These notes were taken down by me (Boris Lerner) during the Galois Theory course taught by Dr Daniel Chan in the second session of 2007 at UNSW. I made a few brief remarks of my own here and there but in general this is my best attempt to reproduce exactly what was written on the board. The last four sections were not examinable so contain far less detail then the other sections. I have also not reproduced all the diagrams which accompanied the text from those sections. If you find any mistakes, please email them to me at boris@unsw.edu.au. Enjoy!

.

Contents

1 Genesis of Galois Theory

Q: What is Galois Theory?
A: Study of field extensions K/F via symmetry.

Original motivating example:
We can find roots of some polynomials /F (field).

Example 1.1. $f(X) = X^2 + bX + c$ has roots $\frac{-b \pm \sqrt{b^2-4ac}}{2}$ if char $F \neq 2$.

Example 1.2. $f(X) = X^3 - pX - q$ has roots

$$X = \sqrt[3]{\frac{1}{2}q + \beta} + \sqrt[3]{\frac{1}{2}q - \beta} \text{ where } \beta = \sqrt{\frac{q^2}{4} - \frac{p^3}{27}} \text{ if char } F \neq 2.$$

Quadratic formula also exists.

Note 1.3. Formulae for roots are in terms of coefficients of polynomials $f(X)$ and uses elementary operations $+, -, \times, \div$ and radical $\sqrt[n]{\ }$.

A major question in the 18th century algebra: can we find a similar formula for a quintic? A: (Abel, Galois, early 1800's) No!

Modern approach: use field extensions. Let K/F be a field extension. Let $\alpha_1, \ldots, \alpha_n \in K$. Recall the field generated by F and $\alpha_1, \ldots, \alpha_n$ is the unique smallest subfield $F(\alpha_1, \ldots, \alpha_n) \subseteq K$ containing $F, \alpha_1, \ldots, \alpha_n$.
Example 1.1 (again). The roots of $f(X) = X^2+bX+c$ lie in $F\left(\sqrt{b^2-4ac}\right)$.
Example 1.2 (again). The roots of $f(X) = X^3 - pX - q$ lie in $F(\beta, \gamma, \delta)$ where $\gamma = \sqrt[3]{\frac{1}{2}q + \beta}$, $\delta = \sqrt[3]{\frac{1}{2}q - \beta}$.

We have a tower of field extensions: $F \subset F(\beta) \subset F(\beta, \gamma) \subset F(\beta, \gamma, \delta)$.

Definition 1.4. *A field extension K/F is* **radical** *if there exists a tower of field extensions*

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = K \text{ where } F_{i+1} = F_i(\alpha_i)$$

where $\alpha_i^{r_i} \in F_i$ for some $r_i \geq 1$.

Upshot: Suppose you can solve for roots of $f(X) \in F[X]$ by radicals i.e. as in note above. Let α be such a root. Then α lies in a radical extension of F. Galois theory gives a good criterion for checking this (in characteristic 0) in terms of symmetry.

1.1 Symmetry and Roots of Polynomials

Q: How does symmetry help you understand roots of polynomials?

Example 1.5. The non-real roots of a real polynomial occur in symmetric complex conjugate pairs.

Example 1.1 (again). Quadratic formula by symmetry: Let x_1, x_2 be roots of $X^2 + bX + c = 0$. Key point: Any symmetric polynomial in roots x_1, x_2 is a polynomial in the coefficients. E.g:

$$x_1 + x_2 = -b$$
$$x_1 x_2 = c$$

Note $x_1 - x_2$ is antisymmetric, which implies $(x_1 - x_2)^2$ is symmetric. But $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c$ - the discriminant. Solve

$$x_1 + x_2 = -b$$
$$x_1 - x_2 = \sqrt{b^2 - 4c}$$

Exercise: repeat for cubic $f(X) = X^3 - pX - q$. Hint: Let x_1, x_2, x_3 be roots. Let ω be a primitive cube root of 1. Suffices to find

$$\Sigma_1 \colon x_1 + x_2 + x_3 = 0$$
$$\Sigma_2 \colon x_1 + \omega x_2 + \omega^2 x_3$$
$$\Sigma_3 \colon x_1 + \omega^2 x_2 + \omega x_3$$

