{2})$

(need to check this is irreducible over $\mathbb{Q}(2)$. Use 5.13.

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{2})(\sqrt{3}) \arrow[r, "\alpha_3"', "\sqrt{3} \mapsto -\sqrt{3}"] \arrow[d, dash] & \mathbb{Q}(\sqrt{2})(-\sqrt{3}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[r, "\phi", "\sqrt{2} \mapsto -\sqrt{2}"'] \arrow[d, dash] & \mathbb{Q}(-\sqrt{2}) = \mathbb{Q}(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, "id"'] & \mathbb{Q}
\end{tikzcd}$$

$\Gamma(\mathbb{Q}(\sqrt{2}; \sqrt{3}) : \mathbb{Q}) = \{id, \alpha_1, \alpha_2, \alpha_3\} = C_2 \times C_2$

$L : K$

$\Gamma(L : K)$ = group of K-automorphisms of L.

Main theorem sets up a correspondence between

Correspondence is a follows:

Let $\mathcal{F} = \{$fields M st $K \subseteq M \subseteq L\}$ (intermediate field

$\mathcal{G} = \{H : H \leq \Gamma(L : K)\}$ (subgroups of galois group)

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

Then $M^* \leq \Gamma(L : K)$ in fact $M^* = \Gamma(L : M)$

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

* and † are order-reversing ie $M \subseteq N \Rightarrow M^* \supseteq N^*$

$H \leq J \Rightarrow H^\dagger \geq J^\dagger$

(Suppose $M \subseteq N$ and $g \in N^*$. Then $g(n) = n$ $\forall n \in N$
Hence $g(m) = m$ $\forall m \in M$ so $g \in M^*$. Thus $N^* \leq M^*$)

$M \leq M^{*\dagger}$, $H \leq H^{\dagger *}$

M^* is group element fixing M

$M^{*\dagger}$ is all field elements fixed by M^*

is all field elements fixed by all groups elements that fix M

includes M.

Let $x \in M$

If $g \in M^*$, then $g(x) = x$ (def^n M^*)

ie $\forall g \in M^*$, $g(x) = x$

ie $x \in M^{*\dagger}$

The Fundemental Theorem of Galois Theory shows that, under some extra hypothesis $M = M^{*\dagger}$ and $H = H^{\dagger *}$ for all M, H

ie $*$ and $\dagger$ are mutal inverses: $*\dagger = \mathrm{id}_{\mathcal{F}}$

$\dagger * = \mathrm{id}_{G}$

This then means there is a 1-1 order reversing correspondence between intermediate fields and subgroups.
Information can then be transferred from subgroups to fields

~~eg. What are all subfields of Q~~

eg. What are all subfields of $\mathbb{Q}(i, \sqrt{2})$?

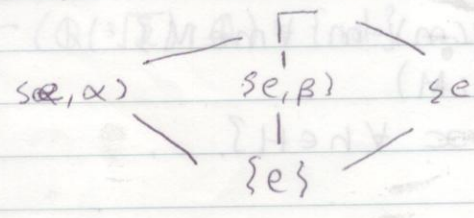
The hypothesis needed for the fundemental theorem

So we can use it to answer this.

$\Gamma(\mathbb{Q}(i,\sqrt{2}) : \mathbb{Q}) = \{\mathrm{id}, \alpha, \beta, \alpha\beta\}$

$\alpha(i) = -i$	$\beta(i) = i$	$\alpha\beta(i) = -i$
$\alpha(\sqrt{2}) = \sqrt{2}$	$\beta(\sqrt{2}) = -\sqrt{2}$	$\alpha\beta(\sqrt{2}) = -\sqrt{2}$
$\alpha(i\sqrt{2}) = -i\sqrt{2}$	$\beta(i\sqrt{2}) = -i\sqrt{2}$	$\alpha\beta(i\sqrt{2}) = i\sqrt{2}$.

What is G?



By Fundemental Theorem $\mathcal{H} \leftrightarrow \mathcal{F} =$ $\{e\}^{\dagger} = \mathbb{Q}(i,\sqrt{2})$

$\mathcal{F}/\mathcal{E}/\mathbb{R}$.

$\{e,\alpha\}^{\dagger} = \{x \in \mathbb{Q}(i,\sqrt{2}) \mid \alpha(x) = x\}$

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

$\underset{\mathbb{Q}(\sqrt{2})}{\overset{\shortparallel}{\{e,\alpha\}^{\dagger}}}$ $\underset{\mathbb{Q}(i)}{\overset{\shortparallel}{\{e,\beta\}^{\dagger}}}$ $\{e,\alpha\beta\}^{\dagger} = \mathbb{Q}(i\sqrt{2})$

$\Gamma^{\dagger} = \mathbb{Q}$

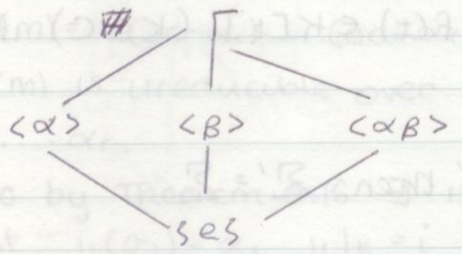
$x = a + bi + c\sqrt{2} + di\sqrt{2} \quad (a,b,c,d \in \mathbb{Q})$

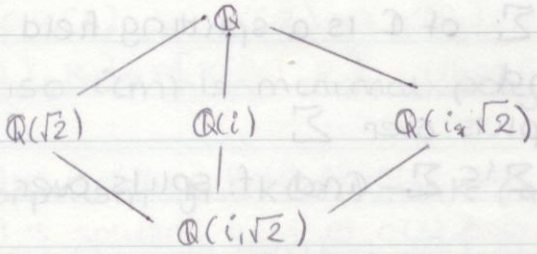
$\alpha(x) = a - bi + c\sqrt{2} - di\sqrt{2}$

Since $\{1, i, \sqrt{2}, i\sqrt{2}\}$ $\mathbb{Q}$ basis

$x = \alpha(x) \iff b = -b,\ d = -d$

$\iff x = a + c\sqrt{2} \quad (a, c \in \mathbb{Q})$.





NORMALITY & SEPERABILITY

There are two properties (to do with roots of irreducible polynomials) which $L:K$ needs for Fundemental Theorem to hold.

Splitting fields

Definition :

If K is a subfield of $\mathbb{C}$, f is a polynomial over K then f splits over K if it can be written as a product of linear factors over K ie $f(x) = k(x-\alpha_1)\dots(x-\alpha_n)$ for some $k, \alpha_i \in K$.

eg. $x^3 - 1$ splits over $\mathbb{C}$.

$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$

x^2-2 splits over $\mathbb{Q}(\sqrt{2})$

$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$

x^2-2 does not split over $\mathbb{Q}$.

Clearly $\alpha_1 \ldots \alpha_n$ are roots of f in $\mathbb{C}$.

Every polynomial has all its roots in $\mathbb{C}$, so f splits over K iff all roots lie in K.

If $f(t) \in K[t]$ and $K \subseteq L \subseteq \mathbb{C}$ then f can be regarded as a polynomial over L so it makes sense to talk about f splitting over L.

