3202 Galois Theory Notes

Based on the 2014 spring 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 whatsoever 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.

MATH3202 — Galois Theory.

14 January 2013
Dr Mark L ROBERTS
Torrington Pl Galton LT

Overview of course. Galois Theory includes:

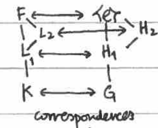
(a) Establishing a 1-to-1 correspondence between field extensions and groups (Fundamental Theorem)

(b) Analysing solutions to polynomial equations by using this correspondence: In particular, showing that the general quintic cannot be solved in "radicals".

(c) Providing solutions to classical geometric problems such as "squaring the circle".

(a) Fundamental Theorem.

We associate to a field extension $K:F$ a group G, called the Galois group of $K:F$ ($F \subseteq K$ e.g. $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$), and under certain conditions this establishes a 1-to-1 correspondence between intermediate fields L (i.e. $F \subseteq L \subseteq K$) and subgroups of G.



Notice that this fits into two general ideas:

① The Galois group G is the automorphism group of the extension $F:K$, i.e. the group of bijections $f: F \to F$ such that f preserves the field structure i.e. $f(e_1+e_2) = f(e_1)+f(e_2)$, $f(e_1e_2) = f(e_1)f(e_2)$ and $f(h)=h$ for all $h \in K$. e.g. Galois group of $\mathbb{C}:\mathbb{R} = \{id, c\}$ where c is complex conjugation.
In general, one of the ways of investigating a mathematical object is to consider its automorphism group. e.g. $X = \{1, \dots, n\}$, $Aut(X) = \{f: X \to X \text{ bijections}\} = S_n$.
e.g. if V is a vector space over $\mathbb{R}$, $Aut(V) = \{f: V \to V, f \text{ linear bijective}\} \cong GL_n$ e.g. G a group, $Aut(G) = \{f: G \to G, f \text{ group isomorphism}\}$.
In each case, the group operation is composition of mappings.
(More general idea).

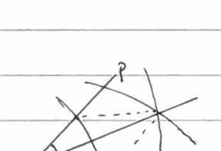
② Attaching an algebraic object (e.g. group) to a different object to analyse it. e.g. In algebraic topology: cohomology groups, homotopy groups etc can be used in classifying surfaces. Consider a surface, with paths (simple) from a point to itself. If we consider all paths that can be deformed uniformly into each other, we get a group of homotopy classes of loops at x. For a sphere, group is $\{e\}$; for a torus, group is $\mathbb{Z} \times \mathbb{Z}$.

(b) Solving polynomial equations.

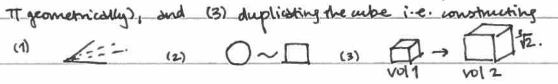
For a general quadratic equation, $t^2+bt+c=0 \Rightarrow t = \frac{-b \pm \sqrt{b^2-4c}}{2}$, the "radical" solution. We then examine higher degrees: degree 3 (cubic) was only solved in general about 400 years ago. Suppose we seek to solve $t^3+at^2+bt+c=0$. Write $y = t + \frac{a}{3}$. Then $y^3 = t^3 + 3t^2\left(\frac{a}{3}\right) + \dots \Rightarrow y^3+py+q=0$. Then let $y = u+v \Rightarrow (u+v)^3 + p(u+v) + q = 0$.
Expanding this gives $u^3+v^3+3u^2v+3uv^2+p(u+v)+q=0 \Rightarrow u^3+v^3+(3uv+p)(u+v)+q=0$. If $\begin{cases} u^3+v^3=-q \\ 3uv=-p \end{cases}$ can be solved, system gives $y=u+v$ as a solution.
$\Rightarrow 27u^3v^3 = -p^3$, then rename $\begin{matrix} u = U^3 \\ v = V^3 \end{matrix} \Rightarrow \begin{matrix} u+v=-q \\ 27uv = -p^3 \end{matrix} \Rightarrow 27u(-q-u) = -p^3 \Rightarrow u^2 + qu - \frac{p^3}{27} = 0$; which is quadratic and soluble. This eventually yields $u = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and therefore $y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$, which is a solution in radicals. The quartic can be resolved similarly. So, could we conjecture that any polynomial equation can be solved by radicals? No! In fact, the general quintic cannot be solved by radicals. This is established using the Fundamental Theorem.
(i) Attach to a polynomial equation a field extension (e.g. $t^2-2=0$ gives the extension $\mathbb{Q}[\sqrt{2}]:\mathbb{Q}$. (ii) suppose quintic can be solved by radicals, then we show that this corresponds to a chain of intermediate fields. (iii) By Fundamental Theorem, the Galois group has a certain chain of subgroups (iv) However, group theory shows it doesn't have such a chain.

(c) Geometric constructions.

These are questions of what can be constructed with a "rule and compass" (dating from classical antiquity). e.g. bisecting an angle:



Likewise, we can construct $\sqrt{2}$ by Pythagoras's Theorem. There are three classical problems left — (1) trisecting the angle, (2) squaring the circle i.e. constructing a square of area equal to a given circle (which reduces to whether we can construct π geometrically), and (3) duplicating the cube i.e. constructing a cube of double the volume of a given cube



All these three can be shown to be impossible using Galois Theory.

Required knowledge for course — Pre-requisites are basic linear algebra (particularly bases and dimension), some knowledge of groups (c.f. MATH7202 e.g. Lagrange's Thm, normal subgroups, Sylow's theorems etc), and a reasonable level of comfort with performing algebraic calculations (e.g. find all subgroups of a given group), as well as ideas from abstract algebra (e.g. quotients G/N).
Set text for course is Ian Stewart's *Galois Theory*. Structure of course will be mainly taught, with volunteer teaching and a mini-project in groups with a presentation (10%) and coursework.
Access moodle page for more resources and handouts.

We review some criteria for evaluating irreducibility: 16 January 2014. Dr Mark L ROBERTS.

(1.) $f \in k[t]$ is irreducible if $f(t) = g(t)h(t)$, $g, h \in k[t] \Rightarrow g$ or h is a unit

(2) Every polynomial $f \in k[t]$ can be factorised uniquely into a product of irreducibles

(3) over $\mathbb{C}[t]$, every irreducible is of degree 1.

(4) Let $f \in \mathbb{Z}[t]$. If f is irreducible over $\mathbb{Z}$, it is irreducible over $\mathbb{Q}$ (Gauss's Lemma)

(5) Let $f \in \mathbb{Z}[t]$, $f(t) = a_n t^n + a_{n-1}t^{n-1} + \dots + a_1 t + a_0$. If p is a prime and $p \nmid a_n$, $p \mid a_{n-1}, \dots, a_1, a_0$, $p^2 \nmid a_0$, then f is irreducible (Eisenstein's criterion).

(6) Let $f \in \mathbb{Z}[t]$, $f(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$. Let $\bar{f}$ be f regarded as a polynomial in $\mathbb{Z}_p[t]$ i.e. $\bar{f} = t^n + \overline{a_{n-1}}\, t^{n-1} + \dots + \bar{a}_0$.

Then $\bar{f}$ irreducible in $\mathbb{Z}_p[t] \Rightarrow f$ irreducible in $\mathbb{Z}[t]$.

21 January 2014
Dr. Mark L ROBERTS.
Torrington Pl Galton LT.

§4 FIELD EXTENSIONS.

Definition 4.1 A field extension is a field monomorphism $i: K \to L$, where K and L are fields ($\subseteq \mathbb{C}$).

Remark – Recall that a monomorphism is an injective homomorphism (map that preserves algebraic structure: $i(1) = 1$, $i(x^{-1}) = i(x)^{-1}$, $i(x+y) = i(x) + i(y)$, $i(xy) = i(x)i(y)$).

Usually, we can identify $i(K)$ with K, since $K \cong i(K)$. Then we have $K \subseteq L$ and we write $L : K$.

Examples – $\mathbb{R} : \mathbb{Q}$ is a field extension, $\mathbb{C} : \mathbb{R}$ is a field extension. If $P = \{a + bi : a, b \in \mathbb{Q}\}$, then P is a field – P contains 0 and 1 and is closed under + and x.

If $a + bi \neq 0$, then $(a+bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in P$. Thus, $P : \mathbb{Q}$ is a field extension.

Definition 4.3 Let X be a subset of $\mathbb{C}$, then the <u>subfield of $\mathbb{C}$ generated by X</u> is the intersection of all subfields of $\mathbb{C}$ containing X, i.e. $\langle X \rangle = \bigcap_{X \subseteq F \subseteq \mathbb{C}} F$ for F fields.

$\langle X \rangle$ is the unique smallest subfield of $\mathbb{C}$ containing X = set of all elements obtained from X by a finite sequence of algebraic operations. e.g. $(x_1 + 2x_2)^{-1} + (x_2 + x_1^2)^{-3}$.

e.g. – $\langle i \rangle = \{a + bi : a, b \in \mathbb{Q}\}$ is the subfield of $\mathbb{C}$ generated by $\{i\}$.

Proposition 4.4 Every subfield of $\mathbb{C}$ contains $\mathbb{Q}$.

Proof – Let $K \subseteq \mathbb{C}$ be a subfield. Then $1 \in K \Rightarrow \therefore \forall n \in \mathbb{N}, n = 1 + \dots + 1 \in K \therefore -n \in K \therefore \forall z \in \mathbb{Z}, z \in K$. $\forall b \neq 0, b \in \mathbb{N}, b^{-1} \in K \Rightarrow \forall a, b \in \mathbb{Z}, b \neq 0, ab^{-1} \in K$

i.e. $\mathbb{Q} \subseteq K$ // q.e.d.

We use notation $\mathbb{Q}(X)$ for some subfield of $\mathbb{C}$ generated by X. e.g. $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$. (less obvious that this is a field).

Definition 4.7 Let $L : K$ be a field extension and $Y \subseteq L$, then $K(Y)$ = field generated by $K \cup Y$. This is called the field obtained by <u>adjoining</u> Y to K.

Note – Here $K(y)$ is an abbreviation for $K(\{y\})$, $K(y_1, \dots, y_n)$ is an abbreviation for $K(\{y_1, \dots, y_n\})$.

e.g. – $\mathbb{Q}(i, \sqrt{5})$ = smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$, i and $\sqrt{5}$. This contains $\{a + bi + c\sqrt{5} + di\sqrt{5} : a, b, c, d \in \mathbb{Q}\} = T$. If we show T is a field, then $\mathbb{Q}(i, \sqrt{5}) = T$.

T is closed under $+, \times, -$; so only need to show that T is closed under inverses. Proof is given in book, pg 62.

Let K be a field. What is $K[t]$? $K[t] = \{(\alpha_0, \alpha_1, \dots, \alpha_n) : \alpha_i \in K, \exists M \text{ s.t. } \alpha_n = 0 \ \forall n > M\}$. ie. it looks like $(\alpha_0, \alpha_1, \dots, \alpha_M, 0, 0, \dots) \leftrightarrow (\alpha_0 + \alpha_1 t + \dots + \alpha_M t^M)$.

We can write down rules for adding and multiplying: adding component-wise, multiplication $(\alpha_0, \alpha_1, \dots)(\beta_1, \dots, \beta_m, \dots) = (\gamma_1, \gamma_2, \dots)$, $\gamma_r = \sum_{i=0}^{r} \alpha_i \beta_{r-i}$. Then $K[t]$ is an integral domain.

$K(t)$ = rational functions = $\{\frac{f(t)}{g(t)} : f(t), g(t) \in K[t], g(t) \neq 0\}$. If we do not want to think of these as functions, we need the more general idea of field of fractions of an integral domain.

e.g. – $\mathbb{Z} \hookrightarrow \mathbb{Q}$. Consider $\mathbb{Z} \times \mathbb{Z}^* = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$. Define an equivalence relation $\sim$ on $\mathbb{Z} \times \mathbb{Z}^*$. [Recall = set X with equivalence relation $\sim$. s.t. $a \sim a$, $a \sim b \Rightarrow b \sim a$, $a \sim b$ and $a \sim c \Rightarrow a \sim c$].

$(a, b) \sim (c, d)$ if $ad = bc$. Let $\mathbb{Q} = \{[a, b] : a, b \in \mathbb{Z}, b \neq 0\}$. $1/2 \leftrightarrow \{(1,2), (2,4), (3,6), \dots\}$. equivalence class $[a] = \{x \in X : a \sim x\}$. X is the disjoint union of equivalence classes.

check: $\mathbb{Q}$ is a field contained in $\mathbb{Z}$ s.t. every element of $\mathbb{Q}$ is of form $r^{-1}s$ ($r, s \in \mathbb{Z}, r \neq 0$). This works in general for R any integral domain.

In particular, $K[t] \hookrightarrow K(t)$.

<u>Simple Extensions.</u>

Definition 4.10 An extension $L : K$ is simple if $\exists \alpha \in L$ s.t. $L = K(\alpha)$.

e.g. – $\mathbb{Q}(i) : \mathbb{Q}$ is simple. What about $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$? Not evidently simple, but in fact it is as $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Clearly $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. For reverse inclusion,

write $\alpha = \sqrt{2} + \sqrt{3}$. We want to show $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha)$. We then see that $\alpha^2 = 2 + 3 + 2\sqrt{6} \in \mathbb{Q}(\alpha)$, so $\sqrt{6} \in \mathbb{Q}(\alpha)$, and $\alpha\sqrt{6} \in \mathbb{Q}(\alpha)$ i.e. $2\sqrt{3} + 3\sqrt{2} \in \mathbb{Q}(\alpha)$.

then $\alpha\sqrt{6} - 2\alpha = 2\sqrt{3} + 3\sqrt{2} - 2\sqrt{3} - 2\sqrt{2} = \sqrt{2} \in \mathbb{Q}(\alpha)$. Thus $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha) \Rightarrow \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha)$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha) \Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$ // q.e.d.

