Galois Theory ①

Intro 1 : Cubics and Quartics

Quadratics

1. $X^2 + b = 0 \Rightarrow X = \pm\sqrt{-b}$

2. $X^2 - aX + b = 0 \Rightarrow (x-\alpha)(x-\beta) = 0$

We reduce to case 1, where $a = 0$.

$\alpha' := \alpha - \frac{a}{2}$, $\beta' : \beta - \frac{a}{2}$

$\Rightarrow \alpha' + \beta' = 0$

$\alpha'\beta' = \alpha\beta - \frac{a}{2}(\alpha+\beta) + a^2/4 = b - a^2/4$

α', β' are roots of $X^2 + (b - a^2/4)$ i.e. $\pm\sqrt{a^2/4 - b}$

$\Rightarrow \alpha, \beta = \frac{a}{2} \pm \sqrt{a^2/4 - b}$

Cubics

3. $X^3 - c \Rightarrow X = \sqrt[3]{c}, \sqrt[3]{c}\,\zeta, \sqrt[3]{c}\,\zeta^2$

where $1, \zeta, \zeta^2$ are the roots of $X^3 - 1 = 0$.

$X^3 - 1 = (x-1)(X^2 + X + 1) \Rightarrow \zeta, \zeta^2 = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$

(i.e. one is ζ and the other is ζ^2. $\zeta^2 + \zeta + 1 = 0$)

4. $X^3 + bX - c = (X-\alpha)(X-\beta)(X-\gamma) = 0$

$a = \alpha + \beta + \gamma$, $b = \alpha\beta + \beta\gamma + \gamma\alpha$, $c = \alpha\beta\gamma$

Lagrange resolvents of this cubic are defined to be

i) $x = \alpha + \beta\zeta + \gamma\zeta^2$, $x\zeta = \alpha\zeta + \beta\zeta^2 + \gamma$, $x\zeta^2 = \alpha\zeta^2 + \beta + \gamma\zeta$

ii) $y = \alpha + \beta\zeta^2 + \gamma\zeta$, $y\zeta = \alpha\zeta + \beta + \gamma\zeta^2$, $y\zeta^2 = \alpha\zeta^2 + \beta\zeta + \gamma$

i) are the roots of $X^3 - x^3 = 0$, ii) the roots of $X^3 - y^3 = 0$

Note that $\zeta^2 + \zeta + 1 = 0$, $\alpha + \beta + \gamma = 0$

$\Rightarrow x + y = 3\alpha$, $x\zeta^2 + y\zeta = 3\beta$, $x\zeta + y\zeta^2 = 3\gamma$

$\Rightarrow (\alpha, \beta, \gamma) = \left(\frac{1}{3}(x+y), \frac{1}{3}(x\zeta^2 + y\zeta), \frac{1}{3}(x\zeta + y\zeta^2)\right)$

Also, $xy = \alpha^2 + \beta^2 + \gamma^2 - \alpha\beta - \beta\gamma - \gamma\alpha$

$= (\alpha + \beta + \gamma)^2 - 3b = -3b$

(using $\zeta \cdot \zeta^2 = 1$, $\zeta + \zeta^2 = -1$)

$\Rightarrow x, y$ determine each other

Now $x^3 + y^3 = (x+y)(x + \zeta y)(x + \zeta^2 y)$ ($\times\zeta$, $\times\zeta^2$)

$= 3\alpha \cdot 3\beta \cdot 3\gamma = 27c$

$x^3 y^3 = -27b^3$

So x^3, y^3 are roots of $X^2 - 27cX - 27b^3 = 0$

and we have reduced to 2.

5. $X^3 - aX^2 + bX - c = (X-\alpha)(X-\beta)(X-\gamma) = 0$

Reduce to 4: $\alpha' := \alpha - \frac{a}{3}$, $\beta' := \beta - \frac{a}{3}$, $\gamma' := \gamma - \frac{a}{3}$

Compute $\alpha' + \beta' + \gamma'$, $\alpha'\beta' + \beta'\gamma' + \gamma'\alpha'$, $\alpha'\beta'\gamma'$

$\Rightarrow \alpha', \beta', \gamma'$ are roots of

$X^3 + \left(b - \frac{a^2}{3}\right)X - \left(\frac{2}{27}a^3 - \frac{ab}{3} + c\right) = 0$

Find α, β, γ by adding $\frac{a}{3}$ to these.

Galois Theory ①

Quartics

6. $X^4 - aX^3 + bX^2 - cX + d = 0 \quad = (X-\alpha)(X-\beta)(X-\gamma)(X-\delta)$

Subtract $a/4$ from $\alpha, \beta, \gamma, \delta$ to reduce to the case $a = 0$.

Now we reduce to the cubic case, 5.

Let $x = \alpha+\beta = -(\gamma+\delta)$, $y = \alpha+\gamma = -(\beta+\delta)$

$z = \alpha+\delta = -(\beta+\gamma)$

$\Rightarrow (\alpha, \beta, \gamma, \delta) = \frac{1}{2}(x+y+z, x-y-z, -x+y-z, -x-y+z)$

Note $xyz = (\alpha+\beta)(\alpha+\gamma)(\alpha+\delta)$

$= \underbrace{\alpha^3 + (\beta+\gamma+\delta)\alpha^2}_{=0} + \underbrace{(\beta\gamma+\gamma\delta+\delta\beta)\alpha + \beta\gamma\delta}_{=c}$

$= c$

Then $x^2 = -(\alpha+\beta)(\gamma+\delta)$, $y^2 = -(\alpha+\gamma)(\beta+\delta)$

$z^2 = -(\alpha+\delta)(\beta+\gamma)$

$\Rightarrow x^2+y^2+z^2 = -2(\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta) = -2b$

$x^2y^2 + y^2z^2 + z^2x^2 = b^2 - 4d$

$x^2y^2z^2 = c^2$

$\Rightarrow x^2, y^2, z^2$ are the roots of $X^3 + 2bX^2 + (b^2-4d)X - c^2 = 0$

This is the <u>resolvent cubic</u> of our quartic, solved by 3, 4, 5.

Then we get x, y, z by 1.

Choosing signs for x and y determines z since $xyz = c$.

$\Rightarrow$ Only four choices of sign are allowed.

1. $\sqrt{-b} \leftrightarrow -\sqrt{-b}$, $S_2 = C_2$

$1 \Rightarrow 2$ involves rational operations $(+, -, \times, \div)$

3. $\sqrt[3]{C} \leftrightarrow \sqrt[3]{C}\zeta$, $A_3 = C_3$

$\sqrt[3]{C}\zeta^2$

4. $x \leftrightarrow x\zeta$ $\quad x\zeta^2$ $\qquad A_3 \qquad$ $y \leftrightarrow y\zeta$ $\quad y\zeta^2$ $\qquad x^3 \leftrightarrow y^3$ $\qquad S_2$

$S_3 \triangleright A_3$, $S_3/A_3 \cong S_2$

$4 \Rightarrow 5$ involves rational operations

6. $S_4 \curvearrowright \{\alpha, \beta, \gamma, \delta\}$ $\qquad S_4 \triangleright$ [permutations of $\alpha, \beta, \gamma, \delta$, fixing each of x^2, y^2, z^2]

$\downarrow$

$S_3 \curvearrowright \{x^2, y^2, z^2\}$

$S_4 \triangleright V_4 = \{id, (\alpha\beta)(\gamma\delta), (\alpha\gamma)(\beta\delta), (\alpha\delta)(\beta\gamma)\}$

$\cong C_2 \times C_2$

$S_4/V_4 \cong S_3$

$V_4 \curvearrowright \begin{bmatrix} x & y & z \\ \updownarrow & \updownarrow & \updownarrow \\ -x & -y & -z \end{bmatrix}$ changing the signs of x, y, z but not xyz

A <u>field</u> is a set closed under $+, -, \times, \div$.

I. Rational Operations occur within the same field $(1 \Rightarrow 2, 4 \Rightarrow 5)$

II. Whenever the field was changed (<u>extended</u>) an additional symmetry was introduced.

Galois' insight was to ignore I but keep track of II.

Exploiting subgroups $\leftrightarrow$ Partially symmetric polynomials.

S_n $(n \geq 5)$ has no proper normal subgroups apart from A_n, so similar reduction is impossible.

26/10/12 Galois Theory (2)

Intro 2 : Circles

a) Abstract ⇔ Intuitive . By a circle, we mean :

(Euclid, BC 300) P: centre, r: radius, $C := \{Q \in \text{plane} \mid |PQ| = r\}$

(Descartes, 17C) $C := \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 = r^2\}$ (+)

(Galois/Lie, 19C) A set on which the following group acts.

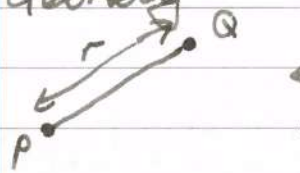
$\mathbb{R}/2\pi\mathbb{Z}$ (*) $= \{T_\theta$: rotation of angle θ such that

i) $T_0 = id$ ii) $T_{\theta'} \circ T_\theta = T_{\theta'+\theta}$ iii) $T_\theta = T_{\theta'} \Leftrightarrow \theta - \theta' \in 2\pi\mathbb{Z}\}$

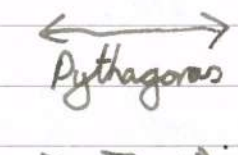
This captures the essence of 'circular' shapes.

b) Dictionaries Intuition ⟷ Manipulate symbols

Geometry ⟷ Algebra ⟷ Groups



Pythagoras



trigonometry $T_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

$(x,y) \in C \Rightarrow T_\theta(x,y) \in C$ gives $\cos^2\theta + \sin^2\theta = 1$

$T_{\theta'} \circ T_\theta = T_{\theta+\theta'} \Rightarrow$ addition formulae

The symmetry group (*) was hidden beneath the equation (+). This is not so obvious.

Similarly beneath $X^2 - 3X + 5 = 0$ lies $X \Leftrightarrow 3 - X$

because $(3-X)^2 - 3(3-X) - 5 = X^2 - 3X - 5$

Beneath the equation $X^4 + 52X^3 - 26X^2 - 12X + 1$ lies the group C_4.

$$X \longrightarrow -\frac{4X}{(1-X)^2}$$

$$\frac{(1-X)(1+3X)}{-4X^2} \longleftarrow \frac{1-X}{1+3X}$$

(from Galois' diary 1797)

Cubic $(\alpha, \beta, \gamma) = \left(\frac{x+y}{3} \quad \frac{x\zeta^2+y\zeta}{3} \quad \frac{x\zeta+y\zeta^2}{3}\right)$

$(\alpha, \beta, \gamma, \delta) = \left(\frac{x+y+z}{2}, \frac{x-y-z}{2}, \frac{-x+y-z}{2}, \frac{-x-y+z}{2}\right)$

1. Classical Galois Theory (as Galois did it)

1.1 Basic Notions

Definition 1 Let L be a field. If a subring k of L is a field, it is a subfield of L. We say that L is an extension of k. We refer to the pair as an extension L/k. (read L/k, NOT a quotient)
Note: if k, L are both subfields of a field F and $k \subset L$ then k is a subfield of L. So we have extensions F/k, F/L and L/k.
Sometimes L/k is called a subextension of F/k.
$k \subset L \subset F$

We are mainly interested in subfields of $\mathbb{C}$, although until 1.3 all will be valid for general field.

Example $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Recall $\mathbb{Q}(\sqrt{2}) := \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
Similarly $\mathbb{Q}(\sqrt{-1})$ etc. Then $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. $\mathbb{Q}(\sqrt{-1}) \not\subset \mathbb{R}$.
Recall that $\mathbb{C}$ is a real vector space. In general, if L/k is an extension, then the multiplication in L makes L into a k-vector space (L is an additive group, by the axioms for rings).
We always consider L as a k vector space in this way. If $k \subset L \subset F$ then L is a sub-k-vector space of F.

Definition 2 We say L/k is finite if L is a finite dimensional k-vector space, otherwise infinite. Its dimension is called the degree of L/k, denoted by $[L:k]$
e.g. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, finite with basis $\{1, \sqrt{2}\}$
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ $[\mathbb{C} : \mathbb{R}] = 2$, $\mathbb{R}/\mathbb{Q}$ infinite.
Recall $k[X]$:= the ring of polynomials with coefficients in k.
Polynomials = formal k-linear combinations of $1, X, X^2$
They form a ring, and a k-vector space but are usually not considered as functions.

06/10/12

Galois Theory (2)

Definition 3 Let L/k be an extension and $\alpha \in L$.
Let $I_\alpha := \{P(x) \in k[x] \mid P(\alpha) = 0\} \subset k[x]$
the set of all polynomials which have α as a root.
We say α is algebraic over k if $I_\alpha \neq \{0\}$ and transcendental over k if $I_\alpha = \{0\}$. We say L/k is algebraic if every $\alpha \in L$ is algebraic $/k$ (over k). Otherwise transcendental

e.g. $\sqrt{2}$, $\sqrt[3]{2}$, algebraic $/\mathbb{Q}$, π, e: transcendental $/\mathbb{Q}$

Proposition 4 Every finite extension is algebraic.

Proof
If $[L:k] = n$, and $\alpha \in L$, then the elements $1, \alpha, \alpha^2, \dots, \alpha^n \in L$ are linearly dependent over k.
Hence $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$, $a_0, a_1, \dots, a_n \in k$ not all zero and hence $P(\alpha) = 0$ for some non-zero $P \in k[x]$.
i.e. $I_\alpha \neq 0$. □

Now note that I_α in Def 3 is the kernel of the ring homomorphism
$\hat{I}_\alpha : k[x] \ni P(x) \mapsto P(\alpha) \in L$ "plug in α".
(It is also a k-linear map) and hence an ideal in $k[x]$.
Also directly checked by $P(\alpha), Q(\alpha) = 0$
$\Rightarrow (P+Q)(\alpha) = 0$, $R(\alpha)P(\alpha) = 0$

09/10/12

Galois Theory ③

1.1 Basic notions (continued)

correct
set
elements
for
prop. 4

Recall - L/k extension. $\alpha \in L$.

$$I_\alpha = \{P(x) \in k[x] \mid P(\alpha) = 0\} = \ker f_\alpha \subset k[x]$$ ← an ideal

$$f_\alpha : k[x] \ni P(x) \mapsto P(\alpha) \in L \quad \text{"plug in } \alpha\text{"}$$

α is algebraic ~~over~~ /k if $I_\alpha \neq \{0\}$

Definition 5

Let L/k be an extension, and $\alpha \in L$ algebraic /k. As $k[x]$ is a PID, we have $I_\alpha = (P_\alpha) = \{\text{multiples of } P_\alpha\}$ for a unique monic $P_\alpha \in k[x]$. This is called the minimal polynomial of α over k.

Note: $\deg P_\alpha$ is minimal among $\deg P$ for $P \neq 0$ in I_α

Examples

i) Min. poly. of $\alpha = \sqrt{2}$ over $\mathbb{Q}$. $P_\alpha = X^2 - 2 \in \mathbb{Q}[x]$

ii) $\alpha = \sqrt{2}$ over $\mathbb{R}$: $P_\alpha = X - \sqrt{2} \in \mathbb{R}[x]$

iii) $\alpha = \sqrt[3]{2}$ over $\mathbb{Q}$: $P_\alpha = X^3 - 2 \in \mathbb{Q}[x]$

Consider $f_\alpha : \mathbb{Q}[x] \to \mathbb{C}$, and

$$\mathbb{Q}(\alpha) := \operatorname{Im} f_\alpha = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{C}$$

This is a field, as it is a ring and every non-zero element is invertible. How do you find $(1+\alpha)^{-1}$?

Use $(1+\alpha)(1-\alpha+\alpha^2) = 1 + \alpha^3 = 3$

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

1.2 Simple Extensions

Note: the intersection of subfields is a subfield, but the union is not in general.

Definition 6

Let L/k be an extension and $\alpha \in L$. We denote by $k(\alpha)$ the intersection of all subfields of L containing k and α, i.e. the minimal such subfield. Then $k(\alpha)/k$ is called the extension generated by α. We say L/k is simple if $L = k(\alpha)$ for some $\alpha \in L$.

$k \subset k(\alpha) \subset L$

Proposition 7 $\quad f_\alpha : k[x] \to L$, $P(x) \mapsto P(\alpha)$

Let L/k be an extension and $\alpha \in L$, algebraic over k.

i) Its minimal poly P_α over k is irreducible in $k[x]$.

ii) $\operatorname{Im} f_\alpha = k(\alpha)$ and $[k(\alpha) : k] = \deg P_\alpha$

(In particular $k(\alpha)/k$ is finite)

Proof ($f_\alpha : P(x) \mapsto P(\alpha)$, $k[x] \to k(\alpha)$)

i) If $P_\alpha(x) = P(x)\,Q(x)$, then $P(\alpha)\,Q(\alpha) = P_\alpha(\alpha) = 0$

Hence $P(\alpha) = 0$ or $Q(\alpha) = 0$. Say $P(\alpha) = 0$. Then, $P \in I_\alpha = (P_\alpha)$ i.e. $P_\alpha \mid P$. Hence Q is a unit (divisor of 1) in $k[x]$

ii) (1) $\operatorname{Im} f_\alpha$ is a subfield of L.

∵) It is a ring (it is the image of a ring homomorphism). Every x in $\operatorname{Im} f_\alpha$ is of the form $P(\alpha)$ for some $P \in k[x]$.

If $x \neq 0$, then $P \notin I_\alpha = (P_\alpha)$ i.e. P is not divisible by P_α.

i.e. P is not divisible by P_α. Hence $\exists Q \in k[X]$ with $PQ \equiv 1 \bmod P_\alpha$ therefore $P(\alpha)^{-1} = Q(\alpha) \in \mathrm{Im} f_\alpha$

(2) $\mathrm{Im} f_\alpha = k(\alpha)$ ~~(do (2) after (3). Create polynomials with $P(\alpha) = \sum a_i \alpha^i$ to show $\mathrm{Im} f_\alpha \supseteq k(\alpha)$)~~ ?

$\because$) As $\mathrm{Im} f_\alpha$ is a subfield of L containing k and α, and any such field must contain $\mathrm{Im} f_\alpha$. We have $\mathrm{Im} f_\alpha = k(\alpha)$.

(3) If $\deg P_\alpha = n$, then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ gives a basis of $k(\alpha)$ as a k-vector space.

$\because$) For every $x = P(\alpha) \in \mathrm{Im} f_\alpha$, $\exists Q, R \in k[X]$ with $P = P_\alpha Q + R$ and $\deg R < n$. Hence $x = P(\alpha) = R(\alpha)$ is a k-linear combination of $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

If $R(\alpha) = 0$ with $\deg R < n$, then $P_\alpha \nmid R$, hence $R =$ □

Remarks

i) Different elements can generate the same field

i.e. we can have $k(\alpha) = k(\alpha')$ with $\alpha \neq \alpha'$

e.g. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1+\sqrt{2})$

ii) By Prop 4 and 7 ii), for an extension L/k and $\alpha \in L$, α algebraic $/k \iff k(\alpha)/k$ finite

iii) If $k \subset L \subset F$ and $\alpha \in F$, then $k[X] \subset L[X]$ implies

(1) α: algebraic $/k \Rightarrow \alpha$: algebraic $/L$

(2) the min. poly. Q_α over L divides the min. poly. P_α over k $\in k[X] \subset L[X]$

We will see: the converse of (1) is true when L/k is finite.

iv) Related Question: $\sqrt{2}$ algebraic over $\mathbb{Q}$ (X^2-2)

$\sqrt[3]{2}$ algebraic over $\mathbb{Q}$ (X^3-2), but is $\sqrt{2}+\sqrt[3]{2}$? What polynomial

We will use $\mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2})(\sqrt[3]{2})$

1.3 Finite Extensions

Note: If $[L:k]=1$ then $L=k$ (1D k-vector space)

Proposition 8 (Tower Law)

Let $k \subset L \subset F$. If L/k and F/L are finite extensions then so is F/k, and $[F:k] = [F:L][L:k]$

Proof

Let $\{a_1, \dots, a_n\} \subset L$ be a basis of L/k (i.e. a basis of L as a k-vector space), and $\{b_1, \dots, b_m\} \subset F$ a basis of F/L.

Then every $x \in F$ is written as $x = \sum_{i=1}^{m} x_i b_i$, $x_j \in L$, and each x_j is written as $x_j = \sum_{i=1}^{n} x_{ij} a_i$, $x_{ij} \in k$.

Hence $x = \sum_j \left(\sum_i x_{ij} a_i\right) b_j = \sum_{i,j} x_{ij} a_i b_j$

If $x = \sum_{i,j} x_{ij} a_i b_j = 0$, then $\sum_j x_{ij} a_i = 0$

$\forall j$ by independence of $\{b_j\}$, therefore $x_{ij} = 0$ $\forall i$ by independence of $\{a_i\}$. Thus $\{a_i b_j\}$ is a basis of F/k [illegible]

11/10/12 Galois Theory (4)

1.3 Finite Extensions (continued)

Recall L/k, an extension. $\alpha \in L$ algebraic $/k$ with min poly P_α.
$\Rightarrow k \subset k(\alpha) \subset L$, $[k(\alpha) : k] = \deg P_\alpha$

Tower Law $k \subset L \subset F$ finite extensions $\Rightarrow [F:k] = [F:L][L:k]$

(proof considering the finite dimensional L-vector space V as a k vector space, we have $\dim_k V = [L:k] \dim_L V$)

Definition 9

Let L/k be an extension and $\alpha_1, \ldots, \alpha_n \in L$. We denote by $k(\alpha_1, \ldots, \alpha_n)$ the intersection of all subfields of L containing k and $\alpha_1, \ldots, \alpha_n$ i.e. the minimal such subfield. Then $k(\alpha_1, \ldots, \alpha_n)/k$ is called the extension generated by $\alpha_1, \ldots, \alpha_n$ over k. The order of $\alpha_1, \ldots, \alpha_n$ is irrelevant and $k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ (both inclusions are immediate from definitions).

Proposition 10

i) If L/k is an extension and $\alpha_1, \ldots, \alpha_n \in L$ are algebraic $/k$, then $k(\alpha_1, \ldots, \alpha_n)/k$ is finite.

ii) Conversely, every finite extension L/k is generated by finitely many elements, i.e. $\exists \alpha_1, \ldots, \alpha_n \in L$, $L = k(\alpha_1, \ldots, \alpha_n)$.

Proof

i) As α_n is alg $/k$, it is *a fortiori* alg $/k(\alpha_1, \ldots, \alpha_{n-1})$, hence $k(\alpha_1, \ldots, \alpha_n) = k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ is finite

over $K(\alpha_1, \ldots, \alpha_{n-1})$ by Proposition 7 ii).

Repeat for each $K(\alpha_1, \ldots, \alpha_i)$, $1 \leq i \leq n$, and use the Tower Law (proposition 8)

ii) Take a basis $\{e_1, \ldots, e_n\}$ of L/K. Then $K(e_1, \ldots, e_n) =$ because every $x \in L$ is a K-linear combination. □

Example

The min poly. of $\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $X^3 - 2$, as it is irreducible in $\mathbb{Q}(\sqrt{2})[X]$ (otherwise its root in $\mathbb{Q}(\sqrt{2})$ generates a field of degree 3 / $\mathbb{Q}$), hence $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ by Proposition 7 ii).

$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ Thus $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] = 6$ (Tower Law + Proposition 8

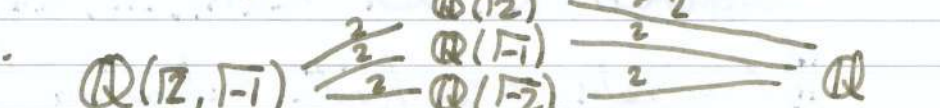
3 | $\mathbb{Q}(\sqrt{2})$ $\sqrt{2} + \sqrt[3]{2}$ What is the min. poly. of $\sqrt{2} + \sqrt[3]{2}$?

2 | (It has to have degree ≤ 6).

$\mathbb{Q}$ In fact, it is 1, 2, 3 or 6 by the Tower Law.

Example

The fields of the form $K(\sqrt{a})$ and $K(\sqrt{a}, \sqrt{b})$ for non-square elements $a, b \in K$, are called quadratic and biquadratic extensions of K.



This is a finite extension of deg 4 / $\mathbb{Q}$ with a basis $\{1, \sqrt{2}, \sqrt{-1}, \sqrt{-2}\}$

Remark

Finite extensions are algebraic (Proposition 4), but there exist infinite algebraic extensions.

11/10/12

Galois Theory ④

1.4 k-Homomorphisms

Lemma 11 (not the zero ring)

If L is a field, any ring homomorphism $\tau : L \to L'$ from L is injective.

Proof

As $\ker \tau$ is an ideal of L, not containing $1 \in L$ ($\because \tau(1) = 1_{L'}$)

Hence $\{0\}$ (A field has ideals $\{0\}$, L). □

Definition 12

Let L/k, L'/k be two extensions of k. A k-homomorphism from L to L' is a ring homomorphism $\tau : L \to L'$ such that $\tau|_k = id$. The set of all k-homomorphisms from L to L' is denoted by $\mathrm{Hom}_k(L, L')$

Note: All k-homomorphisms are injective by the Lemma, also called embeddings, and they are k-linear.

We're mainly interested in the set $\mathrm{Hom}_k(L, \mathbb{C})$ when $k \subset L \subset \mathbb{C}$

Example

i) $\mathbb{C}/\mathbb{R}$, $\mathbb{R}$-homomorphisms $\tau : \mathbb{C} \to \mathbb{C}$, there are two (note $\mathbb{C} = \mathbb{R}(\sqrt{-1})$). $\mathrm{Hom}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{id., \text{complex conjugate}\}$

$id : \sqrt{-1} \mapsto \sqrt{-1}$, complex conjugate : $\sqrt{-1} \mapsto -\sqrt{-1}$

ii) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}$ homomorphisms $\mathbb{Q}(\sqrt{2}) \to \mathbb{C}$, there are two.

$\tau_1 = id : \sqrt{2} \mapsto \sqrt{2}$, $\tau_2 : \sqrt{2} \mapsto -\sqrt{2}$

Note: being a ring-homomorphism (id on k), it must send a root of P to a root of $P \in k[x]$.

iii) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Let $\zeta^3 = 1$, $\zeta \neq 1$

3 $\mathbb{Q}$-homomorphisms $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$

$$\begin{cases} \tau_1 = id: \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \tau_2 \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta \\ \tau_3 \quad \sqrt[3]{2} \mapsto \sqrt[3]{2}\zeta^2 \end{cases}$$

(roots of $X^3 - 2$ in $\mathbb{C}$). In contrast to i), ii), $\mathrm{Im}\,\tau_i$ are different subfields of $\mathbb{C}$.

Definition 13

i) For a non-zero $P \in k[X]$, and an extension L/k, we denote by $\mathrm{Root}_P(L)$, the set of all roots of P in L.

ii) Let $\alpha \in L$ be algebraic/k. A roots of its min. poly. P_α over k in L, i.e. an element of $\mathrm{Root}_{P_\alpha}(L)$ is called a conjugate of α in L over k.

Proposition 14 (Roots and Homomorphisms I)

Let F/k, E/k be two extensions of k and $\alpha \in F$ be algebraic/k. Then we have a bijection

$$\mathrm{Hom}_k(k(\alpha), E) \ni \tau \xmapsto{\varphi} \tau(\alpha) \in \mathrm{Root}_{P_\alpha}(E)$$

In particular we have $|\mathrm{Hom}_k(k(\alpha), E)| \leq [k(\alpha) : k]$

Proof: (every k-hom sends α to its conjugate in k)

Shows that indeed $\varphi(\tau)$ a root

(1) We have a map. :) As $P_\alpha(\alpha) = 0$, τ is a ring hom. and $\tau|_k = id$, hence $P_\alpha(\tau(\alpha)) = \tau P_\alpha(\alpha) = 0$

(2) It is injective. :) All elements in $k(\alpha)$ are polynomials in α with coefficients in k (Proposition 7 ii)) and $\tau|_k = id$. The map is determined by $\tau(\alpha) \in E$.