Definition:

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

1. f splits over Σ
2. If $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ' then $\Sigma' = \Sigma$

Theorem:

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

Proof: Let $f = c(x-\alpha_1)\ldots(x-\alpha_n)$ over $\mathbb{Q}$

Let $\Sigma = K(\alpha_1 \ldots \alpha_n)$

Then f splits over Σ and if f splits over $\Sigma' \subseteq \Sigma$ then by unique factorisation $\alpha_1 \ldots \alpha_n \in \Sigma'$ so $\Sigma \supseteq K(\alpha_1 \ldots \alpha_n) = \Sigma$

$\therefore \Sigma' = \Sigma$

Clearly only field with this property.

$\Sigma = K(\alpha_1 \ldots \alpha_n)$

Each α_i is algebraic over K ie each $[K(\alpha_1 \ldots \alpha_{i-1})(\alpha_i) : K(\alpha_1 \ldots \alpha_{i-1})] < \infty$

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

Lemma:

Let $i : K \rightarrow K'$ be an isomorphism of subfields of $\mathbb{C}$, $f \in K[t]$.

Let Σ be splitting field for f over K.

Let $L \supseteq K'$ be st $i(f)$ splits over L.
Then $\exists$ monomorphism $j : \Sigma \to L$ st $j|_K = i$

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

Proof: Use induction on ∂f
Let $f = c(x-\sigma_1)\dots(x-\sigma_n)$ over Σ
Let m = min poly of σ_1 over K
Then $m|f$. Hence $i(m)|i(f)$ and if $i(f)$ splits over L so $i(m)$ has roots $\alpha_1 \dots \alpha_r$ in L
$i(m) = k(x-\alpha_1)\dots(x-\alpha_r)$.
$i(m)$ is irreducible over K', so $i(m)$ is minimal poly ~~to~~ of $\alpha_1 \dots \alpha_r$.
So by Theorem 5.16 $\exists$ isomorphism $j_1 : K(\sigma_1) \to K'(\alpha_1)$.
st $j_1(\sigma_1) = \alpha_1$, $j_1|_K = i$

$$\begin{tikzcd}
K(\sigma_1) \arrow[r, "j_1", "\sigma_1 \to \alpha_1"'] & K'(\alpha_1) \\
K \arrow[u, dash] \arrow[r, "i"] & K' \arrow[u, dash]
\end{tikzcd}$$

Now let $g(t) = f(t)/(t-\sigma_1) \in K(\sigma_1)[t]$.

Σ is splitting field of g over $K(\sigma_1)$
$j_1(g) \in K'(\alpha_1)[t]$ and $j_1(g)$ ~~span~~ splits over L
$\partial g = n-1$.
By induction $\exists j : \Sigma \to L$ monomorphism st $j|_{K(\sigma_1)} = j_1$

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

Theorem

Let $i : K \to K'$ be an isomorphism $f(t) \in K[t]$. Let Σ be splitting field of f over K and Σ' the splitting field field of $i(f)$ over K. Then $\exists$ iso $j : \Sigma \to \Sigma'$ st $j|_K = i$

ie $\Sigma_1' : K \cong \Sigma_1' : K'$

Proof: By lemma $\exists$ monomorphism J with these properties

$$\begin{tikzcd}
\Sigma_1 \arrow[r, "j"] & \Sigma' \\
K \arrow[u, dash] \arrow[r, "i"'] & K' \arrow[u, dash]
\end{tikzcd}$$

Now $j(\Sigma) \subseteq \Sigma'$ but $i(f)$ splits over $j(\Sigma_1)$

$[f(t) = c(x-\sigma_1)\dots(x-\sigma_n)$ is $\Sigma[t]$ $i(f) = j(f) = j(c)(x-j(\sigma_1)$
$\dots(x-j(\sigma_n))]$

Since Σ' splitting field $j(\Sigma') = \Sigma'$

ie J surjective so isomorphism.

Normality

Definition:

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

The only obvious normal extension is $\mathbb{C}:K$.
$\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ is not normal.
$f(t) = t^3 - 2$. Then f is irreducible over $\mathbb{Q}$.
f has one root in $\mathbb{Q}(\sqrt[3]{2})$ namely $\sqrt[3]{2}$.
f does not split over $\mathbb{Q}(\sqrt[3]{2})$ because other two roots are complex
$f(t) = t^3 - 2 = (t - \sqrt[3]{2})(t^2 - \sqrt[3]{2}t + \sqrt[3]{4})$. irreducible over $\mathbb{Q}(\sqrt[3]{2})$.

Theorem: [illegible]

$L:K$ is normal and finite $\Leftrightarrow$ L is a splitting field over K.

(eg $\mathbb{Q}(i, \sqrt{2}):\mathbb{Q}$ is normal since it is splitting field of $(t^2+1)(t^2-2)$ over $\mathbb{Q}$).

Proof: $\Rightarrow$ Suppose $L:K$ normal and finite.
By 6.11 $L = K(\alpha_1 \dots \alpha_n)$ for some α_i algebraic over K.
Let m_i = min poly of α_i over K and let $f = m_1 \dots m_n$
Since $L:K$ is normal and m_i is irreducible over K with one root α_i in L, m_i splits over L.
Hence f splits over L. Also any field over which f splits contains K and $\alpha_1 \dots \alpha_n$.
Hence contains $K(\alpha_1 \dots \alpha_n) = L$ $\therefore$ L is splitting field of f over K.

$\Leftarrow$ Suppose L = splitting field of $g(t) \in K[t]$

$[L:K] < \infty$ since L is obtained from K by adjoining the roots of g ie. a finite number of algebraic elements.

Let f be an irreducible polynomial over K.

We must show that if f has at least one zero in L then all its zeros are in L.

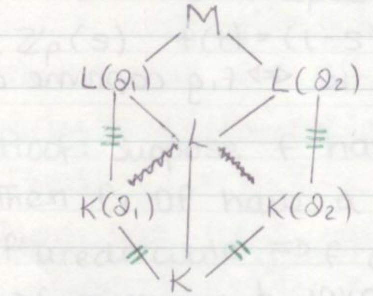
Let M = splitting field for fg over K.

Let θ_1, θ_2 be two roots of f in M

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

(this implies $\theta_1 \in L \Rightarrow \theta_2 \in L$).

$$\begin{tikzcd}
M = K(\text{roots } g, f) \arrow[d, dash] \\
L = K(\text{roots } g) \arrow[d, dash] \\
K
\end{tikzcd}$$



θ_1 and θ_2 are roots of irreducible polynomial $f(t) \in K[t]$ so $K(\theta_1) : K \cong K(\theta_2) : K$ and $[K(\theta_1) : K] = [K(\theta_2) : K]$ (thm 5.13).

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

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

$$\begin{tikzcd}
L(\theta_1) \arrow[r, dashed, "j"] \arrow[d, dash] & L(\theta_2) \arrow[d, dash] \\
K(\theta_1) \arrow[r, "i", "{\substack{\theta_1 \mapsto \theta_2 \\ g \mapsto g}}"'] \arrow[d, dash] & K(\theta_2) \arrow[d, dash] \\
K \arrow[r, "id."'] & K
\end{tikzcd}$$

By 9.6 $\exists$ iso $j : L(\theta_1) \rightarrow L(\theta_2)$ st $j|_{K(\theta_1)} = i$

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

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

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

Two right hand sides are equal

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

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

Seperability

Definition:

An irreducible polynomial over $K (\subseteq \mathbb{C})$ is seperable if it has no repeated roots (in $\mathbb{C}$ or in a splitting field).