More efficient way: $\alpha^{-1} = \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\alpha)$, so $\sqrt{3} = \frac{1}{2}(\alpha + \alpha^{-1}) \in \mathbb{Q}(\alpha)$ etc.

$\mathbb{R} : \mathbb{Q}$ is not simple. Recall that a set X is countable if $\exists$ bijection $\varphi : \mathbb{N} \to X$. $\mathbb{Q}$ is countable, so $\mathbb{Q}(\alpha)$ is countable for any α. However, $\mathbb{R}$ is uncountable.

Therefore $\mathbb{R} \neq \mathbb{Q}(\alpha)$ for any α.

If we take $\mathbb{Q}(s, t) : \mathbb{Q}$, it is not simple [$\mathbb{Q}(s,t)$ = set of rational functions in s and t]. $\mathbb{Q}(e, \pi) : \mathbb{Q}$ is not simple.

202-02

Definition 4.12 let $i: K \to \hat{K}$, $j: L \to \hat{L}$ be two field extensions. then an <u>isomorphism</u> between these two extensions is a pair (λ, μ) of field isomorphisms $\lambda: K \to L$ and $\mu: \hat{K} \to \hat{L}$ s.t. $\forall k \in K$, $\mu(i(k)) = j(\lambda(k))$. if (as often) we think of $K \subseteq \hat{K}$, $L \subseteq \hat{L}$, the condition reduces to $\mu|_K = \lambda$

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

i.e. the diagram on the right commutes. often also $K = L$ and $\lambda = id$, and we get $\mu|_K = id$.

e.g. – consider $\overset{\alpha=}{\sqrt[3]{2}}$ and $\overset{\beta=}{\sqrt[3]{2}\,\omega}$ where $\omega = e^{2\pi i/3}$. these are two cube roots of 2. As far as algebras over $\mathbb{Q}$ are concerned, α and β are indistinguishable. 23 January 2014 Dr Mark L ROBERTS. Chadwick LT.

All we know is that $\alpha^3 = 2$, $\beta^3 = 2$. this means that the extensions $\mathbb{Q}(\alpha):\mathbb{Q}$ and $\mathbb{Q}(\beta):\mathbb{Q}$ are isomorphic.

$$\begin{tikzcd} \mathbb{Q}(\alpha) \arrow[r, "\lambda"] & \mathbb{Q}(\beta) \\ \mathbb{Q} \arrow[u, phantom, "\cup|"] \arrow[r, "id"] & \mathbb{Q} \arrow[u, phantom, "\cup|"] \end{tikzcd}$$

$\lambda\left(\frac{p(\alpha)}{q(\alpha)}\right) = \frac{p(\beta)}{q(\beta)}$.

§5 SIMPLE EXTENSIONS.

A simple extension is of the form $K(\alpha):K$. There are two basic possibilities for α:

Definition 5.1 let $K \subseteq \mathbb{C}$, $\alpha \in \mathbb{C}$. then if $\exists\, p(t) \in K[t]$, $p(t) \not\equiv 0$ s.t. $p(\alpha) = 0$, then α is called <u>algebraic</u> over K. otherwise, α is <u>transcendental</u> over K.

e.g. $\sqrt{2}$ is algebraic over $\mathbb{Q}$: $p(t) = t^2 - 2$. π is transcendental over $\mathbb{Q}$. $\alpha = \sum_{n=1}^{\infty} 10^{-n!} = 0.1\overset{(1)}{1}\overset{(2)}{0}00\overset{(6)}{1}0 \cdots \overset{(24)}{1}0 \cdots$ is transcendental over $\mathbb{Q}$.

$\sqrt{\pi}$ is algebraic over $\mathbb{Q}(\pi)$: $p(t) = t^2 - \pi \in \mathbb{Q}(\pi)[t]$.

We call the extension $K(\alpha):K$ algebraic if α is algebraic over K and transcendental otherwise.

Theorem 5.3 $K(t):K$ is a simple transcendental extension. $\left[K(t) = \left\{ \frac{f(t)}{g(t)} : f, g \in K[t], g \not\equiv 0 \right\} \right]$.

Proof – By definition, $p(t) \not\equiv 0$ for any $p(x) \in K[x]$.

Definition 5.4 A polynomial $f(t) = a_n t^n + \dots + a_0 \in K[t]$ is called <u>monic</u> if $a_n = 1$

Definition 5.5 let $L:K$ be a field extension and $\alpha \in L$, algebraic over K. Then there exists a unique polynomial $m \in K[t]$ of least degree s.t. $m(\alpha) = 0$. m is called the <u>minimal polynomial</u> of α (over K).

Proof – (uniqueness) let m be a polynomial of least degree s.t $m(\alpha) = 0$ [exists as extension is algebraic, least degree valid by well-ordering principle]. Dividing through by the top coefficient, we can assume m monic. Suppose m' is another such polynomial, Then $(m - m')(\alpha) = 0$ and $\deg(m - m') < \deg(m)$. Since m is of least degree, $m - m' = 0 \Rightarrow m = m'$, q.e.d.

e.g. – Minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $t^2 - 2$.

Proposition 5.6 let $L:K$ be a field extension, $\alpha \in L$ with minimal polynomial $m(t) \in K[t]$ over K. Then m is irreducible over K and if $f(t) \in K[t]$, $f(\alpha) = 0$ then f is a multiple of m.

Proof – suppose $m(t) = p(t)q(t)$. Then $0 = m(\alpha) = p(\alpha)q(\alpha) \Rightarrow p(\alpha) = 0$ or $q(\alpha) = 0 \Rightarrow \deg(p) \geq \deg(m)$ or $\deg(q) \geq \deg(m) \Rightarrow q$ constant or p constant $\Rightarrow$ factorisation trivial $\Rightarrow m$ irreducible.

suppose $f(\alpha) = 0$, we can write $f(t) = m(t)q(t) + r(t)$ where $\deg(r) < \deg(p)$. then $0 = f(\alpha) = \overset{0}{\widetilde{m(\alpha)}}\, q(\alpha) + r(\alpha) = r(\alpha) \Rightarrow r(\alpha) = 0 \Rightarrow$ by definition of m, $r(t) = 0$. thus, $f(t) = m(t)q(t)$, so f is a multiple of m.

Remark – Alternatively, this means that if $S = \{f(t) \in K[t] : f(\alpha) = 0\}$, then $S \lhd K[t]$ ideal, $K[t]$ is a PID so $S = mK[t]$ where WLOG m is monic.

30 January 2014
Dr Mark L ROBERTS.
Chadwick LT.

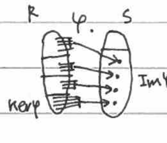
if $I = \{f(t) \in K[t] : f(\alpha) = 0\}$, then $I \lhd K[t]$, $I = m(t)K[t] = \{m(t)g(t) : g(t) \in K[t]\}$. let R be a ring, $I \lhd R$ ideal. $i_1, i_2 \in I \Rightarrow i_1 - i_2 \in I$. $i \in I, r \in R \Rightarrow ir \in I$.

Quotient ring $R/I = \{I + r : r \in R\}$ $I + r = \{i + r : i \in I\}$. e.g. $3\mathbb{Z} \lhd \mathbb{Z}$, $3\mathbb{Z} + 0 = \{\dots, -3, 0, 3, \dots\} = 3\mathbb{Z}$, $3\mathbb{Z} + 1 = \{\dots, -2, 1, 4, \dots\}$, $3\mathbb{Z} + 2 = \{\dots, -1, 2, 5, \dots\}$. $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$.

$(I + r) + (I + s) = I + (r + s)$, $(I + r)(I + s) = I + rs$. Check that this is well-defined, check R/I is a ring.

let R, S be rings. A map $\varphi: R \to S$ is a ring homomorphism if $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$, $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$ e.g. $\pi: R \to R/I$, $\pi(r) = I + r$. is a surjective ring homomorphism.

e.g. $\pi: \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $\pi(z) = 3\mathbb{Z} + z$. Then $\pi(0) = \pi(3) = \dots = \bar{0}$ etc.



Associate to each ring homomorphism $\varphi: R \to S$, we have $\ker\varphi = \{r \in R : \varphi(r) = 0\}$, $\operatorname{Im}\varphi = \{\varphi(r) : r \in R\}$. $\ker\varphi \lhd R$, $\operatorname{Im}\varphi$ is a subring of S.

Isomorphism theorem: let $\varphi: R \to S$ be a ring homomorphism. Then $R/\ker\varphi \cong \operatorname{Im}\varphi$.

Theorem 5.10* $m(t) \in K[t]$ irreducible $\Rightarrow K[t]/(m)$ is a field. $(m) = \{mf : f \in K[t]\} \lhd K[t]$.

Proof – $K[t]/(m)$ is a ring, so just need to show existence of multiplicative inverses. so suppose $\bar{f} \neq \bar{0}$, $\bar{f} \in K[t]/(m)$ [Here $\bar{f}$ means $(m) + f$]. Look at hcf(f, m) in $K[t]$.

since m irreducible, hcf$(f, m) = m$ then $m | f$, so $\bar{f} = \bar{0}$ (which we do not want). Thus hcf$(f, m) = 1$. By Bézout's identity, $\exists\, r, s \in K[t]$ s.t. $fr + ms = 1$. Then if $\pi: K[t] \to K[t]/(m)$, $\pi(f) = \bar{f}$,

$\pi(fr + ms) = \pi(1)$, $\bar{f}\bar{r} + \overset{0}{\overset{\shortparallel}{\bar{m}}}\bar{s} = \bar{1} \Rightarrow \bar{f}\bar{r} = \bar{1} \Rightarrow \bar{r} = \bar{f}^{-1}$ exists.

<u>classifying simple extensions.</u>

Theorem 5.11 let $K(\alpha):K$ be a simple transcendental extension. Then there is an isomorphism of extensions $\varphi: K(t):K \to K(\alpha):K$ s.t. $\varphi|_K = \mathrm{Id}$, $\varphi(t) = \alpha$. i.e. up to isomorphism, $\exists$ only 1 simple transcendental extension

Proof – Define $\varphi: K(t) \to K(\alpha)$ by $\varphi(f/g) = f(\alpha)/g(\alpha)$. this is well-defined since $g(\alpha) \neq 0$, so it is clearly a homomorphism. This is a monomorphism since $f(\alpha) = 0 \Rightarrow f = 0$.

$\varphi|_K = \mathrm{Id}$ and $\varphi(t) = \alpha$.

$$\begin{tikzcd} K(t) \arrow[r, "\varphi"', "t \mapsto \alpha"] & K(\alpha) \\ K \arrow[u, dash] \arrow[r, "\mathrm{Id}."'] & K \arrow[u, dash] \end{tikzcd}$$

Theorem 5.12 Let $K(\alpha):K$ be a simple algebraic extension. Let α have minimal polynomial $m \in K[t]$. Then there is an isomorphism of field extensions $\varphi: \frac{K[t]}{(m)}:K \longrightarrow K(\alpha):K$ s.t. $\varphi|_K = id$, $\varphi(\bar{t}) = \alpha$.

e.g. – Take $\frac{\mathbb{R}[t]}{(t^2+1)} \cong \mathbb{C}$ [$\because$ $t = \sqrt{-1}$] $= \mathbb{R}[i]$.

Proof – Define $\psi: K[t] \to K(\alpha)$ by $\psi(f(t)) = f(\alpha)$. ψ is a ring homomorphism. $\operatorname{Ker}\psi = \{f(t) : f(\alpha) = 0\} = (m)$. By isomorphism theorem, $\exists$ isomorphism $\varphi: \frac{K[t]}{(m)} \to \operatorname{Im}\psi = \operatorname{Im}\varphi$

Clearly, $\operatorname{Im}\varphi \subseteq K(\alpha)$. $\varphi(\bar{t}) = \alpha$. $\varphi|_K = id$. $\operatorname{Im}\varphi$ is a field because it is isomorphic to $\frac{K}{(m)}$ which is a field. It contains $\alpha = \varphi(\bar{t})$ and $K = \varphi(K)$.

Since $K(\alpha)$ by definition is the smallest field containing K and α, $\operatorname{Im}\varphi = K(\alpha)$.

4 February 2014
Dr Mark L ROBERTS.
Torrington Pl

Note that there are two ways of presenting $K[t]/(m)$: $\cdot$ $K[t]/(m) = \{\bar{f}(t) : \partial(f) < \partial(m)\}$ or $\cdot$ $K[t]/(m) = \{a_0 + a_1 t + \cdots + a_n t^n, a_i \in K, n = \partial(m) - 1\}$

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

e.g. $\mathbb{R}(i) \cong \mathbb{R}[t]/(t^2+1) = \{\overline{a+bt} : a, b \in \mathbb{R}\}$, $a + bi \mapsto \overline{a+bt}$. Hence, $K(\alpha) = \{f(\alpha) : f \in K(t) : \partial(f) < n = \text{deg of minimal polynomial}\}$.