(3) It is surjective. Recall $k(\alpha) = \mathrm{Im}\, f_\alpha$ (next time)

11/10/12 Galois Theory ④ Prop 7ii)

(4) $|\mathrm{Hom}_K(K(\alpha), E)| = |\mathrm{Root}_{p_\alpha}(E)| \leq \deg p_\alpha = [K(\alpha) : K$

13/10/12

Galois Theory ⑤

1.4 k-Homomorphisms (continued)

Proof (proposition 14)

We are proving: F/k, E/k, $\alpha \in F$ algebraic/k, min poly P_α

$\mathrm{Hom}_k(\underset{\text{II}}{k(\alpha)}, E) \xrightarrow{\cong} \mathrm{Root}_{P_\alpha}(\underset{\text{II}}{E})$

$\{k\text{-homomorphisms } k(\alpha) \to E\}$ $\{\text{Roots of } P_\alpha \text{ in } E\}$

Remark

We have in mind Chapter 1, $k \subset \mathbb{C}$, $F = E = \mathbb{C}$

(3) Surjectivity: Recall $k(\alpha) = \mathrm{Im} f_\alpha$

$f_\alpha : k[X] \ni P(X) \mapsto P(\alpha) \in F$. Let $\beta \in \mathrm{Root}_{P_\alpha}(E)$.

We will define $\tau : k(\alpha) \to E$ satisfying $\tau(\alpha) = \beta$.

Every $x \in k(\alpha)$ is written $x = P(\alpha)$, $P \in k[X]$, and P is unique up to adding multiples of P_α (i.e. every other choice of P is of the form $P + P_\alpha Q$). $P_\alpha(\beta) = 0$, hence $P(\beta) \in E$ is well defined. So let $\tau(x) := P(\beta)$ i.e. $\tau : k(\alpha) \ni P(\alpha) \to P(\beta) \in E$. This is clearly a ring homomorphism and $\tau|_k = id$ □

1.5 k-Homomorphisms into $\mathbb{C}$

Note

Subfields of $\mathbb{C}$ are always extensions of $\mathbb{Q}$. For $k \subset \mathbb{C}$, $\alpha \in \mathbb{C}$, by conjugates of α over k, we will always mean its conjugate in $\mathbb{C}$, e.g. $\sqrt[3]{2}$ over $\mathbb{Q}$ has conjugates

$\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$, $\zeta^3 = 1$, $\zeta \neq 1$

Proposition 15

Let $k \subset \mathbb{C}$.

i) Let $P \in k[X]$ be an irreducible polynomial in $k[X]$. Then $|\mathrm{Root}_P(\mathbb{C})| = \deg P$ (Separability of P)

ii) Let $\alpha \in \mathbb{C}$ be algebraic/k. Then $|\mathrm{Hom}_k(k(\alpha), \mathbb{C})| = [k(\alpha):k]$

Proofs

i) A multiple root $\alpha \in \mathbb{C}$ of P would also be a root of $P'(x) := \frac{d}{dx} P(x) \in k[X]$, but $\deg P' < \deg P$ and P is irreducible, hence P, P' are coprime in $k[X]$, so we have $PQ + P'R = 1$ in $k[X]$, hence also in $\mathbb{C}[X]$

Alternatively substitute α

Thus P, P' are coprime in $\mathbb{C}[X]$. Hence all roots of P are distinct, and there are $\deg P$ of them, by FTA.

ii) $|\mathrm{Hom}_k(k(\alpha), \mathbb{C})| \underset{\text{Prop 14}}{=} |\mathrm{Root}_{P_\alpha}(\mathbb{C})| \underset{\text{i)}}{=} \deg P_\alpha \underset{\text{Prop 7 ii)}}{=} [k(\alpha):k]$

Next goal: Generalize ii) to

$|\mathrm{Hom}_k(F, \mathbb{C})| = [F:k]$ (separability of F/k)

Method: Break down to simple extensions and stack up.

If $k \subset L \subset F$ and $\rho \in \mathrm{Hom}_k(F, \mathbb{C})$, then

$\rho_L \in \mathrm{Hom}_k(L, \mathbb{C})$ (ring homomorphism. $\rho|_k = \mathrm{id}$)

so we have a restriction map

$\mathrm{Hom}_k(F, \mathbb{C}) \ni \rho \mapsto \rho_L \in \mathrm{Hom}_k(L, \mathbb{C})$

To climb up, count $\#\rho$ with a fixed ρ_L, the fibres of the map.

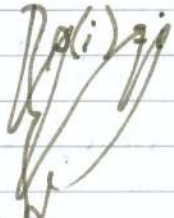
Example

(1) $i := \sqrt{-1}$, $L = \mathbb{Q}(\sqrt{2})$. $\mathrm{Hom}_k(L, \mathbb{C}) = \{\tau_1 = id, \tau_2 : \sqrt{2} \mapsto -\sqrt{2}\}$

$F = \mathbb{Q}(\sqrt{2}, i)$ $\quad \rho \in \mathrm{Hom}_k(F, \mathbb{C})$

$L = \mathbb{Q}(\sqrt{2})$ $\quad \rho|_L = \tau_1 = id$, $\rho(\sqrt{2}) = \sqrt{2}$

$k = \mathbb{Q}$ $\quad \rho|_L = \tau_2$, i.e. $\rho(\sqrt{2}) = -\sqrt{2}$



τ_1: $\rho(i) = i \Rightarrow \rho_1 = id$. $\rho(i) = -i \Rightarrow \rho_2(\sqrt{2}, i) = (\sqrt{2}, -i$

τ_2: $\rho(i) = i \Rightarrow \rho_3(\sqrt{2}, i) = (-\sqrt{2}, i)$. $\rho(i) = -i \Rightarrow \rho_4(\sqrt{2}, i) \mapsto (\sqrt{2}, -$

(2) The min. poly. of $\alpha = \sqrt[4]{2}$ over $\mathbb{Q}$ is $X^4 - 2 \Rightarrow$ We know $\mathrm{Hom}_k(F, \mathbb{C}$

$F = \mathbb{Q}(\sqrt[4]{2})$

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

$k = \mathbb{Q}$

$\rho_1 = id : \sqrt[4]{2} \mapsto \sqrt[4]{2}$

$\rho_2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2}$

$\rho_3 : \sqrt[4]{2} \mapsto \sqrt[4]{2}\, i$

$\rho_4 : \sqrt[4]{2} \mapsto -\sqrt[4]{2}\, i$

Conjugates of α/k

$\{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}\, i, -\sqrt[4]{2}\, i\}$

$X^2 - \sqrt{2}$ $\quad X^2 + \sqrt{2}$

Min. poly. P_α over L is $X^2 - \sqrt{2}$. $X^2 + \sqrt{2}$ is $\tau_2 P_\alpha$

Restrict them to L. Note $\rho(\sqrt{2}) = \rho(\sqrt[4]{2})^2$ (ρ is a homomorphism

Thus $\rho_1, \rho_2 : \sqrt{2} \mapsto \sqrt{2}$, $\rho_3, \rho_4 : \sqrt{2} \mapsto -\sqrt{2}$

$\rho_1|_L = \rho_2|_L = id = \tau_1$, $\rho_3|_L = \rho_4|_L = \tau_2$

Start with $\rho|_L \in \mathrm{Hom}_k(L, \mathbb{C})$ and try to extend

$\rho_\bullet|_L = \tau_1 \Rightarrow \rho_\bullet$ must map α to a root of P_α

$\rho|_L = \tau_2 \Rightarrow \rho$ must map α to a root of $\tau_2 P_\alpha$

Definition 16

Let L be a field and $\tau : L \to L'$ be a ring homomorphism. For $P \in L[X]$ we denote by $\tau P(X) \in L'[X]$ the polynomial obtained by applying τ to the coefficients of P.

Proposition 17 (Roots and Homomorphisms II)

Let F/k, E/k be extensions of k. Let $k \subset L \subset F$ and $\alpha \in F$ be algebraic over L with min poly P_α.

Then, for every $\tau \in \mathrm{Hom}_k(L, E)$ we have a bijection:

$\{\rho \in \mathrm{Hom}_k(L(\alpha), E) \mid \rho|_L = \tau\} \ni \rho \longmapsto \rho(\alpha) \in \mathrm{Root}_{\tau P_\alpha}(E)$

Remark

Proposition 14 was the special case with $L = k$, $\tau = id$.

Proof

(1) $\exists$ a map $\because$) $P_\alpha(\alpha) = 0$, ρ a ring hom. with $\rho|_L = \tau$

$\tau P_\alpha(\rho(\alpha)) = \rho(P_\alpha(\alpha)) = 0$ i.e. $\rho(\alpha) \in \mathrm{Root}_{\tau P_\alpha}(E)$

(2) Injective $\because$) All elements in $L(\alpha)$ are polynomials in α with coefficients in L, so the map ρ is determined by $\rho(\alpha) \in E$.

(3) Surjective $\because$) Let $\beta \in \mathrm{Root}_{\tau P_\alpha}(E)$, and we'll define ρ with $\rho(\alpha) = \beta$. Every $x \in L(\alpha)$ is written as $x = P(\alpha)$ w/ $P \in L[X]$, and P is unique up to adding multiples of P_α. As $\tau P_\alpha(\beta) = 0$, the element $\tau P(\beta)$ is well defined

$[P' = P + P_\alpha Q \Rightarrow \tau P' = \tau P + \tau P_\alpha \cdot \tau Q]$

So let $\rho(x) := \tau P(\beta)$.

i.e. $\rho : L(\alpha) \ni P(\alpha) \mapsto \tau P(\beta) \in E$.

This is clearly a ring homomorphism and $\tau|_k = id$ $\square$

16/10/12

Galois Theory (6)

1.5 k-homomorphisms into $\mathbb{C}$ (continued)

Theorem 18 (Separability)

Let F/k be a finite extension inside $\mathbb{C}$. Then:

$|\mathrm{Hom}_k(F, \mathbb{C})| = [F:k]$

Proof

Let $F = k(\alpha_1, \dots, \alpha_n)$ (Proposition 10 ii)). If $n=1$, then this is Proposition 15 ii). Use induction on n. Let $L := k(\alpha_1, \dots, \alpha_{n-1})$. $F = L(\alpha)$ with $\alpha := \alpha_n$. Consider the restriction map:

$\mathrm{Hom}_k(F, \mathbb{C}) \ni \rho \mapsto \rho|_L \in \mathrm{Hom}_k(L, \mathbb{C})$

By Proposition 17, the inverse image of each $\tau \in \mathrm{Hom}_k(L, \mathbb{C})$ has cardinality $|\mathrm{Root}_{\tau P_\alpha}(\mathbb{C})|$. Now τP_α is irreducible in $\tau(L)[X]$, (P_α, the min poly of α over L) being the image of $P_\alpha \in L[X]$ (irreducible by Proposition 7 ii)) under the ring isomorphism (Lemma 11) $L[X] \xrightarrow{P \mapsto \tau P}{\sim} \tau(L)[X]$ extending $\tau: L \xrightarrow{\sim} \tau(L)$. Hence $|\mathrm{Root}_{\tau P_\alpha}(\mathbb{C})| \overset{\text{Prop 15 ii)}}{=} \deg \tau P_\alpha = \deg P_\alpha$

$\deg P_\alpha \overset{\text{Prop 7 ii)}}{=} [L(\alpha):L]$.

Thus $|\mathrm{Hom}_k(F, \mathbb{C})| = [L(\alpha):L]\,|\mathrm{Hom}_k(L, \mathbb{C})|$

$= [F:L][L:k]$ (induction hypothesis) $= [F:k]$ (Tower Law)

Lemma 19

Let F/k be a finite extension inside $\mathbb{C}$ and $k \subset L \subset F$. Then, the map $\mathrm{Hom}_k(F, \mathbb{C}) \ni \rho \mapsto \rho|_L \in \mathrm{Hom}_k(L, \mathbb{C})$ is surjective i.e. every k-homomorphism can be extended from $\tau: L \to \mathbb{C}$ to $\tau^*: F \to \mathbb{C}$.

Theorem 20 (Primitive Element Theorem)

Every finite extension inside $\mathbb{C}$ is simple.

Proof

We prove the simplicity of every finite extension F/k with $|k|$: infinite and satisfying the following (ok by Theorem 18 in our case):

If $k \subset L \subset F$, ∃ an extension E/k such that (i.e. a separable extension)

$\mathrm{Hom}_k(L, E) = [L:k]$. (*) (so $E = \mathbb{C}$ in this case)

Let $F = k(\alpha_1, \dots, \alpha_n)$. (Proposition 10). We show that $k(\alpha_1, \dots, \alpha_i)/k$ simple by induction on i: By the induction hypothesis, it suffices to prove that $L = k(\alpha, \beta) \subset F$ is simple/k, $\forall \alpha, \beta$. For $r \in L$ with $k \subset k(r) \subset L$, we have

$|\mathrm{Hom}_k(k(r), E)| \overset{\text{Prop 14}}{\leq} [k(r) : k] \leq [L:k] \overset{(*)}{=} |\mathrm{Hom}_k(L, E)|$

and equality implies $L = k(r)$.

Hence letting $d := [L, k]$ and $\mathrm{Hom}_k(L, E) = \{\tau_1, \dots, \tau_d\}$ it suffices to find $r \in L$ such that $\tau_i|_{k(r)}$ $(1 \leq i \leq d)$ are distinct elements of $\mathrm{Hom}_k(k(r), E)$ i.e. $\tau_1(r), \dots, \tau_d(r)$ are all distinct. We try r of the form $r = \alpha x + \beta$, with $x \in k$. We need

$$0 = \prod_{i \neq j} (\tau_i(r) - \tau_j(r)) = \prod_{i \neq j} \left((\tau_i(\alpha)x + \tau_i(\beta)) - (\tau_j(\alpha)x + \tau_j(\beta)) \right)$$

$$= \prod_{i \neq j} \left((\tau_i(\alpha) - \tau_j(\alpha))x + (\tau_i(\beta) - \tau_j(\beta)) \right)$$

So it will do as long as x is not a root of

$$\prod_{i \neq j} \left((\tau_i(\alpha) - \tau_j(\alpha))X + (\tau_i(\beta) - \tau_j(\beta)) \right) \in E[X]$$

This is not identically zero as $\tau_i(\alpha) \neq \tau_j(\alpha)$ or $\tau_i(\beta) \neq \tau_j(\beta$ for $i \neq j$ (because $\tau_i \neq \tau_j$ and $L = k(\alpha, \beta)$) hence has only finitely many roots. As $|k|$ is infinite, our x exists □

Example

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

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

1.6 Galois Extensions

Definition 21

Let L/k, L'/k' be extensions. If a k-homomorphism $\tau: L \to L'$ is a bijection then $\tau^{-1}: L' \to L$ is also a k homomorphism (ring homomorphism, id on k) and we say that τ is a k- isomorphism. A k-isomorphism $L \to L$ is called a k-automorphism of L, and the set of all k-automorphisms of L is denoted by $\mathrm{Aut}_k(L)$, a subset of $\mathrm{Hom}_k(L, L)$. It is a group under composition.

Lemma 22

i) If there is a k-homomorphism $\tau: L \to L'$ then $[L:k] \leq [L':k$

ii) If $[L:k] = [L':k] < \infty$, then every $\tau \in \mathrm{Hom}_k(L, L')$ is a k-isomorphism. In particular, $\mathrm{Hom}_k(L, L) = \mathrm{Aut}_k(L$, for finite L/k.

iii) If L/k is a finite extension inside $\mathbb{C}$, then $|\mathrm{Aut}_k(L)| \leq [L:k$

Proofs (Linear Algebra)

Recall that all k-homomorphisms are injective (Lemma 11).

(i) Let V, V' be k-vector spaces. If $\exists$ a k-linear injection

(ii) $V \to V'$ then $\dim_k V \leq \dim_k V'$. An injective k-linear map is bijective if $\dim_k V = \dim_k V' < \infty$ by Rank-Nullity.

(iii) $\mathrm{Aut}_k(L) \underset{(ii)}{=} \mathrm{Hom}_k(L, L) \underset{L \subset \mathbb{C}}{\subset} \mathrm{Hom}_k(L, \mathbb{C})$

$|\mathrm{Hom}_k(L, \mathbb{C})| = [L : k]$ (Theorem 18) $\square$

Definition 23

A finite extension L/k is called a Galois Extension if $|\mathrm{Aut}_k(L)| = [L : k]$. In this case $\mathrm{Aut}_k(L)$ is called the Galois Group and denoted by $\mathrm{Gal}(L/k)$.

Proposition 24

Let L/k be a finite extension inside $\mathbb{C}$. The following are equivalent:

(i) L/k Galois

(ii) Every k-homomorphism $\tau : L \to \mathbb{C}$ maps L into itself.

(iii) $\forall \alpha \in L$, every conjugate of α over k is in L.

(iv) $L = k(\alpha_1, \dots, \alpha_n)$, and every conjugate of α_i over k is in L $(1 \leq i \leq n)$

Proofs

$\mathrm{Aut}_k(L) = \mathrm{Hom}_k(L, L) \subset \mathrm{Hom}_k(L, \mathbb{C})$

$|\mathrm{Hom}_k(L, \mathbb{C})| = [L : k]$

(i) $\Leftrightarrow$ (ii) By the proof of Lemma 22 iii),

L/k Galois $\Leftrightarrow \mathrm{Hom}_k(L, L) = \mathrm{Hom}_k(L, \mathbb{C})$

e.g. $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ (can map $\sqrt[3]{2} \mapsto \zeta\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$)

18/10/12 Galois Theory (7)

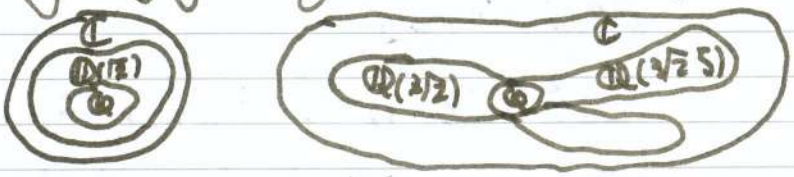
Proposition 24

L/k, a finite extension inside $\mathbb{C}$ is Galois iff:

(ii) Every k-hom $\tau: L \to \mathbb{C}$ maps L into itself

(iii) $\forall \alpha \in L$, every conjugate of α/k is in L.

(iv) $L = k(\alpha_1, \ldots, \alpha_n)$ and every conjugate of α_i/k is in L $(1 \le i \le n)$



(i) $\Leftrightarrow$ (ii) done

(ii) $\Leftrightarrow$ (iii)

Let β be a conjugate of α i.e. $\beta \in \mathrm{Root}_{P_\alpha}(\mathbb{C})$

Then by Prop 14 we have $\tau \in \mathrm{Hom}_k(k(\alpha), \mathbb{C})$ with $\tau(\alpha) = \beta$ and it extends to $\rho \in \mathrm{Hom}_k(L, \mathbb{C})$ (Lemma 19). Then (ii) says that $\beta = \rho(\alpha) \in L$

(iii) $\Rightarrow$ (iv) is clear.

(iv) $\Rightarrow$ (iii) Let $\tau \in \mathrm{Hom}_k(L, \mathbb{C})$. As every $\alpha \in L$ is a poly. in $\alpha_1, \ldots, \alpha_n$ with coefficients in k, $\tau(\alpha)$ is a poly in $\tau(\alpha_1), \ldots, \tau(\alpha_n)$ with coefficients in k. But $\tau(\alpha_i)$ is a conjugate of α_i over k (prop 14), hence in L by (iv), thus $\tau(\alpha) \in L$ □

Definition 25

Let $P \in k[X]$ with $k \subset \mathbb{C}$, and $\mathrm{Root}_P(\mathbb{C}) = \{\alpha_1, \ldots, \alpha_n\}$. Then $k(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ is called the splitting field of P over k.

Corollary 26

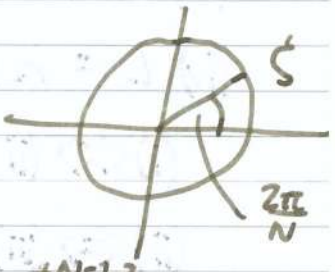
Let $P \in k[X]$, $k \subset \mathbb{C}$. Its splitting field over k is Galois over k

Proof

It is a finite extension of k (Prop 10 ii)) and as all conjugates of α_i over k belong to $\mathrm{Root}_P(\mathbb{L})$ ($\because$ min poly. of α_i divides P)

It is a Galois Extension by Prop 24 iv). □

Big Example! (Cyclotomic Extensions)



Definition 27

Let $N \geq 1$, $\zeta = \zeta_N = \exp\left(\frac{2\pi i}{N}\right) \in \mathbb{C}$

Then $\mu_N := \mathrm{Root}_{X^N-1}(\mathbb{C}) = \{1, \zeta, \zeta^2, \dots, \zeta^{N-1}\}$

is multiplicative, cyclic of order n, and ζ^i is a generator $\Leftrightarrow (i, N) = 1$: they are called primitives.

For $k \subset \mathbb{C}$, the splitting field of $X^N - 1$ over k is denoted $k(\mu_N)$ and called a cyclotomic extension of k. Note

$k(\mu_N) = k(1, \zeta, \zeta^2, \dots, \zeta^{N-1}) = k(\zeta) = k(\zeta^i)$, $(i,N)=1$

Proposition 28

Let $k \subset \mathbb{C}$ and $N \geq 1$. We have an injective ~~map~~ hom. group from

$\mathrm{Gal}(k(\mu_N)/k) \hookrightarrow (\mathbb{Z}/(N))^\times$

$(\tau : \zeta \mapsto \zeta^i) \longmapsto i \bmod N$

where $(\mathbb{Z}/(N))^\times = \{i \bmod N \mid (i,N) = 1\}$ is the multiplicative group of units in the ring $\mathbb{Z}/(N) = \{i \bmod N \mid i \in \mathbb{Z}\}$

Proof

Let $\tau \in \mathrm{Gal}(k(\mu_N)/k)$. As $\zeta \in \mu_N$ and has order N in μ_N, $\tau(\zeta) \in \mu_N$ and has order N

i.e. $\tau(\zeta) = \zeta^i$ with $(i, N) = 1$

i is well defined mod N, so we have a map.

As $\tau(\zeta)$ determines τ, since $k(\mu_N) = k(\zeta)$, this map is injective. If $\tau(\zeta) = \zeta^i$ and $\sigma(\zeta) = \zeta^j$ then $\sigma\tau(\zeta) = \sigma(\zeta^i) = \sigma(\zeta)^i = (\zeta^j)^i = \zeta^{ij}$, hence this is a group homomorphism □

Corollary 29

$k(\mu_N)/k$ is abelian i.e. a Galois extension with an abelian Galois Group.

$\hookrightarrow$ injection
$\twoheadrightarrow$ surjection
$\xrightarrow{\cong}$ bijection

Remark

We will see that this injection is a bijection for $k = \mathbb{Q}$ (the irreducibility of cyclotomic poly, chapter 2)

Big Example 2 (Kummer Extensions)

Definition 30

Let $N \geq 1$ and $\mu_N \subset k \subset \mathbb{C}$. Let $a \in k$, and if $\sqrt[N]{a} \in \mathbb{C}$ is a root of $X^N - a$, then

$\mathrm{Root}_{X^N-a}(\mathbb{C}) = \{\sqrt[N]{a}, \sqrt[N]{a}\zeta, \ldots, \sqrt[N]{a}\zeta^{N-1}\}$, where $\zeta = \zeta_N$. The splitting field of $X^N - a$ over k is called a Kummer Extension of k and is equal to $k(\sqrt[N]{a})$ for any choice of $\sqrt[N]{a}$.

Proposition 31

If $k(\sqrt[N]{a})/k$ is as above, we have an injective group homomorphism. $\mathrm{Gal}(k(\sqrt[N]{a})/k) \hookrightarrow \mathbb{Z}/N\mathbb{Z}$

$(\tau : \sqrt[N]{a} \mapsto \sqrt[N]{a}\zeta^i) \mapsto i \bmod N$

where $\mathbb{Z}/N\mathbb{Z}$ is the additive group of $\mathbb{Z}/(N)$. In particular $k(\sqrt[N]{a})/k$ is abelian.

Proof

Let $\tau \in Gal(k(\sqrt[N]{a})/k)$. Then $\tau(\sqrt[N]{a}) = \sqrt[N]{a}\,\zeta^i$ for some i, well defined mod N and independent of the choice of $\sqrt[N]{a}$ ($\because \tau(\sqrt[N]{a}\,\zeta^j) = (\sqrt[N]{a}\,\zeta^i)\zeta^j = (\sqrt[N]{a}\,\zeta^j)\zeta^i$. As $\tau(\sqrt[N]{a})$ determines τ, this map is injective. If $\tau(\sqrt[N]{a}) = \sqrt[N]{a}\,\zeta^i$, $\sigma(\sqrt[N]{a}) = \sqrt[N]{a}\,\zeta^j$, then $\sigma\tau(\sqrt[N]{a}) = \sqrt[N]{a}\,\zeta^{(i+j)}$ i.e. it is a group hom. □

Example — Splitting field of x^3-2 → $\mathbb{Q}(\sqrt[3]{2}, \zeta)$, 6, $3 \mid \mathbb{Z}/3\mathbb{Z}$ kummer, $\mathbb{Q}(\zeta)$, $2 \mid (\mathbb{Z}/(3))^\times \cong C_2$ cyclotomic, $\mathbb{Q}$

Let $\zeta^3 = 1$, $\zeta \neq 1$.

1.7 Galois Correspondance

Example

$\zeta = \zeta_8 = \frac{\sqrt{2}}{2}(1+i)$, root of x^4+1

$\mathbb{Q}(\mu_8) = \mathbb{Q}(\sqrt{2}, i)$

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

$\mathbb{Q}$

$$Gal\left(\frac{\mathbb{Q}(\mu_8)}{\mathbb{Q}}\right) = \begin{cases} \rho_1 = id \\ \rho_2 : (\sqrt{2}, i) \mapsto (\sqrt{2}, -i) \\ \rho_3 : (\sqrt{2}, i) \mapsto (-\sqrt{2}, i) \\ \rho_4 : (\sqrt{2}, i) \mapsto (-\sqrt{2}, -i) \end{cases}$$

IIS prop 28

$(\mathbb{Z}/(8))^\times \cong C_2 \times C_2 = \{1, 3, 5, 7 \bmod 8\}$

ρ_1 fixes all elements.
ρ_2 fixes $\mathbb{Q}(\sqrt{2})$
ρ_3 fixes $\mathbb{Q}(i)$
ρ_4 fixes $\mathbb{Q}(\sqrt{-2})$
} order 2

$$\begin{cases} \rho_2 : \zeta \mapsto \zeta^7 \\ \rho_3 : \zeta \mapsto \zeta^5 = -\zeta \\ \rho_4 : \zeta \mapsto \zeta^3 \end{cases}$$

End of proofs of Prop 31:

If $\tau(\sqrt[n]{a}) = \sqrt[n]{a}\,\zeta^i$ and $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\,\zeta^j$, then $\sigma\tau(\sqrt[n]{a})$
$= \sigma(\sqrt[n]{a}\,\zeta^i) \overset{\zeta^i \in k}{=} (\sqrt[n]{a}\,\zeta^j)\zeta^i = \sqrt[n]{a}\,\zeta^{i+j}$ i.e. it is a group hom.