Now

$$\Sigma_2^3 = x_1^3 + x_2^3 + x_3^3 + 3!x_1x_2x_3 + 3\omega\left(x_1^2x_2 + x_1x_3^2 + x_2^2x_3\right) + 3\omega^2\left(x_1^2x_3 + x_2x_3^2 + x_2^2x_1\right).$$

Note 1.6. It has A_3-symmetry, i.e. symmetric with respect to cyclic permutations of variables. Show it is the sum of a symmetric polynomials and an anti-symmetric polynomial. Recall: have an anti-symmetric polynomial

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_1 - x_3).$$

Write Σ_3^2 in terms of coefficients and δ.

2 Splitting Fields

Aim: Show that given any polynomial, can factorise it into linear polynomials is some field extension.

2.1 Review of Field Homomorphisms

Proposition/Definition 2.1. *A map of fields $\sigma : F \to F'$ is a* **field homomorphism** *if it is a ring homomorphism.*

1. *σ is injective*
2. *There is a ring homomorphism*

$$\begin{array}{rcl} \sigma[X]\colon F[X] & \longrightarrow & F'[X] \\ \displaystyle\sum_{i=0}^{n} f_i X^i & \longmapsto & \displaystyle\sum_{i=0}^{n} \sigma(f_i) X^i \end{array}$$

Proof. 2. Easy.
1. $\ker\sigma \lhd F$ not containing 1, so $\ker\sigma = 0$. □

2.2 Review of Simple Algebraic Extensions

Let K/F be a field extension and $\alpha \in K$ be algebraic over F, so it is a root of its minimal or irreducible polynomial say $p(X)$.
Fact: There is a field isomorphism

$$\begin{array}{rcl} \dfrac{F[X]}{\langle p(X)\rangle} & \xrightarrow{\sim} & F(\alpha) \\ X + \langle p(X)\rangle & \longmapsto & \alpha \\ a + \langle p(X)\rangle & \longmapsto & a. \end{array}$$

Example 2.2. $\mathbb{Q}\left(\sqrt[3]{2}\right) \simeq \frac{\mathbb{Q}[X]}{\langle X^3-2\rangle}$.

2.3 The Converse: Adjoining Roots of Polynomials

Let $F =$ field, and $p(X) \in F[X]$ be irreducible.

Proposition 2.3. *Then $K := F[X]/\langle p(X)\rangle$ is a field extension of F via the composite ring homomorphism*

$$F \longrightarrow F[X] \longrightarrow \frac{F[X]}{\langle p(X)\rangle}.$$

Also, $K = F(\alpha)$ where $\alpha = x + \langle p(X)\rangle$ is a root of $p(X)$.

Proof. $p(X)$ is irreducible in PID which implies $\langle p(X)\rangle \lhd F[X]$ is maximal and thus $F[X]/\langle p(X)\rangle$ is a field. It is clear that $K = F(\alpha)$ and $p(\alpha) = p(X) + \langle p(X)\rangle = 0$ so α is a root of $p(X)$. □

Have the following uniqueness result:

Proposition 2.4. *Let $\sigma\colon F \xrightarrow{\sim} F'$ be a field isomorphism. Let $p(X) \in F[X]$ be irreducible. Let α and α' be roots of $p(X)$ and $(\sigma p)(X)$ (in appropriate field extensions). Then there is a field isomorphism $\tilde{\sigma}\colon F(\alpha) \xrightarrow{\sim} F'(\alpha')$ such that:*

1. *$\tilde{\sigma}$ extends $\tilde{\sigma}\mid_F = \sigma$*
2. *$\tilde{\sigma} = \alpha'$*

Proof. $\tilde{\sigma}$ is the composite of the following:

$$F(\alpha) \xrightarrow{\sim} \frac{F[X]}{\langle p(X)\rangle} \xrightarrow{\sim} \frac{F'[x]}{\langle (\sigma p)(X)\rangle} \longrightarrow F'(\alpha').$$

$\alpha \longmapsto X + \langle p(X)\rangle \longmapsto X + \langle (\sigma p)(X)\rangle \longmapsto \alpha' \implies (2)$
$a \longmapsto a + \langle p(X)\rangle \longmapsto \sigma(a) + \langle (\sigma p)(X)\rangle \longmapsto \sigma(a)$ □

2.4 Splitting Fields

Definition 2.5. *Let F be a field, $f(X) \in F[X]$. A field extension K/F is a* **splitting field** *for $f(x)$ over F if*

(a) *$f(X)$ factors into linear polynomials over K.*

(b) *$K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(X)$ in K.*

Example 2.6. Let $\omega = e^{\frac{i2\pi}{3}}$. $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for $X^3 - 2$ over $\mathbb{Q}$ but $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ is.