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

This way is easier than representing $K(\alpha)$ as $\{\frac{f(\alpha)}{g(\alpha)} : f, g \in K(t), g \neq 0\}$.

Corollary 5.13 Let α, β be algebraic over K, with the same minimal polynomial. Then $K(\alpha) \cong K(\beta)$. More precisely, the field extensions are isomorphic ($K(\alpha):K \cong K(\beta):K$) by map $\varphi: K(\alpha) \to K(\beta)$, $\varphi(\alpha) = \beta$ s.t. $\varphi|_K = id$.

Proof – We have the following commutative diagram:

$$\begin{tikzcd} K(\beta) & K(t)/(m) \arrow[l, "\varphi_2"', "\beta \leftarrow \bar{t}"] \arrow[r, "\varphi_1", "\bar{t} \to \alpha"'] & K(\alpha) \\ K \arrow[u, dash] \arrow[r, dash, "id"'] & K \arrow[r, dash, "id"'] & K \arrow[u, dash] \end{tikzcd}$$

Then the required isomorphism is $\varphi_2 \circ \varphi_1^{-1}$ // q.e.d.

Definition 5.15 Let $i: K \to L$ be a field monomorphism. Then there is a ring monomorphism $\hat{i}: K(t) \longrightarrow L(t)$, $\hat{i}(a_0 + a_1 t + \cdots + a_n t^n) = i(a_0) + i(a_1)t + \cdots + i(a_n)t^n$. If i is an isomorphism, then so is $\hat{i}$.

Note – Formally, the maps i and $\hat{i}$ are different. However, we often write "i" for denoting both of them.

e.g. – $i: \mathbb{C} \to \mathbb{C}$, $i(a+bi) = a - bi$. Then $\hat{i}: \mathbb{C}[t] \to \mathbb{C}[t]$ by taking the conjugate of all coefficients of the polynomials.

Theorem 5.16 Let $i: K \xrightarrow{\cong} L$ be an isomorphism. If α has minimal polynomial m_α over K, β has minimal polynomial m_β over L, $i(m_\alpha) = m_\beta$; then $\exists$ an isomorphism $j: K(\alpha) \to K(\beta)$ s.t. the following diagram commutes (i.e. $j|_K = i$, if $x \in K$, then $j \circ ind(x) = ind \circ i(x) \Rightarrow j|_K = i$).

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

Remark – This is an extension theorem (the isomorphism extends i to j).

e.g. – Let $i: \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{Q}(\sqrt{2})$, $i(a + b\sqrt{2}) = a - b\sqrt{2}$ be an isomorphism between $\mathbb{Q}(\sqrt{2})$ and itself. Then $\begin{cases} \sqrt{3} \text{ has minimal polynomial } t^2-3 \text{ over } \mathbb{Q}(\sqrt{2}) \\ -\sqrt{3} \text{ has minimal polynomial } t^2-3 \text{ over } \mathbb{Q}(\sqrt{2}), \end{cases}$ $i(t^2-3) = t^2-3$.

Then we get the diagram on the right:

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

§6 DEGREE OF EXTENSIONS.

Theorem 6.1 If $L:K$ is a field extension, then L is a vector space over K.

e.g. – $\mathbb{C}:\mathbb{R}$ is an extension, $\mathbb{C}_{\mathbb{R}} = \{1, i\}$ is a basis for the vector space $\mathbb{C}$ over $\mathbb{R}$.

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

e.g. – $[\mathbb{C}:\mathbb{R}] = 2$ as the basis $\{1, i\}$ has 2 elements.

Theorem 6.7 Let $K(\alpha):K$ be a simple field extension. If α is transcendental over K, then $[K(\alpha):K] = \infty$. If α is algebraic over K, then $[K(\alpha):K] = \partial(m_\alpha)$ where m_α is the minimal polynomial of α over K.

Proof – Let α be transcendental. $K(\alpha) \cong K(t)$ and $\{1, t, t^2, \ldots\}$ are LI over K. $\dim_K K(t) \geq n+1$ $\forall n$ $\therefore \dim_K K(t) = \infty$.

Whereas if α is algebraic over K, then $K(\alpha) = \{f(\alpha) : f(t) \in K[t], \partial(f) < \partial(m_\alpha)\}$. $\therefore \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over $K \Rightarrow \dim_K K(\alpha) = n = \partial(m_\alpha)$ // q.e.d.

e.g. – Consider $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$. $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$. A basis for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$, so $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$.

Theorem 6.4 (Short Tower Law).

Let $K \subseteq L \subseteq M$ be a field extension. Then $[M:K] = [M:L] \cdot [L:K]$

Proof – Let $(x_i)_{i \in I}$ be a basis for L over K, $(y_j)_{j \in J}$ be a basis for M over L. $[L:K] = |I|$, $[M:L] = |J|$. Claim: $(x_i y_j)_{i \in I, j \in J}$ is a basis for M over K, s.t. $[M:K] = |I| \cdot |J| = [L:K][M:L]$

We need to prove LI and spanning. For LI: Suppose $\sum_{i \in I, j \in J} k_{ij} x_i y_j = 0$ $(k_{ij} \in K)$ $\Rightarrow \sum_{j \in J} \underbrace{\left(\sum_{i \in I} k_{ij} x_i\right)}_{\in L} y_j = 0$. Since (y_j) are LI over L, all $\sum_{i \in I} k_{ij} x_i = 0 \Rightarrow$ since (x_i) are LI over K, all $k_{ij} = 0$.

For spanning: Let $m \in M$. Since (y_j) span M over L, $\exists \alpha_j \in L$ s.t. $m = \sum_{j \in J} \alpha_j y_j$. Then since (x_i) span L over K, $\alpha_j = \sum_{i \in I} k_{ij} x_i$ for some $k_{ij} \in K \Rightarrow m = \sum_{j \in J} \alpha_j y_j = \sum_{i,j} k_{ij} x_i y_j$ // q.e.d.

e.g. – $[\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}] = 4$: We see that $\mathbb{Q}(\sqrt{2}, i) \xrightarrow{\text{deg}=2, \text{ because } i \notin \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}} \mathbb{Q}(\sqrt{2}) \xrightarrow{\text{deg}=2, \text{ because minimal polynomial is } t^2-2} \mathbb{Q} \Rightarrow [\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}] = 2 \times 2 = 4$.

Also, by proof of the theorem, a basis for $\mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$ is $\{1, \sqrt{2}\} \times \{1, i\} = \{1, \sqrt{2}, i, \sqrt{2}i\}$, $\mathbb{Q}(\sqrt{2}, i) = \{a + b\sqrt{2} + ci + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\}$.

(An alternative method).

Clearly, $\mathbb{Q}(i+\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, i)$. We then show reverse inclusion: $(\sqrt{2}+i)(\sqrt{2}-i) = 3 \Rightarrow (\sqrt{2}+i)^{-1} = \frac{1}{3}(\sqrt{2}-i) \in \mathbb{Q}(i+\sqrt{2}) \Rightarrow \sqrt{2} - i \in \mathbb{Q}(i+\sqrt{2}) \Rightarrow (\sqrt{2}+i) + (\sqrt{2}-i) = 2\sqrt{2} \in \mathbb{Q}(i+\sqrt{2})$

$\Rightarrow \sqrt{2} \in \mathbb{Q}(i+\sqrt{2})$. Similarly for $i \in \mathbb{Q}(i+\sqrt{2})$ $\therefore \mathbb{Q}(\sqrt{2}, i) \subseteq \mathbb{Q}(i+\sqrt{2}) \Rightarrow$ Together, $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i+\sqrt{2})$. Hence, $[\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}] = [\mathbb{Q}(i+\sqrt{2}):\mathbb{Q}] =$ deg. of minimal polynomial of $i+\sqrt{2}$.

To find the minimal polynomial, set $\alpha = i + \sqrt{2}$. $\alpha^2 = -1 + 2 + 2i\sqrt{2} = 1 + 2i\sqrt{2} \Rightarrow \alpha^2 - 1 = 2i\sqrt{2} \notin \mathbb{Q}$. $\Rightarrow (\alpha^2-1)^2 = -8 \Rightarrow \alpha^4 - 2\alpha^2 + 9 = 0$ and $f(t) = t^4 - 2t^2 + 9$ is [illegible] s.t. $f(\alpha) = 0$.

Then to show that this is indeed minimal, we need to show that it is irreducible. Clearly, $f(\pm 1) \neq 0$, $f(\pm 3) \neq 0$, $f(\pm 9) \neq 0$ so f has no linear factors. Then suppose that f has a quadratic factor i.e. $f(t) = (t^2 + at + b)(t^2 + ct + d) \Rightarrow$ contradiction (upon manipulation). Thus, $\partial(f) = 4 \Rightarrow [\mathbb{Q}(i+\sqrt{2}):\mathbb{Q}] = 4$.

Corollary 6.6 (Tower law).

Let $K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n$. Then $[K_n:K_0] = [K_1:K_0] \times [K_2:K_1] \times \cdots \times [K_n:K_{n-1}]$.

Definition 6.9 A finite extension is one which has a finite degree over K.

Definition 6.10 An extension $L:K$ is algebraic if every element of L is algebraic.

Remark – By following result, simple algebraic is algebraic. ($K(\alpha):K$, α is algebraic over K; $L:K$, all $\beta \in L$ algebraic over K.)

Lemma 6.11 $L:K$ is finite $\Leftrightarrow$ $L = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are algebraic over K $\overset{\text{defn.}}{\Leftrightarrow}$ $L:K$ is algebraic and (finitely generated) $L = K(\alpha_1, \dots, \alpha_n)$ for $\alpha_i \in L$.

Proof – ($\Rightarrow$) $L:K$ finite $\Rightarrow$ $L:K$ algebraic, so let $\{l_1, \dots, l_m\}$ be a K-basis for L over K $\Rightarrow$ is a generating set, $L = K(l_1, \dots, l_m) \Rightarrow L:K$ is f.g.

($\Leftarrow$) consider tower of fields $K \subseteq K(\alpha_1) \subseteq K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \subseteq \cdots \subseteq K(\alpha_1, \dots, \alpha_n) = K$. Each α_{i+1} algebraic over K, so $[K(\alpha_1, \dots, \alpha_{i+1}) : K(\alpha_1, \dots, \alpha_i)]$ finite $\Rightarrow$ by tower law, $[L:K]$ finite, q.e.d.

6 February 2014
Dr Mark L ROBERTS
Chadwick LT.

Refer to Handout « Some notes on end of chapter 6 »:

Lemma 5: If $[L:K]$ is finite, $\beta \in L \Rightarrow \beta$ is algebraic over K. Proof: Let $[L:K] = n < \infty$, $\beta \in L$. Set $\{1, \beta, \dots, \beta^n\}$ has $n+1$ elements, but $[L:K] = n$, so set is LD. $\Rightarrow \exists\, k_i \in K$ not all $0 \Rightarrow \sum_{i=0}^{n} k_i (\beta)^i = 0$.

Let $f(t) = \sum_{i=0}^{n} k_i t^i \Rightarrow$ non-zero polynomial s.t. $f(\beta) = 0 \Rightarrow \beta$ algebraic over K.

Corollary 6: If α is algebraic over K, $\beta \in K(\alpha) \Rightarrow \beta$ also algebraic over K. Proof: $[K(\alpha):K]$ is finite, so by Lemma 5, β is algebraic.

Note about Lemma 6.11 – We can put ($\Leftarrow$) more strongly. Suppose $L = K(\alpha_1, \dots, \alpha_n)$, α_i is algebraic over K $\forall i \Rightarrow [L:K]$ is finite (i.e. need not assume all elements of L are algebraic over K, only α_i).

§8 THE IDEA BEHIND GALOIS THEORY.

Definition 8.1 Let $L:K$ be a field extension ($L \subseteq \mathbb{C}$). Then a K-automorphism of L is a field automorphism $\alpha: L \to L$ s.t. $\alpha|_K = id$. [i.e. $\alpha: L \to L$ is bijective, $\alpha(l_1 - l_2) = \alpha(l_1) - \alpha(l_2)$, $\alpha(l_1 l_2) = \alpha(l_1)\alpha(l_2)$, $\alpha(k) = k$ $\forall k \in K$].

i.e. α is an automorphism of the extension $L:K$

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

Theorem 8.2 Let $L:K$ be a field extension. Then the set of all K-automorphisms of L forms a group under composition.

Proof – omitted

11 February 2014
Dr Mark L ROBERTS.
Torrington Pl.

Definition 8.3 The group in Theorem 8.2 is called the Galois group of $L:K$ denoted $\Gamma(L:K)$ or $Gal(L:K)$.

e.g. – $\cdot\ \mathbb{Q}(i):\mathbb{Q}$. $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$. Let $f: \mathbb{Q}(i) \to \mathbb{Q}(i)$ be an automorphism. Fixing $\mathbb{Q}$, $(f(i))^2 = f(i^2) = f(-1) = -1$, $f(i) = \pm i$. If $f(i) = i$, $f(a+bi) = f(a) + f(b)f(i) = a + bi$, $f = id$.

$f(i) = -i$, $f(a+bi) = a - bi$. This is a field automorphism (complex conjugation). Hence, $\Gamma(\mathbb{Q}(i):\mathbb{Q}) = \{id, c\} \cong C_2$.