Definition:

If $f(t) = a_n t^n + \dots + a_0$, define $Df(t) = n a_n t^{n-1} + \dots + a_1$

NB: This is a formal derivative - no limits needed!

Properties:
- $D(f+g) = Df + Dg$
- $D(fg) = Df g + f Dg$
- $D(\lambda f) = \lambda D(f)$.

Proposition:

Suppose $f, g \in K[t]$ and $K \subseteq L$. Then f, g coprime over $K \Leftrightarrow f, g$ coprime over L

Proof: $\Leftarrow$ f, g coprime over $L \Rightarrow$ over K.

$\Rightarrow$ f, g coprime over over K

$\Rightarrow \exists\, h, k \in K[t]$ st $fh + gk = 1$ $\Rightarrow f, g$ coprime over L.

Lemma:

Let $f(t) \in K[t]$ be polynomial over $K \subseteq \mathbb{C}$. Let Σ = splitting field
Then f has repeated 0 $\Leftrightarrow f$ and Df are not coprime in $K[t]$.
(in Σ or $\mathbb{C}$)

Proof: $\Rightarrow$ Suppose $f(t) = (t-\alpha)^2 g(t) \in \Sigma(t)$

$Df(t) = (t-\alpha)^2 Dg(t) + 2(t-\alpha) g(t)$
$\quad = (t-\alpha)[(t-\alpha)Dg(t) + 2g(t)]$

f, Df not coprime in $\Sigma[t]$ (non trivial common factor $t-\alpha$).

f, Df not coprime in $K[t]$.

$\Leftarrow$ Suppose f has no repeated root

Prove by induction on ∂f that f and Df are coprime. in $\Sigma[t]$, hence in $K[t]$

In $\Sigma(t)$, $f(t) = (t-\alpha) g(t)$, $t-\alpha | g$

$Df = g + (t-\alpha) Dg$

Suppose f and Df have a common irreducible common factor say

$h | f$, $h | Df$

~~If $h | g$, $h | Df$ so $h | (t-\alpha) Dg$ so $h | Dg$~~

If $h = t-\alpha$, $t-\alpha | Df = g + (t-\alpha) Dg$ so $t-\alpha | g$ contradiction

otherwise $h|g$, $h|Df$ so $h|(t-\alpha)Dg$ so $h|Dg$
So h is common factor of g and Dg
$h|g$ and $h|Dg$ and $\partial g < \partial f$ By induction, contradiction
So f and Df are coprime.

Proposition:

If K is a subfield of $\mathbb{C}$, $f \in K[t]$ is [illegible] seperable
(ie doesn't have repeated roots)

[Not true in fields of characteristic p eg $\mathbb{Z}_p(s^p) \subseteq \mathbb{Z}_p(s)$
$f(t) = t^p - s^p \in \mathbb{Z}_p(s^p)[t]$ $f(t)$ irreducible over $\mathbb{Z}_p(s^p)$, but over
$\mathbb{Z}_p(s)$ $f(t) = (t-s)^p$ ie f has the root s repeated p times]

Proof: Suppose f has a repeated root in $\mathbb{C}$.
Then f, Df have a common factor of degree ≥ 1 in $K[t]$
f irreducible $\Rightarrow f$ divides Df. But $\partial(Df) < \partial f$, so $Df = 0$
$\Rightarrow f$ constant.
Any irreducible polynomial (over $K \subseteq \mathbb{C}$) of degree n has exactly n distinct (not repeated) roots in a splitting field.

COUNTING PRINCIPLES.

Lemma:

If K and L are subfields of $\mathbb{C}$, then every set of distinct monomorphisms $K \to L$ is linearly independent over L.

Theorem:

Let G be a finite subgroup of automorphisms of a field K and let K_0 be the fixed field of G. Then $[K:K_0] = |G|$.

Proof: Let $n = |G|$ $G = \{g_1, g_2, \ldots, g_n\}$
$m = [K:K_0]$ $\{x_1 \ldots x_m\}$ basis for K over K_0.

Want to prove $m=n$.

Suppose $m<n$.

Consider the equations in $y_1 \dots y_n$,

$$y_1 g_1(x_1) + \dots + y_n g_n(x_1) = 0$$
$$y_1 g_1(x_2) + \dots + y_n g_n(x_2) = 0$$
$$\vdots \qquad\qquad \vdots$$
$$y_1 g_1(x_m) + \dots + y_n g_n(x_m) = 0$$

m equations in n unknowns (homogeneous), so there is a solution.

Then for any $x \in K$, $x = \alpha_1 x_1 + \dots + \alpha_m x_m$ for some $\alpha_i \in K_0$.

Then
$$y_1 g_1(x) + \dots + y_n g_n(x) = y_1 g_1(\alpha_1 x_1 + \dots + \alpha_m x_m) + \dots + y_n g_n(\alpha_1 x_1 + \dots + \alpha_m x_m)$$
$$= y_1(\alpha_1 g_1(x_1) + \dots + \cancel{y_1}\,\alpha_m g_1(x_m)) +$$
$$y_2(\alpha_1 g_2(x_1) + \dots + \alpha_m g_2(x_m)) +$$
$$\dots$$
$$y_n(\alpha_1 g_n(x_1) + \dots + \alpha_m g_n(x_m))$$
$$= \alpha_1 0 + \alpha_2 0 + \dots + \alpha_m 0 = 0.$$

$\therefore y_1 g_1 + \dots + y_n g_n = 0$

$\therefore g_1, \dots, g_n$ are linearly dependent over K

Contradiction, Dedekin's Lemma.

Suppose $n<m$

Then there exists a set of $n+1$ elements of K, linearly independent over K_0 say $\{x_1, \dots, x_{n+1}\}$

Then there exist y_i, not all zero such that:

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

Take shortest such relation by renumbering $y_1, \dots, y_r \neq 0$, $y_{r+1} = \dots = y_{n+1} = 0$.

$$\left.\begin{aligned} y_1 g_1(x_1) + \dots + y_r g_1(x_r) &= 0 \\ \vdots \qquad\qquad &\vdots \\ y_1 g_n(x_1) + \dots + y_r g_n(x_1) &= 0 \end{aligned}\right\} ①$$

Let $g \in G$.

$$g(y_1)\underbrace{g g_1}_{g_i}(x_1) + \dots + g(y_r)\underbrace{g g_1}_{g_i}(x_1) = 0$$
$$\vdots \qquad\qquad \vdots$$
$$g(y_1)\underbrace{g g_n}_{g_j}(x_r) + \dots + g(y_1)\underbrace{g g_n}_{g_j}(x_r) = 0$$

$$\left.\begin{aligned} g_1(y_1) g_1(x_1) + \dots + g(y_r) g_1(x_r) &= 0 \\ g(y_1) g_2(x_1) + \dots + g(y_r) g_2(x_r) &= 0 \\ \vdots \qquad\qquad &\vdots \\ g(y_1) g_n(x_1) + \dots + g(y_r) g_n(x_r) &= 0. \end{aligned}\right\} ②$$

Multiply system ① by $g(y_1)$ and system ② by y_1 and subtract:

$(g(y_1)y_2 - g(y_2)y_1)g_1(x_1) + \dots = 0$

$(g(y_1)y_2 - g(y_2)y_1)g_2(x_r) + \dots = 0$

$\vdots$

$(g(y_1)y_2 - g(y_2)y_1)g_n(x_r) + \dots = 0$

This is a system like (1) with $y_i' = g(y_1)y_i - y_1 g(y_i)$ $(i = 2, \dots r)$.