Note 2.7. Consider the tower of field extensions $F \subset K \subset L$ and $f(X) \in F[X]$.

1. If L is a splitting field for $f(X)$ over F then L is a splitting field for $f(X)$ over K.
2. If K is generated over F by roots of $f(X)$, then the converse holds.

The proof of this is left as an exercise.

2.5 Existence

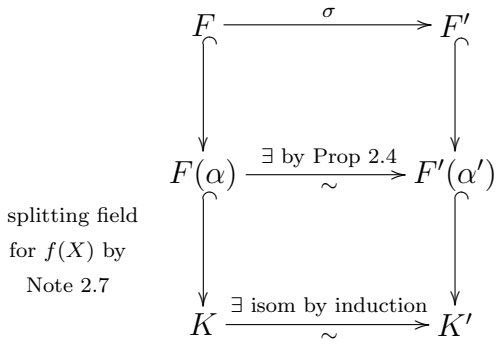
Theorem 2.8. *Let F be a field, $f(X) \in F[X]$. Then there exists a splitting field K of $f(X)$ over F.*

Proof. By induction on the degree of $f(X)$. By Proposition 2.3, there exists a simple algebraic extension $F(\alpha)/F$ where α is a root is a root of $f(X)$. Factorise in $F(\alpha)$ to get $f(X) = (X - \alpha)g(X)$. By induction, there exists a splitting field K of $g(X)$ over $F(\alpha)$. Now K is a splitting field for $f(X)$ over $F(\alpha)$ which by the note above implies, it is also a splitting field of $f(X)$ over F. □

2.6 Uniqueness

Theorem 2.9. *Let $\sigma\colon F \xrightarrow{\sim} F'$ be a field isomorphism and $f(X) \in F[X]$. Suppose K, K' are splitting fields for $f(X)$ and $(\sigma f)(X)$ respectively over F and F' (respectively). Then there is an isomorphism of fields $\tilde{\sigma}\colon K \xrightarrow{\sim} K'$ which extends σ.*

Proof. By induction on $[K : F] = \dim_F K$ using Proposition 2.4. Let $f_0(X) \in F[X]$ be an irreducible factor of $f(X)$. Let $\alpha \in K$, $\alpha' \in K'$ be roots of $f_0(X)$ and $(\sigma f_0)(X)$ respectively. Then get diagram:



□

3 Algebraic Closure

Aim: Prove the existence and uniqueness of algebraic closure of fields.

3.1 Review of Algebraic Extensions

Let F be a field.

Definition 3.1. *A field extension K/F is* **algebraic** *over F is every $\alpha \in K$ is algebraic over F. A field K is* **algebraically closed** *is the only algebraic extensions of K is K itself. We say K is an* **algebraic closure** *of F if it is an algebraic field extension of F such that K is algebraically closed.*

Example 3.2. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Proposition 3.3. *Let $F \subset K \subset L$ be a tower of field extensions. Then:*

1. $[L : F] = [L : K]\,[K : F]$;
2. *L/F is algebraic if and only if both L/K and K/F are algebraic;*
3. *Finite extensions are algebraic;*
4. *If $K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are algebraic over F then K is finite over F. (i.e. finite dimensional over F).*

3.2 Set Theoretical Fact

Lemma 3.4. *Let F be a field. There exists a set S such that for any algebraic field extension K/F, $|K| < |S|$.*

Remember: Either K is countable or $|K| = |F|$.