1.7 Galois Correspondence (continued)

Example ($\zeta = \zeta_3$)

$\mathbb{Q}(\sqrt[3]{2}, \zeta)$ is Galois / $\mathbb{Q}$ as

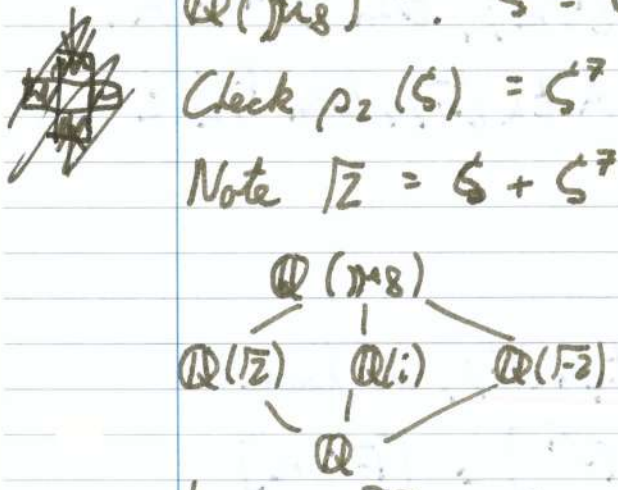
- $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2)$: splitting field of $X^3 - 2$, cor. 26
- Has all conjugates / $\mathbb{Q}$ of $\sqrt[3]{2}$ and ζ. Prop. 24 iv)

Example

$\mathbb{Q}(\mu_8)$. $\zeta = \zeta_8 = \frac{\sqrt{2}}{2}(1+i)$

Check $\rho_2(\zeta) = \zeta^7$, $\rho_3(\zeta) = \zeta^5$, $\rho_4(\zeta) = \zeta^3$

Note $\sqrt{2} = \zeta + \zeta^7$, $i = \zeta^2 = -\zeta \cdot \zeta^5$, $\sqrt{-2} = \zeta + \zeta^3$



Lemma 32

Let F/k be an extension and $G := \mathrm{Aut}_k(F)$

i) Let $k \subset L \subset F$. Then $\mathrm{Aut}_L(F)$ is a subgroup of G

$\mathrm{Aut}_L(F) = \{\sigma \in G \mid \sigma_L = id\} = \{\sigma \in G \mid \sigma(\alpha) = \alpha \ \forall \alpha \in L\} \leq G$

ii) Let H be a subgroup of G. The subset

$F^H := \{\alpha \in F \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$ of all elements in F fixed by all automorphisms of H is a subfield of F called the fixed field of H. We have $k \subset F^G \subset F^H \subset F$
and $H \subset \mathrm{Aut}_{F^H}(F)$

Proof

i) An L-automorphism $F \to F$ is always a k-hom.

ii) As every $\sigma \in G$ is a ring hom, if $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$, then $\sigma(\alpha+\beta) = \alpha+\beta$, $\sigma(\alpha\beta) = \alpha\beta$, $\sigma(\alpha^{-1}) = \alpha^{-1}$ for $\alpha \neq 0$

Hence F^H is a field.

As $\sigma|_k = id$ $\forall \sigma \in G$ we have $k \subset F^G$. As $\sigma|_{F^H} = id$ $\forall \sigma \in H$, we have: $H \subset Aut_{F^H}(H)$ □

Proposition 33

Let F/k be a finite extension inside $\mathbb{C}$.

i) If F/k is Galois and $G := Gal(F/k)$, then $F^G = k$.

ii) If $F^G = k$ for a subgroup $G \subset Aut_k(F)$, then F/k is Galois and $G = Aut_k(F)$

Proof

i) Note $k \subset F^G \subset F$. As $G \subset Aut_{F^G}(F)$, we have

$$|G| \leq |Aut_{F^G}(F)| \underset{\text{Lemma 22 iii)}}{\leq} [F : F^G] \leq [F : k]$$

But since F/k is Galois, $|G| = [F:k]$, all equalities hold and $F^G = k$.

ii) Let $F = k(\alpha)$ by the Primitive Element Theorem (20) and let P_α be the minimal polynomial of α over k.

Set $Q_\alpha := \prod_{\sigma \in G} (X - \sigma(\alpha)) \in F[X]$

It has α as a root and its coefficients are symmetric polynomials of $\{\sigma(\alpha) \mid \sigma \in G\}$, hence in $F^G = k$ (because the elements of G just permute the elements in $\{\sigma(\alpha) \mid \sigma \in G\}$)

Hence $P_\alpha \mid Q_\alpha$. Thus $[F:k] = \deg P_\alpha \leq \deg Q_\alpha = |G|$

$|G| \leq |\mathrm{Aut}_k(F)| \leq [F:k]$ (Lemma 22(iii))

Hence all are equalities, so F/k is Galois, and $G = \mathrm{Aut}_k(F)$ □

Theorem 34 (Fundamental Theorem of Galois Theory)

Let F/k be a Galois extension inside $\mathbb{C}$. Then the following maps (Galois Correspondence) defined by Lemma 32:

$$\left\{\begin{array}{l}\text{subfields } L \\ \text{with } k \subset L \subset F\end{array}\right\} \ni L \mapsto \mathrm{Aut}_L(F) \in \left\{\begin{array}{l}\text{subgroups } H \text{ of} \\ G := \mathrm{Gal}(F/k)\end{array}\right\}$$

$$\left\{\begin{array}{l}\text{subfields } L \\ \text{with } k \subset L \subset F\end{array}\right\} \ni F^H \hookleftarrow H \in \left\{\begin{array}{l}\text{subgroups } H \text{ of} \\ G := \mathrm{Gal}(F/k)\end{array}\right\}$$

are bijections, inverse to each other.

If $L \leftrightarrow H$, then $[F:L] = |H|$, $[L:k] = |G|/|H|$

Proof

Take L, and $F = k(\alpha)$ by the primitive element Theorem (20). Then $F = L(\alpha)$, and the conjugates of α over L are a subset of the conjugates of α over k (∵ the min poly of α/L divides the min poly of α/k), hence are also in F (F/k is Galois, Prop 24 iii)). Hence F/L is Galois (Prop 24 iv)). Now Prop 33 i) says $F^{\mathrm{Aut}_L(F)} = L$.

Take $H \subset \mathrm{Aut}_{F^H}(F)$ (Lemma 32) and Prop 33 ii) shows that $H = \mathrm{Aut}_{F^H}(F)$. If $H = \mathrm{Aut}_L(F)$, then $[F:L] = |H|$ as F/L is Galois, and hence $[L:k] = |G|/|H|$ by the Tower Law (Prop 8) □

Corollary 35

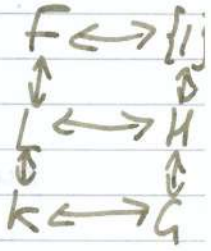
Let F/k be a Galois extension inside $\mathbb{C}$, with $G := Gal(F/k)$, $k \subset L \subset F$.

i) F/L is Galois and $H := Gal(F/L)$ is a subgroup of G.

ii) L/k is Galois $\Leftrightarrow H \triangleleft G$ (normal)

If this holds, then we have an isom. of groups.

$G/H \ni \sigma \bmod H \mapsto \sigma|_L \in Gal(L/k)$



Proof

i) Shown in the proof of Theorem 34

ii) If $\sigma \in G$, then $k \subset \sigma(L) \subset F$, and the subgroup corresponding to $\sigma(L)$ is $\sigma H \sigma^{-1}$, because for $\rho \in G$ we have $\rho|_L = id \Leftrightarrow \sigma\rho\sigma^{-1}|_{\sigma(L)} = id$.

Hence $H \triangleleft G \Leftrightarrow \sigma H \sigma^{-1} = H \ \forall \sigma \in G$.

$\Leftrightarrow \sigma(L) = L \ \forall \sigma \in G$ (*) by Theorem 34

Now, by the surjection (Lemma 19)

$G = Hom_k(F, \mathbb{C}) \ni \sigma \mapsto \sigma|_L \in Hom_k(L, \mathbb{C})$

(*) is equivalent to saying that ~~there~~ every $\tau \in Hom_k(L, \mathbb{C})$ maps L into L, i.e. L/k is Galois (Prop 24 ii))

(continued)

23/10/12

Galois Theory (9)

1.7 Galois Correspondence (continued)

Corollary 35

F/k Galois inside $\mathbb{C}$, $k \subset L \subset F$

L/k Galois $\Leftrightarrow H := Gal(F/L) \triangleleft G$

In this case, $G/H \ni \sigma \bmod H \mapsto \sigma|_L \in Gal(L/k)$

Proof of the last line

In this case, the surjection $G' = Hom_k(F, \mathbb{C})$

$G' \ni \rho \mapsto \rho|_L = Hom_k(L, \mathbb{C})$ is a group homomorphism

$G' \twoheadrightarrow Gal(L/k)$ with kernel $= \{\sigma \in G' \mid \sigma|_L = id\}$ □

Remark

Proposition 33 i) and ii) F/k : Galois $\Leftrightarrow F^{Aut_k(F)} = k$

Example

5^{th} roots of unity : $\zeta = \zeta_5 = \exp(\frac{2\pi i}{5})$, a root of

$X^5 - 1 = (X-1)(\underbrace{X^4 + X^3 + \ldots + 1})$ irreducible in $\mathbb{Q}[X]$

$\Rightarrow$ min poly of ζ over $\mathbb{Q}$ $\not\cong (\frac{\mathbb{Z}}{(5)})^\times \cong C_4$

Recall $\mathbb{Q}(\mu_5) = \mathbb{Q}(\zeta)$, $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{id, \sigma, \sigma^2, \sigma^3\}$

$id : \zeta \mapsto \zeta$, $\sigma : \zeta \mapsto \zeta^2$, $\sigma^2 : \zeta \mapsto \zeta^4$, $\sigma^3 : \zeta \mapsto \zeta^8 = \zeta^3$

It has a subgroup $H = \{id, \sigma^2\}$

$\sigma^2 : \zeta \leftrightarrow \zeta^4$. H fixes $\zeta + \zeta^4$ and

$\sigma(\zeta + \zeta^4) = \zeta^2 + \zeta^3$

$\zeta \mapsto \zeta^2$, σ ↑ ↓ σ, $\zeta^3 \leftarrow \zeta^4$

$L := F^H$ must be quadratic/$\mathbb{Q}$ $\Rightarrow \zeta + \zeta^4$, $\zeta^2 + \zeta^3$ must be roots of a quadratic over $\mathbb{Q}$

$F = \mathbb{Q}(\zeta) \leftrightarrow [:4]$ K_2
$\cup \quad L = ? \leftrightarrow H \quad \wedge_2$
$\cup \quad k = \mathbb{Q} \leftrightarrow \zeta_+$

$(\zeta + \zeta^4) + (\zeta^2 + \zeta^3) = -1$

$(\zeta + \zeta^4)(\zeta^2 + \zeta^3) = \zeta^3 + \zeta^4 + \zeta + \zeta^2 = -1$

$\Rightarrow$ Root of $X^2 + X - 1 \quad \therefore L = \mathbb{Q}\left(\frac{-1+\sqrt{5}}{2}\right) = \mathbb{Q}(\sqrt{5})$

ζ, ζ^4 roots of $X^2 - \left(\frac{-1+\sqrt{5}}{2}\right)X + 1 = 0$ $\quad = \zeta + \zeta^4$

$\therefore \zeta = \frac{(-1+\sqrt{5}) + \sqrt{-10-2\sqrt{5}}}{4}$ (use $\mathrm{Im}\,\zeta > 0$)

1.8 Insolvability of Quintics inside radical extensions

$F = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ — Example

tower $\mathbb{Z}/3\mathbb{Z}$ $\quad \zeta^3 = 1, \zeta \neq 1$, $F/\mathbb{Q}$ the splitting field of $P = X^3 - 2$

$L = \mathbb{Q}(\zeta)$ $\quad \mathrm{Gal}(F/L) = \{id, \sigma, \sigma^2\}$, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\zeta$, $\sigma|_L = id$

cyclo. $|\ C_2$ $\quad \mathrm{Gal}(L/k) = \{id, \tau\}$, $\tau(\zeta) = \zeta^2$

$k = \mathbb{Q}$ $\quad$ Extend τ to $\rho \in \mathrm{Gal}(F/k)$, say $\rho(\zeta) = \zeta^2$, $\rho(\sqrt[3]{2}) = \sqrt[3]{2}$
(3 choices for roots of $x_0 = X^3 - 2$, by Roots + Hom. II)

$\Rightarrow \rho^2 = id$, $\rho\sigma\rho^{-1}$: $\sqrt[3]{2} \xmapsto{\rho^{-1}} \sqrt[3]{2} \xmapsto{\sigma} \sqrt[3]{2}\,\zeta \xmapsto{\rho} \sqrt[3]{2}\,\zeta^2$

$\zeta \xmapsto{\rho^{-1}} \zeta^2 \xmapsto{\sigma} \zeta^2 \xmapsto{\rho} \zeta$

$\Rightarrow \rho\sigma\rho^{-1} = \sigma^2$

$\therefore \mathrm{Gal}(F/k) \cong D_6 \cong S_3$ (non-abelian)

Idea

Solving radicals (cyclo / Kummer) can only produce a tower of abelian extensions. $\rightarrow$ a limited class of Galois Extensions.

Definition 36

Let F/k be a finite extension inside $\mathbb{C}$. It has a finite set of ~~gen~~ generators (Proposition 10 ii), and the extension E/k generated by all conjugates (over k) of all these generators is finite and Galois (Proposition 24 i,ii).

As every Galois extension of k inside $\mathbb{C}$ containing F must contain E (by Proposition 24 iii)), it is the minimal Galois extension of k containing F. In particular, it is independent of the choice of generators. We call E/k the Galois Closure of F/k.

Example

i) $\mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2)$: Galois Closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

ii) $F = k(\alpha)$ (PET Theorem 20) then its Galois closure is E
$E = k(\alpha_1^{\alpha}, \alpha_2, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the conjugates of α over k (i.e. the splitting field of P_α).

Remark

By Galois Theory (Theorem 34), if $G := Gal(E/k)$, then $G' := Gal(E/F) \subset G$ is its subgroup. F/k corresponds to the pair (G, G')

$$\begin{array}{ccc} E & \longleftrightarrow & \{id\} \\ \downarrow & & \cap \\ F & \longleftrightarrow & G' \\ \downarrow & & \cap \\ k & \longleftrightarrow & G \end{array}$$

Definition

We say that a pair $(G; G')$ of a finite group G is soluble if there is a sequence of subgroups (G_i) :

$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = G'$ such that $G_{i-1} \rhd G_i$ (normal) and G_i/G_{i-1} is cyclic for $1 \leq i \leq n$.

We say G is soluble if $(G, \{id\})$ is. A Galois Extension is called soluble if its Galois group is.

Example

The Symmetric groups S_3, S_4 were soluble:

$S_3 \overset{2}{\triangleright} A_3 \overset{3}{\triangleright} \{id\}$, $S_4 \overset{2}{\triangleright} A_4 \overset{3}{\triangleright} V_4 \overset{2}{\triangleright} C_2 \overset{2}{\triangleright} \{id\}$

Lemma 38

i) Let G be a finite group. If $G \triangleright H \triangleright G'$ then (G, G') soluble $\Leftrightarrow$ G/H, (H, G') are both soluble.

ii) Finite Abelian groups are soluble

Proof:

i) Let $p : G \to G/H$ be the surjection $\sigma \mapsto \sigma H$.

($\Rightarrow$) If (G_i) is a sequence (G, G'), then $(p(G_i))$, $(H \cap G_i)$ give sequences for G/H, (H, G')

$$\begin{array}{ccccc} H \cap G_{i-1} & \hookrightarrow & G_{i-1} & \twoheadrightarrow & p(G_{i-1}) \\ \downarrow & & \downarrow & & \downarrow \\ H \cap G_i & \hookrightarrow & G_i & \twoheadrightarrow & p(G_i) \end{array}$$

cyclic $\leftarrow$ cyclic $\rightarrow$ cyclic

($\Leftarrow$) If (G_i), (H_i) are sequences for G/H, (H, G) then combine $(p^{-1}(G_i))$ and (H_i)

$$\begin{array}{ccccccccc} G/H = G_0 & \triangleright & G_1 & \triangleright & \cdots & \triangleright & G_n = \{id\} \\ p \uparrow & & \uparrow & & & & \uparrow \\ G = p^{-1}(G_0) & \triangleright & p^{-1}(G_1) & \triangleright & \cdots & \triangleright & p^{-1}(G_n) = H = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{id\} \end{array}$$

$p^{-1}(G_{i-1})/p^{-1}(G_i) \xrightarrow{\cong} G_i/G_{i-1}$, cyclic

ii) Induction on $|G|$: If $G \ni \sigma \neq id$ and $H = \langle \sigma \rangle$, then H is cyclic and $|G/H| < |G|$; so use i) ($\Leftarrow$) [or Structure Theorem] □

Example

S_n is not soluble for $n \geq 5$ ($\because S_n \triangleright A_n$, A_n is simple, non-abelian $n \geq 5$.

Use Lemma 3.8 i) ($\Rightarrow$). □

25/10/12

Galois Theory (10)

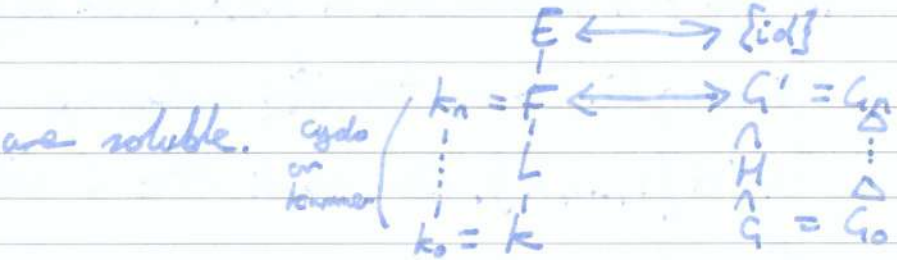
1.8 Insolvability of Quintics (continued)

Definition 39

We say that a Galois Extension L/k inside $\mathbb{C}$ is radical if there is a finite extension F of L such that F/k is a succession of cyclotomic and kummer extensions i.e. $k = k_0 \subset k_1 \subset \dots \subset k_n = F$ with k_i/k_{i-1} cyclotomic or kummer $(1 \leq i \leq n)$

Theorem 40

Radical extensions are soluble.



Proof

Let L/k be radical and take F/L as in the definition. Let E/k be the Galois closure of F/k and $G = Gal(E/k)$, $H = Gal(E/L)$ and $G' := Gal(E/F)$. As cyclotomic and kummer extensions are abelian. (G, G') is soluble by Galois Theory (Theorem 34) and Lemma 38i), 38ii). Then $H \trianglelefteq G$, so $G/H \cong Gal(L/k)$ soluble

1.9 Insolvability of Quintics II (general equations)

Definition 41

Let $k \subset \mathbb{C}$ and $P \in k[X]$. The Galois group $Gal(P)$ of P is defined as the Galois group $Gal(F/k)$ for the splitting field F/k of P over k.

Next: for a general equation P of degree n, we have $Gal(P) \cong S_n$.

Proposition 12

Let $k \subset \mathbb{C}$ and $P \in k[X]$.

i) Then $Gal(P)$ is a subgroup of the automorphism group $Aut(Root_P(\mathbb{C}))$ of the finite set $Root_P(\mathbb{C})$. In particular, a choice of an ordering of the roots $Root_P(\mathbb{C}) = \{\alpha_1, \dots, \alpha_n\}$ gives an injection $Gal(P) \hookrightarrow S_n := Aut(\{1, \dots, n\})$

ii) If P is irreducible in $k[X]$ with $\deg P = n$, then $Gal(P)$ is isomorphic to a transitive subgroup $G \subset S_n$ i.e. for every $i, j \in \{1, \dots, n\}$, there exists $\sigma \in G$ with $\sigma(i) = j$.

Remark

As a reordering in i) amounts to a conjugation in S_n, we can consider $Gal(P)$ as a subgroup of S_n, well-defined up to conjugation

Proof

i) Let F be the splitting field of P over k. An element $\sigma \in Gal(P) = Gal(F/k)$, being a k-hom, maps $Root_P(\mathbb{C})$ into itself. As σ is injective and $Root_P(\mathbb{C})$ is a finite set, $\sigma : Root_P(\mathbb{C}) \to Root_P(\mathbb{C})$ is a bijection (automorphism). As F/k is generated by $Root_P(\mathbb{C})$, the action of σ on $Root_P(\mathbb{C})$ determines σ.

ii) As P is irreducible, $\deg P = n$, then $|Root_P(\mathbb{C})| = n$ by Prop 15 i). If $Root_P(\mathbb{C}) = \{\alpha_1, \dots, \alpha_n\}$, then P is the min poly of α_i for all i. Hence for all i, j, there exists $\tau \in Hom_k(k(\alpha_i), \mathbb{C})$

with $\tau(\alpha_i) = \alpha_j$ by Prop 14 (Roots and Homs I). Extending τ to $\sigma \in \mathrm{Hom}_k(F, \mathbb{C}) = \mathrm{Gal}(F/k)$ by Lemma 19, we get $\sigma(\alpha_i) = \alpha_j$ □

Because F/k Galois, $\mathrm{Hom}_k(F, \mathbb{C}) = \mathrm{Hom}_k(F, F)$

Example

i) A cyclic subgroup of S_n is transitive, then it has order n.

ii) Transitive subgroups of S_3 are : $A_3 \cong C_3$, S_3

iii) For S_4, we have (up to conjugates) : C_4, V_4, D_8, A_4, S_4
(Here $V_4 = \{id, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$, klein-4-group)

iv) For S_5, up to conjugacy : C_5, D_{10}, F_{20}, A_5, S_5
(Here $F_{20} = \langle (12345), (1)(2453) \rangle$, the Frobenius group of order 20)

Definition 43

Let k be a field, $X_1, \dots, X_n$ indeterminates, and $k[X_1, \dots, X_n]$ be the ring of polynomials in $X_1, \dots, X_n$ with coefficients in k (an integral domain). Its field of fractions is denoted by $k(X_1, \dots, X_n)$, the field of rational functions in n variables over k

Proposition 44 ($n \geq 1$)

i) There exist $\alpha_1, \dots, \alpha_n$ transcendental over $\mathbb{Q}$, such that the field $F := \mathbb{Q}(\alpha_1, \dots, \alpha_n) \subset \mathbb{C}$ is isomorphic to $\mathbb{Q}(X_1, \dots, X_n)$ by $X_i \mapsto \alpha_i$ for $(1 \leq i \leq n)$.

ii) The symmetric group $G := S_n$ acts on F by permuting $\alpha_1, \dots, \alpha_n$ and F/F^G is Galois with Galois group G.

Proof:

i) Use induction on n. As $L := \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})$ is isomorphic to $\mathbb{Q}(X_1, \dots, X_{n-1})$ by the induction hypothesis, it is countable, hence only countably many elements in $\mathbb{C}$ are algebraic over L. So choose $\alpha_n \in \mathbb{C}$ which is transcendental $/L$. Then there is no non-zero polynomial $P(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]$ with $P(\alpha_1, \dots, \alpha_n) = 0$. Hence, the ring hom $f: \mathbb{Q}[X_1, \dots, X_n] \ni P \mapsto P(\alpha_1, \dots, \alpha_n) \in \mathbb{C}$ is injective, and extends to a ring hom $\hat{f}: \mathbb{Q}(X_1, \dots, X_n) \to \mathbb{C}$, $\hat{f}\left(\frac{P}{Q}\right) = \frac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n)}$ since $\mathbb{C}$ is a field. Then $F := \operatorname{Im} \hat{f}$ is isomorphic to $\mathbb{Q}(X_1, \dots, X_n)$ and it is the maximal field containing $\alpha_1, \dots, \alpha_n$ i.e. $F = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$

ii) G acts on $\mathbb{Q}(X_1, \dots, X_n)$ by permuting X_i, hence also on F i.e. $\sigma \in G$ acts as $\hat{f} \sigma \hat{f}^{-1}$ i.e. permuting α_i. Let $k = F^G$. Then $F = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ implies $F = k(\alpha_1, \dots, \alpha_n)$ and $G \subset \operatorname{Aut}_k(F)$ (Lemma 32 ii)). The coefficients of $P := \prod_{i=1}^{n} (X - \alpha_i) \in F[X]$ are the elementary symmetric polynomials in α_i, hence in k. Hence $\alpha_1, \dots, \alpha_n$ are the roots of $P \in k[X]$ i.e. algebraic $/k$. Thus F/k is finite (Proposition 10 i)) and Proposition 33 ii) shows that F/k is Galois and $G = \operatorname{Gal}(F/k)$ □

25/10/12

Galois Theory ⑩

Theorem 45 (Insolubility of Quintics)

For $n \geq 5$, there is no formula involving only radicals and rational functions, which expresses $\alpha_1, \ldots, \alpha_n$ in terms of their elementary symmetric polynomials.

Proof

The Galois extension F/F^{S_n} in Prop 44 is not soluble, hence is not radical by Theorem 40 $\square$

27/10/12

Galois Theory (11)

(end of proof of Theorem 40)

As cyclo/Kummer extensions are abelian, (G, G') is soluble by the Galois correspondence (Theorem 34, Corollary 35) and Lemma 38 ii), i) $\Leftarrow$.

Hence $G/H \cong \mathrm{Gal}(L/k)$ (Corollary 35) is soluble by Lemma 38 i) $\Rightarrow$.

1.10 Solving by Radicals

Next goal: Converse of Theorem 40 i.e. soluble extensions are radical.

Recall that soluble groups are built out of cyclic groups.

Definition 46

A Galois extension is called cyclic if its Galois group is.

Recall, $N \geq 1$, $\mu_N \subset k \subset \mathbb{C}$. Kummer extensions of k are $k(\sqrt[N]{a})/k$ for $a \in k$. The Galois groups inject to $\mathbb{Z}/N\mathbb{Z}$ (Prop 31), hence they are cyclic.

Example

$N \geq 2$. Since $\mu_2 = \{\pm 1\} \subset k$ for any $k \subset \mathbb{C}$. Every quadratic extension is Kummer (i.e. every fixed equation is solved by $\sqrt{\ }$)

Theorem 47 (Kummer Theory)

Let $N \geq 1$ and $\mu_N \subset k \subset \mathbb{C}$. Then every cyclic extension of k with degree N is a Kummer extension.

Proof

Let L/k be cyclic of degree N. Choose a generator σ of $\mathrm{Gal}(L/k) = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{N-1}\}$. Let $\zeta = \zeta_N \in \mu_N$

Suppose we found $\alpha \in L^\times (= L \setminus \{0\})$ with $\sigma(\alpha) = \alpha\zeta$

Then the conjugates of α over k are $\sigma^i(\alpha) = \alpha\zeta^i$ for $1 \le i \le N$ (Prop 14), and they are all distinct. Hence $[k(\alpha) : k] = N$ (Prop 7 ii)) therefore $k(\alpha) = L$. Let $a = \alpha^N$. Then $\sigma(a) = \sigma(\alpha^N) = \sigma(\alpha)^N = (\alpha\zeta)^N = a$, hence a is fixed by all σ^i, i.e. $a \in L^{\mathrm{Gal}(L/k)} = k$

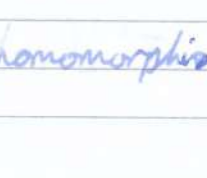
So, it suffices to prove that α exists. Consider σ as a k-linear transformation of L as a k-vector space. ζ is an eigenvalue of σ. Let $Q \in k[X]$ be the (linear algebraic) min. poly. of σ. Then $\Lambda = \mathrm{Root}_Q(k)$ is the set of all eigenvalues of σ. We want $\zeta \in \Lambda$. As $\sigma^N = \mathrm{id}$, we have $Q \mid X^N - 1$, hence $\Lambda \subset \mu_N$. Now Λ is a multiplicative subgroup of μ_N, because if $\lambda, \mu \in \Lambda$, and $\sigma(\alpha) = \lambda\alpha$, $\sigma(\beta) = \mu\beta$, some $\alpha, \beta \in L^\times$, then, as σ is a ring homomorphism $\sigma(\alpha\beta) = (\lambda\alpha)(\mu\beta) = \lambda\mu(\alpha\beta)$, $\sigma(\alpha^{-1}) = \lambda^{-1}\alpha^{-1}$ i.e. $\lambda\mu, \lambda^{-1} \in \Lambda$. Hence, $\Lambda = \mu_d$ for some $d \mid N$ i.e. $Q = X^d - 1$.