$\cdot\ \mathbb{Q}(\alpha):\mathbb{Q}$ where $\alpha = \sqrt[3]{2}$. Let $f \in \Gamma(\mathbb{Q}(\alpha):\mathbb{Q})$, $(f(\alpha))^3 = f(\alpha^3) = f(2) = 2$. $f(\alpha) \in \mathbb{Q}(\alpha)$, so $f(\alpha) = \alpha$. $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 : a,b,c \in \mathbb{Q}\}$. Hence,

$f(a + b\alpha + c\alpha^2) = f(a) + f(b)f(\alpha) + f(c)f(\alpha^2) = a + b\alpha + c\alpha^2$. Hence $f = id$, $\Gamma(\mathbb{Q}(\alpha):\mathbb{Q}) = \{id\}$.

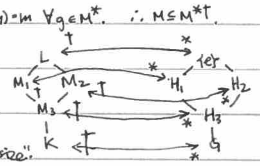
The fundamental theorem gives in some circumstances a 1-1 correspondence between (1) $\mathcal{F} = \{$fields M s.t. $K \subseteq M \subseteq L\}$, (2) $\mathcal{G} = \{$subgroups H of G$\}$. Define $*: \mathcal{F} \to \mathcal{G}$ by $M^* = \{g \in G : g(m) = m\ \forall m \in M\} \in \mathcal{G}$ and $\dagger: \mathcal{G} \to \mathcal{F}$ by $H^\dagger = \{x \in L : g(x) = x\ \forall g \in H\} \in \mathcal{F}$. Let $g, h \in M^*$. Then $\forall m \in M$, $(gh)(m) = g(h(m)) = g(m) = m$ (Definition 8.6) so $gh \in M^*$. Also, $g(m) = m$ $\forall m \in M$, so $g^{-1}(m) = m$ $\forall m \in M$.

i.e. $g^{-1} \in M^*$. $id \in M^*$ $\therefore M^* \in \mathcal{G}$. Similarly, $H^\dagger$ is a field containing K, and $H^\dagger$ is the fixed field of H.

Let $M_1 \subseteq M_2 \in \mathcal{F}$. Suppose $g \in M_2^*$. Then $g(x) = x$ $\forall x \in M_2$. Hence, $g(x) = x$ $\forall x \in M_1$, i.e. $g \in M_1^*$ s.t. $M_2^* \subseteq M_1^*$. Suppose $H_1 \subseteq H_2 \in \mathcal{G}$. Let $x \in H_2^\dagger$. Then $h(x) = x$ $\forall h \in H_2$. Then $h(x) = x$ $\forall h \in H_1$

$\therefore x \in H_1^\dagger \Rightarrow H_2^\dagger \subseteq H_1^\dagger$. In terms of inclusion, $*$ and $\dagger$ are order-reversing. $M \subseteq M^{*\dagger} = (M^*)^\dagger = \{x \in L : g(x) = x\ \forall g \in M^*\}$. But if $m \in M$, $g(m) = m$ $\forall g \in M^*$. $\therefore M \subseteq M^{*\dagger}$.

Note – M^* denotes things that fix M, $M^{*\dagger}$ denotes things that are fixed by things that fix M.



Under conditions of normality and separability, $M = M^{*\dagger}$ and $H = H^{\dagger *}$ for all M, H. Hence, $*\dagger = \dagger * = id$. $*$ and $\dagger$ are mutually inverse maps.

$H \subseteq H^{\dagger *}$ and these are finite sets, so to prove equality, we need to show $|H| = |H^{\dagger *}|$. Next two chapters deal with showing that things are the "right size".

If $\mathbb{Q}(\alpha):\mathbb{Q}$ for $\alpha = \sqrt[3]{2}$, it does not satisfy conditions, so correspondence breaks down. $\mathbb{Q}(\alpha) \xrightarrow{*} \{id\}$, $\mathbb{Q} \xrightarrow{*} \{id\}$ and $*$ is not injective.

§9 NORMALITY AND SEPARABILITY.

Definition 9.1 If K is a subfield of $\mathbb{C}$ and f is a polynomial over K, then f splits over K if it can be expressed as a product of linear factors $f(t) = k(t - \alpha_1)\cdots(t - \alpha_n)$ where $k, \alpha_1, \dots, \alpha_n \in K$.

Note – Here, the zeros of f in K are precisely $\alpha_1, \dots, \alpha_n$

If f is a polynomial over K, $L:K$ an extension, then f is also a polynomial over L.

Definition 9.3 A subfield Σ of $\mathbb{C}$ is a splitting field for polynomial f over subfield $K \subseteq \mathbb{C}$ if $K \subseteq \Sigma$ and (1) f splits over Σ, (2) if $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

Remark – (2) is equivalent to (2') $\Sigma = K(\sigma_1, \dots, \sigma_n)$ where $\sigma_1, \dots, \sigma_n$ are zeros of f in Σ.

Theorem 9.4 If $f \in K[t]$, $K \subseteq \mathbb{C}$, then there exists a unique splitting field Σ for f over K. Moreover, $[\Sigma:K]$ is finite.

Proof – Let $\sigma_1, \dots, \sigma_n$ be the roots of n in $\mathbb{C}$. Then $\Sigma = K(\sigma_1, \dots, \sigma_n)$. Then $K(\sigma_1, \dots, \sigma_n):K$ is finitely generated by algebraic elements, so finite.

Lemma 9.5 Let $K, K' \subseteq \mathbb{C}$, $i: K \to K$ an isomorphism. $f \in K[t]$ with splitting field Σ. $L \supseteq K'$ s.t. $i(f)$ split over L. Then $\exists$ monomorphism $j: \Sigma \to L$ s.t. $j|_K = i$.

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

Proof – Induction on ∂f. $f(t) = k(t-\sigma_1)\cdots(t-\sigma_n)$ in $\Sigma[t]$. Let m be the minimal polynomial of σ_1 over K. $m | f$, $i(m)$ divides $i(f)$.

Hence $i(m)$ splits over L, say $i(m) = (t-\alpha_1)(t-\alpha_2)\cdots(t-\alpha_r)$. Since $i(m)$ irreducible, $i(m)$ is the minimal polynomial of α_1 over K'.

By Thm 5.16, $\exists$ isomorphism $j_1: K(\sigma_1) \to K'(\alpha_1)$ s.t. $j_1|_K = i$. Now Σ is the splitting field of $f(t)/(t-\sigma_1)$ over $K(\sigma_1)$ and $i\left(\frac{f(t)}{t-\sigma_1}\right)$ splits over $K'(\alpha_1)$.

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

$\partial g < \partial f$, so by induction, $\exists j: \Sigma \to L$ monomorphism s.t. $j|_{K(\sigma_1)} = j_1$, $j|_K = j_1|_K = i$, q.e.d.

Theorem 9.6 Let $i: K \to K'$ be an isomorphism, $f \in K[t]$, Σ be the splitting field of f over K, Σ' splitting field of $i(f)$ over K'. Then $\exists$ isomorphism $j: \Sigma \to \Sigma'$ s.t. $j|_K = i$.

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

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

Definition 9.8 A field extension $L:K$ is normal if whenever f is an irreducible polynomial over K with one root in L, then f splits in L.

e.g. $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ is not normal. $f(t) = t^3 - 2$ irreducible, f has one root $\sqrt[3]{2}$ in $\mathbb{Q}(\sqrt[3]{2})$, but doesn't split, since $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2 \notin \mathbb{Q}(\sqrt[3]{3})$. $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ is normal, but why?

Theorem 9.9 $L:K$ is normal and finite $\iff$ L is a splitting field over K (of some polynomial f) [Note – there is no need for f to be irreducible]

Proof – ($\Rightarrow$) Suppose $L:K$ normal and finite. By 6.11, $\exists \alpha_1, \ldots, \alpha_n \in L$ s.t. $L = K(\alpha_1, \ldots, \alpha_n)$ and each α_i is algebraic over K. Let m_i = minimal polynomial of α_i over K,

$f = m_1 \cdots m_n$. Claim L = splitting field of f over K. m_i is irreducible over K and has one root (α_i) in L. Since $L:K$ normal, m_i splits in $L \Rightarrow f$ splits in L.

Also, if f splits in Σ, $\Sigma \supseteq K(\alpha_1, \ldots, \alpha_n) = L$. $\therefore L$ splitting field. [e.g. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(t^2-2)(t^2-3)$ over $\mathbb{Q}$.

($\Leftarrow$) Suppose L = splitting field of g over K. $L:K$ is finite. Need to show $L:K$ normal. Let f be an irreducible polynomial over K. Let M be the splitting field of fg over K.

Let θ_1 and θ_2 be roots of f in M. Want to show: $\theta_1 \in L \Rightarrow \theta_2 \in L$. Look at diagram. Then θ_1 and θ_2 have same minimal

$$\begin{tikzcd}[column sep=small] & M \arrow[dl, dash] \arrow[dr, dash] & \\ L(\theta_1) \arrow[d, dash] \arrow[r, dash] & L \arrow[d, dash] & L(\theta_2) \arrow[l, dash] \arrow[d, dash] \\ K(\theta_1) \arrow[r, dash] & K & K(\theta_2) \arrow[l, dash] \end{tikzcd}$$

polynomial f over K. By 6.7, $K(\theta_1):K \cong K(\theta_2):K$ $\therefore$ $[K(\theta_1):K] = [K(\theta_2):K]$. We know $L(\theta_i)$ is splitting field of g

over $K(\theta_i)$, and by 9.6 $L(\theta_1):K(\theta_1) \cong L(\theta_2):K(\theta_2)$, so $[L(\theta_1):K(\theta_1)] = [L(\theta_2):K(\theta_2)]$.

Applying Tower Law multiple times, $[L(\theta_1):L] = [L(\theta_2):L] \Rightarrow$ since $\theta_1 \in L$, $[L(\theta_1):L] = 1 \Rightarrow [L(\theta_2):L] = 1 \Rightarrow \theta_2 \in L. \Rightarrow L:K$ normal.

13 February 2014
Dr. Mark L ROBERTS.
Chadwick LT.

Definition 9.10
Separability: If $K \subseteq \mathbb{C}$, and $f(t) \in K[t]$ is irreducible, then f does not have repeated roots i.e. every irreducible polynomial is separable.

§10 COUNTING PRINCIPLES.

Main result: If H is a finite group of automorphisms of field L, where $H^\dagger$ = fixed field of $H = \{x \in L : h(x) = x \ \forall h \in H\}$, then $[L:H^\dagger] = |H|$.

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

If $L:K$ is finite normal and separable, $H \leq \Gamma(L:K)$ subgroup, then $|H^{\dagger *}| = [(H^\dagger)^*] = [L:H^\dagger] = |H|$. Since $H \subseteq H^{\dagger *}$, $H = H^{\dagger *}$.

Lemma 10.1 (Dedekind's Lemma)

Let $K, L \subseteq \mathbb{C}$. Then every set of distinct monomorphisms $K \to L$ are linearly independent over L.

Proof – Let $\lambda_1, \ldots, \lambda_n : K \to L$ be monomorphisms, $\lambda_i(k_1 + k_2) = \lambda_i(k_1) + \lambda_i(k_2)$, $\lambda_i(k_1 k_2) = \lambda_i(k_1)\lambda_i(k_2)$. Then for $a_i \in L$, define $a_1\lambda_1 + \cdots + a_n\lambda_n : K \to L$ by $(a_1\lambda_1 + \cdots + a_n\lambda_n)(k) = a_1\lambda_1(k) + \cdots + a_n\lambda_n(k)$

25 February 2014
Dr MARK L ROBERTS
Chadwick LT.

Then we show that if they are LD, we get a contradiction on shortest length condition (see book).

e.g. – consider $2\lambda_1 + 3\lambda_2 - 4\lambda_3 = 0$. Then $2\lambda_1(x) + 3\lambda_2(x) - 4\lambda_3(x) = 0$ ① $\forall x \in K$. If $y \in K$, $2\lambda_1(yx) + 3\lambda_2(yx) - 4\lambda_3(yx) = 0 \ \forall x \in K \Rightarrow 2\lambda_1(y)\lambda_1(x) + 3\lambda_2(y)\lambda_2(x) - 4\lambda_3(y)\lambda_3(x) = 0$. ②

But ①: $2\lambda_3(y)\lambda_1(x) + 3\lambda_3(y)\lambda_2(x) - 4\lambda_3(y)\lambda_3(x) = 0 \Rightarrow 2[\lambda_1(y) - \lambda_3(y)]\lambda_1(x) + 3[\lambda_2(y) - \lambda_3(y)]\lambda_2(x) = 0$. Since λ_1, λ_3 distinct, $\exists y$ s.t. $\lambda_1(y) \neq \lambda_3(y) \Rightarrow$ this is a non-zero

relation $\Rightarrow \exists$ dependence relation $a\lambda_1 + b\lambda_2 = 0$ ($a \neq 0$) which is shorter $\Rightarrow$ eventually $\lambda_1 = 0$ which is a contradiction, q.e.d.

Lemma 10.3 If $n > m$, then a system of m homogeneous linear equations in n unknowns $a_{m1}x_1 + \cdots + a_{mn}x_n = 0$ with $a_{ij} > 0$ has a solution in which x_i are not all 0.

Lemma 10.4 If G is a group with distinct elements $g_1, \ldots, g_n$ and $g \in G$, then as j varies from 1 to n, gg_j runs through whole of G, each element of G occurring exactly once.

Theorem 10.5 Let G be a finite group of automorphisms of a field K. Let $K_0 = \{x \in K : g(x) = x \ \forall g \in G\}$ be the fixed field. Then $[K:K_0] = |G|$.