Proof. There is a finite-to-one map

$$\begin{array}{ccc} K & \longrightarrow & F[X] \\ \alpha & \longmapsto & \text{monic mimimal} \\ & & \text{polynomial of } \alpha \end{array}$$

$\Longrightarrow \quad |K| \leq |F[X] \times \mathbb{N}|$
Let S be the power set of $F[X] \times \mathbb{N}$. Then we are done since $|F[X] \times \mathbb{N}| < |S|$. □

3.3 Splitting Fields for Families of Polynomials

Let F be a field, $\{f_i(X)\}_{i \in I} \subset F[X] - 0$.

Definition 3.5. *A field extension K/F is a* **splitting field** *for $\{f_i(X)\}$ over F if*

(a) *Every $f_i(X)$ factors into linear factors over K;*

(b) *K is generated as a field over F by all the roots of the $f_i(X)$.*

Note 3.6. Consider a field extension K/F. Let $\{\alpha_i\}_{j\in J} \subseteq K$. Then the subfield of K generated by F and the α_j's is

$$\bigcap \text{of all subfields of } K \text{ contating } F \text{ and all the } \alpha_j\text{'s} = \bigcup_{\{j_1,\ldots,j_n\}\subseteq J} F(\alpha_{j_1},\ldots,\alpha_{j_n})$$

Why? ($\supseteq$) is clear.
($\subseteq$) Suffices to check RHS is a subfield. But closure axioms are easy to check (exercise). For example: let $\alpha \in F(\alpha_{j_1},\ldots,\alpha_{j_n})$ and $\beta \in F(\alpha_{l_1},\ldots,\alpha_{l_m})$ then $\alpha+\beta,\ \alpha\beta \in F(\alpha_{j_1},\ldots,\alpha_{j_n}\alpha_{l_1},\ldots,\alpha_{l_m})$, etc.

Example 3.7. If K is a splitting field for all non-constant polynomials over F then K is an algebraic closure of F. Why? Check first K/F is algebraic. Any $\alpha \in K$ lies in some $F(\alpha_1,\ldots,\alpha_n)$ where $\alpha_1,\ldots,\alpha_n$ are roots of some non-constant over F and therefore algebraic over F. Proposition 3.3 (part 4) is algebraic over F and thus α is algebraic over F. Therefore K/F is algebraic. Check K is algebraically closed. Suppose $\tilde{K}/K$ is and algebraic extension. Then K/F is algebraic, which implies by Proposition 3.3 (part 2) that $\tilde{K}/F$ is algebraic. Let $\alpha \in \tilde{K}$ be arbitrary. Now α is algebraic over F so satisfies minimal polynomial $f(X)$. But K is a splitting field for all non-constant polynomials over F and thus $\alpha \in K$. Therefore $\tilde{K} = K$ and hence K is algebraically closed.

Converse is also true (exercise).

3.4 Existence and Uniqueness

Theorem 3.8. *Let F be a field, $\{f_i(X)\}_{i\in I} \subseteq F[X] - 0$.*

1. *There exists a splitting field K for $\{f_i(X)\}$ over F.*
2. *Suppose there is a field isomorphism $\sigma\colon F \to F'$ and K' is a splitting field for $\{(\sigma f_i)(X)\}_{i\in I}$ over F'. Then there exists a field isomorphism $\tilde{\sigma}\colon K \xrightarrow{\sim} K'$ which extends σ.*

Proof. Same as Theorems 2.8 and 2.9, except we replace induction with Zorn's Lemma. We will prove (1) here, (2) similar. Let S be the set as in Lemma 3.4. Let $\mathscr{L}$ be the set of subsets of S equipped with a field structure such that $L \in \mathscr{L}$ is a splitting field for some subset of $\{f_i(X)\}_{i\in I}$ over F. Let's partially order $\mathscr{L}$ by $L_1 \leq L_2$ if L_1 is a subfield of L_2. Given a totally ordered chain $\{L_j\}_{j\in J}$ of elements of $\mathscr{L}$, we note it has an upper bound $\cup L_j \in \mathscr{L}$. Hence by Zorn's Lemma, there exists a maximal $K \in \mathscr{L}$.