But σ has order N, so $\sigma^d \neq \mathrm{id}$ unless $d = N$.

$\therefore Q = X^N - 1$, $\Lambda = \mu_N$, $\zeta \in \Lambda$ □

Lemma 48

Let $k \subset L \subset F$ and $\alpha \in F$. If $k(\alpha)/k$ is Galois, then so is $L(\alpha)/L$ and $\mathrm{Gal}(L(\alpha)/L) \ni \sigma \mapsto \sigma|_{k(\alpha)} \in \mathrm{Gal}(k(\alpha)/k)$ is an injective group homomorphism.



Proof:

As the min. poly. of α over L divides that of α over k, all conjugates of α over L are in $k(\alpha) \subset L(\alpha)$. Hence $L(\alpha)/L$ is Galois (Prop 24 (iv)). The map is clearly a group hom, and injective since σ is determined by $\sigma(\alpha)$, hence by $\sigma|_{k(\alpha)}$ □

Remark:

The image corresponds to $k(\alpha) \cap L$ by Galois Theory i.e. $\mathrm{Gal}(L(\alpha)/L)$ is isomorphic to $\mathrm{Gal}(k(\alpha)/k(\alpha)\cap L)$

Theorem 49

Soluble extensions inside $\mathbb{C}$ are radical.

Proof:

Let L/k be Galois with $\mathrm{Gal}(L/k) = G_0 \rhd G_1 \rhd \dots \rhd G_n = \{id\}$ and G_i/G_{i-1} cyclic. Let $k_i = L^{G_i}$ be the corresponding subfields under Galois Theory (Theorem 34). So $k = k_0 \subset k_1 \subset \dots \subset k_n = L$ with k_i/k_{i-1} cyclic. $\mathrm{Gal}(k_i/k_{i-1}) \cong G_i/G_{i-1}$ (Corollary 35). Let $N_i = |G_i/G_{i-1}|$ for $1 \le i \le n$ and $N = N_1 N_2 \dots N_n$. Then we have a tower of fields $k \subset k(\mu_N) \subset k_1(\mu_N) \subset \dots \subset k_n(\mu_N) = L(\mu_N)$. Applying Lemma 48 to $k_i = k_{i-1}(\alpha)$ (PET Theorem 20), we see that $k_i(\mu_N) = k_{i-1}(\mu_N)(\alpha)$ is cyclic over $k_{i-1}(\mu_N)$ of degree dividing N_i (∵ its Galois group is isomorphic to a subgroup of G_{i-1}/G_i, hence dividing N_i. Thus $k_i(\mu_N)/k_{i-1}(\mu_N)$

is a Kummer extension by Kummer Theory (Theorem 47) □

1.11 Discriminants, and revisiting Intro 1

Any possible formula for solving equations by radicals? We need normal subgroups $Gal(P)$ to climb up the splitting field of P, but the only non-trivial normal subgroups of S_n are A_n and V_4.

Definition 50

Let $n \geq 1$. $k \subset \mathbb{C}$ and $P \in k[x]$, with $\deg P = |Root_P(\mathbb{C})| = n$

Let $i : Gal(P) \hookrightarrow S_n$ be the injection in Prop 42, defined up to conjugation in S_n. If $H \lhd S_n$ (normal) then we have a well defined normal subgroup $Gal(P) \cap H := i^{-1}(H)$ of $Gal(P)$.

First $H = A_n$.

Let P be as in definition 50. F/k is its splitting field and $Root_P(\mathbb{C}) = \{\alpha_1, \dots, \alpha_n\}$. $(F = k(\alpha_1, \dots, \alpha_n)^{Gal(P)})$

Let $\Delta_P := \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$, the discriminant

As the RHS is clearly fixed by $Gal(P)$, it's in k by prop 33 ii).

Note $\Delta_P \neq 0$ because we assumed $|Root_P(\mathbb{C})| = n$.

Example

$P = x^2 - ax + b = (x-\alpha)(x-\beta) \Rightarrow \Delta_P = (\alpha-\beta)^2 = a^2 - 4b$

$P = x^3 + bx - c = (x-\alpha)(x-\beta)(x-\gamma)$

$\Rightarrow \Delta_P = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2 = -4b^3 - 27c^2$

30/10/12

Galois Theory (12)

1.11 Discriminants, and revisiting Intro (1)

Let $k \subset \mathbb{C}$, $P \in k[x]$, $\deg P = |\mathrm{Root}_P(\mathbb{C})| = n \geq 1$.

Let F/k be the splitting field generated by $\mathrm{Root}_P(\mathbb{C}) = \{\alpha_1, \ldots, \alpha_n\}$

$\mathrm{Gal}(P) \leq S_n$

$\mathrm{Gal}(P)$ permutes the roots, so $i : \mathrm{Gal}(P) \hookrightarrow S_n$ (Prop 4.2) is well defined up to conjugation in S_n.

If $H \lhd S_n$, then $\mathrm{Gal}(P) \cap H = i^{-1}(H) \lhd \mathrm{Gal}(P)$, well defined.

$\Delta P := \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) \in F$ (discriminant of P) is non-zero, and in k since fixed by $\mathrm{Gal}(P)$ (Prop. 3.3 i)).

Proposition 5.1

For P as in definition 5.0, we have

$\mathrm{Gal}(P) \subset A_n \iff \Delta P$ is square in k (*)

and the subgroup $\mathrm{Gal}(P) \cap A_n$ corresponds to $k(\sqrt{\Delta P})$ by Galois Theory.

Proof

Take one of the square roots of ΔP (depending on the ordering of the roots). $\sqrt{\Delta P} := \prod_{i<j} (\alpha_i - \alpha_j)$ and consider the action of $\sigma \in \mathrm{Gal}(P) \hookrightarrow S_n$ on it. As a transposition $(i\ j)$ changes the signs of $\alpha_i - \alpha_j$, $\alpha_i - \alpha_m$, $\alpha_m - \alpha_j$, for $i < m < j$, it sends $\sqrt{\Delta P}$ to $-\sqrt{\Delta P}$. Hence we have

$\sigma \in \mathrm{Gal}(P) \cap A_n \iff \sigma(\sqrt{\Delta P}) = \sqrt{\Delta P}$ (☆)

Now, we prove (*): ($\Leftarrow$) If $\sqrt{\Delta P} \in k$, then every $\sigma \in \mathrm{Gal}(P)$ is in $\mathrm{Gal}(P) \cap A_n$ by (☆).

($\Rightarrow$) As (*) says that $\sqrt{\Delta_P}$ is fixed by all $\sigma \in Gal(P) = Gal(F$ it is in k by Prop. 33 i).

The latter claim is clear if either side of (*) is true. If not, then $Gal(P) \cap A_n$ has index 2 in $Gal(P)$, and its fixed field L satisfies $[L:k] = 2$ by Theorem 34 (FTGT). Now (*) says $k(\sqrt{\Delta_P}) \subset L$, and (*) says that $[k(\sqrt{\Delta_P}) : k] = 2$.

Hence $k(\sqrt{\Delta_P}) = L$ (Tower Law, Proposition 8). $\square$

Example

Let $P = X^3 + bX - c \in k[X]$ be irreducible, with $Root_P(\mathbb{L})$ equal to $\{\alpha, \beta, \gamma\}$ (distinct). Then, $Gal(P)$ is A_3 or S_3 (Prop 42 ii)) and Prop 51 tells you which e.g. $k = \mathbb{Q}$.

$P = X^3 - 3X + 1 \quad : \quad \Delta_P = 81 \Rightarrow Gal(P) \cong A_3$

$P = X^3 + 2X + 2 \quad : \quad \Delta_P = -140 \Rightarrow Gal(P) \cong S_3$

Now we revisit Lecture 1. To make the Kummer Theory work for cyclic cubic extensions, we assume $\zeta = \zeta_3 \in k$. For a cubic with distinct roots, $P = X^3 + bX - c = (X-\alpha)(X-\beta)(X-\gamma)$

The Lagrange Resolvents are $x = \alpha + \beta\zeta + \gamma\zeta^2$, $y = \alpha + \beta\zeta^2 + \gamma\zeta$.

The elements x^3, y^3, were the roots of $X^2 - 27cX - 27b^3$.

Let $L := k(x^3) = k(y^3)$.

$$\begin{array}{ccc} k(\alpha,\beta,\gamma) = F & = & k(x) \longleftrightarrow \{id\} \\ | \leq 3 & & \wedge \\ L = k(x^3) & \longleftrightarrow & Gal(P) \cap A_3 \\ | \leq 2 & & \wedge \\ k & \longleftrightarrow & Gal(P) \end{array}$$

30/10/12

Galois Theory (12)

Solving the quadratic shows that $L = k(\sqrt{-27\Delta P})$, but

$-27 = (3\sqrt{-3})^2 = (3(2\zeta+1))^2$ is a square in k, hence

$L = k(\sqrt{\Delta P})$.

For a quartic with distinct roots, $P = x^4 + bx^2 + cx + d$,

$P = (x-\alpha)(x-\beta)(x-\gamma)(x-\delta)$

We had: $x := \alpha+\beta = -(\gamma+\delta)$, $y := \alpha+\gamma = -(\beta+\gamma)$, $z := \alpha+\delta = -(\beta+\gamma)$

$xyz = c$, x^2, y^2, z^2 are roots of $X^3 + 2bX^2 + (b^2-4d)X - c^2$

$k(\alpha,\beta,\gamma,\delta) = F = k(x,y,z) \longleftrightarrow \{id\}$

$G_4 = C_2 \times C_2$ $\quad$ ≤ 4 $\quad$ $L = k(x^2, y^2, z^2)$ $\quad$ $\mathrm{Gal}(P) \cap V_4$

biquadratic $\quad$ ≤ 3 $\quad$ $k(\sqrt{\Delta P})$ $\quad$ $\mathrm{Gal}(P) \cap A_4$

≤ 2 $\quad$ k $\longleftrightarrow$ $\mathrm{Gal}(P)$

For $G_1 := \mathrm{Gal}(P)$, $G_1 \triangleright G_1 \cap A_4 \triangleright G_1 \cap V_4 \triangleright \{id\}$

From the solubility of S_4, $S_4 \triangleright A_4 \triangleright V_4 \triangleright C_2 \triangleright \{id\}$

$S_4/V_4 \cong S_3$, $V_4 = C_2 \times C_2$. S_3 permutes x^2, y^2, z^2.

Exercise

Every cyclotomic extension is contained in a tower of Kummer extensions (use induction on N for $k(\mu_1, \mu_2, \ldots, \mu_N)$). So cyclotomic extensions are not needed in the definition of radical extension.

Solving equations is related to ruler and compass constructions. In terms of Cartesian coordinates, $(x,y) \in \mathbb{R}^2$ or $x+iy \in \mathbb{I}$, it can only do $+, -, \times, \div$, and solve quadratic equations

(e.g. intersections with circles), so all coordinates of the constructed points lie in successive quadratic extensions of the field generated over $\mathbb{Q}$ by the coordinates of given points.

Example

i) Cannot trisect a given angle, $\cos\alpha$ generates a cubic extension $\mathbb{Q}(\cos 3\alpha)$. Successive quadratic extensions have degree 2^n, hence cannot contain a cubic extension by the Tower Law (Prop 8). Similarly, we cannot double a given cube. $x^3 - 2$.

ii) Construction of regular n-gons. Essential cases are when $n = p$, prime. We need to solve $\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Q}[x]$, which is irreducible (set $x = y + 1$, use Eisenstein's Criterion 9, we prove more general results later). The only known such primes are $2, 3, 5, 17, 65537$ (of the form $2^{2^n} + 1$, Fermat primes, as $2^b + 1 \mid 2^{ab} + 1$ if a is odd). We will see that these cases are constructible (Gauss).

HANDOUT 1: WHY GENERAL FIELDS, AND HOW?

Most of the essential features of Galois Theory were covered in §1.

Motivations.

(A) *Eliminate analysis.* We used the "fundamental theorem of algebra", hence relied on real analysis. But the whole business seems to have little to do with $\mathbb{R}, \mathbb{C}$ (Birth of abstract algebra — early 20c).

(B) *Number theory.* There are *finite* fields, e.g. $\mathbb{F}_p := \mathbb{Z}/(p)$ for primes p. Any Galois Theory for these? (Yes; moreover, they have applications to Galois groups over $\mathbb{Q}$, as we will see. Also used in coding theory, etc.)

(C) *Algebraic geometry.* Discussions of "general equations" suggests that we'd like to do Galois Theory for $K(X_1, \ldots, X_n)$ (*function fields*); when $K = \mathbb{Q}$ they were isomorphic to subfields of $\mathbb{C}$, but will no longer be so for $K = \mathbb{C}$. Fields like $\mathbb{C}(X)$ occur as fields of *meromorphic functions on compact Riemann surfaces*, and Galois Theory translates itself into geometry (and $\mathbb{C}(X_1, \ldots, X_n)$ for n-dimensional manifolds [varieties]); for $K = \mathbb{F}_p$, it points to algebraic geometry over $\mathbb{F}_p$.

Problems.

Let K be an arbitrary field. All of §1 will work for extensions of K, if we have a sufficiently large field $\overline{K}/K$ (an *algebraic closure* of K, analogue of the field of all algebraic numbers $\overline{\mathbb{Q}} \subset \mathbb{C}$ for $K = \mathbb{Q}$), which plays the role of $\mathbb{C}$. But:

(A) *Set theoretic difficulty.* When K is uncountable, the construction of $\overline{K}$ requires the *axiom of choice* (in fact for any K if we want to prove its uniqueness). But Galois Theory deals mainly with *finite* extensions, so this must be unnecessary.

(B) *Generality.* We want to treat fields like

$$K_P := K[X]/(P), \quad \text{for } P \in K[X] : \text{irreducible},$$

as extensions of K, i.e. we don't want to restrict ourselves to subfields of (a particular) $\overline{K}$.

(C) *Separability.* In characteristic $p > 0$, irreducible polynomials can have multiple roots (i.e. Prop. 15(i) is false)! This happens when taking p-th power roots, e.g. $K = \mathbb{F}_p(T)$ where T is an indeterminate and $P(X) := X^p - T = \left(X - \sqrt[p]{T}\right)^p$, irreducible in $K[X]$.

Review of §1. Boldface items were for subfields of $\mathbb{C}$.

Def. 1: Subfields, extensions. Def. 2: Finite/infinite extensions, Degrees.

Def. 3: Algebraic/transcendental (elements/extensions).

Prop. 4: Finite ext'ns are algebraic. Def. 5: Minimal polynomials.

Def. 6: Simple ext'ns. Prop. 7: Min. poly. are irreducible, degree of simple ext'ns.

Prop. 8: Tower Law. Def. 9: Ext'ns generated by finitely many generators.

Prop. 10: Finite $\iff$ generated by finitely many algebraic generators.

Lem. 11: Field hom's are injective.

Def. 12: K-hom's, $\mathrm{Hom}_K(L, L')$. Def. 13: $\mathrm{Root}_P(L)$, conjugates.

Prop. 14: Roots and Hom's I (simple ext'ns).

Prop. 15: Separability of irred. poly., $|\mathrm{Hom}_K(K(\alpha), \mathbb{C})| = [K(\alpha) : K]$. Def. 16: τP.

Prop. 17: Roots and Hom's II (extending K-hom's to simple ext'ns).

Th. 18: Separability $|\mathrm{Hom}_K(F, \mathbb{C})| = [F : K]$. **Lem. 19**: $\mathrm{Hom}_K(F, \mathbb{C}) \twoheadrightarrow \mathrm{Hom}_K(L, \mathbb{C})$.

Th. 20: Primitive Element Theorem. Def. 21: K-isomorphisms, K-automorphisms.

Lem. 22: $\mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$ for finite L/K.

Lem. 22(iii): $|\mathrm{Aut}_K(L)| \leq [L : K]$. Def. 23: Galois ext'ns, Galois groups.

Prop. 24: Characterisation of Galois ext'ns (has all conjugates).

Def. 25: Splitting fields. **Cor. 26**: Splitting fields are Galois.

Def. 27: $\boldsymbol{\mu}_N$, primitive roots of unity, cyclotomic ext'ns.

Prop. 28: $\mathrm{Gal}\big(K(\boldsymbol{\mu}_N)/K\big) \hookrightarrow \big(\mathbb{Z}/(N)\big)^\times$. **Cor. 29**: Cyclotomic ext'ns are abelian.

Def. 30: Kummer ext'ns. **Prop. 31**: $\mathrm{Gal}\big(K(\sqrt[N]{a})/K\big) \hookrightarrow \mathbb{Z}/N\mathbb{Z}$.

Lem. 32: Subfields $\leftrightarrow$ subgroups, fixed fields.

Prop. 33: F/K : Galois $\iff$ $F^{\mathrm{Aut}_K(F)} = K$.

Th. 34: Fundamental Theorem of Galois Theory.

Cor. 35: Galois subextensions $\leftrightarrow$ normal subgroups. **Def. 36**: Galois closures.

Def. 37: Soluble groups & ext'ns. Lem. 38: Solubility & sub/quotients, abelian groups.

Def. 39: Radical ext'ns. **Th. 40**: Radical ext'ns are soluble.

Def. 41: Galois groups of polynomials.

Prop. 42: $\mathrm{Gal}(P)$ for irreducible P is a transitive subgroup of S_n.

Def. 43: Fields of rational functions. **Prop. 44**: Galois ext'ns with Galois group S_n.

Th. 45: Insolvability of Quintics. Def. 46: Cyclic ext'ns. **Th. 47**: Kummer Theory.

Lem 48: Galois groups of $K(\alpha)/K$ and $L(\alpha)/L$.

Th. 49: Soluble ext'ns inside $\mathbb{C}$ are radical.

Def. 50: $\mathrm{Gal}(P) \cap H$ for $H \lhd S_n$. discriminants.

Prop. 51: $\mathrm{Gal}(P) \subset A_n \iff$ discriminant is a square.

t.yoshida@dpmms.cam.ac.uk

2. General Fields and Applications

2.1 General Remarks

Definition 52

Let k be a field. The kernel of a unique ring homomorphism $f: \mathbb{Z} \ni n \mapsto \underbrace{1+\dots+1}_{n \text{ times}} \in k$, from $\mathbb{Z}$, is a prime ideal in $\mathbb{Z}$. Hence $\ker f = (p)$ with $p = 0$ or a prime number p, the characteristic, denoted by $\operatorname{char} k$. If $\operatorname{char} k = 0$, then f is injective and extends to $\mathbb{Q} \hookrightarrow k$, hence its image is a subfield isomorphic to $\mathbb{Q}$ (unique isomorphism). If $\operatorname{char} k = p > 0$ then $\operatorname{Im} f \cong \mathbb{Z}/(p) = \mathbb{F}_p$ is a subfield isomorphic to $\mathbb{F}_p$ (again a unique isomorphism). In both cases $\operatorname{Im} f$ is the smallest subfield (prime field) of k.

Remark

When we have a fixed ring homomorphism $\tau: k \to L$ of fields (hence injective by Lemma 11) we may want to identify the isomorphic fields k and $\tau(k)$, and consider L as an extension of k. We do this when τ is unique and canonical i.e. uniquely fixed by context.

i) (unique) Every field can be considered as an extension of $\mathbb{Q}$ or $\mathbb{F}_p$ in a unique way, as its prime field is uniquely isomorphic to $\mathbb{Q}$ or $\mathbb{F}_p$.

ii) (Canonical) If $P \in k[X]$ is an irreducible polynomial, then (P) is a maximal ideal of $k[X]$, and $k_P := k[X]/(P)$ is a field.

The canonical injection $k \hookrightarrow k[X]$ gives a ring homomorphism $k \hookrightarrow k[X] \twoheadrightarrow k[X]/(P)$. Hence $k \hookrightarrow k_P$ (lemma 11, or observe that non-zero constants are not in (P)). We consider $k \subset k_P$, and call k_P the extension obtained by adjoining a root of P (the root $\bar{X} := X \bmod (P) \in k_P$ is an "abstract root" of P, which generates k_P/k.

Example

$X^2 + 1 \in \mathbb{F}_3[X]$ is irreducible ($\because 0^2 = 0, 1^2 = 1, 2^2 = 1 \neq -1$ in $\mathbb{F}_3$)

$\Rightarrow \mathbb{F}_3[X]/(X^2+1) = \{0, 1, 2, X, X+1, X+2, 2X, 2X+1, 2X+2\}$ mod (X^2+1)

This is a quadratic extension of $\mathbb{F}_3$ (a field of 9 elements isomorphic to $\mathbb{Z}[i]/(3)$).

iii) (non-example) $k = \mathbb{Q}(\sqrt[3]{2})$ has three $\mathbb{Q}$-homomorphisms $\tau_1, \tau_2, \tau_3 : k \hookrightarrow \mathbb{C}$. Apart from $\tau_1 = id$, we would rather not identify k with $\tau_2(k)$ or $\tau_3(k)$. These are different subsets of $\mathbb{C}$, though isomorphic as fields.

"k isomorphic" – "look the same" from the k point of view

2.2 Splitting Fields and Algebraic Closures

The only tool from GRM:

Lemma 53

For any field k, the ring $k[X]$ is a Euclidean Domain.

7/11/12

Galois Theory (13)

Hence:

i) $\alpha \in Root_p(k) \Leftrightarrow (X-\alpha) \mid P$ (use $P = (X-\alpha)Q + \beta$)

ii) $k[x]$ is a PID, hence a UFD. In particular $|Root_p(k)| \leq \deg f$

Definition 54

For $P \in k[x] \setminus k$ (i.e. non-constant) and an extension E/k, we say P splits in E if P is a product of linear factors in $E[x]$. If moreover E is generated by $Root_p(E)$ then we say that E is a splitting field of P over k.

Lemma 55

Let E/k be a splitting field of P over k. Then for an extension E'/k we have P splits in $E' \Leftrightarrow Hom_k(E, E') \neq \emptyset$

The number $|Root_p(E')|$ is constant in any E' in which P splits.

Proof

($\Rightarrow$) For a root α_1 of P, its min. poly. P_1 over k divides P, hence splits in E'. Choose $\beta \in Root_{P_1}(E')$ and let $\tau \in Hom_k(k(\alpha_1), E')$ be the k-homomorphism with $\tau(\alpha_1) = \beta$. (proposition 14). Now factor $P = (X-\alpha_1)Q$ in $k(\alpha_1)[x]$ and choose a root α_2 of Q. Its min. poly. P_2 over $k(\alpha_1)$ divides Q, hence P. As $P_2 \mid P$ we know $\tau P_2 \mid \tau P = P$, hence τP_2 splits in E'. So choosing $\beta_2 \in Root_{\tau P_2}(E')$, we get $\rho \in Hom_k(k(\alpha_1, \alpha_2), E')$ with $\rho(\alpha_i) = \beta_i$, $i = 1, 2$, by Proposition 17.

Repeating, we arrive at an element in $Hom_k(E, E')$

because $E = k(\alpha_1, \dots, \alpha_n)$ if $\mathrm{Root}_p(E) = \{\alpha_1, \dots, \alpha_n\}$

($\Leftarrow$): If $\tau \in \mathrm{Hom}_k(E, E')$ and $P(X) = \hat{\prod_{i=1}} (X - \alpha_i)^{m_i}$ in $E[X]$, then $P(X) = \tau P(X) = \hat{\prod_{i=1}} (X - \tau(\alpha_i))^{m_i}$ in $E'[X]$, as $\tau|_k = id$. This also shows that $|\mathrm{Root}_p(E')| = n = |\mathrm{Root}_p(E)|$ by the unique factorisation in $E'[X]$.

Remark

As $|\mathrm{Root}_p(E)|$ is finite (Lemma 53), a splitting field is finite/k (Prop 10 i)). If P splits in E, then it contains a unique splitting field i.e. its subfield generated by $\mathrm{Root}_p(E)$ over k.

Prop 56

For every $P \in k[X] \setminus k$, its splitting field exists, and is unique (over k) up to k-isomorphism (i.e. there exists (possibly many) k-isomorphisms between any two of them).

Proof

(Existence) Adjoin a root of an irreducible factor of P to get L/k with a root α_1 of P in L, so that $L = k(\alpha_1)$ and $P = (X - \alpha_1)G$ in $L[X]$. Then adjoin a root of an irreducible factor of G, and repeat. Each step is a simple extension generated by a root of P, hence after $\deg P$ steps we get a finite extension L/k, in which P splits, and generated by $\mathrm{Root}_p(E)$.

(Uniqueness)

If E, E' are both splitting fields of P over k, then by Lemma 55 we have $\mathrm{Hom}_k(E, E') \neq \emptyset$, hence $[E:k] = [E':k]$ by Lemma 22 i) and any element in $\mathrm{Hom}_k(E, E')$ is an isomorphism by Lemma 22 ii) $\square$

inequalities in both directions

HANDOUT 2: ZORN'S LEMMA AND ALGEBRAIC CLOSURES (NON-EXAMINABLE)

In order to prove the existence of the algebraic closure of an arbitrary field, it is necessary to use an axiom of set theory known as *Zorn's lemma*. It is equivalent to the Axiom of Choice (see e.g. Halmos's *Naive Set Theory*), which roughly says that we are allowed to make infinitely many choices at once. Some believe that one should avoid the Axiom of Choice wherever possible, as it is less intuitive than the other axioms of set theory. However a lot of algebra (not to say analysis) would be very awkward without it. If one is really concerned about its validity, it is worth pointing out that one can often avoid using Zorn's Lemma, at the expense of some notational complexity (for example, instead of the algebraic closure of a field one can often make do with the splitting field of a sufficiently large finite set of polynomials).

Definition. Let S be a set. A relation $\leqslant$ on S is said to be a *partial order* if it satisfies:

(i) For all $x \in S$, $x \leqslant x$;
(ii) For all $x, y, z \in S$, if $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$;
(iii) For all $x, y \in S$, if $x \leqslant y$ and $y \leqslant x$ then $x = y$.

S is said to be *totally ordered* by $\leqslant$ if moreover:

(iv) For all $x, y \in S$, either $x \leqslant y$ or $y \leqslant x$.

A *chain* is a partially ordered set $(S, \leqslant)$ is a subset $T \subset S$ which is totally ordered by $\leqslant$. If $T \subset S$ is a chain then so is any subset of T.

Example. (i) $\mathbb{N}$ and $\mathbb{R}$ are totally ordered sets (with the usual order relation).
(ii) Let $S = \{x \in \mathbb{Z} \mid x > 1\}$ ordered by reverse divisibility:

$$x \preccurlyeq y \quad \Longleftrightarrow \quad x/y \in \mathbb{Z}.$$

Then $(S, \preccurlyeq)$ is a partially ordered set. Let $m > 1$ and $T = \{m^i \mid i > 1\}$. Then T is a chain in S. So is the subset $\{n! \mid n > 1\}$.
(iii) Let X be any set, S the set of all subsets of X with inclusion as the order relation. Then S is a partially ordered set.

Definition. Let $(S, \leqslant)$ be a partially ordered set, and T any subset of S. An *upper bound* for T is an element $z \in S$ such that $x \leqslant z$ for all $x \in T$. (We don't require that $z \in T$.) An element $y \in S$ is said to be *maximal* if for any $x \in S$, $y \leqslant x$ iff $x = y$.

If S is totally ordered, then it can have at most one maximal element (easy). A general partially ordered set can have many maximal elements. In the above examples:

Example. (i) In $\mathbb{R}$ an upper bound for a subset is an upper bound in the usual sense. There are no maximal elements.
(ii) In $S = \{x \in \mathbb{Z} \mid x > 1\}$ an element $x \in S$ is maximal iff it is prime. Every chain has an upper upper bound (take the element which is smallest for the usual ordering on $\mathbb{N}$).

Zorn's Lemma. *Let S be a nonempty partially ordered set. Assume that every chain in S has an upper bound. Then S has a maximal element.*

Zorn's lemma is equivalent to two other axioms of Set Theory:

The Axiom of Choice. *Let X_i $(i \in I)$ be a collection of sets, indexed by a set I. If each X_i is nonempty then so is the Cartesian product* $\prod_{i \in I} X_i$.