Proof – Let $|G| = n$, $G = \{g_1, g_2, \ldots, g_n\}$. $[K:K_0] = m$ with $\{x_1, \ldots, x_m\}$ a K_0-basis for K. Claim: $n \leq m$. Let $V = \{f: K \to K \mid f \text{ is } K_0\text{-linear}\}$. V is a vector space over K with dimension m.

Basis is $\{\delta_1, \ldots, \delta_m\}$ where $\delta_i(x_j) = \delta_{ij}$. By Dedekind's Lemma, $g_1, \ldots, g_n$ are LI over K, $g_i \in V \Rightarrow n \leq m$. Claim: $m \leq n$. Suppose $m > n$; $m \geq n+1 \Rightarrow \{x_1, \ldots, x_{n+1}\} \in K$

is LI over K_0. Then consider the system of n equations in $n+1$ unknowns (y_i) $\sum_{i=1}^{n+1} y_i g_j(x_i) = 0$ where $j = 1, \ldots, n$. By Lemma 10.3, $\exists$ solution $\{y_1, \ldots, y_{n+1}\}$ not all zero.

[e.g. suppose $G = C_3 = \{e, g, g^2\}$ $g^3 = e$. Then if $\{x_1, x_2, x_3, x_4\}$ are LI over K_0, $\sum y_i x_i = 0$, $\sum y_i g(x_i) = 0$, $\sum y_i g^2(x_i) = 0$, $\sum y_i g_j(x_i) = 0$ has non trivial soln].

Pick a shortest non-trivial soln (as few as possible non-zero y_i terms. By reordering, we get $\sum_{i=1}^{r} y_i g_j(x_i) = 0$ ② $(j = 1, \ldots, n)$, $y_i \neq 0$ for $i = 1, 2, \ldots, r$. There is no shorter

non-trivial solution. Let $g \in G$. Apply g to ②: $g\left(\sum_{i=1}^{r} y_i g_j(x_i)\right) = \sum_{i=1}^{r} g(y_i)\, g g_j(x_i) = 0 \ \forall j = 1, \ldots, n$. As g_j varies through G, so does gg_j, so sum is $\sum_{i=1}^{r} g(y_i) g_j(x_i) = 0$ ③

Compare ② and ③: $g(y_1)$② $- y_1$③ $\Rightarrow \sum_{i=1}^{r} [g(y_1) y_i - y_i g(y_i)]\, g_j(x_i) = 0$ ④. First coefficient is 0, so ④ is a solution to the system with fewer variables (unless all

3202-06

coefficients are 0) i.e. $g(y_1)y_i = y_1 g(y_i)\ \forall i \Rightarrow y_i y_1^{-1} = g(y_i y_1^{-1})$. This holds $\forall g \in G \Rightarrow y_i y_1^{-1} \in K_0$ (fixed field). Say $y_i y_1^{-1} = z_i \in K_0$. $\Rightarrow y_i = y_1 z_i$. Since we had ②: $\sum_{i=1}^{r} y_i\, g_j(x_i) = 0$, take $g_1 = id$, then $\sum_{i=1}^{r} y_i x_i = 0$. $\Rightarrow y_1 x_1 + y_1 z_2 x_2 + \cdots + y_1 z_r x_r = 0$. K field and $y_1 \neq 0$, so $x_1 + z_2 x_2 + \cdots + z_r x_r = 0$. Since this is a nontrivial dependence relation for $\{x_1, \ldots, x_r\} \Rightarrow$ set is LD $\Rightarrow$ contradiction. Hence $m \leq n$. $\Rightarrow m \leq n \leq m \Rightarrow m = n$ // q.e.d.

$\varphi: \mathbb{C}(t) \to \mathbb{C}(t)$

let $\varphi(t) = \frac{1}{t}$. $\varphi^2 = id$. $G = \{id, \varphi\}$, then G is a finite group of automorphisms of K. Use theorem 10.5 to find K_0: clearly, $[\mathbb{C}(t) : K_0] = 2$, so we work from that. Find a non-trivial element of K_0 ($\mathbb{C} \in K_0$). One such element is $t + \frac{1}{t}$. [Trick: if $\varphi^2 = id$, $a + \varphi(a) \in K_0$, $\varphi^n = id$, $a + \varphi(a) + \cdots + \varphi^{n-1}(a) \in K_0$]. Take $\alpha = t + \frac{1}{t}$, then $\mathbb{C}(\alpha) \subseteq K_0 \subseteq \mathbb{C}(t)$. We know $[\mathbb{C}(t) : K_0] = 2$. Then $[\mathbb{C}(t) : \mathbb{C}(\alpha)] = 2$, because $\mathbb{C}(t) = \mathbb{C}(\alpha)(t)$, need to find $[\mathbb{C}(\alpha)(t) : \mathbb{C}(\alpha)]$, m.p. of t over $\mathbb{C}(\alpha)$. $\alpha = t + \frac{1}{t}$, $t\alpha = t^2 + 1 \Rightarrow t^2 - t\alpha + 1 = 0 \Rightarrow$ $f(x) = x^2 - x\alpha + 1 \in \mathbb{C}(\alpha)[x]$, $f(t) = 0$, this is min polynomial so $[\mathbb{C}(t) : \mathbb{C}(\alpha)] = 2$. By Tower law, $[K_0 : \mathbb{C}(\alpha)] = 1 \Rightarrow K_0 = \mathbb{C}(\alpha) = \mathbb{C}(t + \frac{1}{t})$ //.

§11 FIELD AUTOMORPHISMS.

$\boxed{\text{Definition}}$ 11.1 Suppose $K \subseteq M, L$. Then a K-monomorphism $\varphi: M \to L$ is a field monomorphism s.t. $\varphi(h) = h\ \forall h \in K$.

e.g. – $\mathbb{Q}$-monomorphisms from $\mathbb{Q}(\sqrt[3]{2})$ to $\mathbb{C}$ are? Let $\varphi: \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, $\varphi(x) = x\ \forall x \in \mathbb{Q}$. $(\varphi(\sqrt[3]{2}))^3 = \varphi(\sqrt[3]{2}^3) = \varphi(2) = 2$ $\therefore \varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ or $\sqrt[3]{2}\omega$ or $\sqrt[3]{2}\omega^2$. where $\omega = e^{2\pi i/3}$. This yields 3 $\mathbb{Q}$-monomorphisms.

If $K \subseteq M \subseteq L$ and $\varphi: L \to L$ is a K-automorphism, then $\varphi|_M$ is a K-monomorphism $M \to L$ (restriction). For expansion, consider the following –

$$\begin{array}{ccc} L & \overset{\sigma}{\dashrightarrow} & L \\ | & & | \\ M & \xrightarrow{\tau} & \tau(M) \\ | & & | \\ K & \xrightarrow{id} & K \end{array}$$

$\boxed{\text{Theorem}}$ 11.3 Let $K \subseteq M \subseteq L$ and suppose $L:K$ is finite normal. Let $\tau: M \to L$ be a K-monomorphism. Then τ extends to a K-automorphism $\sigma: L \to L$ i.e. $\sigma|_M = \tau$.

Proof – Since $L:K$ is finite normal, L is the splitting field of some polynomial f over $K \Rightarrow L$ is the splitting field of f over M. $\Rightarrow$ also splitting field of f over $\tau(M)$.

$\tau(f) = f$ since $f \in K[t]$ and $\tau|_K = id$. $\begin{array}{ccc} L & & L \\ | & & | \\ M & \xrightarrow{\tau} & \tau(M) \end{array}$ $f \mapsto \tau(f) = f$, so by theorem 9.6, $\exists$ isomorphism σ s.t. $\sigma|_M = \tau$.

$\boxed{\text{Proposition}}$ 11.4 Let $L:K$ be finite normal, $\alpha, \beta \in L$ roots of the same irreducible polynomial $p(t) \in K[t]$. Then there exists a K-automorphism σ of L s.t. $\sigma(\alpha) = \beta$.

Proof – Since α, β have same minimal polynomial, by theorem 5.13, $K(\alpha) \cong K(\beta)$, say $\begin{array}{ccc} K(\alpha) & \xrightarrow[\alpha \mapsto \beta]{\tau} & K(\beta) \\ | & & | \\ K & \xrightarrow[id]{} & K \end{array}$. By Theorem 11.3, τ extends to a K-automorphism of L, σ s.t. $\sigma|_{K(\alpha)} = \tau$. Hence, $\sigma(\alpha) = \tau(\alpha) = \beta$ // q.e.d.

27 February 2014
Dr Isidoros STROUTHOS.
Chadwick LT.

Normal closures

Guiding example (Ex 11.7). Consider the extension $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ where $\sqrt[3]{2} \in \mathbb{R}$. Minimal polynomial of $\sqrt[3]{2}$ is $t^3 - 2$ (over $\mathbb{Q}$). This has complex roots, as well as $\sqrt[3]{2}$, but $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$ so not all roots of $t^3 - 2$ lie in $\mathbb{Q}(\sqrt[3]{2}) \Rightarrow \mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ not normal. We can "make it normal" by adjoining missing roots. Roots are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ where $\omega = \frac{-1 + i\sqrt{3}}{2}$. So the splitting field of $t^3 - 2$ over $\mathbb{Q}$ is the field $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$. So $\mathbb{Q}(\sqrt[3]{2}, \omega):\mathbb{Q}$ is a normal extension. Hence $\mathbb{Q}(\sqrt[3]{2}, \omega):\mathbb{Q}(\sqrt[3]{2})$ is an "enlargement" of $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ that is normal. In fact, $\mathbb{Q}(\sqrt[3]{2}, \omega)$ is the normal closure of $\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$.

$\boxed{\text{Definition}}$ 11.5 Let L be a finite extension of K. A normal closure of $L:K$ is an extension N of L which is the smallest extension of L that is normal over K, i.e.

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

When working within $\mathbb{C}$, we will show that normal closures exist and are unique:

$\boxed{\text{Theorem}}$ 11.6 Let $L:K$ be a finite extension in $\mathbb{C}$. There exists a unique normal closure N of $L:K$, and N is also a finite extension of K.

Proof – Let $x_1, \ldots, x_r$ be a basis for L over K (note that $L:K$ is finite), and consider the respective minimal polynomials over K, say $m_1, \ldots, m_r$. Consider the polynomial $f = m_1 m_2 \cdots m_r$ and let N be the splitting field for f over L. Then N is also the splitting field for f over K. As a splitting field for f over K, N is a normal and finite extension of K, as required. We now show that N is the smallest extension of L that is normal over K. Suppose $L \subseteq P \subseteq N$ and that $P:K$ is normal. Then each m_i has a root $x_i \in L$, and also has a root $x_i \in P$. So given that $P:K$ is normal, each m_i splits in P. As a result, $f = m_1 \cdots m_r$ also splits in P. Hence P contains the splitting field of f, i.e. P contains N. Since $P \subseteq N$ and $N \subseteq P$, we have $P = N \Rightarrow N$ is indeed a normal closure of $L:K$. For uniqueness, suppose M and N are normal closures. Then f splits in M and in $N \Rightarrow$ each of M and N contains the splitting field for f over K. Hence, since the splitting field is also normal, it must be the case that $M = N$ (and M, N are equal to splitting field).

e.g. – If $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$, then $N = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is the normal closure of $L:K$.

$$\begin{array}{c} M \\ | \\ N \\ | \\ L \\ | \\ K \end{array}$$

$\boxed{\text{Lemma}}$ 11.8 Suppose that $K \subseteq L \subseteq N \subseteq M$ where $L:K$ is finite and N is the normal closure of $L:K$. Then any K-monomorphism $\tau: L \to M$ satisfies $\tau(L) \subseteq N$.

Proof – Let $\alpha \in L$, and consider minimal polynomial of α over K, say m. Then $m(\alpha) = 0 \Rightarrow \tau(m(\alpha)) = \tau(0) = 0$ as τ is injective. Also, since τ is a K-monomorphism, $\tau(m(\alpha)) = m(\tau(\alpha))$. So $m(\tau(\alpha)) = 0$ i.e. $\tau(\alpha)$ is a zero of minimal polynomial m. Since extension N is normal, m splits over N, so $\tau(\alpha) \in N$. $\Rightarrow \tau(L) \subseteq N$ // q.e.d.

$\boxed{\text{Theorem}}$ 11.9 Let $L:K$ be a finite extension. Then the following are equivalent:

(i) $L:K$ is normal (ii) $\exists$ finite normal extension $N:K$ with $N \supseteq L$ s.t. every K-monomorphism $\tau: L \to N$ is a K-automorphism of L. [i.e. $\tau(L) \subseteq L$].

(iii) For every finite extension $M:K$ s.t. $M \supseteq L$, every K-monomorphism $\tau: L \to M$ is a K-automorphism of L. [i.e. $\tau(L) \subseteq L$].

$$\begin{array}{ccc} N & & N \\ | & & | \\ L & \xrightarrow{\tau} & \tau(L) \\ | & & | \\ K & & K \end{array}$$

Remark – If $L:K$ is finite dimensional, $\tau: L \to L$ is a K-monomorphism. It must be surjective i.e. a K-automorphism. [$\tau(L) \leq L \Rightarrow \tau(L) = L$].