Claim: K is a splitting field for $\{f_i(X)\}_{i\in I}$ over F. Why? Suppose not. Some $f_i(X)$ is not split in K. Let $\tilde{K}$ be a splitting field for $f_i(X)$ over K. So

$\tilde{K}$ is algebraic over F. Lemma 3.4 implies there is a map $\tilde{K} - K \to S - K$. This gives a map $\phi\colon \tilde{K} \to S$ extending id on K. The image of ϕ is bigger than K which contradicts maximality of K. This proves the first part of the theorem. □

Corollary 3.9. *For any field F, there exists a unique (up to isomorphism) algebraic closure, denoted $\bar{F}$.*

4 The Galois Group

Aim: Encode the symmetry of field extension K/F in the Galois group.

4.1 Field Automorphism over F

Let $K,\ K'$ be field extensions of F.

Proposition/Definition 4.1. *We say a field homomorphism $\sigma : K \to K'$* **fixes** *F, or σ is a* **field homomorphism over** *F, if $\sigma(\alpha) = \alpha$ for all $\alpha \in F$. Such homomorphisms are linear over F. If, furthermore, $K = K'$, and σ is an isomorphism, then we say σ is a* **field automorphism over** *F.*

Proof. σ is additive and for $\alpha \in F,\ \beta \in K,\ \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\sigma(\beta)$. So it preserves scalar multiplication by elements of F. □

Example 4.2. $K = \mathbb{C},\ F = \mathbb{R}$. $c :=$ conjugation: $\mathbb{C} \to \mathbb{C}$ is a field automorphism over R because if $\alpha \in \mathbb{R}$ it implies $c(\alpha) = \bar{\alpha} = \alpha$.

Proposition/Definition 4.3. *Let K/F be a field extension and G a set of field automorphisms of K over F. Then G is a group when endowed with composition for group multiplication. It is called the* **Galois group** *of K/F and is denoted by* $\mathrm{Gal}\,(K/F)$.

Proof. Suffices to check $G \leq \mathrm{Perm}\ K$. Let $\sigma, \tau \in G$. $\sigma\tau$ is a field automorphism. It fixes any $\alpha \in F$ since $(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) = \sigma(\alpha) = \alpha$. Therefore $\sigma\tau \in G$. Similarly $\sigma^{-1} \in G$ and $1 \in G$. □

4.2 Galois Group as Group of Permutations

Let F be a field.

Lemma 4.4. *Let $f(X) \in F[X]$, K/F a field extension and $\alpha \in K$ a root of $f(X)$. Let $\sigma\colon K \to K'$ be a field homomorphism over F. The $\sigma(\alpha)$ is also a root of $f(X)$.*

Proof. If $f(X) = \sum_{i=0}^{n} a_i X^i$ then $0 = f(\alpha) = \sigma(f(\alpha)) = \sigma\left(\sum a_i \alpha^i\right) = \sum \sigma(a_i)\sigma(\alpha)^i = \sum a_i \sigma(\alpha)^i = f(\sigma(\alpha))$. □

Remark 4.5. Any field homomorphism $\sigma\colon F(\alpha_1, \ldots, \alpha_n) \to K$ over F is determined by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$.

Example 4.6. Let $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ and $F = \mathbb{Q}$. Then $\mathrm{Gal}\,(K/F) = 1$ since any $\sigma \in \mathrm{Gal}\,(K/F)$ sends $\sqrt[3]{2}$ to a cube root of 2 in $\mathbb{Q}\left(\sqrt[3]{2}\right)$ i.e. $\sigma\colon \sqrt[3]{2} \mapsto \sqrt[3]{2} \implies \sigma = \mathrm{id}_K$.

Corollary 4.7. *Let K be a splitting field for $f(X) \in F[X]$ over F. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(X)$ so $K = F(\alpha_1, \ldots, \alpha_n)$. Then any $\sigma \in G := \mathrm{Gal}\,(K/F)$ permutes the roots $\alpha_1, \ldots, \alpha_n$ so gives an injective group homomorphism $G \hookrightarrow \mathrm{Perm}(\alpha_1, \ldots, \alpha_n) \simeq S_n$.*

Example 4.2 (again). $\mathrm{Gal}\,(\mathbb{C}/\mathbb{R}) = \{1, c\} \simeq \mathbb{Z}/2\mathbb{Z}$. Why? $\mathbb{C}$ is the splitting field for $X^2 + 1$ over $\mathbb{R}$ ($\mathbb{C} = \mathbb{R}(i)$). Let $\sigma \in \mathrm{Gal}\,(\mathbb{C}/\mathbb{R})$. There are 2 possibilities. Either:

(a) $\sigma(i) = -i$ so $\sigma(a + bi) = a - bi$ $\therefore \sigma$ is conjugation;

(b) $\sigma(i) = i$ so $\sigma(a + bi) = a + bi$ $\therefore \sigma$ is the identity.