The Well-Ordering Theorem. *Every set can be well-ordered, i.e. we can define a total order on it so that every non-empty subset contains a minimal element.*

For example, using Zorn's lemma one can prove that *every vector space has a basis*, by looking at the set of all linearly independent subsets, ordered by inclusion.

Theorem. (i) *For any ring R and an ideal $I \neq R$, there exists a maximal ideal which contains R. In particular (taking $I = 0$), any non-zero ring has a maximal ideal.*

(ii) *(Th. 58) For any field K, its algebraic closure $\overline{K}$ exists and is unique up to K-isomorphism. Any algebraic extension of K is K-isomorphic to a subextension of $\overline{K}/K$.*

Proof. (i): Let S be the set of all proper ideals (i.e. $\neq R$) containing I, ordered by inclusion. It is nonempty since $I \in S$. Let $T \subset S$ be a chain. Define $J := \bigcup_{I \in T} I$. We claim J is an upper bound for T. What is not obvious is that $J \in S$. As J is a union of ideals containing I, it is clearly an ideal containing I. Moreover it is a proper ideal, for if not then $1 \in J$ which is true iff $1 \in I$ for some $I \in T$, which is impossible as I is a proper ideal. Therefore $J \in S$ and so J is an upper bound for T. By Zorn's Lemma, S has a maximal element.

(ii): Consider the set Λ of all pairs $\lambda = (P, i)$ where $P \in K[X]$ is an irreducible monic and $1 \leq i \leq \deg P$. Consider a variable $X_\lambda = X_{P,i}$ for each $\lambda \in \Lambda$, and the polynomial ring $A := K[X_\lambda \mid \lambda \in \Lambda]$ in all these variables (but note that each of its elements (polynomials) involves only finitely many variables). For each irred. monic $P \in K[X]$, consider the polynomial $P'(X) := P(X) - \prod_{i=1}^{\deg P} (X - X_{P,i}) \in A[X]$, and let $x_{P,i} \in A$ be the coeff. of X^i in $P'(X)$ for $0 \leq i < \deg P$. Let I be the ideal of A generated by all $x_{P,i} \in A$ for all P.

We first show $I \neq A$. Assume $I = A$, i.e. $1 \in I$. Then:

$$\exists a_1, \ldots, a_n \in A, \ \sum_{j=1}^{n} a_j x_{P_j, i_j} = 1 \in A.$$

Let F be a splitting field of $P_1 \cdots P_n$ (Prop. 56). Then each P_j splits as $P_j(X) = \prod_{i=1}^{\deg P_j} (X - \alpha_{ji})$ in $F[X]$, with $\alpha_{ji} \in F$. Consider the "substitution" map $f : A \to F$ defined by $f(X_{P_j,i}) = \alpha_{ji}$ for $1 \leq j \leq n$ and $1 \leq i \leq \deg P_j$, and $f(X_\lambda) = 0$ for all the other X_λ. Then under this ring hom. f, the poly. $P_j'(X) \in A[X]$ is sent to $P_j(X) - \prod_i (X - \alpha_{ji}) = 0 \in F[X]$, thus we see that $f(x_{P_j,i}) = 0 \in F$ for all $1 \leq i \leq \deg P_j$. Therefore $1 = f(1) = f\left(\sum_j a_j x_{P_j,i_j}\right) = 0$ in F, a contradiction.

Hence take a maximal ideal Q of A containing I by (i), and consider the field $\overline{K} := A/Q$, which is an extension field of K. Let $\alpha_\lambda := X_\lambda \bmod Q \in \overline{K}$. Then every irred. monic $P \in K[X]$ splits as $P(X) = \prod_i (X - \alpha_{P,i})$ in $\overline{K}[X]$. In particular α_λ is alg. $/K$, and $\overline{K}/K$ is algebraic, as every el't of $\overline{K}$ is a poly. in α_λ. If $L/\overline{K}$ is alg., for every $x \in L$ its min. poly. lies in $K(\alpha_{\lambda_1}, \ldots, \alpha_{\lambda_m})$ for some $\lambda_1, \ldots, \lambda_m$, thus x is alg. over K. As the min. poly. of x over K splits in $\overline{K}$, we have $x \in \overline{K}$. Hence $L = \overline{K}$. Therefore $\overline{K}$ is alg. closed.

Now let F/K be alg., and let S be the set of all pairs (L, τ) where L is a subext'n of F/K and $\tau \in \mathrm{Hom}_K(L, \overline{K})$. It is an ordered set if we define $(L_1, \tau_1) \leq (L_2, \tau_2) \iff L_1 \subset L_2,\ \tau_2|_{L_1} = \tau_1$. For any totally ordered subset T of S, the el't (L_T, τ_T), defined by $L_T := \bigcup_{(L,\tau) \in T} L$ and $\tau_T|_L = \tau$ for $(L, \tau) \in T$, is an upper bound of T. Thus we can take a maximal el't (M, ρ) of S by Zorn's Lemma. For all $x \in F$, we have $\mathrm{Hom}_M(M(x), \overline{K}) \neq \emptyset$ by Prop. 14, as $\overline{K}$ is alg. closed and the min. poly. of x over M splits in $\overline{K}$, therefore the maximality of (M, ρ) implies $M(x) = M$. Thus $M = F$, and F is K-isomorphic to $\rho(F) \subset \overline{K}$ by ρ. If F is an alg. closure of K, then so is $\rho(F)$, and as $\overline{K}$ is alg. over $\rho(F)$ we have $\rho(F) = \overline{K}$, i.e. ρ is a K-isomorphism. $\square$

t.yoshida@dpmms.cam.ac.uk

2.2 Splitting Fields and Algebraic Closures

Clarification: The definition of extension has not been changed.

Remark after Definition 52: We do this when τ is unique and canonical.

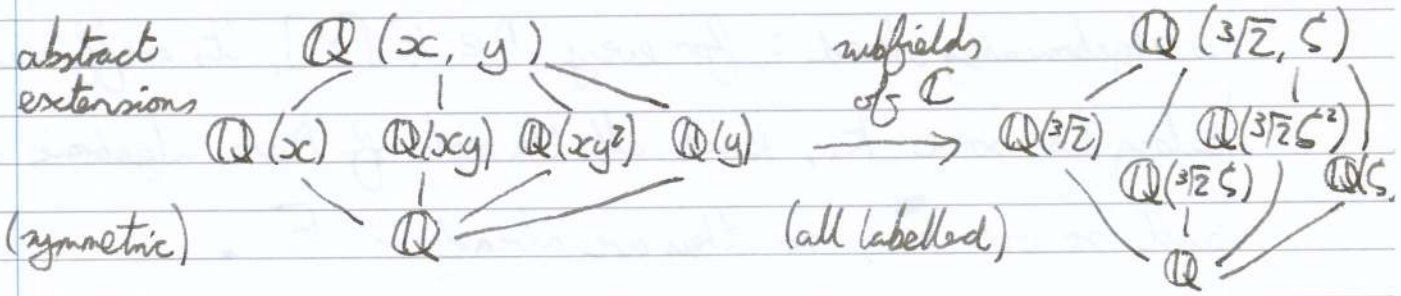
$\Rightarrow$ We do this only in the following two cases i), ii)

Beginning of proof of Proposition 56 (Existence). Let L/k be the extension obtained by adjoining a root of an irreducible factor of P, as in Remark ii) after Definition 52. Then $L = \underset{k[x]/(P)}{k(\alpha_1)} = \underset{x \bmod P_1}{k(\alpha_1)}$ with $\alpha = \mathrm{Root}_P(L)$, and $P = (X - \alpha_1)Q$ in $L[X]$.

$P_1 | P$, $k \hookrightarrow k[x] \twoheadrightarrow k[x]/(P)$

Example

$\mathbb{Q}(x,y) = \mathbb{Q}[X,Y]/(X^3-2, Y^2+Y+1)$, $x := \bar{X}$, $y := \bar{Y}$, $\zeta := \zeta_3$



$\exists$ 6 $\mathbb{Q}$-homomorphisms $\mathbb{Q}(x,y) \to \mathbb{C}$

$x \mapsto$ any of $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$, $y \mapsto$ any of ζ, ζ^2

Definition 57

A field F is called algebraically closed if every $P \in k[X] \setminus F$ splits in F itself. An algebraic extension F/k is called an algebraic closure of k if F is algebraically closed.

Theorem 58

For every field k, its algebraic closure $\bar{k}$ exists, and is unique up to k-isomorphism. Any algebraic extension of k is k-isomorphic to a subextension of $\bar{k}/k$.

(Almost) Proof

(Existence) Suppose that $\{P_1, P_2, \dots\}$ is the set of all irreducible monics in $k[X]$. Let k_1 be a splitting field of P_1 over k.

(A) Then let k_2 be a splitting field of P_2 over k_1, and so on. Then we obtain a sequence $k = k_0 \subset k_1 \subset \dots$, and let $\bar{k} : \bigcup_{i=0}^{\infty} k_i$. Then it is algebraic over k (since each step is a finite extension), and all irreducibles over $k[X]$ split. Then $\bar{k}$ is algebraically closed: for every $P \in \bar{k}[X]$, its coefficients belong to some k_i, hence all the roots of P are algebraic over k_i, and so over k, so they are already in $\bar{k}$.

(Uniqueness) Let F be another algebraic closure of k. As P_1 splits in F, we have $\tau_1 \in \mathrm{Hom}_k(k_1, F)$ by Lemma 55. As $P_2^{\tau_1}$ splits in F, we have $\tau_2 \in \mathrm{Hom}_k(k_2, F)$, extending τ_1.

(B) Repeating this, after making infinitely many choices, we obtain $\tau \in \mathrm{Hom}_k(\bar{k}, F)$. As every element in F is algebraic over k, and hence a root of some P_i, it is in $\tau(\bar{k})$, $\therefore \tau : \bar{k} \xrightarrow{\cong} F$ (B)

Remark

Axiom of Choice, Well Ordering Theorem

The real proof makes (A), (B) valid using Zorn's Lemma (Handout 2).

2.3 Example I - Finite Fields

Lemma 59

Let k be a field with q elements ($q \in \mathbb{N}$, suppose such a k exists)

Then i) $q = p^n$ for some $n \geq 1$, where $p = \operatorname{char} k$.

ii) Every element in k is a root of $X^q - X \in \mathbb{F}_p[X]$, which splits in k. In particular, k is a splitting field of $X^q - X$ over $\mathbb{F}_p$.

Proof

i) As $\mathbb{Q} \not\subseteq k$, we have $\operatorname{char} k =: p > 0$ and $\mathbb{F}_p \hookrightarrow k$.

If $[k : \mathbb{F}_p] = \infty$, then $|k| = \infty$. Hence $[k : \mathbb{F}_p] = n < \infty$

Then $k \cong \mathbb{F}_p^n$ as $\mathbb{F}_p$-vector space, hence $|k| = p^n$.

ii) $k^\times = k \setminus \{0\}$ (multiplicative group) is a finite group of order $q-1$. Hence every $x \in k^\times$ satisfies $x^{q-1} = 1$ by Lagrange. Thus $X^q - X = X(X^{q-1} - 1)$ has q distinct roots in k (= all elements of k) hence splits in k. The roots clearly generate k over $\mathbb{F}_p$ □

Remark

Recall $x^p = x$ $\forall x \in \mathbb{F}_p$ by Fermat. Conversely, we will show the existence of k by proving that $X^q - X$ has q distinct roots in its splitting field.

Definition 60

Let k be a field. Recall that $k[X]$ has $\{1, X, X^2, \dots\}$ as its basis as a k-vector space. Let the derivation $D: k[X] \to k[X]$ be the k-linear map defined by $D(1) = 0$ and $D(X^n) = nX^{n-1}$ ($n \geq 1$).

Proposition 61

Let k be a field.

i) $D(PQ) = D(P)\,Q + D(Q)\,P$ $\quad (\forall P, Q \in k[X])$

ii) $\alpha \in k$ a multiple root of $P \iff X - \alpha$ divides both P, $D(P)$ in $k[X]$

Proof

i) Both sides are k-bilinear in P, Q and $D(X^m X^n) = D(X^m)X^n + D(X^n)X^m$ $(\forall m, n \geqslant 0)$

ii) If $P = (X-\alpha)Q$ then $D(P) = Q + (X-\alpha)D(Q)$ by i). Hence $(X-\alpha) \mid D(P) \iff (X-\alpha) \mid Q \iff \alpha$ a multiple root $\square$

Corollary 62 (i.e. $\mathrm{char}\, k = 0$ or doesn't divide N)

If $(\mathrm{char}\, k, N) = 1$ then $X^N - 1$ has no multiple root in k.

Proof

Since $N \neq 0$ in k, the only root of $D(X^N - 1) = NX^{N-1}$ is $X = 0$ which is not a root of $X^N - 1$ (Proposition 61 ii)) $\square$

Remark

If $\mathrm{char}\, k = p > 0$, then $D(X^p - 1) = pX^{p-1} = 0$ and $X^p - 1 = (X-1)^p$ (multiple root! see below)

Lemma 63

If $\operatorname{char} k = p > 0$ then the map $k \to k$ defined by $x \mapsto x^p$ is a ring homomorphism (hence an $\mathbb{F}_p$-homomorphism).

Proof

$0^p = 0$, $1^p = 1$, $(ab)^p = a^p b^p$

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^{p-i} + b^p = a^p + b^p$$

since $\frac{p!}{i!(p-i)!}$ is divisible by p, $1 \leq i \leq p-1$ $\square$

Definition 64

The $\mathbb{F}_p$-hom in Lemma 63 is called the Frobenius Map of k, which we denote by $F_{\mathbb{F}_p}$. For $q = p^n$, the n^{th} iterate $Fr_q := (Fr_p)^n : k \to k$ is the q^{th} power Frobenius Map

2.3 Finite Fields (continued)

Last time, we had Lemma 59 : Any finite field must be a splitting field of $X^g - X$ over $\mathbb{F}_p$, where $g = p^n$. Also,

Corollary 62 : $X^N - 1$ has no multiple root unless $p \mid N$.

Lemma 63 : Any field k of character $p > 0$ has an $\mathbb{F}_p$ homomorphism $Fr_p : k \ni x \mapsto x^p \in k$ (Frobenius map)

$Fr_g := (Fr_p)^n$

Theorem 65

i) For each prime power $g = p^n$, there exists a finite field with g elements, unique up to $\mathbb{F}_p$-isomorphism (i.e. field isomorphism). This field is denoted by $\mathbb{F}_g$.

ii) Let $m, n \geq 1$ and $g = p^n$, $g' = p^m$. Then $\mathbb{F}_{g'}$ contains $\mathbb{F}_g$ if and only if g' is a power of g, i.e. $n \mid m$. If $g' = g^d$, then $[\mathbb{F}_{g'} : \mathbb{F}_g] = d$

Proof

i) Let k be a splitting field of $X^q - X$ over $\mathbb{F}_p$ (prop. 56). By Corollary 62, $X^g - X$ has g distinct roots in k (as p does not divide $q-1$). Then the set of all roots $\{x \in k \mid x^g = x\}$ is a subfield of k by Lemma 63. ($\because a^g = a$, $b^g = b$ $\Rightarrow (a+b)^g = a+b$, $(ab)^g = ab$, $(a^{-1})^g = a^{-1}$). As k is a splitting field, i.e. generated by these roots, it is equal to

this subfield and $|k| = q$. By Lemma 59, every field with q elements is $\mathbb{F}_p$-isomorphic to this one, by the uniqueness of splitting fields (Proposition 56).

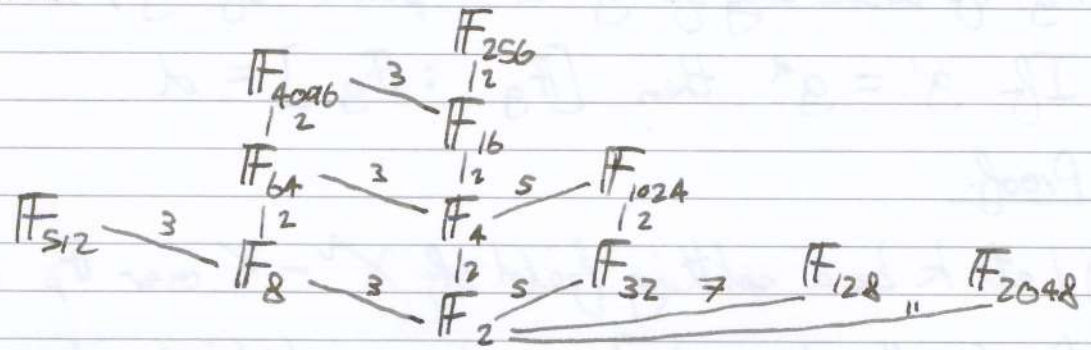
ii) If $q' = q^d$, then every root of $x^q - x$ is a root of $x^{q'} - x$, since $x^q = x \Rightarrow (\dots (x^q)^q \dots)^q = x$, hence $\mathbb{F}_{q'}$ contains $\mathbb{F}_q$. Conversely, if $\mathbb{F}_q \subset \mathbb{F}_{q'}$, then $\mathbb{F}_{q'}$ is an $\mathbb{F}_q$-vector space, and if $[\mathbb{F}_{q'} : \mathbb{F}_q] = d$, then $q' = |\mathbb{F}_{q'}| = |\mathbb{F}_q|^d = q^d$

Remark

Any field contains at most one copy of $\mathbb{F}_q$ by Lemma 59

Example

We have the same diagram for every p, but $p = 2$, ~~which~~ shown below:



The union of all these fields is $\overline{\mathbb{F}_p}$, and

$\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} \mid x^q = x\}$ for $q = p^n$

Lemma 66

Consider a finite extension $\mathbb{F}_{q^n} / \mathbb{F}_q$. Then $Fr_q : x \mapsto x^q$ is an $\mathbb{F}_q$ automorphism of $\mathbb{F}_{q^n}$ with order n

i.e. $\{id, Fr_g, Fr_g^2, \dots, Fr_g^{n-1}\} \subset Aut_{\mathbb{F}_g}(\mathbb{F}_{g^n})$

Proof

The map Fr_g fixes all elements in $\mathbb{F}_g$ (the roots of $x^g - x$), hence is an $\mathbb{F}_g$-homomorphism. Being an injective map (Lemma 11) of a finite set $\mathbb{F}_{g^n}$ into itself, it is an $\mathbb{F}_g$-automorphism. Since $x^{g^n} = x$ $(\forall x \in \mathbb{F}_{g^n})$, we have $Fr_g^n = id$ on $\mathbb{F}_{g^n}$ i.e. the order of Fr_g in $Aut_{\mathbb{F}_g}(\mathbb{F}_{g^n})$ divides n. But, for each $m \mid n$, the elements fixed by Fr_g^m are exactly the elements of $\mathbb{F}_{g^m}$, so the order is n □

Remark

For non-finite k with $\mathrm{char}\, k = p$, the Frobenius map is injective but not an automorphism (e.g. $Fr : \mathbb{F}_p(X) \to \mathbb{F}_p(X)$ has image $\mathbb{F}_p(X^p)$).

Lemma 67

Let k be a field, and $k^\times := k \setminus \{0\}$ be its multiplicative group. Then every finite subgroup G of $k^\times$ is cyclic.

Proof

Let $x \in G$ be an element with the maximal order; call the order n. We show that for any $y \in G$, the order of y, m, has to divide n. Suppose not. Then $\exists p$, a prime, such that $m = p^j m'$, $n = p^k n'$, and $j > k$. $(p \nmid m', n')$.

Let $z := x^{p^k} y^{m'}$. Then $z^i = 1 \Rightarrow x^{p^k i} = y^{-im}$

$$\Rightarrow \begin{cases} x^{p^j p^k i} = y^{-im} = 1 \Rightarrow n \mid p^{j+k} i \Rightarrow n' \mid i \\ 1 = x^{ni} = y^{-im'n'} \Rightarrow m \mid im'n' \Rightarrow p^j \mid i \end{cases}$$

$\Rightarrow p^j n' \mid i$ i.e. the order of z is $p^j n' > n$ ⚡

Now $x^{in/m}$ $(1 \leq i \leq m)$ are m distinct roots of $X^m - 1$ in k, hence all the roots (Lemma 53). As y is a root, it is a power of x □

Theorem 68

Every finite extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ of finite fields is simple and Galois with $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \{id, Fr_q, Fr_q^2, \ldots, Fr_q^{n-1}\}$ which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$

Proof

$\simeq \mathbb{F}_{q^n} \setminus \{0\}$

By Lemma 67, $\mathbb{F}_{q^n}^\times$ is cyclic, i.e. $\mathbb{F}_{q^n} = \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{q^n-2}\}$ for some $\zeta \in \mathbb{F}_{q^n}$, hence $\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta)$ (simple).

If P_ζ is the minimal polynomial of ζ over $\mathbb{F}_q$, then $|\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})| \leq |\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n}, \mathbb{F}_{q^n})| = |\mathrm{Root}_{P_\zeta}(\mathbb{F}_{q^n})| \leq n$, by Proposition 14 (Roots and Homomorphisms). Now, Lemma 66 implies the rest □

Remark

Theorem 68 and Proposition 14

$\Rightarrow$ Conjugates of ζ are $\{Fr_q^i(\zeta) = \zeta^{q^i} \mid 0 \leq i \leq n-1\}$

i.e. $P_\zeta(X) = (X-\zeta)(X-\zeta^q)(X-\zeta^{q^2})\dots(X-\zeta^{q^{n-1}})$

$(\deg P_\zeta = n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$

Example.

Not all generators ζ of the group $\mathbb{F}_{q^n}^\times$ are conjugate over $\mathbb{F}_q$.

In $\mathbb{F}_2[X]$

$$X^{16} - X = X(X+1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1)(X^4+X^3+1)$$

whose roots are all the elements in $\mathbb{F}_{16}$.

$\underbrace{X(X+1)}_{\mathbb{F}_2}\underbrace{(X^2+X+1)}_{\mathbb{F}_4}\underbrace{(X^4+X^3+X^2+X+1)(X^4+X+1)(X^4+X^3+1)}_{\text{roots all generate } \mathbb{F}_{16}/\mathbb{F}_2}$

roots are generators of $\mathbb{F}_{16}^\times \cong C_{15} \cong C_3 \times C_5$

(Lemma 67. & different generators)

HANDOUT 3: GAUSS' LEMMA (FROM GROUPS, RINGS & MODULES)

Let A be an integral domain, and $a, b, p, \ldots \in A$. We write $(a) := \{ad \mid d \in A\} \subset A$.

Definition. We say a is a *divisor* of b, or $a \mid b$, if $b \in (a)$. A *unit* is a divisor of 1, and $A^\times$ denotes the multiplicative group of all units in A. Note $A[X]^\times = A^\times$. We say a, b are *associates* if $a \mid b$ and $b \mid a$, i.e. $b = ad$ with $d \in A^\times$. An element p, not 0 nor a unit, is called *irreducible* if all its divisors are its associates and units; *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$ for any a, b. We say A is a *unique factorisation domain (UFD)* if every el't of A, except 0 and units, is a product of primes.

Fact. If a is a unit/irreducible/prime, then so is its associate. Every prime is irreducible. A factorisation of an element into a product of primes, if exists, is unique up to associates.

Definition. Let A be a UFD and $a_1, \ldots, a_n \in A$, not all zero. For a prime p, let p^m be its maximal power dividing all of $a_1, \ldots, a_n$. Then $p^m \neq 1$ for only finitely many p up to associates, and their product, defined up to associates, is called the *greatest common divisor (GCD)* of $a_1, \ldots, a_n$. Every el't in the field of fractions K of A is written as a/b where the GCD of a, b is 1, and b is called its *denominator*. For $P \in A[X] \setminus \{0\}$, its *content* $c(P) \in A$ is the GCD of its coefficients.

Lemma. *Let A be a UFD. If $P, Q \in A[X] \setminus \{0\}$, then $c(PQ) = c(P)c(Q)$ (up to associates).*

Proof. Note $c(P) \mid P$ and $P = c(P) \cdot P'$ with $c(P') = 1$. So STP if $c(P) = c(Q) = 1$ then $c(PQ) = 1$. Let $P = \sum a_i X^i$, $Q = \sum b_j X^j$, and $PQ = \sum d_k X^k$. For a prime $p \in A$, let i, j be minimal such that $a_i, b_j \notin (p)$. Then every term in $d_{i+j} = \sum a_k b_{i+j-k}$ is in (p) except for $a_i b_j$, which is not divisible by p, hence $d_{i+j} \notin (p)$. Hence $c(PQ) = 1$. □

Gauss' Lemma. *Let A be a UFD and K be its field of fractions. Consider $A \subset A[X] \subset K[X]$.*

(i) *A prime p of A is a prime of $A[X]$. If $P \in A[X]$ is a prime of $K[X]$ and $c(P) = 1$, then it is a prime of $A[X]$.*

(ii) *The poly. ring $A[X]$ is also a UFD (hence so is $A[X_1, \ldots, X_n]$), all whose primes are as seen in* (i). *For every monic in $A[X]$, its prime factorisation in $K[X]$ into monics gives its prime factorisation in $A[X]$.*

Proof. (i): If p is a prime of A and $p \mid PQ$ for $P, Q \in A[X]$, then $p \mid c(PQ) = c(P)c(Q)$ by the Lemma. So wlog p divides $c(P)$, hence divides P. Suppose $P \in A[X]$ is a prime of $K[X]$ and $c(P) = 1$. If $P \mid QR$ for $Q, R \in A[X]$, then wlog $Q = PS$ in $K[X]$. Clearing the denominators of S (i.e. multiply the GCD of the denom's of all its coeff's) to get $S' \in A[X]$ with $c(S') = 1$, we have $aQ = PS'$ with $a \in A$. Then $a \cdot c(Q) = 1$ by Lemma, so $c(Q) \in A^\times$, thus $P \mid Q$ in $A[X]$.

(ii): STP: every $P \in A[X]$, not a unit or 0, is a product of primes of the form seen in (i). Firstly $P = c(P) \cdot P'$ with $c(P') = 1$, and $c(P)$ is a product of primes of A, seen in (i). So assume $c(P) = 1$. Let d be the leading coeff. of P, and $P = dP_1 \cdots P_n$ be the prime fact'n in $K[X]$ into monics. Clearing the denom's of P_i to get $P_i' \in A[X]$ with $c(P_i') = 1$, we have $aP = bP_1' \cdots P_n'$ with $a, b \in A \setminus \{0\}$. These P_i' are primes of $K[X]$ of the form seen in (i). Now the Lemma (taking c) shows a, b are associates in A, hence $P = P_1' \cdots P_n'$ by replacing P_1' with its associate in $A[X]$. When $d = 1$, the leading coeff. d_i of P_i' is in $A^\times$ since $d_i \mid d$, hence $P_i = d_i^{-1} P_i' \in A[X]$. □

t.yoshida@dpmms.cam.ac.uk

2.4 Application I: Cyclotomic fields

Definition 69

For a field k and $N \geq 1$, let $k(\mu_N)$ be a splitting field of $X^N - 1$ over k (cyclotomic extension of k), and $\mu_N : \mathrm{Root}_{X^N-1}(k(\mu_N)) \subset k(\mu_N)^\times$ which lies in a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p$ inside $k(\mu_N)$. Then μ_N is a finite multiplicative group, hence cyclic (Lemma 67). If $(\mathrm{char}\, k, N) = 1$, then $|\mu_N| = N$, by Corollary 62. Hence there exists a primitive N^{th} root of unity i.e. $\zeta \in \mu_N$ with order N. There are $|(\mathbb{Z}/(N))^*|$ of them, but no canonical choice like $e^{\frac{2\pi i}{N}} \in \mathbb{C}$.