Proof – (i)$\Rightarrow$(iii). By lemma 11.8, if $\tau: L \to M$, then $\tau(L) \subseteq \underset{\text{of } L:K}{\text{normal closure}} = L$. (iii)$\Rightarrow$(ii). This is a special case, just take N = normal closure of $L:K$

(ii)$\Rightarrow$(i). Let $f \in K[t]$ be irreducible over K with one root $\alpha \in L$. Let β be any other root of f lying in N, the normal closure. By proposition 11.4, $\exists$ K-automorphism $\sigma: N \to N$ st. $\sigma(\alpha) = \beta$. Then $\sigma|_L : L \to N$ is a K-monomorphism. So by (ii), $\sigma(L) \subset L$. $\therefore \beta = \sigma(\alpha) \in L$. $\therefore f$ splits over $L \Rightarrow L:K$ normal, q.e.d.

$\boxed{\text{Theorem}}$ 11.10 Suppose $L:K$ is a finite extension of degree n, then there are exactly n K-monomorphisms of L into the normal closure N of $L:K$ (and hence into any normal extension $M:K$ st. $M \supseteq L$)

$\boxed{\text{Corollary}}$ 11.11 Let $L:K$ be normal with $[L:K] = n$. Then there are exactly n K-automorphisms of L, i.e. $|\Gamma(L:K)| = [L:K]$

$$\begin{array}{l} L \\ |\ s \\ K(\alpha) \quad rs = k \\ |\ r \\ K \end{array}$$

(Thm 11.10)
Proof – Induct on $[L:K]$. Suppose $[L:K] = k > 1$. Let $\alpha \in L \backslash K$ with minimal polynomial m over K. $\partial m [K(\alpha):K] = r > 1$. Let $s = k/r$. Then m has one zero $\alpha \in N$, so splits in N. Let roots be $\alpha = \alpha_1, \alpha_2, \dots, \alpha_r$. These are all distinct (for separable case). By Proposition 11.4, there are r K-automorphisms of N, $\tau_1, \dots, \tau_r$ st. $\tau_i(\alpha) = \alpha_i$.

$N:K(\alpha)$ is a normal extension, and let $[L:K(\alpha)] = s < k$, so by inductive hypothesis there are exactly s $K(\alpha)$-monomorphisms $L \to N$, say $\rho_1, \dots, \rho_s$. Let $\varphi_{ij} = \tau_i \rho_j$, $\tau_i \rho_j : L \to N$. ($L \xrightarrow{\rho_j} N \xrightarrow{\tau_i} N$.) The φ_{ij} are K-monomorphisms. Claim they are distinct and exhaust all possible K-monomorphisms $L \to N$. (Distinctness) Suppose $\varphi_{ij} = \varphi_{rs}$, then $\tau_i \rho_j = \tau_r \rho_s$. Apply to α, then $\tau_i \rho_j(\alpha) = \tau_r \rho_s(\alpha) \Rightarrow \tau_i(\alpha) = \tau_r(\alpha) \Rightarrow \alpha_i = \alpha_r \Rightarrow i = r \Rightarrow \tau_i = \tau_r$. Thus, $\rho_j = \rho_s \Rightarrow j = s \Rightarrow$ clearly distinct. (Exhaustive) Let $\tau: L \to N$ be a K-monomorphism. Then $m(\alpha) = 0 \Rightarrow \tau(m(\alpha)) = \tau(0) = 0 \Rightarrow m(\tau(\alpha)) = 0 \Rightarrow \tau(\alpha)$ is a root of $m \Rightarrow \tau(\alpha) = \alpha_i$ for some i. $\varphi = \tau_i^{-1}\tau : L \to N$, $\tau_i^{-1}\tau(\alpha) = \tau_i^{-1}(\alpha_i) = \alpha$. Hence, φ is a $K(\alpha)$-monomorphism $L \to N \Rightarrow \varphi = \rho_j$ for some j $\therefore \tau_i^{-1}\tau = \rho_j \Rightarrow \tau = \tau_i \rho_j = \varphi_{ij}$. Then there are exactly $rs = k$ of the φ_{ij} terms. Result holds by induction// q.e.d.

§12.

$$\begin{tikzcd} M \arrow[r, "\tau"] \arrow[loop below, "g"] & \cdot \arrow[loop below, "\tau g \tau^{-1}"] \end{tikzcd}$$

$\boxed{\text{Lemma}}$ 12.2 Let $K \subseteq M \subseteq L$, $\tau: L \to L$ is a K-automorphism. Then $\tau(M)^* = \tau M^* \tau^{-1}$.

Proof – Let $g \in M^*$ i.e. $g(m) = m$ $\forall m \in M$. Let $x \in \tau(M)$, say $x = \tau(m)$ for some $m \in M$. Then $(\tau g \tau^{-1})(x) = \tau g \tau^{-1}(\tau(m)) = \tau g(m) = \tau(m) = x$. $\therefore \tau g \tau^{-1} \in \tau(M)^*$.

Similarly, $\tau(M)^* \supseteq \tau M^* \tau^{-1} \Rightarrow \tau(M)^* = \tau M^* \tau^{-1}$// q.e.d.

For more details on this chapter, refer to Handout.

6 March 2013
Dr Mark L ROBERTS
Chadwick LT.

§13.

The stages and theory are covered in a separate handout. We will apply it to the following example:

$\boxed{\text{Task}}$
Let L be the splitting field of $f(t) = t^7 - 1$ over $\mathbb{Q}$. Find the Galois group $G = \Gamma(L:\mathbb{Q})$ and all intermediate fields M, $\mathbb{Q} \subseteq M \subseteq L$.

Stage 1: Find L.
Roots of $f(t) = 0$ are ω^i $(i = 0, \dots, 6)$, $\omega = e^{\frac{2\pi i}{7}}$. $L = \mathbb{Q}(1, \omega, \dots, \omega^6) = \mathbb{Q}(\omega)$.

Stage 2: Find $[L:\mathbb{Q}]$
ω satisfies $t^7 - 1 = 0$, but its minimal polynomial is $m(t) = \frac{t^7-1}{t-1} = t^6 + \dots + 1$. This is irreducible, setting $t = s+1$ s.t. $m(s+1) = s^6 + 7s^5 + \dots + 7$, Eisenstein for $p = 7$. So $[L:\mathbb{Q}] = 6$.

Stage 3: Apply Fund. Thm
By Fund. Thm, $|G| = [\mathbb{Q}(\omega):\mathbb{Q}] = 6$

Stage 4 + 5
Find elements of G. If $g \in G$, g is determined by $g(\omega)$, $g(\omega)$ must be a root of $m(t) = 0$. So $g(\omega) = \omega^i$ for some $1 \leq i \leq 6$. Let $g(\omega) = \omega^i$, so any element of G must be one of $g_1, \dots, g_6$. On the other hand, $|G| = 6$, so in fact $G = \{g_1, \dots, g_6\}$ exactly.

Stage 6: Find presentation of G
Consider g_2 first: $g_2(\omega) = \omega^2$, $g_2^2(\omega) = g_2(\omega^2) = \omega^4$, $g_2^3(\omega) = \omega^8 = 1$. So $g_2^3 = \mathrm{Id}$. Consider g_3: $g_3(\omega) = \omega^3$, $g_3^2(\omega) = \omega^9 = \omega^2$; hence $g_3, g_3^2, g_3^3 \neq \mathrm{Id} \Rightarrow$ by Lagrange's Theorem, $o(g_3) = 6$. Since $\exists$ element of order 6, we postulate that $G \cong C_6$. Let $g = g_3$, then $G = \{e, g, g^2, \dots, g^5 \mid g^6 = e\} = \langle g \mid g^6 = e \rangle \cong C_6$.

Stage 7: Find subgroups of G
These are $H = \langle g^2 \rangle = \{e, g^2, g^4\} \cong C_3$, $K = \langle g^3 \rangle = \{e, g^3\} \cong C_2$.

Stage 8: Lattice of subgroups
By the Fundamental theorem, we obtain the lattice as on right; which is the lattice of intermediate fields.

$$\begin{tikzcd} & \{e\} \arrow[rrr, leftrightarrow] \arrow[dl, dash] \arrow[dr, dash] & & & \mathbb{Q}(\omega) \arrow[dl, dash] \arrow[dr, dash] & \\ H = \langle g^2 \rangle \arrow[rrr, leftrightarrow] \arrow[dr, dash] & & K = \langle g^3 \rangle \arrow[rrr, leftrightarrow] \arrow[dl, dash] & \langle g^2 \rangle^\dagger \arrow[dr, dash] & & \langle g^3 \rangle^\dagger \arrow[dl, dash] \\ & G = \langle g \rangle \arrow[rrr, leftrightarrow] & & & \mathbb{Q} & \end{tikzcd}$$

Stage 9: Find fixed fields
(Long Method)
- $\langle g^2 \rangle^\dagger$: $\{x \in \mathbb{Q}(\omega) : g^2(x) = x\}$. $x \in \mathbb{Q}(\omega) \Rightarrow x = a_0 + a_1\omega + \dots + a_5\omega^5$ for $a_i \in \mathbb{Q}$ $\Rightarrow g^2(x) = a_0 + a_1\omega^2 + a_2\omega^4 + a_3\omega^6 + a_4\omega + a_5\omega^3 = a_0 + a_1\omega^2 + a_2\omega^4 + a_3(-1-\omega-\dots-\omega^5) + a_4\omega + a_5\omega^3$
$= (a_0 - a_3) + (a_4 - a_3)\omega + (a_1 - a_3)\omega^2 + (a_5 - a_3)\omega^3 + (a_2 - a_3)\omega^4 - a_3\omega^5$. Then if $x \in \langle g^2 \rangle^\dagger$, $g^2(x) = x$, so we must have $\left\{\begin{array}{ll} a_0 = a_0 - a_3 & a_3 = a_5 - a_3 \\ a_1 = a_4 - a_3 & a_4 = a_2 - a_3 \\ a_2 = a_1 - a_3 & a_5 = -a_3 \end{array}\right\} \Rightarrow \begin{array}{l} a_3 = a_5 = 0 \\ a_1 = a_4 = a_2 \\ a_0 \text{ free.} \end{array}$

Thus, $x = a_0 + a_1\omega + a_1\omega^2 + a_1\omega^4 = a_0 + a_1(\omega + \omega^2 + \omega^4)$, and $\langle g^2 \rangle^\dagger = \{a_0 + a_1(\omega + \omega^2 + \omega^4) : a_0, a_1 \in \mathbb{Q}\} = \mathbb{Q}(\omega + \omega^2 + \omega^4)$.

(Short Method)
$g^2(\omega) = \omega^2$, $g^2(\omega^2) = \omega^4$, $g^2(\omega^4) = \omega$ $\Rightarrow g^2$ cycles the elements $\omega^2, \omega^4, \omega$, so $\alpha = \omega + \omega^2 + \omega^4 \in \langle g^2 \rangle^\dagger$. By the diagram (or Tower Law), there are no fields between $\langle g^2 \rangle^\dagger$ and $\mathbb{Q}$, so clearly $\mathbb{Q}(\alpha) = \mathbb{Q}$ or $\mathbb{Q}(\alpha) = \langle g^2 \rangle^\dagger$. If $\mathbb{Q}(\alpha) = \mathbb{Q}$, then $\alpha \in \mathbb{Q}$ i.e. $\omega^4 + \omega^2 + \omega = q \in \mathbb{Q}$, i.e. $\omega^4 + \omega^2 + \omega - q = 0$. Then if we define $f(t) = t^4 + t^2 + 1 - q \in \mathbb{Q}[t]$, $f(\omega) = 0$, but $\overset{4}{\overset{\shortparallel}{\partial f}} < \partial m = 6$, which is a contradiction. Hence, $\mathbb{Q}(\alpha) \neq \mathbb{Q} \Rightarrow \mathbb{Q}(\alpha) = \langle g^2 \rangle^\dagger$. Use this again for g^3.

- $\langle g^3 \rangle^\dagger$. $g^3(\omega) = \omega^6$, $\therefore \beta = \omega + \omega^6 \in \langle g^3 \rangle^\dagger$, so $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \langle g^3 \rangle^\dagger$. $\mathbb{Q} = \mathbb{Q}(\beta)$ [contradiction] or $\mathbb{Q}(\beta) = \langle g^3 \rangle^\dagger$. contradiction: $\omega + \omega^6 \in \mathbb{Q} \Rightarrow \exists q \in \mathbb{Q}$ st. $f(t) = t^6 + t - q \in \mathbb{Q}[t]$ gives $f(\omega) = 0$. f is clearly not a multiple of m. Thus $\mathbb{Q}(\beta) = \langle g^3 \rangle^\dagger$.

Hence, finally we get the tower
$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\omega) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\alpha) \arrow[dr, dash] & & \mathbb{Q}(\beta) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

Note that we can simplify $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$. $\beta = 2\cos(\frac{2\pi}{7})$, so $\mathbb{Q}(\beta) = \mathbb{Q}(\cos\frac{2\pi}{7}) \subseteq \mathbb{R}$. $\alpha = \omega + \omega^2 + \omega^4 \Rightarrow \alpha^2 = \omega^2 + \omega^4 + \omega + 2(\omega^3 + \omega^5 + \omega^6)$, so $\alpha^2 + \alpha = 2(\omega + \omega^2 + \dots + \omega^6) = -2$.

Thus $\alpha^2 + \alpha + 2 = 0 \Rightarrow \alpha = \frac{-1 \pm \sqrt{7}}{2} \Rightarrow \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7}) \subseteq \mathbb{C}$.