4.3 Constructing Field Automorphisms Over F

Use Proposition 2.4 and Theorem 2.9.

Lemma 4.8. *Let F be a field, $f(X) \in F[X] - F$. Let K be the splitting field of $f(X)$ over F. Suppose α, α' are two roots if an irreducible factor $f_0(X)$ of $f(X)$ (over F). Then there is a $\sigma \in G := \mathrm{Gal}\,(K/F)$ such that $\sigma(\alpha) = \alpha'$. In particular G acts transitively on roots of $f_0(X)$.*

Proof. By Proposition 2.4, there exists a field isomorphism

$$\begin{array}{ccc} \tilde{\sigma}\colon F(\alpha) & \xrightarrow{\sim} & F(\alpha') \\ \downarrow & & \downarrow \\ K & \xrightarrow{\exists \text{ unique??}} & K \end{array}$$

over F. But K is a splitting field for $f(X)$ over $F(\alpha)$ and $F(\alpha')$. Therefore, by the uniqueness of splitting fields Theorem 2.9 we can extend $\tilde{\sigma}$ to a field automorphism over F, $\sigma\colon K \to K$ so that $\alpha \mapsto \alpha'$. □

Example 4.9. $K = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right)$, $\omega = e^{\frac{i2\pi}{3}}$, $F = \mathbb{Q}$, $G := \mathrm{Gal}\,(K/\mathbb{Q})$. K is a splitting field for $X^3 - 2$ over $\mathbb{Q}$. Conjugation, $\tau\colon K \to K$ is a field automorphism over $\mathbb{Q}$. It swaps $\sqrt[3]{2}\omega \leftrightarrow \sqrt[3]{2}\omega^2$ and fixes $\sqrt[3]{2}$. Note $\langle\tau\rangle \leq G \hookrightarrow S_3$-order 6. Lagrange's Theorem implies $G = \langle\tau\rangle$ or S_3. Lemma 4.8 implies there exists $\sigma \in G$ such that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega \notin \langle\tau\rangle$. Thus, $G \simeq S_3$.

Example 4.10 (Biquadratic Extension)**.** $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) \overset{\text{ex}}{=} \mathbb{Q}(\sqrt{2}+\sqrt{3})$ is a splitting field for $(X^2-2)(X^2-3)$ over $\mathbb{Q}$. Ant $\sigma \in G := \mathrm{Gal}\,(K/\mathbb{Q})$ must map

$$\sqrt{2} \longmapsto \pm\sqrt{2}$$
$$\sqrt{3} \longmapsto \pm\sqrt{3}$$
$$\therefore G \overset{\phi}{\hookrightarrow} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Claim: ϕ is an isomorphism. Why? K is a splitting field for $X^2 - 3$ over $\mathbb{Q}(\sqrt{2})$. So Proposition 2.4 $\implies$ there exists a field automorphism σ of K fixing $\mathbb{Q}(\sqrt{2})$ and sending $\sqrt{3} \mapsto -\sqrt{3}$, $\sigma \in G$. Similarly, there exists $\tau \in G$ such that $\tau(\sqrt{2}) = -\sqrt{2}$ and $\tau(\sqrt{3}) = \sqrt{3}$. Now, σ, τ generate $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This shows $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}\right) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise: Compute $\mathrm{Gal}\left(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}\right)$. (Answer: D_4)

5 Weak Galois Correspondence

Aim of next three sections: Show $\mathrm{Gal}\,(K/F)$ gives info about intermediate fields L i.e. where $F \subseteq L \subseteq K$ (subfields).

5.1 Fixed Fields

Let K be a field, and G a group of field automorphism of K.