Proposition 70

Let $(\mathrm{char}\, k, N) = 1$

i) We can define the N^{th} cyclotomic polynomial, $\Phi_N \in \mathbb{Z}[X]$ inductively by $X^N - 1 = \prod_{d|N} \Phi_d(X)$ where d runs through all positive divisors of N. We will also denote the image of Φ_N in $k[X]$ by Φ_N. We have $\mathrm{Root}_{\Phi_N}(k(\mu_N)) = \{\text{all primitive } N^{th} \text{ roots of } 1\} \subset \mu_N$

ii) $k(\mu_N)/k$ is Galois, with an injective group homomorphism.

$$\mathrm{Gal}(k(\mu_N)/k) \hookrightarrow (\mathbb{Z}/(N))^\times$$
$$(\zeta \mapsto \zeta^i \ \forall \zeta \in \mu_N) \mapsto i \bmod N$$

If $[k(\mu_N) : k] = n$, then all irreducible factors of Φ_N in $k[X]$ have degree

Example

$\Phi_2(X) = X+1$, $\Phi_3(X) = X^2+X+1$, $\Phi_4(X) = X^2+1$

$\Phi_5(X) = X^4+X^3+X^2+X+1$, $\Phi_6(X) = X^2-X+1$, ...

Proofs

i) (By induction on N). By our induction hypothesis $\prod_{d<N,\, d|N} \Phi_d(X)$ is in $\mathbb{Z}[X]$, and its roots in $k(\mu_N)$ are all the non-primitive N^{th} roots of 1, all distinct (Corollary 62). So it divides X^N-1 in $k(\mu_N)[X]$, and the roots of the quotient Φ_N are the primitive N^{th} roots of 1. Now consider $k=\mathbb{Q}$. Then $\Phi_N \in \mathbb{Q}(\mu_N)[X]$ is obtained by the division algorithm as the quotient of X^N-1 by a monic $\in \mathbb{Z}[X]$. Hence $\Phi_N \in \mathbb{Z}[X]$.

ii) Let $[k(\mu_N):k] = n$ and ζ be a primitive N^{th} root of 1. As $k(\mu_N) = k(\zeta)$ and the minimal polynomial P_ζ has $\deg P_\zeta = n$ distinct roots in μ_N (Corollary 62), (X^N-1 has no multiple roots unless $p \mid N$.) $k(\mu_N)/k$ is Galois by Proposition 14 (R+H). If $\sigma(\zeta) = \zeta^i$ then $\sigma(\zeta^j) = (\zeta^i)^j = (\zeta^j)^i$ for all j. The map is injective as $i \bmod N$ determines σ ($\because k(\mu_N) = k(\zeta)$, and is a group homomorphism as $(\zeta \mapsto \zeta^i) \circ (\zeta \mapsto \zeta^j) \equiv (\zeta \mapsto \zeta^{ij})$.

Finally, every irreducible factor of Φ_N is the minimal polynomial of some primitive N^{th} root by i), hence has degree $[k(\zeta):k] = n$

Example

Recall that in $\mathbb{F}_2[X]$, we have

$$X^{15}-1 = (X+1)(X^2+X+1)(X^4+X^3+X^2+X+1)(X^4+X+1)(X^4+X^3+1)$$
$$= (\Phi_2 \bmod 2)(\Phi_3 \bmod 2)(\Phi_5 \bmod 2)\ (\Phi_{15} \bmod 2)$$

so $\Phi_{15} \bmod 2$ is a product of two ireducible factors. Note that roots of $\Phi_5 \bmod 2$ are not generators of μ_{15}, but still generate $\mathbb{F}_{16}/\mathbb{F}_2$

Example

Let $k = \mathbb{F}_q$ and $n \geq 1$. Since $\mathbb{F}_{q^n}^\times = \mu_{q^n-1}$, we have $\mathbb{F}_{q^n} = \mathbb{F}_q(\mu_{q^n-1})$ (the splitting field of $X^{q^n}-X$ and also of $X^{q^n-1}-1$). So every finite extension of finite fields is a cyclotomic extension. Note that $(\operatorname{char} k, q^n-1) = 1$.

More generally, for $N \geq 1$, and prime to q, let n be the order of $q \bmod N$ in $(\mathbb{Z}/N)^\times$. Then, by Theorem 68 and Proposition 70 ii),

$$\operatorname{Gal}\left(\frac{\mathbb{F}_q(\mu_N)}{\mathbb{F}_q}\right) \xrightarrow{\sim} \{1, q, q^2, \dots, q^{n-1}\} \subset (\mathbb{Z}/N)^\times$$
$$(\mathrm{Fr}: x \mapsto x^q) \mapsto q \bmod N$$

is an isomorphism i.e. $\mathbb{F}_q(\mu_N) = \mathbb{F}_{q^n}$, and all ireducible factors of Φ_N in $\mathbb{F}_q[X]$ have degree n. The previous example is $q=2$, and $N=5, 15$, $n=4$.

(not necessarily to the whole of $\mathbb{Z}_N^*$)

So we know how $\Phi_N \bmod p$ factorises for p prime to N.

What about $\operatorname{char} k = 0$?

The simplest case is where $(\mathbb{Z}/(N))^\times$ is cyclic and has a generator p mod N with p prime, then Φ_N mod p is irreducible (previous example), hence so is Φ_N. But for $N=8$, for example, $\Phi_8 = X^4+1$. Φ_8 mod p is reducible for every prime p, but Φ_8 is still irreducible in $\mathbb{Z}[X]$.

Theorem 71 (Gauss, Irreducibility of Cyclotomic Polynomials)

For all $N \geq 1$, Φ_N is irreducible in $\mathbb{Q}[X]$ (hence also in $\mathbb{Z}[X]$ by Gauss' Lemma).

In other words, the group homomorphism

$\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \to (\mathbb{Z}/(N))^\times$ in Proposition 70 ii) is an isomorphism.

Proof

It is sufficient to prove that Φ_N is the minimal polynomial over $\mathbb{Q}$ of every primitive N^{th} root of 1 i.e. all elements of $\mathrm{Root}_{\Phi_N}(\mathbb{Q}(\mu_N)) = \{\zeta^a \mid a \in (\mathbb{Z}/(N))^\times\}$ are conjugate over $\mathbb{Q}$.

As every $a \in (\mathbb{Z}/(N))^\times$ is some product of p mod N for primes p not dividing N. It is sufficient to prove that ζ^p is a conjugate of ζ over $\mathbb{Q}$ for every p prime to N and every primitive ζ.

Let P_ζ be the minimal polynomial of ζ over $\mathbb{Q}$, and $\Phi_N = P_\zeta Q$ in $\mathbb{Q}[X]$. As Φ_N, P_ζ are monics, so is Q, hence P_ζ, $Q \in \mathbb{Z}[X]$ by Gauss' Lemma ($\because \Phi_N \in \mathbb{Z}[X]$)

Suppose that ζ^p is not a root of P_ζ, and then it is a root of Q.

Then ζ is a root of $Q(X^p)$, hence $P_\zeta(x) \mid Q(X^p)$ in $\mathbb{Q}[x]$, hence also in $\mathbb{Z}[x]$ (division by a monic).

Reducing this mod P (and writing $\bar{P} := P \bmod p$)

$\bar{P}_\zeta(x) \mid \bar{Q}(x^p) = (\overline{Q(x)})^p$ in $\mathbb{F}_p[x]$. Thus $\bar{P}_\zeta$, $\bar{Q}$ have common roots in $\mathbb{F}_p(\mu_N)$, but this contradicts Corollary 62 since $\overline{\Phi_N} \mid \overline{x^N - 1}$ ☐

$x^N - 1$ has no multiple roots unless $\mathrm{char}\, k = p \mid N$

2.4 Cyclotomic Fields (continued)

Proof of Theorem 71

$\Phi_N \in \mathbb{Z}[X]$ irreducible $\leftarrow$ $\Phi_N = P_\zeta Q$ (P_ζ irreducible)

It is sufficient to prove that for ζ a root of P_ζ, ζ^p is also a root of P_ζ, but $p \nmid N$.

ζ a root of P_ζ, ζ^p a root of Q

$\Rightarrow \zeta$ a root of $Q(X^p)$, $\bar{P} := P \bmod p$

$\overline{Q(X^p)} = (\bar{Q}(X))^p$ in $\mathbb{F}_p[X]$

$\uparrow$ $(\sum a_i X^i)^p = \sum (a_i X_i)^p = \sum a_i (X^p)^i$

$a_i^p = a_i \quad \because a_i \in \mathbb{F}_p$.

$\Rightarrow P_\zeta(X) \mid Q(X^p) \rightarrow \bar{P}_\zeta, \bar{Q}$ have a common root in $\mathbb{F}_p(\mu_N)$ $*$

Remark

i) Later we will see another "mod p proof" i.e. proving that $Gal(P)$ for $P \in \mathbb{Q}[X]$ is large by showing that $Gal(P \bmod p)$ is large for some p (Theorem 84)

ii) $N = 8$ $\zeta = \zeta_8$ $\Phi_8(X) = (X-\zeta)(X-\zeta^3)(X-\zeta^5)(X-\zeta^7)$

By building the theory of number fields and reducing $\mathbb{Z}[\zeta]$ modulo p to get $\mathbb{F}_p(\mu_N) \ni \bar{\zeta} = \zeta \bmod p$ [in fact this is as natural way to obtain all finite extensions of $\mathbb{F}_p$] one sees from the remark after Theorem 68 that the factorisation of $\bar{\Phi}_8 = \Phi_8 \bmod p$ in $\mathbb{F}_p[X]$ is as

$p \equiv 1 \bmod 8 \Rightarrow \bar{\Phi}_8 = (X-\bar{\zeta})(X-\bar{\zeta}^3)(X-\bar{\zeta}^5)(X-\bar{\zeta}^7)$

$p \equiv 3 \bmod 8 \Rightarrow \bar{\Phi}_8 = [(X-\bar{\zeta})(X-\bar{\zeta}^3)][(X-\bar{\zeta}^5)(X-\bar{\zeta}^7)]$

$p \equiv 5 \bmod 8 \Rightarrow \bar{\Phi}_8 = [(X-\bar{\zeta})(X-\bar{\zeta}^3)][(X-\bar{\zeta}^3)(X-\bar{\zeta}^7)]$

e.g. $p = 3$, $\Phi_8 \pmod 3 = (X^2+X-1)(X^2-X-1)$

$\Phi_8 \pmod 5 = (X^2-2)(X^2+2)$, $\Phi_8 \pmod 7 = (X^2+3X+1)(X^2-3X+1)$

which explains why Φ_ℓ is irreducible in $\mathbb{Q}[X]$ :: if it were factorised in $\mathbb{Z}[X]$ (say into $(X-\zeta)(X-\zeta^3)$ etc), every mod ℓ reduction must respect this.

iii) Theorem 71 says $\mathbb{Q}(\mu_N)/\mathbb{Q}$ has Galois group $(\mathbb{Z}/(N))^\times$, an abelian group of order $\varphi(N) := \{i \bmod N \mid 1 \le i \le N, (i,N) = 1\}$ (Euler's Totient Function). For $N = \prod_i p_i^{m_i}$ then $\varphi(N) = \prod_i \varphi(p_i^{m_i})$, and $\varphi(p^m) = p^{m-1}(p-1)$ for p prime.

Revisit the ruler and compass construction (1.11). A regular N-gon i.e. points in $\mathbb{Q}(\mu_N)$ are constructible iff $[\mathbb{Q}(\mu_N) : \mathbb{Q}] = \varphi(N)$ is a power of 2 iff $N = 2^a p_1 \cdots p_r$ where the p_i are distinct Fermat primes e.g. $p = 17$ (Gauss, example sheet 2.10)

$\mathbb{Q}(\mu_{17}) \leftrightarrow \{id\}$ — $\zeta = \zeta_{17}$, $\alpha = \zeta + \zeta^{16} = 2\cos\frac{2\pi}{17}$, $\alpha' = \zeta^{13} + \zeta^4$

$\mathbb{Q}(\alpha) \leftrightarrow \{1, 16\}$ — roots of $X^2 - \beta_1 X + \beta_3$

$\mathbb{Q}(\beta) \leftrightarrow \{1, 13, 16, 4\}$ — where $\beta = \beta_1 = \zeta + \zeta^{13} + \zeta^{16} + \zeta^4$, $\beta_2 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2$

$\mathbb{Q}(r) \leftrightarrow$ — roots of $X^2 - rX - 1$

$\mathbb{Q} \leftrightarrow$ — β_3, β_4 roots of $X^2 - r'X - 1$, $r = \zeta + \zeta^9 + \cdots + \zeta^2$ (8 terms), $r' = \zeta^3 + \zeta^{10} + \ldots$ (the rest)

$r + r' = -1$, $rr' = -4$, $r = \frac{-1+\sqrt{17}}{2}$

2.5 Separability

Definition 72

Let k be a field. $P \in k[X]$ is separable if $|\mathrm{Root}_P(E)| = \deg P$ (i.e. no multiple roots) whenever P splits in an

extension E/k.
By Lemma 55 $|\mathrm{Root}_p(E)|$ is independent of E.

Lemma 73

Let $P \in k[X]$.

i) Let L/k be an extension. If P is separable and $Q \in L[X]$ divides P in $L[X]$ then Q is separable.

ii) P is separable $\Leftrightarrow$ P and $D(P)$ are coprime in $k[X]$.

iii) If P is irreducible, then P is separable iff $D(P) \neq 0$ i.e. P is not a poly in X^p for $p = \mathrm{char}\, k$. In particular, all irreducible polynomials are separable if $\mathrm{char}\, k = 0$.

iv) Suppose P is separable. If $\tau : k \hookrightarrow E$ is a field homomorph then $\tau P \in E[X]$ is separable. In particular P is separable as a polynomial in $L[X]$ for any extension L/k.

Proof

i) As P has no multiple root when split, neither does Q.

ii) Let E be a splitting field of P. If P, $D(P)$ are coprime, then $\exists\, Q, R \in k[X]$, with $PQ + D(P)R = 1$ in $k[X]$, recalling Proposition 15 ii)) which remains true in $E[X]$, so P, $D(P)$ have no common root in E. If P and $D(P)$ had a common factor in $k[X]$, then they have a common root in E hence this is a multiple root.

iii) As $\deg D(P) < \deg P$ and P is irreducible, P, $D(P)$ are coprime unless $D(P) = 0$

iv) τP and $\tau D(P) = D(\tau P)$ are coprime in $E[X]$,
(consider the image of $PQ + D(P)R = 1$ by τ')

HANDOUT 4: A SLIGHTLY BETTER PROOF OF PRIMITIVE ELEMENT THEOREM

I found (in my old friend's notes) a slightly better statement/proof of PET (Th. 20). It doesn't use induction on the number of generators, and instead of linear combinations of two generators uses more general polynomials and proves in one go. It has the advantage of weakening the hypothesis $(*)$ there — now we don't need to care about the intermediate fields, so for example we immediately see that any Galois extension is simple. At the same time, it proves that number of K-hom's are bounded by the degree (which we postponed until Lem. 76). This would have enabled us to prove the Fundamental Theorem over general infinite fields in §1 with exactly the same proof. (But we were mainly interested in subfields of $\mathbb{C}$ there, so it's a minor improvement.)

Primitive Element Theorem. *(Th. 20) Let F/K be a finite ext'n. Then we have $|\mathrm{Hom}_K(F,E)| \leq [F:K]$ for any ext'n E/K. Moreover if it is an equality for some E/K, then F/K is simple. (In particular, every finite ext'n inside $\mathbb{C}$ is simple by Th. 18.)*

Proof. When $|K| < \infty$ (finite fields), the simplicity is proved directly (Th. 68) and the first claim follows by Prop. 14. So we assume $|K| = \infty$ (e.g. any $K \subset \mathbb{C}$, in which case $\mathbb{Q} \subset K$).

Let $F = K(\alpha_1, \ldots, \alpha_n)$ (Prop. 10), and $\tau_1, \ldots, \tau_d \in \mathrm{Hom}_K(F,E)$ be distinct. If we find $\alpha \in F$ such that $\tau_1(\alpha), \ldots, \tau_d(\alpha)$ are all distinct, then $\tau_j|_{K(\alpha)} \in \mathrm{Hom}_K\big(K(\alpha),E\big)$ $(1 \leq j \leq d)$ are all distinct, hence

$$d \leq |\mathrm{Hom}_K\big(K(\alpha),E\big)| \overset{\text{Prop.14}}{\leq} [K(\alpha):K] \leq [F:K],$$

and moreover if $d = [F:K]$ then it forces $K(\alpha) = F$, so we win.

Let $P = \sum_{i=1}^{n} \alpha_i X^i \in F[X]$, and we try $\alpha \in F$ of the form $\alpha = P(x)$ with $x \in K$. Since $\alpha_1, \ldots, \alpha_n$ generate F/K, if $j \neq j'$ then we cannot have $\tau_j(\alpha_i) = \tau_{j'}(\alpha_i)$ for all $1 \leq i \leq n$. Thus $\tau_j P \in E[X]$ are all distinct poly's, so

$$\prod_{j \neq j'} \big(\tau_j P(X) - \tau_{j'} P(X)\big) \in E[X]$$

is a non-zero poly., hence $\exists x \in K$ which is not its root, since $|K| = \infty$ (Lem. 53(ii)). Then $\tau_j P(x) \neq \tau_{j'} P(x)$ for any $j \neq j'$, i.e. for $\alpha := P(x)$ the el'ts $\tau_j(\alpha)$ are all distinct. □

Consequences. (i) *Lem. 22(iii) (i.e. $|\mathrm{Aut}_K(L)| \leq [L:K]$ for finite L/K), without "inside $\mathbb{C}$"*, follows from Lem. 22(ii) (i.e. $\mathrm{Hom}_K(L,L) = \mathrm{Aut}_K(L)$) and this PET.

(ii) *Every Galois ext'n (for general fields) is simple by this PET.* If $L = K(\alpha)$, then L/K is Galois iff $|\mathrm{Root}_{P_\alpha}(L)| = \deg P_\alpha$ (i.e. it splits into distinct linear factors in $F[X]$), where P_α is the min. poly. of α over K, by Prop. 14 and 7(ii).

(iii) Thus *Prop. 33 and Th. 34 (FTGT) are proved for general fields.* The first half of the proof of Th. 34 will go as follows: let $F = K(\alpha)$ by PET. The remark (ii) says $|\mathrm{Root}_{P_\alpha}(F)| = \deg P_\alpha$, where P_α is the min. poly. of α $/K$. Take L. The min. poly. Q_α of α over L divides P_α, hence $|\mathrm{Root}_{Q_\alpha}(F)| = \deg Q_\alpha$. As $F = L(\alpha)$, the same remark says F/L is Galois. Now Prop. 33(i) shows $F^{\mathrm{Aut}_L(F)} = L$. The rest is unchanged.

t.yoshida@dpmms.cam.ac.uk

2.5 Separability (continued)

Definition 74

An algebraic extension F/k is called separable (respectively normal) iff every $\alpha \in F$ its min poly. P_α over k is separable (respectively splits in F).

We relate the separability with the k-homomorphisms in Section 1:

Lemma 75

Let F/k, E/k be two extensions of k. Let $k \subset L \subset F$ and $\alpha \in F$ be algebraic/L with minimal polynomial P_α over L. Then $|\mathrm{Hom}_k(L(\alpha), E)| \leq \deg P_\alpha \, |\mathrm{Hom}_k(L, E)|$ where the equality holds iff $|\mathrm{Root}_{\tau P_\alpha}(E)| = \deg P_\alpha$ for all $\tau \in \mathrm{Hom}_k(L, E)$

Proof

Immediate from Proposition 17 (Roots and Homs II) which gives a bijection for every $\tau \in \mathrm{Hom}_k(L, E)$

$$\{\rho \in \mathrm{Hom}_k(L(\alpha), E) \mid \rho_L = \tau\} \xrightarrow{\cong} \mathrm{Root}_{\tau P_\alpha}(E) \quad \cdots (\star)$$
$$\rho \mapsto \rho(\alpha)$$

□

Proposition 76

If F/k is finite then $|\mathrm{Hom}_k(F, E)| \leq [F : k]$ for any extension E/k. If the equality holds for E/k, then for any intermediate field $k \subset L \subset F$ we have:

i) $|\mathrm{Hom}_k(L, E)| = [L:k]$

ii) $\mathrm{Hom}_k(F, E) \to \mathrm{Hom}_k(L, E)$, $\rho \mapsto \rho|_L$ is surjective

Proof

Let $F = k(\alpha_1, \dots, \alpha_n)$ (Proposition 10 ii)) and $k_i := k(\alpha_1, \dots, \alpha_i)$ so that $k = k_0 \subset k_1 \subset \dots \subset k_n = F$ is a tower of simple extensions.

By repeating Lemma 75 $|\mathrm{Hom}_k(F, E)| \leq [F : k_{n-1}] |\mathrm{Hom}_k(k_{n-1}, E)$

$\leq \dots \leq [F : k_{n-1}][k_{n-1} : k_{n-2}] \dots [k_{i+1} : k_i] |\mathrm{Hom}_k(k_i, E)$

$\leq \dots \leq [F : k_{n-1}] \dots [k_1 : k] = [F:k]$ (Tower Law, Proposition 8). If our equality holds, then each $\leq$ is $=$.

For $k \subset L \subset F$, choose $\alpha_1, \dots, \alpha_n$ so that $L = k_i$.

Then $[F : L] |\mathrm{Hom}_k(L, E)| = [F : k]$. Hence i) by the Tower Law and the condition in Lemma 75 shows that the LHS of (☆) is non-empty for every step from $L = k_i$ to F, hence ii) □

Theorem 77

Let F/k be a finite extension. i) The following are equivalent:

i) a) There exists an extension E/k with $|\mathrm{Hom}_k(F, E)| = [F:k]$

b) F/k separable

c) $F = k(\alpha_1, \dots, \alpha_n)$ and the minimal polynomial Q_i of α_i over k is separable $(1 \leq i \leq n)$

d) $F = k(\alpha_1, \dots, \alpha_n)$ and the minimal polynomial P_i of α_i over $k(\alpha_1, \dots, \alpha_{i-1})$ is separable $(1 \leq i \leq n)$

ii) If $k \subset L \subset F$ then F/k separable $\Leftrightarrow$ F/L, L/k separable

iii) The following are equivalent:

a) F/k is Galois

b) F/k is separable and normal

c) $F = k(\alpha_1, \dots, \alpha_n)$ and the minimal polynomial Q_i of α_i over k is separable and splits in F $(1 \le i \le n)$

Proofs

i) (a) $\Rightarrow$ (b) : For every $\alpha \in F$, we have

$|\mathrm{Root}_{P_\alpha}(E)| \overset{\text{Prop 14}}{=} |\mathrm{Hom}_k(k(\alpha), E)| \overset{\text{Prop 76}}{=} [k(\alpha) : k] = \deg P_\alpha$

(b) $\Rightarrow$ (c) is clear.

(c) $\Rightarrow$ (d) $P_i \mid Q_i$, no use Lemma 73 i) (Q_i separable, $P_i \mid Q_i$ $\Rightarrow$ P_i separable)

(d) $\Rightarrow$ (a) Take E/k such that $Q_1, \dots, Q_n$ splits in E. We show that every $\le$ in the proof of Proposition 76 is $=$ by checking the condition in Lemma 75. For every $\tau \in \mathrm{Hom}_k(k_{i-1}, E)$, we have τP_i separable by Lemma 73 iv). As $\tau P_i \mid \tau Q_i = Q_i$ and Q_i splits in E, we have $|\mathrm{Root}_{\tau P_i}(E)| = \deg P_i$.

ii) Choose $\alpha_1, \dots, \alpha_n$ with $L = k_i$, and use (b) $\Leftrightarrow$ (d)

iii) The same proof as i), in which we can take E to be F everywhere $\square$

Now we can revisit sections 1-5 - 1-7.

For every finite separable extension F/k, we have the following assertions:

Theorem 18 and Lemma 19 hold with $\mathbb{C}$ replaced by some field E by Theorem 77 i) a).

Theorem 78 (Primitive Element Theorem)

Every finite separable extension is simple.

Proof

By Theorem 77 i) (b) $\Rightarrow$ (a) and Proposition 76 i) the condition (*) in the Proof of Theorem 20 holds $\square$

Proposition 79

The following hold unconditionally (i.e. without "inside $\mathbb{C}$")

Lemma 22 (iii), Corollary 26 with the condition "P is a product of separable polynomials", Proposition 33, Theorem 34 (FTGT), Corollary 35, Proposition 42.

Proof

Lemma 22 iii) is Proposition 76. Theorem 77 iii) corresponds to Proposition 24 (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv). The rest will follow. In the proof of Corollary 35, Proposition 42, replace $\mathbb{C}$ with F, and use Proposition 76 for $E = F$ $\square$

For example, applying Prop 42 i) to finite fields gives:

Proposition 80

Let $P \in \mathbb{F}_p[x]$ be a monic separable polynomial of degree n. If $P = Q_1 Q_2 \dots Q_n$ is the irreducible factorisation in $\mathbb{F}_p[x]$

with $\deg Q_i = n_i$ (so $n = \sum n_i$) then $Fr_p \in Gal(P) \hookrightarrow S_n$ has cycle type $(n_1, \dots, n_m)$ when viewed as an element of S_n.

Remark

$Gal(P) \hookrightarrow S_n$ is defined up to conjugates in S_n $\rightarrow$ cycle type is well defined.

Proof

Let $\mathbb{F}_q$ be the splitting field of P over $\mathbb{F}_p$. As $Gal(\mathbb{F}_q/\mathbb{F}_p) = \{id, Fr_p, Fr_p^2, \dots, Fr_p^{N-1}\}$ if $q = p^N$ [Theorem 68], the conjugates of α over $\mathbb{F}_p$ are $\{\alpha, \alpha^p, \alpha^{p^2}, \dots, \alpha^{p^{d-1}}\}$ for some $d \mid N$, which are permuted cyclically by Fr_p.

Now $P = Q_1 Q_2 \dots Q_m$ and each Q_i, being irreducible, is the min poly of its root $\alpha_i \in \mathbb{F}_q$. So in $\mathbb{F}_q[X]$:

$$P(X) = (X-\alpha_1)(X-\alpha_1^p)\dots(X-\alpha_1^{p^{n_1-1}}) \quad (\leftarrow Q_1)$$
$$(X-\alpha_2)(X-\alpha_2^p)\dots(X-\alpha_2^{p^{n_2-1}}) \quad (\leftarrow Q_2)$$
$$\dots \quad (X-\alpha_m)\dots(X-\alpha_m^{p^{n_m-1}}) \quad (\leftarrow Q_m)$$

and Fr_p acts on these roots by a permutation of cycle type $(n_1, \dots, n_m)$ □

2.6 Example II: Symmetric Function Theorem

Let k be a field and $n \geq 1$. Recall (Definition 4.3) $F := k(X_1, \ldots, X_n)$, the field of rational functions in n variables. (the field of fractions of $k[X_1, \ldots, X_n]$. As used in the proof of Proposition 4.2, the symmetric group $G := S_n$ acts on F by permuting $X_1, \ldots, X_n$, i.e. $G \subset \mathrm{Aut}_k(F)$. The fixed field F^G is the subfield consisting of all symmetric rational functions in $X_1, \ldots, X_n$.

Definition 8.1

Let k, n, F, G be as above. For $1 \leq i \leq n$, let

$$S_i = \sum_{\{\lambda_1, \ldots, \lambda_i\} \subset \{1, 2, \ldots, n\}} X_{\lambda_1} \ldots X_{\lambda_i} \in F^G$$

be the i^{th} elementary symmetric polynomials.

Proposition 8.2 (Rational Symmetric Function Theorem)

Let k, n, F, G be as above, and let $L := k(S_1, \ldots, S_n) \subset F$ be the subfield of F consisting of all rational functions in $S_1, \ldots, S_n$ with coefficients in k. Then $F^G = L$ i.e. all symmetric functions are in L.

Proof

As $S_1, \ldots, S_n \in F^G$, we have $L \subset F^G$. As $X_1, \ldots, X_n$ are the roots of $P(X)$: $(X - X_1) \ldots (X - X_n) = X^n - S_1 X^{n-1} + S_2 X^{n-2} - \ldots + (-1)^n S_n$

$P(X) \in L[X]$, $F = L(X_1, \ldots, X_n)$ is a splitting field of P, finite over L.