This would be a system with less non-zero terms, a contradiction unless all $y_i' = 0$

$\therefore g(y_1)y_i - y_1 g(y_i) = 0 \ \forall i$

$g(y_1)y_i = y_1 g(y_i)$

$y_i y^{-1} = g(y_i y_i^{-1})$

This is true for all $g \in G$, so $y_i y_1^{-1} \in K_0$

Say $y_i y_i^{-1} = z_i \in K_0$

Then $y_i = y_1 z_i$ $(z_i \neq 0)$

Now the first equations (1) with $g_1 = id$ is

$y_1 x_1 + \dots + y_r x_r = 0$

$\therefore y_1 z_1 x_1 + \dots + y_1 z_r x_r = 0$

$z_1 x_1 + \dots + z_r x_r = 0$

Then $\{x_1, \dots x_r\}$ are linearly independent over K_0.

Contradiction to assuming $m > n$.

Hence $m = n$ QED.

Field Automorphisms

K-monomorphisms

Definition:

Let $K \subseteq M$, $L \subseteq \mathbb{C}$. Then a K-monomorphism $\varphi : L \longrightarrow M$ is a field monomorphism such that $\varphi_K|_K = id$

ie $\varphi(x) = x \ \forall x \in K$.

eg. $\alpha = \sqrt[3]{2}$, $\omega = e^{2\pi i/3}$ then there are 3 $\mathbb{Q}$-monomorphism

$\varphi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{C}$

$\varphi(\alpha^3 - 2) = \varphi(\alpha^3) - \varphi(2) = \varphi(\alpha)^3 - 2$

$\shortparallel$

$\varphi(0) = 0$

$\varphi(\alpha)^3 = 2$

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

$\varphi_1 = id$, $\varphi_2(\alpha) = \alpha\omega$ $\varphi_3(\alpha) = \alpha\omega^2$

$\mathbb{Q}(\alpha) \cong \mathbb{Q}(\alpha\omega)$.

Theorem:

Let $L:K$ be a finite, normal extension, $K \leq M \leq L$.
Let $\tau : M \rightarrow L$ be a K-monomorphism. Then $\exists\ \sigma : L \rightarrow L$
K-automorphism st $\sigma|_M = \tau$

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

Proof: L = splitting field for some poly f over K
L = splitting field for some poly f over M
($L = K(\alpha_1 \ldots \alpha_n)$ α_i roots of $f \in K[t]$
$M(\alpha_1 \ldots \alpha_n) \subseteq L$, $M(\alpha_1 \ldots \alpha_n) \supseteq K(\alpha_1 \ldots \alpha_n) = L$
$\Rightarrow L = M(\alpha_1 \ldots \alpha_n)$).
L = splitting field for f over $\tau(M)$. ($\tau(f) = f$)

By thm 9.6 $\exists$ isomorphism
$\sigma : L \rightarrow L$ st $\sigma|_M = \tau$

$$\begin{tikzcd}
L \arrow[r, "\sigma"] & L \\
M \arrow[u, dash] \arrow[r, "\tau"] & \tau(M \arrow[u, dash] \\
f \arrow[r, mapsto, "\cong"] & f
\end{tikzcd}$$

Proposition:

Suppose $L:K$ is a finite normal extension and α and β are roots of the same ~~polynomial~~ irreducible polynomial $m(t) \in K[t]$.
Then $\exists$ a K-automorphism of L, σ, st $\sigma(\alpha) = \beta$
(note $\sigma \in \Gamma(L:K)$).

Proof:

$$\begin{tikzcd}
L \arrow[r, dashed, "\sigma"] & L \\
K(\alpha) \arrow[u, dash] \arrow[r, dashed, "\rho"', "\alpha \mapsto \beta"'] & K(\beta) \arrow[u, dash] \\
K \arrow[u, dash] \arrow[r, dash, "id"'] & K \arrow[u, dash]
\end{tikzcd}$$

← by 11.3

← by 5.13

Now $\rho : K(\alpha) \rightarrow L$

Normal Closures

Definition:

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

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

eg. Normal closure of $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$

$\alpha = \sqrt[4]{2}$, $\alpha^4 - 2 = 0$

$f(x) = x^4 - 2$, roots $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$

$N = \mathbb{Q}(\sqrt[4]{2}, i)$ N normal since it is splitting field for f.

No smaller normal extension.

eg. Normal closure of $\mathbb{Q}(e^{2\pi i/5}) : \mathbb{Q}$

$\omega = e^{2\pi i/5}$ $\omega^5 = 1$, $\omega^5 - 1 = 0$, roots $1, \omega, \omega^2, \omega^3, \omega^4$

$\mathbb{Q}(\omega) : \mathbb{Q}$ is in fact ~~split~~ a normal closure.

Theorem:

If $L:K$ a finite extension in $\mathbb{C}$, then there exists a unique normal closure $N \subseteq \mathbb{C}$ of $L:K$, which is a finite extension of K.

Proof: Need field extension $N:K$ normal finite $\Leftrightarrow$ N splitting field.

Existence: Let $x_1 \dots x_r$ be a basis for L over K and let m_j be minimal polynomial of x_j over K. Let N be splitting field for $f = \prod_{j=1}^{r} m_j$ over L. As $K \subseteq L$ and N splitting field for f over L, N is also a splitting field for f over K. Hence $N:K$ normal and finite.

Suppose $L \subseteq P \subseteq N$ where $P:K$ is normal. Each polynomial m_j has a zero at $x_j \in P$, so by normality f splits in P. Since N is splitting field for f, we have $P = N$.

There fore N is normal closure.

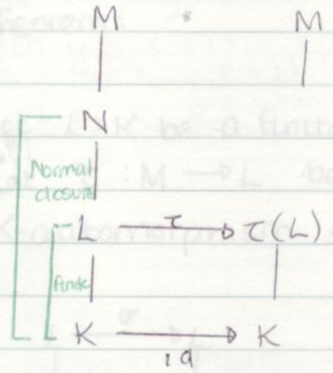
Uniqueness: Suppose M and N are both normal closures. Then f splits in M and N, so $\Sigma \subseteq M$, $\Sigma \subseteq N$, Σ splitting field of f. $L \subseteq \Sigma$, so $L \subseteq \Sigma \subseteq M$, $L \subseteq \Sigma \subseteq N$. $\Sigma : K$ is normal

So by def^n of normal closure $\Sigma = M$, $\Sigma = N \Rightarrow N = M$.

Normal closure of $K(\alpha)$ = splitting field of m_α

Normal closure of $K(\alpha,\beta)$ = splitting field of $m_\alpha m_\beta$.

Lemma:



Then $\tau(L) \subseteq N$

ie K-monomorphism from L can't get outside N.

In particular if $L:K$ is normal, so $N=L$ then any K-monomorphism $L \to \mathbb{C}$ has $\tau(L) \leq L$.

Proof: Let $\alpha \in L$ with min poly m over K.