Proposition/Definition 5.1. *The* **fixed field** *of G (in K) is*

$$K^G := \{\alpha \in K \mid \sigma(\alpha) = \alpha,\ \forall\, \sigma \in G\}.$$

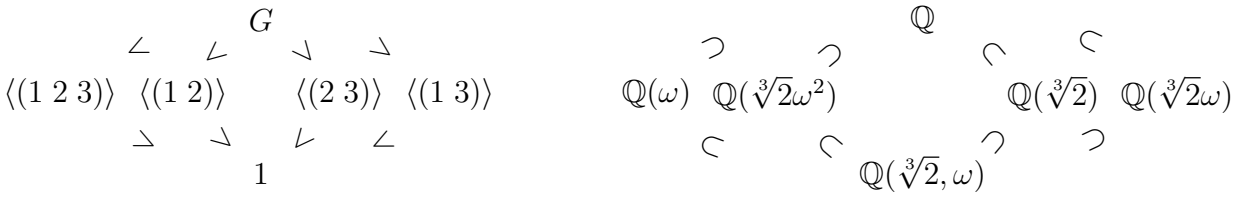
K^G is a subfield of K.

Proof. Simply check closure axioms (under $+, 0, -, \times, 1$ and inverses). Let us just check closure under $+$. Let $\alpha, \beta \in K^G$ and $\sigma \in G$. $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$. $\therefore \alpha + \beta \in K^G$. etc. □

Example 5.2. $c\colon \mathbb{C} \to \mathbb{C}$ is conjugation. $\mathbb{C}^{\langle c\rangle} = \mathbb{R}$.

Example 5.3. $K = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right) = \mathbb{Q}(\sqrt[3]{2}, \omega),\ \omega = e^{\frac{2\pi i}{3}}$. We saw in the previous section $G := \mathrm{Gal}\,(K/\mathbb{Q}) = S_3$ (on identifying 1,2,3 with 1st, 2nd, 3rd root) e.g. (2 3) is conjugation. We will show

$$\begin{array}{ccc} H \leq G & \longmapsto & K^H \subseteq K \end{array}$$



Exercise: Show $K^{\langle(2\ 3)\rangle} = \mathbb{R} \cap \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2})$.
Surprise: We will show in this case, all intermediate fields are obtained from K^H as above.

Let K/F be a field extension and $G := \mathrm{Gal}\,(K/F)$. We define two maps both called prime '.

$$H \longmapsto H' := K^H$$

$$\left\{\begin{array}{c}\text{subgroups}\\ \text{of } G\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{intermediate}\\ \text{fields } K/F\end{array}\right\}$$

$$K_0' := \mathrm{Gal}\,(K/K_0) \longmapsfrom K \supseteq K_0 \supseteq F$$

Check well-defined. (i.e. codomains are what we say they are). 1) Know $H' := K^H$ is a subfield of K. Need $K^H \supseteq F$. For $\alpha \in F$, $\sigma \in H \leq G$, $\sigma \in \mathrm{Gal}\,(K/F)$, so fixes $F \ \ \therefore \sigma(\alpha) = \alpha \implies \alpha \in K^H \ \therefore K^H$ is an intermediate field.

2) Know $K_0' := \mathrm{Gal}\,(K/K_0)$ this is a group of field automorphisms of K (which fix K_0). They all fix K_0 and therefore fix F (as $F \subseteq K_0$. So it is a group of automorphism fixing F. Therefore it is a subgroup o G.

Example 5.4.

$$\begin{array}{ccc} H = 1 & \longmapsto & 1' := K^1 = K \end{array}$$

$$\begin{array}{ccc} K' = \mathrm{Gal}\,(K/K) & \longmapsfrom & K \\ \| & & \\ 1 & & \end{array}$$

$$\begin{array}{ccc} F' = \mathrm{Gal}\,(K/F) & \longmapsfrom & F \\ \| & & \\ G & & \end{array}$$

But suppose $K/F = \mathrm{Gal}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$ so $\mathrm{Gal}\,(K/F) = 1$ (from Section 4) and so $G \longmapsto G' = 1' = \mathbb{Q}(\sqrt[3]{2})$. Therefore prime is not always a bijection.

Let K/F be a field extension, $G = \mathrm{Gal}\,(K/F)$. Below we let $H_1, H_2, \ldots$ denote subgroups of G and $K_1, K_2, \ldots$ denote intermediate fields of K/F.