So F/F^G is also finite.

Path I

Proposition 33 ii) says that F/F^G is Galois with $G = Gal(F/F^G)$

F | F^G | L

As F is a splitting fields of P over L, and P has no multiple roots, we know that F/L is Galois and $Gal(P) = Gal(F/L)$ injects into G (permutations of X_i) by Proposition 79 (Corollary 26, Proposition 42). Thus $F^G = L$ follows from

$$|G| = |Gal(F/F^G)| = [F : F^G] \leq [F : L] = |Gal(F/L)| \leq |G|$$

Thus $G = S_n$ contains everything. □

Path II

We build from first principles. As $G \subset Aut_{F^G}(F)$, we have

$$n! = |G| \leq |Aut_{F^G}(F)| \leq [F : F^G] \leq [F : L] \quad (*)$$

by Lemma 22 iii). But a splitting field has degree at most $n!$.

More explicitly, let $L_i := L(X_1, \dots, X_i)$ for $1 \leq i \leq n$, so that $L = L_0 \subset L_1 \subset \dots \subset L_n = F$. Then X_i is a root of:

$$P_i(X) := \frac{P(X)}{(X - X_1)\dots(X - X_{i-1})} = (X - X_i)\dots(X - X_n) \in L_{i-1}[X] \quad (\star)$$

which has degree $n - i + 1$, hence $L_i = L_{i-1}(X_i)/L_{i-1}$ has degree at most $n - i + 1$. Thus $[F : L] \leq n(n-1)\dots 2 \cdot 1 = n!$.

Hence $(*)$ implies that $[F : L] = n!$ and $F^G = L$ □

Remark

On the example sheet, 3.9, 3.11, 3.18* are similar to Path I

In Path II, as $[F:L]=n!$, we need $[L_i : L_{i-1}] = n-i+1$ for all i, i.e. $Z_i := \{1, X_i, X_i^2, \dots, X_i^{n-i}\}$ is a basis for L_i/L_{i-1}. Hence

$$Z := \{z_1 \dots z_n \mid z_i \in Z_i\} = \{X_1^{m_1} \dots X_n^{m_n} \mid 0 \le m_i \le n-i\}$$

is a basis of F/L (recall the proof of the Tower Law)

Now revisit (☆) with $n=3$, $k=\mathbb{Q}$, $(\alpha, \beta, \gamma) = (X_1, X_2, X_3)$

$$P(X) = X^3 - (\underbrace{\alpha+\beta+\gamma}_{=S_1})X + (\underbrace{\alpha\beta+\beta\gamma+\gamma\alpha}_{=S_2})X - \underbrace{\alpha\beta\gamma}_{=S_3}$$

$$= P_1(X) \in \mathbb{Z}[S_1, S_2, S_3][X]$$

$$= (X-\alpha)\left(X^2 - (S_1-\alpha)X + (S_2 - \alpha(S_1-\alpha))\right) \quad = P_2(X) \in \mathbb{Z}[S_1, S_2, S_3, \alpha]$$

$$= (X-\alpha)(X-\beta)(X-(S_1-\alpha-\beta)) = P_3(X) \in \mathbb{Z}[S_1, S_2, S_3, \alpha, \beta][X]$$

Theorem 83 (Symmetic Function Theorem)

Let k, n, F, G be as above and let R be any sub-ring of k (e.g. $R = \mathrm{Im}(\mathbb{Z} \to k)$ i.e. $\mathbb{Z}$ or $\mathbb{F}_p$ according to char k). Then, inside F, we have $R[X_1, \dots, X_n] \cap F^G = R[S_1, \dots, S_n]$ i.e. every symmetic polynomial with coefficients in R is a polynomial in $S_1, \dots, S_n$ with coefficients in R.

Proof

Clearly $R[S_1, \dots, S_n] \subset R[X_1, \dots, X_n] \cap F^G$. In (☆), note that $P(X) \in R[S_1, \dots, S_n][X]$ and $(X-X_1)(X-X_2)\dots(X-X_{i-1}) \in R[X_1, \dots, X_{i-1}][X]$ are both monics, with coefficients in the

ing $R[S_1, \ldots, S_n, X_1, \ldots, X_{i-1}]$, hence by the division algorithm we have $P_i(x) \in R[S_1, \ldots, S_n, X_1, \ldots X_{i-1}][x]$, a monic of degree $n-i+1$. As $P_i(X_i) = 0$, we see that X_i^{n-i+1} is an $R(S_1, \ldots, S_n, X_1, \ldots, X_{i-1})$ linear combination of $Z_i = \{1, X_i, X_i^2, \ldots, X_i^{n-i+1}\}$, hence so is any higher power of X_i. Repeating this for $1 \leq i \leq n$, eventually every monomial $X_1^{m_1}, \ldots, X_n^{m_n}$ is an $R[S_1, \ldots, S_n]$ - linear combination of ~~$Z_i = \{1, X_i, X_i^2, \ldots, X_i^{n-i}\}$, hence so is any higher power of X_i. Repeating this for $1 \leq i \leq n$, eventually, every monomial $X_1^{m_1} \cdots X_n^{m_n}$ is~~

Z, which is a basis for F/L. If we write $f \in R[X_1, \ldots, X_n] \cap F^G$ as an $R[S_1, \ldots, S_n]$ linear combination of Z, then it must be the unique expression of $f \in F^G \subseteq L$ as an L-linear combination of Z, namely $f = f \cdot 1$. Thus $f \in R[S_1, \ldots, S_n]$

Remark

The proof shows that $R[X_1, \ldots, X_n]$ is a free $R[S_1, \ldots, S_n]$ module of rank $n!$ with a basis Z.

We can prove that $R[S_1, \ldots, S_n]$ is isomorphic to the poly. ring in $S_1 \ldots S_n / R$.

Example

Recall (Definition 50) the discriminant for the splitting field F, $F = \mathbb{Q}(X_1, \dots, X_n)$ over $L = \mathbb{Q}(S_1, \dots, S_n) = F^G$

$$\Delta P = \prod_{i<j} (X_i - X_j)^2 \in \mathbb{Z}[X_1, \dots, X_n] \cap L = \mathbb{Z}[S_1, \dots, S_n]$$

e.g. $P = X^2 - S_1 X + S_2 \Rightarrow \Delta P = S_1^2 - 4S_2$

$P = X^3 + S_2 X - S_3 \Rightarrow \Delta P = -4S_2^3 - 27S_3^2$

2.7 Application II: Galois Groups over $\mathbb{Q}$

Theorem 84

Let $P \in \mathbb{Z}[X]$ be a monic, separable polynomial (as $P \in \mathbb{Q}[X]$) of degree n, and let p be a prime such that $P \bmod p \in \mathbb{F}_p[X]$ is also separable. If $P \bmod p = Q_1 \dots Q_m$ is the irreducible factorisation in $\mathbb{F}_p[X]$, and $\deg Q_i = n_i$, then $\mathrm{Gal}(P)$ contains an element of cycle type $(n_1, \dots, n_m)$ as an element of S_n (see the remark after Proposition 80)

Example

Let $P = X^5 + 2X + 6$. As $P \bmod 3 = X^5 - X = X(X-1)(X+1)(X^2+1)$ in $\mathbb{F}_3[X]$, Theorem 84 shows that $\mathrm{Gal}(P)$ contains an element of cycle type $(1,1,1,2)$ i.e. a transposition. If moreover $\mathrm{Gal}(P)$ has a 5-cycle, then $\mathrm{Gal}(P) \cong S_5$, by Group Theory (Sheet 4, Q4.

Proof

By Proposition 80, it is sufficient to prove that $\mathrm{Gal}(P \bmod p) < \mathrm{Gal}($

inside S_n, up to conjugation. We use the setup in section 2.6.

Let $F := \mathbb{Q}(X_1, \dots, X_n)$ on which $G : S_n$ acts by permuting the X_i i.e. $\rho(X_i) = X_{\rho(i)}$ for $\rho \in G$. Recall $F^G = \mathbb{Q}(S_1, \dots, S_n)$ (Proposition 8.2). Let $A := \mathbb{Z}[S_1, \dots, S_n]$, a sub-ring of $B := \mathbb{Z}[X_1, \dots, X_n]$. Then SFT (Theorem 8.3) says $B \cap F^G = A$

$B \hookrightarrow F$
$\cup \quad \cup$
$A \hookrightarrow L = F^G$
rings ↑ fields
fractions

Note that the action of G on F restricts to its action on B (permuting X_i), and define the second G-action on the ring $B[T_1, \dots, T_n] = \mathbb{Z}[X_1, \dots, X_n, T_1, \dots, T_n]$ by permuting T_i as $\rho(T_i) = T_{\rho(i)}$. Write $\underline{T}$ for $T_1, \dots, T_n$. Now take a monic of degree $n!$ in X with coefficients in $B[\underline{T}]$:

$$R := \prod_{\sigma \in G} R_\sigma \quad , \quad R_\sigma := X - \sum_{i=1}^{n} \sigma(X_i) T_i = X - (X_{\sigma(1)} T_1 + \dots + X_{\sigma(n)} T_n)$$

$R_\sigma \in B[\underline{T}][X]$

Then the two ~~factor~~ actions of $\rho \in G$ permute the factors R_σ as: $R_\sigma \mapsto R_{\rho\sigma}$ and $R_\sigma \mapsto R_{\sigma\rho^{-1}}$ respectively. In particular, the product R is fixed under both actions of G. As R is fixed by the first action, so is each coefficient of $T_1^{m_1} \dots T_n^{m_n} X$ (elements in B), hence they are in $B \cap F^G = A$. Thus $R \in A[\underline{T}][X]$

Lemma 8.5

Let k be a field. $P := X^n - a_1 X^{n-1} + \dots + (-1)^n a_n \in k[X]$ and E/k be a splitting field of P over k, with

with $\mathrm{Root}_P(E) = \{\alpha_1, \ldots, \alpha_n\}$. This ordering gives the injection $H := \mathrm{Gal}(P) = \mathrm{Gal}(E/k) \hookrightarrow S_n = G$. Let A, B, R and R_σ be as above. Define a ring-homomorphism $\tau : B \to E$ by $\tau(x_i) = a_i$. Then $\tau R = E[I][X]$ lies in $k[I][X]$, and its irreducible factorisation in $k(I)[X]$ is given by $\tau R = \prod_{H\sigma \in H\backslash G} \tau R_{H\sigma}$, where $H\backslash G$ is the set of right cosets, and $R_{H\sigma} := \prod_{\rho \in H\sigma} R_\rho \in B[I][X]$. The stabiliser of $\tau R_{H\sigma} \in k(I)[X]$ under the second G-action is $\sigma^{-1} H \sigma$

Proof (of Lemma)

As τ is a ring-homomorphism, $\tau R = \prod_{\sigma \in G} \tau R_\sigma$ in $E[I][X]$. As $\tau(S_i) = a_i$, we know $\tau(A) \subset k$. Since $R \in A[I][X]$ we have $\tau R \in k[I][X]$. For each coset $H\sigma$, the polynomial, $R_{H\sigma} \in B[I][X]$ is fixed by the first action of $H \subset G$. Note that the 1st action of $H \subset G$ on X_i is sent by τ to the $H = \mathrm{Gal}(E/k)$ action on the α_i. Hence $\tau R_{H\sigma} \in B[I][X]$ is fixed by the first action of $H = \mathrm{Gal}(E/k)$. Therefore, so is each coefficient of $T_1^{m_1} \ldots T_n^{m_n} X$ (elements in E) thus they are in $E^H = k$ (Proposition 33;)). Hence $\tau R = \prod_{H\sigma \in H\backslash G} \tau R_{H\sigma}$ in $k[I][X]$. We show that this is the irreducible factorisation in $k(I)[X]$. If Q is a monic irreducible factor of τR in $k(I)[X]$, such that $\tau R_\sigma \mid Q$ in $E(I)[X]$, then for

$$\begin{array}{ccc} B & \to & E \\ \cup & & \cup \\ A & \to & k \end{array}^H$$

every $\rho \in H$, we have $\tau R_{\rho\sigma} = \tau(\rho(R_\sigma)) = \rho(\tau(R_\sigma)) \mid \rho Q = Q$ ($\because \rho|_K = id$). As each $\tau R_{\rho\sigma}$ is a distinct linear polynomial their product $\tau R_{H\sigma}$ must divide Q in $E(I)[X]$, hence also in $K(I)[X]$. Hence $\tau R_{H\sigma} = Q$.

Now that the second G-action on T_i is simply sent by τ to the G-action on T_i, we have that $\rho \in G$ sends $\tau R_{H\sigma}$ to $\tau R_{H\sigma\rho^{-1}}$, and ρ fixes it iff $\rho \in \sigma^{-1} H \sigma$ □

Now we finish the proofs of Theorem 84.

Let $P = X^n - a_1 X^{n-1} + \dots + (-1)^n a_n \in \mathbb{Z}[X]$ with its splitting field $E/\mathbb{Q}$ and $Root_P(E) = \{\alpha_1, \dots, \alpha_n\}$, so that $H := Gal(P) = Gal(E/\mathbb{Q}) \subset G$. Define $\tau : B \to E$ as in Lemma 85 by $X_i \mapsto \alpha_i$. Then $\tau(S_i) = a_i$, hence $\tau R \in \mathbb{Z}[I][X]$.

By Gauss' Lemma, the irreducible factorisation of τR monic in $\mathbb{Z}[I][X]$ is the same as the irreducible factorisation in $\mathbb{Q}(I)[X]$, since $\mathbb{Z}[X]$ is a UFD (handout) and $\mathbb{Q}(I) = Frac(\mathbb{Z}[I])$.

Similarly, for $P \bmod p \in \mathbb{F}_p[X]$, let $\mathbb{F}_q / \mathbb{F}_p$ be its splitting field with the roots $\beta_1, \dots, \beta_n$ in $\mathbb{F}_q$, so that $H' := Gal(P_{\bmod p}) = Gal(\mathbb{F}_q/\mathbb{F}_p) \subset G$.

Define $\tau' : B \to \mathbb{F}_q$ by $X_i \mapsto \beta_i$. Then $\tau'(S_i) = a_i \bmod p$ Hence $\tau' R = \tau R \bmod p \in \mathbb{F}_p[I][X]$.

Its factorisation in $\mathbb{F}_p[\underline{T}][X]$ respects the factorisation of τR in $\mathbb{Z}[\underline{T}][X]$, i.e. each $\tau' R_{H\sigma} \in \mathbb{F}_p[\underline{T}][X]$ must divide the mod p of some $\tau R_{H\sigma} \in \mathbb{Z}[\underline{T}][X]$.

As the 2nd G-action (permuting T_i) is compatible with mod p the stabiliser $\sigma'^{-1} H' \sigma'$ of the former is contained in the stabiliser $\sigma^{-1} H \sigma$ of the latter. Hence $H' \subset \sigma' \sigma^{-1} H \sigma \sigma'^{-1}$

□

$$\begin{array}{ccccc} E & \xleftarrow{\tau} & B & \xrightarrow{\tau'} & \mathbb{F}_q \\ \cup & & \cup & & \cup \\ \mathbb{Q} & \longleftarrow & A & \longrightarrow & \mathbb{F}_p \end{array} \quad \begin{matrix} H \\ \big) \\ H' \end{matrix}$$

3. Modern Galois Theory (Linear Algebraic Approach)

How do we rebuild Galois theory using more linear algebra, without ever mentioning polynomials? PET is avoided.

We only assume Definitions 1 and 2, Proposition 8, Definition 12 Lemma 11, 22 i), ii)

3.1 Dedekind's and Artin's Lemma

Lemma 86

Let V be a finite dimensional k-vector space, and E/k an extension. Let $\mathrm{Hom}_{k\text{-vs}}(V, E)$ be the set of all k linear maps $V \to E$, and define the addition and E-action by

$(\rho + \rho')(x) := \rho(x) + \rho'(x)$, $(a\rho)(x) := a\rho(x)$

$(\forall x \in V, \forall \rho \in \mathrm{Hom}_{k\text{-vs}}(V, E))$. Then it is an E-vector space with $\dim_E(\mathrm{Hom}_{k\text{-vs}}(V, E)) = \dim_k V$

Proof

It satisfies the axioms of an E-vector space. Let $\{e_1, \dots, e_n\}$ be a basis of V. If we define $\rho_i \in \mathrm{Hom}_{k\text{-vs}}(E)$ by $\rho_i(a_1 e_1 + \dots + a_n e_n) = a_i$, then every ρ is uniquely written as

$\rho = \rho(e_1)\rho_1 + \dots + \rho(e_n)\rho_n$ $\left(\because \rho(x) = \rho\left(\sum_i a_i e_i\right)\right.$

$\left. = \sum_i a_i \rho(e_i) = \sum_i \rho_i(x)\rho(e_i) \in E\right)$. Hence $\{\rho_1, \dots, \rho_n\}$ is a basis of $\mathrm{Hom}_{k\text{-vs}}(V, E)$ as an E-vector space

□

Proposition 87 (Dedekind's Lemma)

Let F/k be a finite extension. Then for any extension E/k, the subset $\mathrm{Hom}_k(F,E)$ of the E-vector space $\mathrm{Hom}_{k\text{-vs}}(F,E)$ is E-linearly independent. In particular

$|\mathrm{Hom}_k(F,E)| \leq [F:k]$ (by Lemma 86)

Remark

We proved this $\leq$ in Proposition 76.

Proof:

We prove that any finite subset $\{\rho_1, \dots, \rho_k\}$ of $\mathrm{Hom}_k(F,E)$ is E-linearly independent, by induction on k. Let

$a_1\rho_1 + \dots + a_k\rho_k = 0$ (*) be an E-linear relation. If $k=1$ then $\rho_1 \neq 0$ so $a_1 = 0$, hence the claim.

Let $k \geq 1$. For any $x, y \in F$, we have

$a_1\rho_1(x)\rho_1(y) + \dots + a_k\rho_k(x)\rho_k(y) = a_1\rho_1(xy) + \dots + a_k\rho_k(xy)$, with the right-hand side $= 0$.

As y is arbitrary, as a k-linear map (i.e. in $\mathrm{Hom}_{k\text{-vs}}(F,E)$)

$a_1\rho_1(x)\rho_1 + \dots + a_k\rho_k(x)\rho_k = 0$

Now multiply (*) by $\rho_k(x)$ to get

$a_1\rho_k(x)\rho_1 + \dots + a_k\rho_k(x)\rho_k = 0$, so subtracting

$a_1(\rho_1(x) - \rho_k(x))\rho_1 + \dots + a_{k-1}(\rho_{k-1}(x) - \rho_k(x))\rho_{k-1} = 0$

Then all coefficients are 0 by the induction hypothesis, and as x is arbitrary, we have $a_i(\rho_i - \rho_k) = 0$ $(1 \leq i \leq k-1)$

If $a_i \neq 0$, then multiplying by a_i^{-1} gives $\rho_i = \rho_k$ ✗

Hence $a_i = 0$ $(1 \leq i \leq k-1)$. The case $k=1$ gives $a_k = 0$ □

This implies that $|Aut_K(F)| \leq [F:k]$ for finite F/k (Lemma 22 iii)

Now recall Definition 23, Lemma 32. Then Proposition 33 i) (F/k Galois $\Rightarrow F^G = k$) follows. We do Proposition 33 ii) next.

Proposition 88 (Artin's Lemma)

Let F/k be any extension. If G is a finite subgroup of $Aut_k(F)$ then F/F^G is Galois and $Gal(F/F^G) = G$.

Proof:

Let $G = \{\rho_1, \ldots, \rho_n\}$ $(\rho_1 = id)$ and write $\rho(x) := (\rho_1(x), \ldots, \rho_n(x))$ which is in F^n for $x \in F$. For $\underline{x} = (x_1, \ldots, x_n) \in F^n$ and $\rho \in G$ write $\rho(\underline{x}) := (\rho(x_1), \ldots, \rho(x_n))$. Then $\rho(a\underline{x}) = \rho(a) \cdot \rho(\underline{x})$, since ρ is a ring homomorphism, and the components of $\rho(\rho(x)) = (\rho\rho_1(x), \ldots, \rho\rho_n(x)) \in F^n$ are a permutation of those of $\rho(x)$. Hence if $a_1\rho(x_1) + \ldots + a_k\rho(x_k) = 0$ (*) for $a_1, \ldots, a_k \in F$, then $\rho(a_1)\rho(x_1) + \ldots + \rho(a_k)\rho(x_k) = 0$ (✱) by applying ρ to (*).

Now we prove that if $\{x_1, \ldots, x_k\}$ is an F^G linearly independent subset of F then $\{\rho(x_1), \ldots, \rho(x_k)\}$ is F-linearly independent in F^n, which implies that $k \leq n = |G|$. Use induction on k.

If $k=1$, then $\rho(x_1) \neq 0$ since $x_1 \neq 0$, so this is ok.
Assume an F-linear relation (*). Replacing a_i by a_i/a_k when $a_k \neq 0$, we can assume $a_k = 0$ or 1. Then as $\rho(a_k) = a_k$ for all $\rho \in G$, (*) $-\rho$(*) gives

$$(a_1 - \rho(a_1))\rho(x_1) + \dots + (a_{k-1} - \rho(a_{k-1}))\rho(x_{k-1}) = 0$$

The induction hypothesis shows that all coefficients are zero, and since ρ was arbitrary, we have $a_i \in F^G$ $(1 \le i \le k-1)$. Now the first component of (*) reads $a_1 x_1 + \dots + a_k x_k = 0$ $(\because \rho_1 = id)$ and the F^G-linear independence of $\{x_1, \dots, x_n\}$ implies that all a_i are 0. Thus F/F^G is finite with $[F : F^G] \le n = |G|$
Since we had $|G| \le |Aut_{F^G}(F)| \le [F : F^G]$ already, $|Aut_{F^G}(F)| = [F : F^G]$ and $G = Gal(F/F^G)$ □

3.2 Towers of Extensions

We almost reproved FTGT (Theorem 34). It remains to prove that for $k \subset L \subset F$, F/k Galois $\Rightarrow$ F/L Galois.
To deal with the towers, we generalise the notion of extensions.

Definitions

Let k be a field. We call a pair (F, τ) of a field F and a ring homomorphism $\tau : k \to F$ an extension of k, and denote it by F_τ.

A <u>morphism</u> $\rho : F_\tau \to F'_{\tau'}$ of extensions is a ring homomorphism $\rho : F \to F'$ such that $\rho\tau = \tau'$.

$\tau \nwarrow_K \quad \nearrow_{\tau'}$

We denote the set of all morphisms from F_τ to $F'_{\tau'}$ by $\mathrm{Hom}(F_\tau, F'_{\tau'})$. If ρ is bijective, then ρ^{-1} is also a morphism, and we call ρ an <u>isomorphism</u>. An <u>automorphism</u> of F_τ is an isomorphism from F_τ to itself and $\mathrm{Aut}(F_\tau)$ is the group of all automorphisms of F_τ

<u>Remark</u>

K and $\tau(K)$ are isomorphic (<u>Lemma 11</u>) and $F/_{\tau(K)}$ is an extension in our previous sense.

22/11/12

Galois Theory (22)

3-2 Towers of Extensions (continued)

Recall: Extension F_τ of k - homomorphism $\tau: k \to F$

Morphism $F_\tau \xrightarrow{\rho} F'_{\tau'}$ - homomorphism $\rho: F \to F'$

$$\begin{array}{ccc} & & F' \\ & \tau \nearrow & \uparrow \tau' \\ k & & \end{array}$$

$$\begin{array}{ccc} F & & F \\ | & \tau \nearrow & | \\ L & & \\ | & k \xrightarrow{\cong} \tau(k) & \\ k & & \end{array}$$

Remark

If $F_\tau, F'_{\tau'}$ are extensions in our previous sense (i.e. τ, τ' are inclusion maps) then $\rho\tau = \tau'$ means $\rho|_k = id$ i.e. morphisms are just k-homomorphisms. Every morphism is injective (Lemma 11) and τ is itself a morphism, $\tau: k_{id} \to F_\tau$. If ρ is an automorphism of F_τ then $\rho|_{\tau(k)} = id$ hence $Aut(F_\tau) = Aut_{\tau(k)}(F)$

Let k be a field.

Definition 90

Let F_τ be an extension of k. We consider F as a k-vector space by letting $x \in k$ act on F via multiplication by $\tau(x)$ in F. We say that F_τ is <u>finite</u> if it is a finite dimensional k-vector space and let $[F_\tau] := \dim_k F$ be its <u>degree</u>. A finite extension is called <u>Galois</u> if $|Aut(F_\tau)| = [F_\tau]$

Remark

We have $[F_\tau] = [F : \tau(k)]$. If $[F_\tau] = 1$ then τ is

bijective and $\tau(k) = F$. Morphisms are injective k-linear maps so $\mathrm{Aut}(F_\tau) = \mathrm{Hom}(F_\tau, F_\tau)$ for finite F_τ by Rank-Nullity.

Lemma 91

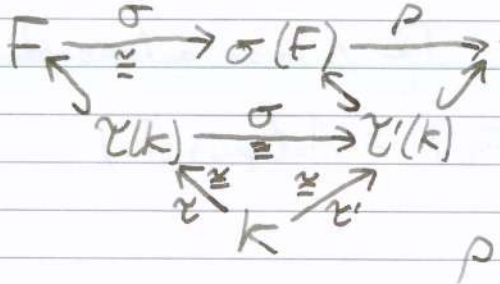
If $\sigma \in \mathrm{Hom}(F_\tau, F'_{\tau'})$, then $\sigma(F), F'$ are extensions of $\tau(k)$ in our previous sense, and we have a bijection

$$\mathrm{Hom}_{\tau'(k)}(\sigma(F), F') \ni \rho \xmapsto{\cong} \rho\sigma \in \mathrm{Hom}(F_\tau, F'_{\tau'})$$

In particular, if F_τ is finite, then $|\mathrm{Hom}(F_\tau, F'_{\tau'}) \leq [F_\tau]$ by Dedekind (Proposition 87)

Proof

In the diagram, $\hookrightarrow$ indicates inclusion maps. As $\rho|_{\tau'(k)} = \mathrm{id}$ implies $\rho\sigma\tau = \tau'$ we have the claimed map. We have the inverse map $\rho' \mapsto \rho'\sigma^{-1}$ since $\rho'\tau = \tau'$ implies that $\rho'\sigma^{-1}|_{\tau(k)} = \rho'\tau\tau'^{-1} = \mathrm{id}$. If $[F_\tau]$ is finite, then so is the extension $\sigma(F)\sigma$ of $\tau(k)$, hence so is $\sigma(F)/\tau'(k)$



Definition 92

Let L_τ be an extension of k, and F_σ an extension of L: $k \xrightarrow{\tau} L \xrightarrow{\sigma} F$. Then $\sigma\tau : k \to F$ is an extension $F_{\sigma\tau}$ of k. We call this a tower L_τ, F_σ, of extensions.

Proposition 93

Let L_τ, F_σ be a tower.