202-08

11 March 2014
Dr Mark L ROBERTS
Torrington Pl 115.

Most of the content on groups is summarised in a separate handout. Here we focus on some key points.

$\boxed{\text{Definition}}$ A group G is *simple* if it has no non-trivial normal subgroups. If G is not simple, then $\exists N \trianglelefteq G$, $N \neq \{e\}$ and G is in some way made up of 2 "smaller" groups, N and G/N.

$\boxed{\text{Proposition}}$ A_n is a simple group for $n \geq 5$.

Proof – see book (Theorem 14.7 – non-examinable).

Moreover, we know that $A_n \trianglelefteq S_n$, $|S_n| = n!$, $|A_n| = \frac{1}{2}n!$ S_n is generated by $\tau = (1\ 2)$, $\sigma = (1\ 2\ 3\ \cdots\ n)$. Observe that $\sigma\tau\sigma^{-1} = \sigma\ (1\ 2)\sigma^{-1}$, and $\sigma\tau\sigma^{-1}(1) = \sigma(1\ 2)(n) = \sigma(n) = 1$.
$(\sigma\tau\sigma^{-1})(2) = \sigma(1\ 2)(1) = \sigma(2) = 3$, $(\sigma\tau\sigma^{-1})(3) = \sigma(1\ 2)(2) = \sigma(1) = 2$. $\sigma(1\ 2)\sigma^{-1}(4) = \sigma(1\ 2)(3) = \sigma(3) = 4$ etc, so $\sigma\tau\sigma^{-1} = (2\ 3)$, $\sigma^2\tau\sigma^{-2} = (3\ 4)$ etc. Hence, every adjacent transposition is a combination of σ and τ. Since every permutation is a product of adjacent transpositions, S_n is generated by σ, τ.

Soluble groups.

$\boxed{\text{Definition}}$ 14.1 A group G is soluble if there is a finite sequence of subgroups of G, $\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$, such that $G_i \trianglelefteq G_{i+1}$ $(i = 0, \ldots, n-1)$ and G_{i+1}/G_i is abelian.

Examples –

1. Any abelian group is soluble: $\{e\} = G_0 \leq G_1 = G$.

2. S_3 is soluble, $\{e\} = G_0 \leq G_1 = A_3 \leq S_3$. Certainly $G_0 \trianglelefteq G_1$, $G_1/G_0 = A_3 \cong C_3$ which is abelian. $G_1 \trianglelefteq G_2$, $|G_2/G_1| = 2 \Rightarrow G_2/G_1 \cong C_2$ which is abelian.

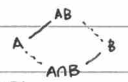
3. D_{2n} is soluble. $D_{2n} = \langle x, y : x^n = y^2 = e,\ yx = x^{-1}y \rangle = \{x^i y^j : 0 \leq i \leq n-1,\ 0 \leq j \leq 1\}$. $N = \langle x \rangle$, $N \trianglelefteq D_{2n}$ • either by working out conjugates $yxy^{-1} = x^{-1} \in \langle x \rangle$ etc. • Or use $H \leq G$, $|H| = \frac{1}{2}|G| \Rightarrow H \trianglelefteq G$.
[since $G = H \cup Hg$, and $G = H \cup gH$, so $Hg = gH = G \setminus H$]. Recall: if $H \leq G$ subgroup, $H \trianglelefteq G$ if (i) $g^{-1}Hg \in H\ \forall g \in G$ or (ii) $gH = Hg\ \forall g \in G$.
Hence $\{e\} = G_0 \leq G_1 = \langle x \rangle \leq G_2 = D_{2n}$. Then $G_1/G_0 = \langle x \rangle \cong C_n$, $G_2/G_1 \cong C_2$ which are abelian.

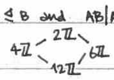
4. S_4 is soluble, with $\{e\} \leq V \leq A_4 \leq S_4$ where $V = C_2 \times C_2$ is the Klein 4-group, $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Indeed $(1\ 2)(3\ 4)\ (1\ 3)(2\ 4) = (1\ 4)(2\ 3)$, closed under products. $V \trianglelefteq A_4$, $v \in V \Rightarrow \sigma^{-1}v\sigma \in V$. If we conjugate a product of two 2cycles, we obtain a product of two 2-cycles (same cycle type) $\in V$: $\sigma(a\ b)(c\ d)\sigma^{-1}$. Then we get that $\sigma(a\ b)(c\ d)\sigma^{-1}(\sigma(a)) = \sigma(a\ b)(c\ d)(a) = \sigma(b)$, $\sigma(a\ b)(c\ d)\sigma^{-1}(\sigma(b)) = \sigma(a\ b)(c\ d)(b) = \sigma(a)$, $\sigma(a\ b)(c\ d)\sigma^{-1} = (\sigma(a)\ \sigma(b))(\sigma(c)\ \sigma(d))$. Then $V/e \cong V \cong C_2 \times C_2$ abelian.
$|A_4/V| = 12/4 = 3$, so $A_4/V \cong C_3$ abelian. $|S_4/A_4| = 2$, so $S_4/A_4 \cong C_2$ abelian.

Remark – for $n \geq 5$, S_n is not soluble. We will establish why below:

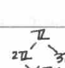
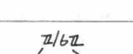
To begin with, we review Noether's isomorphism theorems.

① Let $\varphi: G \to H$ be a group isomorphism. $[\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2),\ \varphi(g^{-1}) = \varphi(g)^{-1},\ \varphi(e) = e]$. Then $\underset{\{g \in G : \varphi(g) = e\}}{\ker\varphi} \trianglelefteq G$, $\operatorname{Im}\varphi \leq H$ and $G/\ker\varphi \cong \operatorname{Im}\varphi$.



② Let $A \trianglelefteq G$, $B \leq G$. Then $AB = \{ab \mid a \in A, b \in B\} \leq G$ and $A \trianglelefteq AB$, $A \cap B \trianglelefteq B$ and $AB/A \cong B/(A \cap B)$.
Example: $G = \mathbb{Z}_+$, $A = 4\mathbb{Z}$, $B = 6\mathbb{Z}$. Everything is normal as it is abelian  $4\mathbb{Z} \cap 6\mathbb{Z} = 12\mathbb{Z}$, $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$. Then $\underset{\{\bar{0}, \bar{2}\}}{2\mathbb{Z}/4\mathbb{Z}} \cong \underset{\{\bar{0}, \bar{6}\}}{6\mathbb{Z}/12\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z} \cong C_2$.

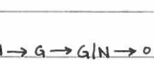
③ Suppose $N \trianglelefteq G$. Then $\exists$ a 1-to-1 correspondence between subgroups (K) of G containing N and subgroups (K/N) of G/N. $K \to K/N$. Then $K \trianglelefteq G \Leftrightarrow K/N \trianglelefteq G/N$.
Then $\frac{G}{N}/\frac{K}{N} \cong G/K$.

Example: $G = \mathbb{Z}$, $N = 6\mathbb{Z}$.   $3\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{3}\}$, $2\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{2}, \bar{4}\}$. Then $\frac{\mathbb{Z}}{2\mathbb{Z}} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{2\mathbb{Z}/6\mathbb{Z}}$, $\frac{\mathbb{Z}}{3\mathbb{Z}} \cong \frac{\mathbb{Z}/6\mathbb{Z}}{3\mathbb{Z}/6\mathbb{Z}}$.

$\boxed{\text{Theorem}}$ 14.4 Let G be a group, $H \leq G$, $N \trianglelefteq G$. Then (i) G soluble $\Rightarrow$ H soluble (property closed under subgroups...) (ii) G soluble $\Rightarrow$ G/N soluble (under taking quotients...) (iii) N and G/N soluble $\Rightarrow$ G soluble (under taking extensions). $(0 \to N \to G \to G/N \to 0)$

Proof – (i) $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$, $G_i \leq G$, $G_i \trianglelefteq G_{i+1}$, G_{i+1}/G_i abelian. Let $H_i = G_i \cap H$. Then $H_i \leq H$, $\{e\} = H_0 \leq H_1 \leq \cdots \leq H_n = H$, $H_i \trianglelefteq H_{i+1}$ [let $x \in H_i$, $g \in H_{i+1}$. $g^{-1}xg \in G_i$ since $x \in G_i$, $g \in G_{i+1}$, $G_i \trianglelefteq G_{i+1}$. Also, $g, x \in H$, so $g^{-1}xg \in H$; and $g^{-1}xg \in G_i \cap H = H_i$]. $\frac{H_{i+1}}{H_i} = \frac{G_{i+1} \cap H}{G_i \cap H} \cong \frac{G_{i+1} \cap H}{G_i \cap (G_{i+1} \cap H)}$ [since G_i is contained in G_{i+1}]

By 2nd isom thm, $\frac{H_{i+1}}{H_i} \cong \frac{G_i(G_{i+1} \cap H)}{G_i} \leq \frac{G_{i+1}}{G_i}$, which is abelian, so subgroups are abelian $\Rightarrow \frac{H_{i+1}}{H_i}$ abelian // q.e.d.



(ii), (iii) proven similarly. (refer to book).

$\boxed{\text{Theorem}}$ 14.6 Suppose G is soluble and simple. Then $G \cong C_p$ for some prime p.

Proof – Let $\{e\} = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n$ be solubility series. $G_{n-1} \trianglelefteq G_n = G$. Since G is simple, $G_{n-1} = \{e\}$, so $G_n/G_{n-1} = G/\{e\} = G$ is abelian. If $g \in G$, $g \neq e$, $\langle g \rangle \trianglelefteq G$, so $\langle g \rangle = G$. $G = C_n$. If $a \mid n$, then $C_a \trianglelefteq C_n$, so by simplicity $a = 1$ or n $\therefore$ n prime, $G = C_p$ // q.e.d.

$\boxed{\text{Theorem}}$ 14.8 For $n \geq 5$, S_n is not soluble.

Proof – Suppose S_n soluble. Then $A_n \leq S_n$, so A_n soluble. However A_n is simple, so it is cyclic of prime order $\Rightarrow$ contradiction. Hence, S_n is not soluble // q.e.d.

By Lagrange's theorem, if $g \in G$, then $o(g) \mid |G|$. (Cauchy's Theorem) $\boxed{\text{Theorem}}$ 14.15 If $p \mid |G|$, p prime, then $\exists g \in G$ with $o(g) = p$.

Proof – (Using Sylow's theorem). $|G| = p^a m$, $p \nmid m \Rightarrow \exists H \leq G$, $|H| = p^a$. Let $e \neq h \in H$. By Lagrange's theorem, $o(h) = p^b$ for some $b \geq 1$. Then $o(h^{(p^{b-1})}) = p$. This gives us the element $g = h^{(p^{b-1})}$ // q.e.d.

§15 SOLUTION BY RADICALS.

$\boxed{\text{Definition}}$ 15.1 An extension $L:K$ is radical if $L=K(\alpha_1,\dots,\alpha_m)$, where for $j=1,\dots,m$, $\exists n_j\in\mathbb{N}$ st. $\alpha_j^{n_j}\in K(\alpha_1,\dots,\alpha_{j-1})$. The elements $\alpha_1,\dots,\alpha_m$ form a radical sequence for L.

Remark – This means $\alpha_1^{n_1}\in K$, $\alpha_2^{n_2}\in K(\alpha_1)$, $\alpha_3^{n_3}\in K(\alpha_1,\alpha_2)$ etc...

Example – $\alpha_1=\sqrt[3]{2}$, $\alpha_2=\sqrt[7]{\sqrt[3]{2}+3}$, $\alpha_3=\sqrt{7}$, $\alpha_4=\sqrt{\sqrt{7}-\alpha_2^2}$ etc. Then $\alpha_1^3\in\mathbb{Q}$, $\alpha_2^7\in\mathbb{Q}(\alpha_1)$, $\alpha_3^2\in\mathbb{Q}\subseteq\mathbb{Q}(\alpha_1,\alpha_2)$, $\alpha_4^2\in\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$. Thus, we conclude that $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4):\mathbb{Q}$ is radical.

$\boxed{\text{Definition}}$ 15.2 A polynomial $f(t)\in K[t]$ is soluble by radicals if $K\subseteq\Sigma\subseteq L$, where Σ is the splitting field for f over K and $L:K$ is radical.

$\boxed{\text{Theorem}}$ 15.3 Let $K\subseteq L\subseteq M$ be a tower of fields, and $M:K$ be radical. Then $\Gamma(L:K)$ is soluble.

13 March 2014
Dr Mark L ROBERTS.
Chadwick LT.

$\boxed{\text{Lemma}}$ 15.4 Suppose $L:K$ is radical, $M:K$ is the normal closure of $L:K$. Then $M:K$ is radical.

Proof – Let $L=K(\alpha_1,\dots,\alpha_r)$, $\alpha_i^{n_i}\in K(\alpha_1,\dots,\alpha_{i-1})$. Then let f_i be the minimal polynomial of α_i over K. Then M is a splitting field of $f=f_1\cdots f_r$ over K. Let the roots of f_i be $\alpha_i=\beta_{i1},\beta_{i2},\dots,\beta_{is_i}$. $\sigma:\alpha_i\mapsto\beta_{ij}$.