$m(\alpha)=0$

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

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

ie $\tau(\alpha)$ is another root of m.

m irreducible, $N:K$ normal, m has one root α in N

$\Rightarrow$ all roots of m are in N $\Rightarrow$ $\tau(\alpha) \in N$.

Theorem:

For a finite extension $L:K$, F.A.E

1 $L:K$ normal

2. $\exists$ finite, normal extension N of K containing L st every K-monomorphism $\tau: L \to N$ is a K-aut of L.

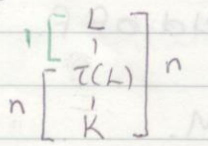
3. For every finite extension M of K containing L, every K-monomorphism $\tau: L \to M$ is a K-automorphism of L.

Proof: First note any K-mono, $\tau: L \to L$ is in fact a K-aut of L.

This is because if $\tau: L \to L$ K-mono, $K \subseteq \tau(L) \subseteq L$ and

$L:K \cong \tau(L):K$, so $[L:K]=[\tau(L):K]$

By Tower Law $\tau(L)=L$



1 ⟹ 3 By last result, $\tau(L) \subseteq L$ so by remark above τ is K-aut of L.

3 ⟹ 2. Take N = normal closure of L:K, by 3, N has required property.

2 ⟹ 1. Let f be irreducible over K with one root α in L. Let β be any other root of f: then $\beta \in N$ since N:K is normal. By 11.4 $\exists$ an K-aut σ of N st $\sigma(\alpha) = \beta$. Then $\sigma|_L$ is a K-mono from L into N. By 2, this is a K-aut of L ie $\sigma(L) \subseteq L$ so $\beta = \sigma(\alpha) \in L$. $\therefore$ L:K normal.

2 says
$$\begin{tikzcd} N \arrow[d, dash] & N \arrow[d, dash] \\ L \arrow[r, dash, "\tau"] \arrow[d, dash] & \tau(L) \arrow[d, dash] \\ K \arrow[r, dash, "id"] & K \end{tikzcd}$$
$\Rightarrow \tau(L) \subseteq L$

$\alpha \in L$
$\|$
$\beta \in L$

$$\begin{tikzcd} N \arrow[r, "\sigma"] \arrow[d, dash] & N \arrow[d, dash] \\ L \arrow[r, "\sigma|_L"] \arrow[d, dash] & {} \\ K(\alpha) \arrow[r] \arrow[d, dash] & K(\beta) \arrow[d, dash] \\ K \arrow[r, "id"] & K \end{tikzcd}$$

Theorem:

~~Suppose~~ Let that L:K be a finite extension of degree n. Then there are exactly n K-automorphisms from L into N, the normal closure of L:K (and hence into any normal extension M:K contains L).

In particular:

Corollary:

Let L:K be finite and normal. Then there are precisely [L:K] K-automorphism of L ie. $|\Gamma(L:K)| = [L:K]$.

Proof of thm: Use induction on $n = [L:K]$.

n=1, nothing to prove.

Suppose $[L:K] = k > 1$ and result holds for all extensions of degree < k.

Let $\alpha \in L \setminus K$. Let m = min poly of α over K.

$\partial m = [K(\alpha):K] = r$, $r > 1$

$s = k/r < k$.

$$\begin{tikzcd} N \arrow[d, dash] \\ L \arrow[d, dash, "s<k"] \arrow[dd, dash, bend right, "k"'] \\ K(\alpha) \arrow[d, dash, "r"] \\ K \end{tikzcd}$$

m has one root, α in N, so m splits in N.

Let roots be $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_3$ (all distinct)

Now $L:K(\alpha)$ is a finite extension, $N:K(\alpha)$ is normal closure of $L:K(\alpha)$ and $[L:K(\alpha)] = s < k$.

By induction there are exactly s $K(\alpha)$-monomorphisms $L \to N$ say $\rho_1 \ldots \rho_s$

Now α and α_i have the same minimal polynomial m over K and $\alpha_i \in N$ and $N:K$ normal

By 11.4 $\exists$ K-aut τ_i of N st $\tau_i(\alpha) = \alpha_i$ $(i = 1, 2, \ldots, r)$

Let $\rho_{ij} = \tau_i \rho_j$

$$\begin{tikzcd}
N \arrow[d, dash] & N \arrow[r, "\tau_i"] \arrow[d, dash] & N \arrow[d, dash] \\
L \arrow[r, "\rho_j"] \arrow[d, dash] & \rho_j(L) \arrow[r, "\tau_i"] \arrow[d, dash] & \tau_i\rho_j(L) \arrow[d, dash] \\
K(\alpha) \arrow[r, "id"] \arrow[d, dash] & K(\alpha) \arrow[r] \arrow[d, dash] & K(\alpha_i) \arrow[d, dash] \\
K \arrow[r, "1d"'] & K \arrow[r, "1d"'] & K
\end{tikzcd}$$

It remains to show
i) all ρ_{ij} distinct
ii) any K-mono $L \to N$ is $=$ some ρ_{ij}

i) Suppose $\rho_{ij} = \rho_{pq}$

$\tau_i \rho_j = \tau_p \rho_q$

$\tau_i \rho_j(\alpha) = \tau_p \rho_q(\alpha)$

$\tau_i(\alpha) = \tau_p(\alpha)$

$\alpha_i = \alpha_p \Rightarrow i = p$

$\tau_i \rho_j = \tau_i \rho_q$

$\tau_i^{-1} \tau_i \rho_j = \tau_i^{-1} \tau_i \rho_q$

$\rho_j = \rho_q \Rightarrow j = q$.

ii) Let $\tau : L \to N$ be a K-mono

α has min poly m over K, $\tau(\alpha)$ root of m

$\tau(\alpha) = \alpha_i$ for some i.

$(\tau_i^{-1}\tau)(\alpha) = \tau_i^{-1}(\alpha_i) = \alpha$

$\tau_i^{-1}\tau$ is a K-mono that fixes α

so $\tau_i^{-1}\tau : L \to N$ is a $K(\alpha)$-mono

$\tau_i^{-1}\tau = \rho_j$ for some j

$\tau = \tau_i \rho_j = \rho_{ij}$

Theorem:

Let $L:K$ be a finite normal extension. Then the fixed field of $\Gamma(L:K)$ is K.

$$\begin{tikzcd}
L \arrow[r] \arrow[d, dash] & \{e\} \arrow[d, dash] \\
K \arrow[r, shift left] & \Gamma(L:K) \arrow[l, shift left]
\end{tikzcd}$$

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

$\Gamma(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) = \{id, \tau\}$, $\tau(\sqrt{2}) = -\sqrt{2}$

$\Gamma(\mathbb{Q}(\sqrt{2}):\mathbb{Q})^{\dagger} = \{x \in \mathbb{Q}(\sqrt{2}) : \tau(x) = x\}$.

$= \mathbb{Q}$

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

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

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

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

Proof:

$$\begin{tikzcd} L \arrow[d, dash, "n"] \\ K_0 \arrow[d, dash, "1"] \\ K \end{tikzcd}$$

n (whole tower) K_0 = fixed field of $\Gamma(L:K)$

$[L:K] = n$

By 11.11 $|\Gamma(L:K)| = n$

By 10.5 $[L:K_0] = n$

By tower law $K_0 = K$.

Theorem:

Suppose $K \subseteq L \subseteq M$ and $M:K$ finite. Then the number of K-monomorphisms $L \to M$ is less than or equal too $\leq [L:K]$.