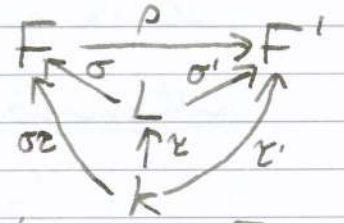
22/11/12

Galois Theory 22

i) If $F'_{\tau'}$ is an extension of k, then the set $\mathrm{Hom}(F_{\sigma\tau}, F'_{\tau'})$ is a disjoint union of $\mathrm{Hom}(F_\sigma, F'_{\sigma'})$ for each $\sigma' \in \mathrm{Hom}(L_\tau, F'_{\tau'})$. In particular, $\mathrm{Aut}(F_\sigma)$ is a subgroup of $\mathrm{Aut}(F_{\sigma\tau})$

ii) $F_{\sigma\tau}$ finite $\Leftrightarrow$ F_σ, L_τ finite

If this holds then $[F_{\sigma\tau}] = [F_\sigma][L_\tau]$



iii) Suppose L_τ, F_σ are finite. If $F_{\sigma\tau}$ is Galois, then so is F_σ

Proof

i) If $\rho \in \mathrm{Hom}(F_{\sigma\tau}, F'_{\tau'})$, then $\sigma' := \rho\sigma : L \to F'$ is an extension $F'_{\sigma'}$ of L, and $\rho \in \mathrm{Hom}(F_\sigma, F'_{\sigma'})$. Then $\sigma'\tau = \rho\sigma\tau = \tau'$ shows $\sigma' \in \mathrm{Hom}(L_\tau, F'_{\tau'})$. Conversely, if $\sigma' \in \mathrm{Hom}(L_\tau, F'_{\tau'})$ and $\rho \in \mathrm{Hom}(F_\sigma, F'_{\sigma'})$ then $\rho\sigma\tau = \sigma'\tau = \tau'$ shows $\rho \in \mathrm{Hom}(F_{\sigma\tau}, F'_{\tau'})$

ii) (The same as Proposition 8, the tower law)

iii) As $F_{\sigma\tau}$ is Galois, ~~suppose~~ ii) says that $|\mathrm{Aut}(F_{\sigma\tau})| = [F_{\sigma\tau}] = [F_\sigma][L_\tau]$

Applying i) to $F'_{\tau'} = F_{\sigma\tau}$, together with the Remark after Definition 90 gives $|\mathrm{Aut}(F_{\sigma\tau})| \underset{\text{Remark}}{=} |\mathrm{Hom}(F_{\sigma\tau}, F_{\sigma\tau})| = \sum_{\sigma' \in \mathrm{Hom}(L_\tau, F_{\sigma\tau})} |\mathrm{Hom}(F_\sigma, F'_{\sigma'})|$

But $|\mathrm{Hom}(L_\tau, F_{\sigma\tau})| \leq [L_\tau]$, $|\mathrm{Hom}(F_\sigma, F'_{\sigma'})| \leq [F_\sigma]$, by Lemma 91, hence both are equalities. In particular, for $\sigma' = \sigma$ we have $|\mathrm{Aut}(F_\sigma)| = [F_\sigma]$ □

This iii) gives FTGT (Theorem 34). Corollary 35 is proved as in the proof of Proposition 79 since $|\mathrm{Hom}(L_\tau, F_{\sigma\tau})| = [L_\tau]$ and $\mathrm{Hom}(F_\sigma, F'_{\sigma'}) \neq \emptyset$ for each σ' (shown above).

3.3 Traces and Norms

We return to our old notion of extensions (L/k means $K \subset L$)

Definition 9.4

Let L/k be a finite extension. For $\alpha \in L$, let $m_\alpha : L \to L$ be the multiplication by α map $m_\alpha(\beta) := \alpha\beta$ $(\forall \beta \in L)$, viewed as a k-linear transformation of the k-vector space L. We define the trace $T_{L/k}(\alpha)$ and the norm $N_{L/k}(\alpha)$, as the trace/determinant of m_α:

$T_{L/k}(\alpha) := tr(m_\alpha)$, $N_{L/k} := \det(m_\alpha)$

If $\{\beta_1, \dots, \beta_n\}$ is a basis of L as a k-vector space then $m_\alpha(\beta_j) = \alpha\beta_j = \sum_{i=1}^{n} \beta_i a_{ij}$ $(a_{ij} \in k)$, and m_α is represented by a matrix $A := (a_{ij}) \in M_n(k)$, so $T_{L/k}(\alpha) = tr(A)$ and $N_{L/k}(\alpha) = \det A$. From Linear Algebra

$\alpha \neq 0 \Leftrightarrow m_\alpha$: invertible $\Leftrightarrow N_{L/k}(\alpha) = \det(m_\alpha) \neq 0$

Example

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ $\quad 1 \leftrightarrow \begin{pmatrix}1\\0\end{pmatrix}$, $\sqrt{2} \leftrightarrow \begin{pmatrix}0\\1\end{pmatrix}$

$(1+\sqrt{2})\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$, $(1+\sqrt{2})\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}2\\1\end{pmatrix}$

$m_{1+\sqrt{2}}$ represented by $\begin{pmatrix}1 & 2\\ 1 & 1\end{pmatrix}$

$T_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1+\sqrt{2}) = 2$

$N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = -1$

3.3 Traces and Norms (continued)

Recall L/k a finite extension, $\alpha \in L$, $m_\alpha : \begin{matrix} L \to L \\ \beta \mapsto \alpha\beta \end{matrix}$

$T_{L/k}(\alpha) = tr(m_\alpha)$ $\quad$ $N_{L/k}(\alpha) = \det(m_\alpha)$

Lemma 95

Let L/k be a finite extension

i) $T_{L/k} : L \to k$ is k-linear and $N_{L/k} : L^* \to k^*$ is a (multiplicative) group homomorphism.

ii) If $[L:k] = n$ and $x \in k$, then $T_{L/k}(x) = nx$, $N_{L/k}(x) = x^n$

Proof

i) $tr(A+B) = tr(A) + tr(B)$, $tr(xA) = x \cdot tr(A)$, $\det(AB) = \det(A)\det(B)$

ii) tr, det of the scalar matrix $x I_n$ $\square$

a) Traces "can see" the separability.

Lemma 96

Let L/k be a finite extension.

i) If $L = k(\alpha)$ and $P_\alpha = X^n + a_1 X^{n-1} + \dots + a_n \in k[X]$ is the minimal polynomial of $\alpha \in L$, then $T_{L/k}(\alpha) = -a_1$, $N_{L/k}(\alpha) = (-1)^n a_n$

ii) If $k \subset L \subset F$ with F/k finite, then we have $T_{F/k} = T_{L/k} \circ T_{F/L}$ (in fact the same holds for norms)

Proof

i) For the basis $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ of L/k, the matrix of m_α is $\begin{pmatrix} 0 & & & -a_n \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_2 \\ 0 & & 1 & -a_1 \end{pmatrix}$ since $\alpha^n = -a_1 \alpha^{n-1} - \dots - a_{n-1}\alpha - a_n$

ii) Let $\{\beta_1, \dots, \beta_n\}$ be a basis of L/k and $\{r_1, \dots, r_m\}$ be a basis of F/L. For $\alpha \in F$, let $(\beta_{ij}) \in M_n(L)$ be the matrix for $m_\alpha : F \to F$ (as an L-vector space) and for each β_{ij}, let $A_{ij} \in M_n(k)$ be the matrix for $m_{\beta_{ij}} : L \to L$ (as a k-vector space). Then, with respect to the k-basis $\{r_1\beta_1, \dots, r_1\beta_n, r_2\beta_1, \dots, r_m\beta_n\}$ of F, the matrix for $m_\alpha : F \to F$ (as a k-vector space) is $A = \begin{pmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & & \vdots \\ A_{m1} & \cdots & A_{mm} \end{pmatrix} \in M_{mn}(k)$.

Thus $T_{F/k}(\alpha) = \operatorname{tr}(A) = \sum_{i=1}^{m} \operatorname{tr}(A_{ii})$

$= \sum_{i=1}^{m} T_{L/k}(\beta_{ii}) = T_{L/k}\left(\sum_{i=1}^{m} \beta_{ii}\right) = T_{L/k}(\operatorname{tr}(\beta_{ij})) = T_{L/k}(T_{F/L}(\alpha))$ □

Proposition 97

If F/k is finite and not separable, then $T_{F/k} = 0$ (zero map)

Proof

Take $\alpha \in F$ such that its minimal polynomial P_α is not separable, hence $P_\alpha(x) = Q(x^p)$ for $Q \in k[x]$, where $\operatorname{char} k = p > 0$ (Lemma 73 ii)). Then $k \subset L := k(\alpha^p) \subset L' := k(\alpha) \subset F$ and $L' = L(\alpha)$. As P_α is irreducible in $k[x]$, so is Q. Hence Q is the minimal polynomial of α^p over k. Therefore $[L : k] = \deg Q$ and $[L' : k] = \deg P_\alpha = p \cdot \deg Q$, hence $[L' : L] = p$ (Tower Law).

Let $1 \le i \le p-1$. If $\alpha^i \in L$, then $\alpha^p \in L$ implies $\alpha \in L$, which is false. Hence $\alpha^i \notin L$ and $L(\alpha^i) = L'$, so the minimal polynomial of α^i over L is $x^p - (\alpha^p)^i \in L[x]$.

Thus $T_{L'/L}(\alpha^i) = 0$ by Lemma 96 ii). Also $T_{L'/L}(1) = p \cdot 1 = 0$ (Lemma 95 iii)). As $\{1, \alpha, \ldots, \alpha^{p-1}\}$ is a basis for L'/L and $T_{L'/L}$ is L-linear (Lemma 95 i)) we get $T_{L'/L} = 0$. Thus $T_{F/k}$ has $T_{F/k} = T_{L/k} \circ T_{L'/L} \circ T_{F/L'} = 0$ by Lemma 96 ii) □

Proposition 98

Let F/k be separable with $[F:k] = n$. Take E/k with $\mathrm{Hom}_k(F, E) = \{\tau_1, \ldots, \tau_n\}$ (it exists by Theorem 77 i) (a) $\Leftrightarrow$ (b) taking $\mathbb{C}$ if $F \subset \mathbb{C}$). Then $T_{F/k}(\alpha) = \hat{\sum_{i=1}} \tau_i(\alpha)$, $N_{F/k}(\alpha) = \hat{\prod_{i=1}} \tau_i(\alpha)$ where $\alpha \in F$.

Proof

Let $\{\beta_1, \ldots, \beta_n\}$ be a basis for F/k. As $\tau_1, \ldots, \tau_n$ are E-linearly independent in $\mathrm{Hom}_{k\text{-vs}}(F, E)$ by Dedekind (Proposition 87), the vectors $(\tau_i(\beta_j)) \in E^n$ $(1 \leq i \leq n)$ must be E-linearly independent hence the matrix $P := (\tau_i(\beta_j)) \in M_n(E)$ is invertible.

For $\alpha \in F$, let $A := (a_{ij}) \in M_n(k)$ with $\alpha\beta_j = \hat{\sum_{k=1}} \beta_k a_{kj}$. Then $\tau_i(\alpha)\tau_i(\beta_j) = \hat{\sum_{k=1}} \tau_i(\beta_k) a_{kj}$ $(1 \leq i \leq n)$. If A' is the diagonal matrix with entries $\tau_1(\alpha), \ldots, \tau_n(\alpha)$ then this reads $A'P = PA$, i.e. $A' = PAP^{-1}$ in $M_n(E)$. Hence $T_{F/k}(\alpha) = \mathrm{tr}(A) = \mathrm{tr}(A')$ $N_{F/k}(\alpha) = \det(A) = \det(A')$ □

Theorem 99

If F/k is a finite extension, F/k separable $\Leftrightarrow$ $T_{F/k} \neq 0$.

Proof

($\Leftarrow$) By Proposition 97

($\Rightarrow$) Let E/k be as in Proposition 98. Then $T_{F/k} : F \to k \subset E$ is just $T_{F/k} = \tau_1 + .. + \tau_n \in \mathrm{Hom}_{k\text{-vs}}(F, E)$, which is $\neq 0$ by Dedekind (Proposition 87) $\square$

Remark

Theorem 99 and Lemma 96 ii) $\Rightarrow$ Theorem 77 ii)

b) Norms and cyclic extensions

Theorem 100 (Hilbert's Theorem 90)

Let F/k be a cyclic extension, and σ be a generator of $\mathrm{Gal}(F/k)$. If $N_{F/k}(\alpha) = 1$, then there exists $\beta \in F$ with $\alpha = \beta / \sigma(\beta)$.

Proof

Let $[F:k] = n$. By Dedekind (Proposition 87) the subset $\{id, \sigma, ..., \sigma^{n-1}\}$ of $\mathrm{Hom}_{k\text{-vs}}(F, F)$ is F-linearly independent. Hence $\sum_{i=1}^{n} (\alpha \cdot \sigma(\alpha) \dots \sigma^{i-1}(\alpha))\sigma^i \neq 0$. So take $r \in F$ such that $\sum_{i=1}^{n} (\alpha \cdot \sigma(\alpha) \dots \sigma^{i-1}(\alpha))\sigma^i(r) =: \beta \neq 0$

Applying σ to the above gives $\sigma(\beta) = \sum_{i=1}^{n} (\sigma(\alpha)\sigma^2(\alpha) \dots \sigma^i(\alpha))\sigma^{i+1}(r)$ and since $\alpha \cdot \sigma(\alpha) \dots \sigma^{n-1}(\alpha) = N_{F/k}(\alpha) = 1$, we see $\beta = \alpha \cdot \sigma(\beta)$ $\square$

Corollary 101 (Kummer Theory)

Let $\mu_N \subset K$ with $(\text{char } k, N) = 1$, hence K has a primitive N^{th} root of 1 (ζ of 1). If F/K is cyclic of degree N, then $F = K(\sqrt[N]{a})$ for some $a \in K$

Proof

As $N_{F/K}(\zeta) = \zeta^N = 1$ by Lemma 95 ii), then by Theorem 100 there is $\beta \in F$ with $\beta/\sigma(\beta) = \zeta$ i.e. $\sigma(\beta) = \zeta\beta$. Then $a = \beta^N$ will do (see proof of Theorem 47) □

Remark

Lagrange resolvent $x : \alpha + \beta\zeta + \gamma\zeta^2$ for cubics (see 1.11) is the element satisfying $x/\sigma(x) = \zeta$ where $\sigma = (\alpha\ \beta\ \gamma)$ so is the special case of above.

Hilbert 90 generalises Kummer Theory, in turn generalised to arbitrary Galois extensions (Galois Cohomology)

3.4 Infinite Extensions

a) What was it all about?

Let k be a field. Galois Theory $/k$ is the theory of fields that are finite dimensional k-vector spaces (finite extensions) and morphisms i.e. k-homomorphisms (k-linear ring homomorphisms) between them.

Principle of Category Theory: sets of morphisms control the objects.

FTGT: Galois Groups (automorphism groups $Aut_k(F) = Hom_k(F,F)$) control the fields. 19C (concrete) algebra → 20C (abstract) algebra

1. Equations ⟶ Fields (rings) $\quad P \in k[x]$, irreducible $\rightarrow k_p := \frac{k[x]}{k}$
2. Solutions (roots) → Ring homomorphisms

E/k an extension $\quad Root_p(E) \xrightarrow{\cong} Hom_k(k_p, E), \quad \alpha \mapsto (x \bmod p \mapsto \alpha)$

Principle of Algebraic Geometry (over any ring k)

1. Any ring A, finitely generated over k is a quotient ring of a polynomial ring $A = k[x_1, \ldots, x_n]/I$ with I an ideal. Here $I = (f_1, \ldots, f_m)$ and f_i are the "equations" in $x_1, \ldots, x_n$ over k.
2. A "solution" of these equations in a ring E is a ring homomorphism $A \to E$ e.g. $x, y \in \mathbb{Q}$ of $x^n + y^n = 1$ (only $xy = 0$ for $n > 2$) is equivalent to a ring homomorphism $\frac{\mathbb{Q}[X,Y]}{(X^n+Y^n-1)} \to \mathbb{Q}$ with $\begin{matrix} X \mapsto x \\ Y \mapsto y \end{matrix}$

b) Subfields of algebraic closures, and the absolute Galois groups.

Definition 102

Let E/k be an extension, and F, F' be subfields of

E containing k. Their <u>composite field</u> FF' is the intersection of all subfields of E containing F, F' i.e. the minimal such subfield. If $F = k(\alpha_1, \dots, \alpha_n)$ and $F' = k(\beta_1, \dots, \beta_m)$ then $FF' = k(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$. So if F, F' are finite then so is FF'/k

<u>Lemma 103</u>

Let F, F', E be as above, with F/k, F'/k finite.

i) If F/k, F'/k are separable (respectively Galois, soluble, abelian) then so is FF'/k.

ii) Let $E = \bar{k}$ be an algebraic closure of k. Let k^{sep} (resp k^{sol}, k^{ab}, k^{cyc}) be the union of all finite (separable, soluble, abelian, cyclotomic) extensions of k inside $\bar{k}$. Then they are fields, hence algebraic extensions. The field k^{sep}, called a <u>separable closure</u> of k, is equal to the union of all finite Galois extensions of k inside $\bar{k}$.

<u>Proof</u>

i) <u>Theorem 77</u> i) d) $\Rightarrow$ b) iii) c) $\Rightarrow$ a) imply the separable and Galois cases. Now $Gal(FF'/k) \ni \sigma \mapsto (\sigma|_F, \sigma|_{F'}) \in Gal(F/k) \times Gal(F'/k)$ is injective. The soluble / abelian cases follow.

ii) For each family of subfields, any two members are contained in a larger member by i), so the union is a field (for cyclotomic,

note $k(\mu_N), k(\mu_{N'}) \subset k(\mu_{NN'})$). Any finite separable extension $F = k(\alpha_1, \ldots, \alpha_n)$ is contained in the splitting field (inside $\bar{k}$) of the product of the minimal polynomials of α_i over k, which is Galois (Proposition 79). □

Definition 104

An algebraic extension F/k (not necessarily finite) is called a Galois Extension if it is a union of finite Galois extensions. The group $G_k := \mathrm{Gal}(k^{sep}/k)$, well defined up to isomorphism, is called the absolute Galois group of k.

By Lemma 103, for any field k, we have a sequence of Galois extensions $k \subset k^{cyc} \subset k^{ab} \subset k^{sol} \subset k^{sep} \subset \bar{k}$.

Every finite Galois extension F/k has a k-isomorphic copy inside k^{sep}. If $F \subset k^{sep}$ then every element of $\mathrm{Gal}(F/k)$ can be extended to k^{sep} using Proposition 76 ii) hence $\sigma \to \sigma|_F$ gives a surjection $G_k \to \mathrm{Gal}(F/k)$

c) Algebra Abel/Galois $\Rightarrow k^{sol} \neq \bar{k}$ in general.

Little can be said about G_k for general k.

On the contrary, G_k knows a lot about each specific field k.

Example

i) $k = \mathbb{F}_p$. Then $\mathbb{F}_p^{cyc} = \ldots = \overline{\mathbb{F}_p}$

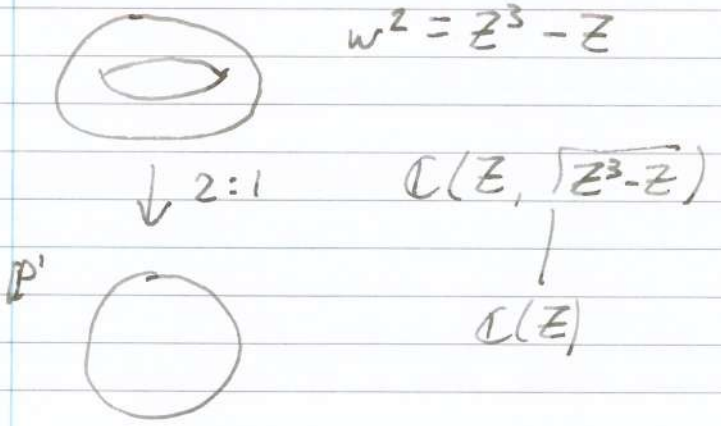
ii) $k = \mathbb{Q}_p$. We know $\mathbb{Q}^{cyc} = \mathbb{Q}$ (Kronecker-Weber Theorem)

For every finite soluble group G, there is a Galois extension $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) = G$ (Shefarevich Theorem). Is it true for an arbitrary finite group? (Inverse Galois Problem)

iii) $k/\mathbb{Q}$ finite (number fields). Class field theory describes $\mathrm{Gal}(k^{ab}/k)$

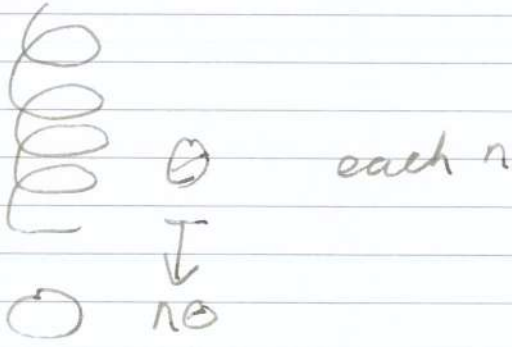
In some cases k^{ab} is understood via modular / elliptic functions (this is where Abel started).

Geometry



$G_k \sim$ fundamental groups

e.g. $\mathbb{F}_p$ has cyclic deg n extension, each n



HANDOUT 5: WHAT NEXT?

Galois Theory is related to many areas of pure mathematics.

Part II courses.

(A) *Number Fields*. Natural continuation of our study of Galois groups over $\mathbb{Q}$ leads to *algebraic number theory*. By defining the ring of integers for *number fields* (finite ext'ns of $\mathbb{Q}$), the contents of §2.4, §2.7 receive a cleaner treatment and further generalisations.

(B) *Algebraic Geometry*. The theory of finite ext'ns of fields is nothing other than 0-dimensional algebraic geometry. Algebraic manipulations of function fields (with many variables) and their subrings are imbued with geometric intuitions by the study of *algebraic varieties* (geometric objects defined as zero sets of polynomials in many variables).

(C) *Riemann Surfaces, Algebraic Topology*. 1-dim'l algebraic geometry over $\mathbb{C}$ grew out of complex analysis via theory of Riemann surfaces. The function fields over $\mathbb{C}$ appear as fields of meromorphic functions, which are at first treated by analytical methods. Geometry of complex manifolds, including their topological properties, are translated into algebraic theory of fields. Topological analogues of the field ext'ns and their Galois groups are the *covering spaces* and the *fundamental groups* in algebraic topology.

(D) *Representation Theory*. The Fundamental Theorem of Galois Theory says that the symmetry groups (automorphism groups) control mathematical objects — then in turn one can study a group by studying how it acts on various objects. Representations are the most important examples of this principle, namely vector spaces on which a group acts.

Further afield.

Progress in many areas of maths and physics were philosophically based on Galois Theory, but here we mention some research areas directly connected to Galois Theory.

(A) *Categories, Schemes, Toposes*. FTGT can be seen as a classification of fields in terms of objects (here Hom sets) acted on by the Galois group. This is best understood in the language of *categories*. Grothendieck pushed this idea further to revolutionise algebraic geometry by the theory of *schemes* and *toposes*, where Galois groups and fundamental groups are unified. Now Galois Theory is an example of *descent theory*, obtaining global objects by glueing local objects.

(B) *Number Theory*. There are many unsolved mysteries on the absolute Galois group of $\mathbb{Q}$, not only the inverse Galois problem. Its representations, *Galois representations*, are the main object of study in modern algebraic number theory (e.g. solution of Fermat's Last Theorem). Generalising *class field theory* (the theory of abelian ext'ns of number fields), deep connections with algebraic geometry and representation theory (*modular forms*) are proposed (*the Langlands program*).

(C) *Arithmetic Geometry*. Grothendieck's reformulation of Galois Theory lead to the conjectural existence of the *motivic Galois group*, a huge extension of the absolute Galois group of a field, which controls the motives (cohomology theories) of algebraic varieties of arbitrary dim'n (as opposed to 0-dim'n in Galois Theory). The theory rests on many unsolved conjectures, but gives a dream vision of a vastly extended Galois Theory.

Review of §§2–3.

Def. 52: Characteristics, prime fields. Lem. 53: $K[X]$ is a UFD; $|\mathrm{Root}_P(K)| \leq \deg P$.

Def. 54: Splits in E, splitting fields.

Lem. 55: Splits $\iff$ $\exists K$-hom from a splitting field; $|\mathrm{Root}_P(E)|$ constant when split.

Prop. 56: Splitting field exists, unique up to K-isom.

Def. 57: Algebraically closed, alg. closures. Th. 58: Alg. closure exists, unique up to K-isom.

Lem. 59: K finite $\Rightarrow |K| = q = (\mathrm{char}\, K)^d$, and K is a splitting field of $X^q - X$.

Def. 60: Derivation. Prop. 61: Leibniz's law; multiple root of P = common root of $P, D(P)$.

Cor. 62: $X^N - 1$ has no multiple root unless $\mathrm{char}\, K \mid N$.

Lem. 63: $x \mapsto x^p$ is $\mathbb{F}_p$-hom. in char. p. Def. 64: Frobenius map Fr_p; q-th power Frob. Fr_q.

Th. 65: $\exists \mathbb{F}_q$, unique up to $\mathbb{F}_p$-isom., for each q; $\mathbb{F}_q \subset \mathbb{F}_{q'} \iff q' = q^n$.

Lem. 66: $\mathrm{Fr}_q \in \mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$, order n. Lem. 67: Finite subgroups of $K^\times$ are cyclic.

Th. 68: $\mathbb{F}_{q^n}/\mathbb{F}_q$ is simple and Galois. Def. 69: Cyclotomic ext'ns, primitive roots of unity.

Prop. 70: Cyclotomic poly. $\Phi_N \in \mathbb{Z}[X]$ has all prim. N-th roots of 1 as roots ($(\mathrm{char}\, K, N) = 1$);
$\mathrm{Gal}\big(K(\boldsymbol{\mu}_N)/K\big) \hookrightarrow \big(\mathbb{Z}/(N)\big)^\times$, all irred. factors of Φ_N in $K[X]$ have deg. $[K(\boldsymbol{\mu}_N) : K]$.

Th. 71: Irreducibility of Cyclotomic Polynomials. Def. 72: Separable polynomials.

Lem. 73: P separable $\iff$ coprime to $D(P)$; Irred. P separable $\iff$ $D(P) \neq 0$;
Every irred. P separable in char. 0; Separability is stable under K-hom's/factors.

Def. 74: Separable/normal ext'ns. Lem. 75: Inequality from Roots & Hom's II.

Prop. 76: $|\mathrm{Hom}_K(F, E)| \leq [F : K]$ when F/K finite. If equal, then for any $K \subset L \subset F$,
$|\mathrm{Hom}_K(L, E)| = [L : K]$ and $\mathrm{Hom}_K(F, E) \twoheadrightarrow \mathrm{Hom}_K(L, E)$.

Th. 77: Characterisation of separable/Galois ext'ns; Finite F/K sep. $\iff$ $F/L, L/K$ sep.

Th. 78: Primitive Element Th'm (Finite separable $\Rightarrow$ simple).

Prop. 79: For a product of separable poly's, splitting field is Galois and Prop. 42 valid.

Prop. 80: Cycle type of Fr_p in $\mathrm{Gal}(P) \hookrightarrow S_n$. Def. 81: Elementary symmetric polynomials.

Prop. 82: Rational Symmetric Function Theorem. Th. 83: SFT.

Th. 84: $\mathrm{Gal}(P)$ for $P \in \mathbb{Z}[X]$ and factorisation of $P \bmod p$. (Lem. 85: auxiliary.)

Lem. 86: $\mathrm{Hom}_{K\text{-vs}}(V, E)$ is an E-v.s. with dim.$= \dim_K V$.

Prop. 87: Dedekind's Lemma (linear independence of K-hom's).

Prop. 88: Artin's Lemma (G finite $\Rightarrow F/F^G$ Galois with $\mathrm{Gal}(F/F^G) = G$).

Def. 89: Ext'ns/morphisms (generalised). Def. 90: Finite/Galois ext'ns, degrees.

Lem. 91: Hom sets bijective with the old Hom_K sets. Def. 92: Towers of ext'ns.

Prop. 93: Hom for towers, Tower Law, Towers & Galois ext'ns.

Def. 94: Traces/norms. Lem. 95: Trace is K-linear, norm is multiplicative.

Lem. 96: Trace/norm & min. poly.; transitivity of traces. Prop. 97: Insep. $\Longrightarrow$ trace map $= 0$.

Prop. 98: Sep. $\Longrightarrow$ trace/norm is sum/product of conjugates. Th. 99: Sep. $\iff$ trace map $\neq 0$.

Th. 100: Hilbert's Th. 90. Cor. 101: Kummer theory.

t.yoshida@dpmms.cam.ac.uk