$M=K(\alpha_1,\beta_{12},\beta_{13},\dots,\alpha_2,\dots)$. Claim: $\alpha_1=\beta_{11},\beta_{12},\dots,\beta_{1s_1}$; $\alpha_2=\beta_{21},\dots$ is a radical sequence for M. Then $K(\alpha_i)\cong K(\beta_{ij})$. By 11.4, σ extends to a K-automorphism $\tau:M\to M$.

$$\begin{tikzcd} M \arrow[r, "\tau", dashed] & M \\ K(\alpha_i) \arrow[u, dash] \arrow[r, "\sigma"] & K(\beta_{ij}) \arrow[u, dash] \\ K \arrow[u, dash] \arrow[r, "id"] & K \arrow[u, dash] \end{tikzcd}$$

Now, $\alpha_i^{n_i}\in K(\alpha_1,\dots,\alpha_{i-1})$, $\tau(\alpha_i^{n_i})\in K(\tau(\alpha_1),\dots,\tau(\alpha_{i-1}))$, $\tau(\alpha_i^{n_i})\in K(\beta_{1x_1},\dots,\beta_{i-1\,x_{i-1}})$, since α_1 is root of f_1, $\tau(\alpha_1)$ is also root of irreducible f_i i.e.
$\tau(\alpha_1)=$ some β_{1,x_1}. Then $\beta_{ij}^{n_i}\in K(\beta_{1,x_1},\dots,\beta_{i-1,x_{i-1}})$, $\beta_{ij}^{n_i}\in K(\alpha_1=\beta_{11},\dots,\beta_{1,s_1},\alpha_2=\beta_{21},\dots,\beta_{2,s_2},\dots\dots,\beta_{i-1,s_{i-1}})$.

[Short Illustrative Example – suppose $L=K(\alpha_1,\alpha_2)$, $\alpha_1^2\in K$, $\alpha_2^3\in K(\alpha_1)$. Moreover, α_1,α_2 have minimum polynomials f_1,f_2 over K respectively. f_1 has roots $\alpha_1=\beta_{11},\beta_{12}$, f_2 has roots $\alpha_2=\beta_{21},\beta_{22},\beta_{23}$. $M=K(\overbrace{\beta_{11},\beta_{12}},\overbrace{\beta_{21},\beta_{22},\beta_{23}})$ $\beta_{11}^2=\alpha_1^2\in K$. $\sigma:K(\alpha_1)\cong K(\beta_{12})$ extend to $\tau:M\to M$, $\tau|_{K(\alpha_1)}=\sigma$. $\alpha_1^2\in K$, $\tau(\alpha_1^2)\in K$, $\tau(\alpha_1)^2\in K$, $\beta_{12}^2\in K$.
$\alpha_2^3\in K(\alpha_1)$. $\sigma:K(\alpha_2)\cong K(\beta_{22})$, $\tau:M\to M$ $\tau(\alpha_2)=\beta_{22}$, $\alpha_2^3=g(\alpha_1)$, $\overset{\beta_{12}^3=}{\tau(\alpha_2)^3}=g(\tau(\alpha_1))\in K(\alpha_1=\beta_{11},\beta_{12})$

$\boxed{\text{Lemma}}$ 15.5 Let $L=$ splitting field for t^p-1 over K. Then $\Gamma(L:K)$ is abelian.

Proof – Let $L=K(\omega)$, $\omega=e^{\frac{2\pi i}{p}}$. Any $g\in\Gamma(L:K)$ is determined by $g(\omega)=\omega^i$ for some i. If $g(\omega)=\omega^i$, $h(\omega)=\omega^j$, $gh(\omega)=g(\omega^j)=\omega^{ji}$, $hg(\omega)=h(\omega^i)=\omega^{ij}$. Therefore $gh=hg$.

$\boxed{\text{Lemma}}$ 15.6 Let K be such that t^n-1 splits in K. Let $a\in K$, L be the splitting field of t^n-a over K. Then $\Gamma(L:K)$ is abelian.

Proof – Let $\alpha_1\in L$ be a root of t^n-a. Then roots of t^n-a are $\alpha\omega^i$ $(\omega=e^{2\pi i/n})$ so $L=K(\alpha)$ as $\omega\in K$. Any $g\in\Gamma(L:K)$ is determined by $g(\alpha)=\alpha\omega^i$. Let $g,h\in\Gamma(L:K)$, $g(\alpha)=\alpha\omega^i$, $h(\alpha)=\alpha\omega^j$.
Then $(gh)(\alpha)=g(\alpha\omega^j)=\alpha\omega^i\omega^j$, $(hg)(\alpha)=h(\alpha\omega^i)=\alpha\omega^j\omega^i\Rightarrow gh=hg_{//}$ q.e.d.

$$\begin{tikzcd} L \arrow[d, dash, "\text{soluble.}"] \\ M(\alpha_1) \arrow[d, dash, "\text{abelian}"] \\ M \arrow[d, dash] \\ K. \end{tikzcd}$$

$\boxed{\text{Lemma}}$ 15.7 Let $L:K$ be normal and radical, then $\Gamma(L:K)$ is soluble.

Proof – Let $L=K(\alpha_1,\dots,\alpha_n)$ with $\alpha_j^{n_j}\in K(\alpha_1,\dots,\alpha_{j-1})$. WLOG, all $n_j\geq 1$ and all n_j prime. Prove by induction on n (assuming all n_j prime). Let f be minimal polynomial of α_i over K.
Since $L:K$ is normal, f splits over L. Let β be another root of f over L. Take $\varepsilon=\frac{\alpha}{\beta}$. Then $\varepsilon^p=\alpha_1^p/\beta^p=1$ $(\alpha_1^p=a\in K$, so $f(t)$ divides t^p-a, $f(\beta_1)=0$ so $\beta^p-a=0$.
$1\neq\varepsilon$ is a p^{th} root of unity, so t^p-1 splits in L. Let M be the splitting field of t^p-1 over $K=K(\omega)$. Consider the tower of fields $K\subseteq M\subseteq M(\alpha_1)\subseteq L$. By induction, for $L:M(\alpha_1)$
Γ is soluble. For $M(\alpha_1):M$, Γ is abelian; as is it for $M:K$. $M(\alpha_1)$ is splitting field for $t^p-\alpha_1^p\in M[t]$ over M. $M(\alpha_1):M$ is normal and radical, so by induction $\Gamma(L:M(\alpha_1))$ is soluble. By the Fundamental theorem, $\overset{\text{soluble}}{\Gamma(M(\alpha_1):M)}\cong\overset{\text{abelian}\Rightarrow\text{soluble}}{\Gamma(L:M)/\Gamma(L:M(\alpha_1))}$. $\Rightarrow$ By result
14.4(3), $\Gamma(L:M)$ is soluble. Likewise, apply same argument to $K\subseteq M\subseteq L$, so we get that $\Gamma(L:K)$ is soluble.

18 March 2014
Dr Mark L ROBERTS
Torrington Pl LT.

We now return to prove a more general result – Theorem 15.3.

Proof – Let K_0 be the fixed field of $\Gamma(L:K)$, $N:K_0$ the normal closure of $M:K_0$. $L:K_0$ is normal as well since K_0 is fixed field (by 11.14). $M:K_0$ is radical,
so by Lemma 15.4, $N:K_0$ is radical. $N:K_0$ is also normal $\Rightarrow\Gamma(N:K_0)$ is soluble. By Fundamental theorem, $\Gamma(L:K_0)=\overset{\text{soluble}}{\Gamma(N:K_0)}/\Gamma(N:L)$
By 15.4(2), $\Gamma(L:K_0)$ is soluble, and $\Gamma(L:K)=\Gamma(L:K_0)$ is soluble$_{//}$ q.e.d.

$$\begin{array}{c} N \\ | \\ M \\ | \\ L \\ | \\ K_0 \\ | \\ K. \end{array} \quad \text{normal.}[\,L - K_0\,]$$

$\boxed{\text{Definition}}$ 15.8 Let $f\in K[t]$ with splitting field Σ. Then the Galois group of f over K is $\Gamma(\Sigma:K)$.

Let f have roots $\sigma_1,\dots,\sigma_n\in\Sigma$, so $\Sigma=K(\sigma_1,\dots,\sigma_n)$. Let $g\in\Gamma(\Sigma:K)$. Then we know that (i) g is determined by $g(\sigma_1),\dots,g(\sigma_n)$ and (ii) $g(\sigma_i)=\sigma_j$ for some j. $[\because f(\sigma_i)=0\Rightarrow g\cdot f(\sigma_i)=0\Rightarrow f(g(\sigma_i))=0\Rightarrow g(\sigma_i)$ also root.$]$
We can therefore think of g as a permutation of the roots. Define $F:\Gamma(\Sigma:K)\to S_n$ by $F(g)=\tau$, where $\tau(i)=j$ if $g(\sigma_i)=\sigma_j$. (i.e. $g(\sigma_i)=\sigma_{\tau(i)}$). F is a group embedding.

So we can think of $\Gamma(\Sigma:K)$ as a subgroup of S_n.

Example – consider $f=(t^2-3)(t^2-2)\in\mathbb{Q}[t]$. Roots are $\pm\sqrt{2},\pm\sqrt{3}$, so $\Sigma=\mathbb{Q}(\sqrt{2},\sqrt{3})$ is splitting field. Then for $\Gamma(\Sigma:K)$, $id(\sqrt{2})=\sqrt{2}$, $id(\sqrt{3})=\sqrt{3}$, $g(\sqrt{2})=-\sqrt{2}$, $g(\sqrt{3})=\sqrt{3}$, $h(\sqrt{2})=\sqrt{2}$, $h(\sqrt{3})=-\sqrt{3}$, $gh(\sqrt{2})=-\sqrt{2}$, $gh(\sqrt{3})=-\sqrt{3}$.

Let $\sigma_1=\sqrt{2}$, $\sigma_2=-\sqrt{2}$, $\sigma_3=\sqrt{3}$, $\sigma_4=-\sqrt{3}$. $id:\begin{smallmatrix}\sigma_1\to\sigma_1\\ \sigma_2\to\sigma_2\\ \sigma_3\to\sigma_3\\ \sigma_4\to\sigma_4\end{smallmatrix}$, $id=id$. $g:(1\ 2)$ $h:(3\ 4)$ $gh:(1\ 2)(3\ 4)$. Thus, $\Gamma(\Sigma:K)\cong\{e,(1 2),(3 4),(1 2)(3 4)\}\leq S_4$.

$\boxed{\text{Theorem}}$ 15.9 Let $f\in K[t]$ $(K\subseteq\mathbb{C})$. Then f is soluble by radicals $\Rightarrow$ Galois group of f over K is soluble.

$\boxed{\text{Lemma}}$ 15.10 Let p be a prime and f an irreducible polynomial of degree p over $\mathbb{Q}$ with precisely two non-real zeros. Then the Galois group of f over $\mathbb{Q}$, $Gal(f)$ is S_p.

Proof – We can regard $Gal(f)$ as a subgroup of S_p. Let Σ be the splitting field, so $Gal(f)=\Gamma(\Sigma:K)$. If α is one root of f in Σ, then $\mathbb{Q}\subseteq\mathbb{Q}(\alpha)\subseteq\Sigma$ is a tower and $[\mathbb{Q}(\alpha):\mathbb{Q}]$
$=p$. Then by the Tower Law, $p\mid[\Sigma:\mathbb{Q}]$. $\therefore p\mid|Gal(f)|$. By Cauchy's theorem, $Gal(f)$ contains an element of order p, i.e. a p-cycle. Also, complex conjugation $c:\mathbb{C}\to\mathbb{C}$
restricts to a $\mathbb{Q}$-automorphism of Σ. But there are just two non-real roots, so c must give a 2-cycle as an element of $Gal(f)$. WLOG, let this 2-cycle be $(1\ 2)$ by renumbering roots.

If σ is the p-cycle, $\sigma^i(1)=2$ for some i. Replacing σ by σ^j WLOG, $\sigma(1)=2$. By renumbering roots 3 to p, $\sigma=(1\ 2\ 3 \cdots p)$. So $\mathrm{Gal}(f) \leq S_p$, $\overset{\tau}{\overset{\shortparallel}{(1\ 2)}}, \overset{\sigma}{\overset{\shortparallel}{(1\ 2 \ldots p)}} \in \mathrm{Gal}(f)$.

By combining τ and σ, we can generate all of S_p: $(\sigma\tau\sigma^{-1})\sigma(i) = \sigma\tau(i)$, so $(\sigma\tau\sigma^{-1})(2) = \sigma\tau(1) = \sigma(2) = 3$, $(\sigma\tau\sigma^{-1})(3) = \sigma\tau(2) = \sigma(1) = 2$, fixing others. Then $(\sigma\tau\sigma^{-1}) = (2\ \ 3)$, Hence $(2\ 3) \in \mathrm{Gal}(f)$. Similarly $(3\ 4) \in \mathrm{Gal}(f)$ etc $\Rightarrow$ all adjacent transpositions are in $\mathrm{Gal}(f)$, so $\mathrm{Gal}(f) = S_p$. // q.e.d.

$\boxed{\text{Theorem}}$ 15.11 Let $f(t) = t^5 - 6t + 3 \in \mathbb{Q}[t]$. Then f is not soluble by radicals.

Proof – f is irreducible over $\mathbb{Q}$ by Eisenstein $p=3$. f has exactly 3 real roots (by sketching). Hence it has exactly 2 complex roots $\Rightarrow \mathrm{Gal}(f) \cong S_5$, which is not soluble. If f were soluble by radicals, then $\mathrm{Gal}(f)$ would be soluble. By contrapositive, f is not soluble by radicals // q.e.d.

END OF SYLLABUS.

END OF COURSE.