Proof: Let N be normal closure of M:K

N:K is finite and there are exactly $[L:K]$ K-monomorphisms $L \to N$ (by 11.10)

Any K-mono $L \to M$ is a K-mono $L \to N$

$\therefore$ Number of K-monos $L \to M$ is $\leq [L:K]$

Theorem:

Let $L:K$ be a finite extension s.t fixed field of $\Gamma(L:K)$ is K

Then $L:K$ is normal.

Proof: Apply 10.5 to $\Gamma(L:K)$

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

Let N = normal closure of L:K

There are $[L:K] = n$ K-monos $L \to N$

But there are $|\Gamma(L:K)| = n$ K-auts of L

Hence very K-mon $L \to N$ is a K-aut of L. By 11.9 L:K normal

A Worked Example

Using Handout 8.

Find splitting field L of t^7-1 over $\mathbb{Q}$.
Find $\Gamma(L:\mathbb{Q})$
Find all intermediate fields.

1. $t^7-1=0 \Leftrightarrow t=e^{2\pi i r/7}$
   $\omega = e^{2\pi i/7}$, Roots are $1, \omega, \omega^2, \dots, \omega^6$
   $L=\mathbb{Q}(\omega)$.

2. $\omega^7-1=0$
   $m(t) = \dfrac{t^7-1}{t-1}$
   $t=s+1 \quad m = \dfrac{(s+1)^7-1}{s}$
   $= s^6+7s^5+\dots+7$

By eisenstiens (prime 7) m is irreducible ($7 \mid {}^7C_r \;\forall\, 1\le r\le 6$).
$\therefore$ m is min polynomial of ω over $\mathbb{Q}$
$\therefore [L:\mathbb{Q}] = \partial m = 6$

3. $G=\Gamma(L:K)$ By Fundemental Thm $|G|=6$.

4. Let $g\in G$, g is determined by $g(\omega)$
   $g(\omega)$ must be a root of m
   ie $g(\omega)=\omega^i$ for some $1\le i\le 6$.
   This gives us 6 possible elements of G: g_i where $g_i(\omega)=\omega^i$

5. Since $|G|=6$ and only possibilities for elements of G are $g_1 \dots g_6$, they must be in fact be K-aut and make up G
   ie $G=\{\overset{id}{\overset{\shortparallel}{g_1}}, g_2, g_3, g_4, g_5, g_6\}$

6. $g_2(\omega)=\omega^2$
   $g_2^2(\omega)=g_2(\omega^2)=(g_2(\omega))^2=\omega^4$
   $g_2^3(\omega)=g_2(\omega^4)=\omega^8=\omega \quad g_2^3=id$

   $g_3(\omega)=\omega^3$,
   $g_3^2(\omega)=\omega^9=\omega^2 \quad g_3^3(\omega)=g_3(\omega^2)=\omega^6$

$\therefore \ o(g_3) > 3$

$\therefore \ o(g_3) = 6$

$G = C_6 = \langle g_3 : g_3^6 = id \rangle$

Rename $g_3 = g$ $\quad G = \langle g : g^6 = id \rangle \cong C_6 \quad g(\omega) = \omega^3$

7/8

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

9.

$$\begin{tikzcd}
 & \{id\} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] \arrow[rrrr, leftrightarrow] & & & & L = \mathbb{Q}(\omega) \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
\langle g^2 \rangle \arrow[dr, dash, "2"'] \arrow[rrrr, leftrightarrow, bend left] & & \langle g^3 \rangle \arrow[dl, dash, "3"] \arrow[rrrr, leftrightarrow, bend right] & & \langle g^2 \rangle^+ \arrow[dr, dash, "2"'] & & \langle g^3 \rangle^+ \arrow[dl, dash, "3"] \\
 & G \arrow[rrrr, leftrightarrow] & & & & \mathbb{Q} &
\end{tikzcd}$$

Find $\langle g^2 \rangle^+$

Two methods:

i) "Literal minded"

Let $x \in L$ $\quad x = a + b\omega + c\omega^2 + d\omega^3 + e\omega^4 + f\omega^5 \quad (a, b, c, d, e, f \in \mathbb{Q})$ uniquely

$\langle g^2 \rangle^+ = \{x \in L : h(x) = x \ \forall$ ~~x~~ $h \in \langle g^2 \rangle\}$.

$\quad = \{x \in L : g^2(x) = x\}$.

$g^2(\omega) = \omega^9 = \omega^2$

$$g^2(a + b\omega + c\omega^2 + d\omega^3 + e\omega^4 + f\omega^5) = a + b\omega^2 + c\omega^4 + d\omega^6 + e\omega^8 + f\omega^{10}$$

$$= a + b\omega + c\omega^4 + d(-1 - \omega - \omega^2 - \omega^3 - \omega^4 - \omega^5) + e\omega + f\omega^3$$

$$= (a-d) + \omega(e-d) + \omega^2(b-d) + \omega^3(f-d) + \omega^4(c-d) - d\omega^5$$

$\Rightarrow d = 0, \ b = e, \ b = c, \ f = d = 0$

~~$x = a + b\omega^2 + b\omega^2 \quad (a, b \in \mathbb{Q})$~~ $x = a + b\omega + b\omega^2 + b\omega^4 \quad (a, b \in \mathbb{Q})$

$\langle g^2 \rangle^+ = \{a + b(\omega + \omega^2 + \omega^4) : a, b \in \mathbb{Q}\}$

$\quad = \mathbb{Q}(\omega + \omega^2 + \omega^4)$

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

$g^3(\omega^2) = \omega^4$

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

$$\begin{tikzcd}
\omega \arrow[rr, bend left, "g^2"] & & \omega^2 \arrow[dl, "g^2"] \\
 & \omega^4 \arrow[ul, "g^2"] &
\end{tikzcd}$$

$\therefore \ x = \omega + \omega^2 + \omega^4 \in \langle g^2 \rangle^+ \quad \mathbb{Q}(x) \subseteq \langle g^2 \rangle^+$

By Fundemental Thm $\mathbb{Q}(x) = \mathbb{Q}$ or $\langle g^2 \rangle^\dagger$

If $\mathbb{Q}(x) = \mathbb{Q} \Rightarrow x \in \mathbb{Q}$

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

$f(t) = t^4 + t^3 + t - q \quad f(\omega) = 0$

Contradicton min poly of ω of degree 6.

So $\mathbb{Q}(x) = \langle g^2 \rangle^\dagger$

$g^3(\omega) = \omega^6, \quad g^3(\omega^6) = \omega$

$\omega + \omega^6 \in \langle g^3 \rangle^\dagger$

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

$\mathbb{Q}(\omega + \omega^6) \neq \mathbb{Q}$ (similar argument as above)

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

ω^6 conjugate of ω so $\mathbb{Q}(\omega + \omega^6) = \mathbb{Q}(\cos 2\pi/7)$.

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

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

$\alpha + \alpha^2 = 2\omega + 2\omega^2 + 2\omega^3 + 2\omega^4 + 2\omega^5 + 2\omega^6$
$= -2$

$\alpha^2 + \alpha + 2 = 0$

$$\alpha = \frac{-1 \pm \sqrt{-7}}{2}$$

Soluble Subgroups.

Definition:

A group G is soluble if $\exists$ subgroups $G_0 \dots G_n$ of G such that $\{e\} = G_0 \leq G_1 \leq \dots \leq G_n = G$. such that $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i ~~are~~ is abelion

eg. G abelion $\Rightarrow G$ soluble

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

$G_1/G_0 = G$ abelion

D_n is soluble

$D_n = \langle x, y : x^n = y^2 = e, \ yx = x^{-1}y \rangle$

$\{e\} = G_0 \leq G_1 = \langle x \rangle \leq G_n = G$.

$$\begin{tikzcd}
G_2 = G \arrow[d, dash, "\triangle"] & \\
G_1 = \langle x \rangle \arrow[d, dash, "\triangle"] & G_2/G_1 \cong C_2 \\
\{e\} = G_0 & G_1 \cong C_n.
\end{tikzcd}$$

Theorem:

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

i) G soluble $\Rightarrow$ H soluble.
ii) G soluble $\Rightarrow$ G/N soluble
iii) N and G/N soluble $\Rightarrow$ G soluble.

Proof:
i) Let $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_n = G$, $G_i \trianglelefteq G_{i+1}$. G_{i+1}/G_i abelion.
Let $H_i = G_i \cap H$
Then $\{e\} = H_0 \leq H_1 \leq \ldots \leq H_n = H$
$H_i \trianglelefteq H_{i+1}$ (if $x \in H_{i+1}$, $h_i \in H_i$ then $x^{-1} h_i x \in G_i$ (because $h_i \in G_i$
$x \in G_i$, $G_i \trianglelefteq G_{i+1}$) $x^{-1} h_i x \in H$ (because $x, h_i \in H$)
so $x^{-1} h_i x \in H_i$).

$$\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)}$$
$$\cong \frac{G_i (G_{i+1} \cap H)}{G_i} \leq \frac{G_{i+1}}{G_i} \leftarrow \text{abelion}$$

$\frac{H_{i+1}}{H_i}$ is abelion

H soluble.

Theorem:

Let G be a finite simple soluble group. Then $G \cong C_p$.

Proof: We have $\{e\} = G_0 \leq G_1 \leq \ldots \leq G_{n-1} \leq G_n = G$ st $G_i \trianglelefteq G_{i+1}$ and G_{i+1}/G_i is abelion.
$G_{n-1} \trianglelefteq G$. By simplicity $G_{n-1} = \{e\}$.
$G = G_n / G_{n-1}$ is abelion
G abelion simple
Let $e \neq g \in G$.
Then $\langle g \rangle \trianglelefteq G$
$\langle g \rangle = G$
$G = C_n$
If n is not prime, C_n has subgroups, so $G = C_p$.

Corollary:

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

Proof: Suppose S_n is soluble
Then $A_n \trianglelefteq S_n$ soluble
But A_n is simple (proof omitted, look in book).
$A_n \cong C_p$, not true, A_n not soluble
S_n not soluble.

Solutions By Radicals.

Definition:

An extension $L:K$ is radical if $\exists\ \alpha_1, \dots \alpha_n \in L$ such that

1) $L = K(\alpha_1, \dots, \alpha_n)$
2) $\exists\ n_i \in \mathbb{N}$ st $\alpha_i^{n_i} \in K(\alpha_1, \dots, \alpha_{i-1})$ $(i = 1 \dots n)$.

eg. $n = 3$
$L = K(\alpha_1, \alpha_2, \alpha_3)$
$\alpha_1^{n_1} \in K$
$\alpha_2^{n_2} \in K$
$\alpha_3^{n_3} \in K$
The α_i are called the radical sequence for $L:K$.

$$\begin{tikzcd}
K(\alpha_1,\alpha_2)(\alpha_3) \arrow[d, dash] & \mathbb{Q}(\sqrt[5]{2}, \sqrt[3]{3-\sqrt[5]{2}}, \sqrt{2+3\sqrt[3]{3-\sqrt[5]{2}}}) \arrow[d, dash] \\
K(\alpha_1)(\alpha_2) \arrow[d, dash] & \mathbb{Q}(\sqrt[5]{2})(\sqrt[3]{3-\sqrt[5]{2}}) \arrow[d, dash] \\
K(\alpha_1) \arrow[d, dash] & \mathbb{Q}(\sqrt[5]{2}) \arrow[d, dash] \\
K. & \mathbb{Q}.
\end{tikzcd}$$

Idea to show quintic not soluble by radicals.

1. S_5 not soluble
2. $M:K$ radical then $\Gamma(L:K)$ is soluble for any $K \leq L \leq M$.
3. $\exists$ quintic f over $\mathbb{Q}$, splitting field Σ st $\Gamma(\Sigma:\mathbb{Q}) \cong S_5$.

Lemma:

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

Proof: Let $L = K(\alpha_1 \ldots \alpha_r)$ $\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$.

Let f_i = min poly of α_i over

$f = f_1 \ldots f_r$. Then M splitting field of f over K.

Let the roots of f_i $\alpha_i = \beta_{i1}, \ldots \beta_{i,p_i}$

$M = K(\beta_{11}, \beta_{12}, \ldots \beta_{1p_1}, \beta_{2,1}, \ldots \beta_{2,p_2}, \ldots \beta_{r1}, \ldots \beta_{r,p_r})$.

Since α_i and β_{ij} are roots of the same min poly f_i, by 6.13

$\exists$ K-isomorphism $\sigma : K(\alpha_i) \longrightarrow K(\beta_{ij})$.

By 11.4 σ extents to a K-automorphism $\tau : M \longrightarrow M$.

$\alpha_i^{n_i} \in K(\alpha_1, \ldots, \alpha_{i-1})$ say $\alpha_i^{n_i} = g(\alpha_1 \ldots \alpha_{i-1})$

$\tau(\alpha_i^{n_i}) = \tau(g(\alpha_1, \ldots, \alpha_{i-1}))$

$\tau(\alpha_i^{n_i}) = g(\tau(\alpha_1) \ldots \tau(\alpha_{i-1}))$.

$\beta_{ij}^{n_i} \in g(\tau(\alpha_1), \ldots, \tau(\alpha_{i-1}))$

~~$\in$~~ $f_i(\alpha_i) = 0$

$\tau(f_i(\alpha_i)) = \tau(0) = 0$

$f_i(\tau(\alpha_i)) = 0$

$\tau(\alpha_i)$ = some β_{i,q_i}

$\beta_{ij}^{n_i} = g(\beta_{1q_1} \ldots \beta_{i-1 q_{i-1}})$

$\beta_{ij}^{n_i} \in K(\beta_{11} \ldots \beta_{1p_1} \ldots \beta_{i-1 p_1}, \ldots \beta_{i-1, p_{i-1}})$.

$\beta_{11}, \beta_{12}, \ldots \beta_{1p_1}, \beta_{2,1} \ldots \beta_{2p_2} \ldots \beta$ is a radical sequence for M.

Lemma

Let p be a prime, L splitting field of $t^p - 1$ over K. Then $\Gamma(L:K)$ is abelian

Proof: Roots of $t^p - 1$ are ω^i $(i = 0, 1 \ldots, p-1)$ $\omega = e^{2\pi i/p}$, so $L = K(\omega)$.

Any $g \in \Gamma(L:K)$ is determined by $g(\omega)$ and $g(\omega) = \omega^i$ for some i

Suppose $g(\omega) = \omega^i$, $h(\omega) = \omega^j$

$(gh)(\omega) = g(h(\omega)) = g(\omega^j) = g(\omega)^j = \omega^{ij}$

$(hg)(\omega) = \ldots \ldots = \omega^{ij}$

$gh = hg$ so $\Gamma(L:K)$ is abelian.

Lemma:

Suppose $t^n - 1$ splits & in K (ie $\omega = e^{2\pi i/n} \in K$). Let a be splitting field of $t^n - a$ over K for some $a \in K$. Then $\Gamma(L:K)$ is abelian.

Proof: Let α be a root of $t^n - a$ in L.

Then the other roots are $\alpha\omega, \alpha\omega^2, \ldots \alpha\omega^{n-1}$

So $L = K(\alpha, \omega) = K(\alpha)$

Any $g \in \Gamma(L:K)$ is determined by $g(\alpha)$ and $g(\alpha) = \alpha\omega^i$ for some i

Then if $h(\alpha) = \alpha\omega^j$, then $(gh)(\alpha) = \alpha\omega^{ij} = (hg)(\alpha)$

$gh = hg$.

$\Gamma(L:K)$ abelian.

Lemma:

$L:K$ normal and radical $\Rightarrow \Gamma(L:K)$ soluble.

Proof: $L = K(\alpha_1 \ldots \alpha_m)$ $\alpha_i^{n_i} \in K(\alpha_1 \ldots \alpha_{i-1})$

wlog, all n_i prime

Prove by induction on m, write $p = n_1$

$\alpha_1^p \in K$, may assume $\alpha_1 \notin K$.

Let f = min poly of α_1 over K.

Since $L:K$ normal, f splits in L.

Let β be another root of f in L.

Let $\varepsilon = \alpha_1/\beta$ so $\varepsilon^p = \alpha_1^p/\beta^p = 1$

Hence $\varepsilon \neq 1$ has order p. and $1, \varepsilon, \ldots, \varepsilon^{p-1}$ are the p^{th} roots of unity.

$t^p - 1$ splits in L.

Let $M \subseteq L$ be the splitting field of $t^p - 1$ over K

ie $M = K(\varepsilon)$.

Consider

$$\begin{tikzcd} L \arrow[d, dash, "1"] \\ M(\alpha_1) \arrow[d, dash, "2"] \\ M \arrow[d, dash, "3"] \\ K \end{tikzcd}$$

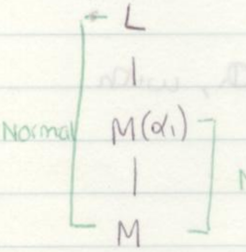
1 $L:M(\alpha_1)$ normal

$L:M(\alpha_1)$ is radical, with radical sequence $\alpha_1, \alpha_2, \ldots \alpha_m$.

By induction $\Gamma(L:M(\alpha_1))$ is soluble

2. $M(\alpha_1)$ = splitting field of $t^p - \alpha_1^p$ over M.
By 15.6 $\Gamma(M(\alpha_1):M)$ is abelian.

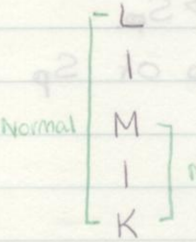
3. $\Gamma(M:K)$ is an abelian by 15.5.



By Fundemental Thm
$$\underbrace{\Gamma(M(\alpha_1):M)}_{\text{soluble}} \cong \Gamma(L:M) \big/ \underbrace{\Gamma(L:M(\alpha_1))}_{\text{soluble}}.$$

$\Gamma(L:M)$ has a normal subgroup $\Gamma(L:M(\alpha_1))$ which is soluble with soluble quotient

By 14.4(3) $\Gamma(L:M$ is soluble.



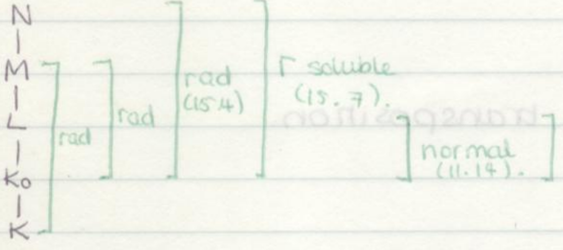
$$\underbrace{\Gamma(M:K)}_{\text{soluble}} \cong \Gamma(\cancel{R}L:K) \big/ \underbrace{\Gamma(L:M)}_{\text{soluble.}}$$

By same argument $\Gamma(L:K)$ is soluble.

Theorem:

Let $K \subseteq L \subseteq M$ and $M:K$ radical. Then $\Gamma(L:K)$ soluble.

Proof: Let K_0 = fixed field of $\Gamma(L:K)$ and let $N:K_0$ = normal closure of $M:K_0$.



$$\overbrace{\underbrace{\Gamma(L:K_0) \cong \Gamma(N:K_0)/\Gamma(N:L)}_{\text{Soluble}} \quad \underbrace{\Gamma(L:K)}_{\text{soluble.}}}^{=}$$

Theorem:

Let $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$ is not soluble by radicals.

Proof:

1. L = splitting field of f over $\mathbb{Q}$. Show $\Gamma(L:\mathbb{Q}) \cong S_5$.

2. Hence $\Gamma(L:\mathbb{Q})$ is not soluble

3. Hence by 15.3 if $K \subseteq L \subseteq M$, M is not radical.

4. So by def^n, f is not soluble by radicals.

Lemma

Let f be an irreducible polynomial of degree p (prime) over $\mathbb{Q}$, with exactly 2 non-real roots.
Let L = splitting field of f over $\mathbb{Q}$. Then $\Gamma(L:\mathbb{Q}) \cong S_p$.

Proof: If roots of f are $\alpha_1 \dots \alpha_p$ (all distinct since f irr), then any $g \in \Gamma(L:\mathbb{Q})$ is determined by $g(\alpha_1) \dots g(\alpha_p)$. and each $g(\alpha_i) = \alpha_j$ for some j.
Say $g(\alpha_i) = \alpha_{\sigma(i)}$. Then $\sigma \in S_p$
The map $g \mapsto \sigma$ is a group homomorphism $\Gamma(L:\mathbb{Q}) \rightarrow S_p$.
We can think of ~~the galois group~~ $\Gamma(L:\mathbb{Q})$ as a subgroup of S_p
So $G \leq S_p$.
$[L:\mathbb{Q}]$ is divisible by p (Tower Law: $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq L$).
$\therefore$ p divides $|G|$.
$\therefore$ G has an element of order p (Cauchy's Thm or from Sylow Thm).
Only elements of order p is S_p are the p-cycles.
t = complex conjugation induces an element of G, which is a 2-cycle (switches 2 non-real roots, fixes others).
wlog $t = (1\ 2)$
Also by taking a power of p-cycle, wlog $c = (1\ 2\ 3 \dots p) \in G$.
$c t c^{-1} = (2\ 3)$
$c^2 t c^{-2} = (3\ 4)$
all adjacent transpositions $\in G$.
every $\sigma \in S_p$ is a product of adjacent transposition
$\therefore$ $G \cong S_p$.

it only remains to show that $f(t) = t^5 - 6t + 3$ is irreducible with exactly 2 non-real roots
Irreducible by Eisenstiens prime 3