Proposition 5.5. *Priming reverses inclusion. i.e.*

1. $H_1 \subseteq H_2 \implies H_1' \supseteq H_2'$.
2. $K_1 \subseteq K_2 \implies K_1' \supseteq K_2'$.

Proof. 1. Suppose $H_1 \subseteq H_2$ and let $\alpha \in H_2' := K^{H_2}$ For any $\sigma \in H_1 \subseteq H_2$ we have $\sigma(\alpha) = \alpha$. $\therefore \alpha \in K^{H_1} =: H_1'$.

2. Suppose $K_1 \subseteq K_2$ and let $\sigma \in K_2' := \mathrm{Gal}\,(K/K_2)$. For any $\alpha \in K_1$ $\sigma(\alpha) = \alpha$ (as σ fixes K_2 and $\therefore K_2$) $\implies \sigma \in \mathrm{Gal}\,(K/K_1) = K_1'$.

□

Proposition 5.6. 1. $H_1 \subseteq H_1''$.

2. $K_1 \subseteq K_1''$.

Proof. 1. Let $\sigma \in H_1$, $\alpha \in H_1' := K^{H_1}$. $H_1'' := \mathrm{Gal}\left(K/K^{H_1}\right)$. $\sigma(\alpha) = \alpha$ (as $\alpha \in K^{H_1}$) $\implies \sigma$ fixes all of K^{H_1}. So $\sigma \in \mathrm{Gal}\left(K/K^{H_1}\right) = H_1''$.

2. Let $\alpha \in K$, $\sigma \in K_1' =: \mathrm{Gal}\,(K/K_1)$. $K_1'' := K^{\mathrm{Gal}(K/K_1)}$. Now $\sigma(\alpha) = \alpha$ (as $\sigma \in \mathrm{Gal}\,(K/K_1)$) $\therefore \alpha$ is fixed by any $\sigma \in K_1' \implies \alpha \in K^{K_1'} = K_1''$.

□

Definition 5.7. *We say H_1 is a* **closed subgroup** *of G if $H_1 = H_1''$. We say K_1 is a* closed intermediate field *of K/F if $K_1 = K_1''$. The* **closure** *of H_1, respectively K_1, is H_1'', respectively K_1''.*

Proposition 5.8. 1. $H_1' = H_1'''$.

2. $K_1' = K_1'''$.

Proof. 1. Previous proposition applied to $K_1 = H_1' \implies H_1' \subseteq H_1'''$. Proposition 5.5 applied to $H_1 \subseteq H_1'' \implies H_1' \supseteq H_1'''$. Thus $H_1' = H_1'''$.

2. Proved identically.

□

We may restrict the Galois correspondence to closed objects to get:

Theorem 5.9. *Priming induces a well defined bijection:*

$$H \longmapsto H' := K^H$$

$$\left\{\begin{array}{c}\textit{closed subgroups}\\ \textit{of } G\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\textit{closed intermediate}\\ \textit{fields } K/F\end{array}\right\}$$

$$K_0' := \mathrm{Gal}\,(K/K_0) \longmapsto K \supseteq K_0 \supseteq F$$

Proof. Check well defined. By Proposition 5.8, prime maps anything to a closed object. Therefore codomains are legitimate. Thus by the definition of "closed" we get that priming induces a bijection on closed objects. Hence theorem. □

6 Technical Results

Aim: Relate $[H_2 : H_1]$ to $[H_1' : H_2']$ and $[K_2 : K_1]$ to $[K_1' : K_2']$.
Setup: Fix, for this section, K/F - a field extension with $G := \mathrm{Gal}\,(K/F)$.
Correspondence

$$H_i \longmapsto H_i' := K_i^H$$

$$\left\{\begin{array}{c}\text{subgroups}\\ \text{of } G\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{intermediate}\\ \text{fields } K/F\end{array}\right\}$$

$$K_i' := \mathrm{Gal}\,(K/K_i) \longmapsto K_i$$

Theorem 6.1. *Let $K_1 \subseteq K_2$ be intermediate fields with $n := [K_2 : K_1] < \infty$, then $[K_1' : K_2'] \leq [K_2 : K_1]$.*

Proof. We reduce to the case of a simple extension by:
Claim: It suffice to prove the theorem when $K_2 = K_1(\alpha)$.
Proof: Pick $\alpha \in K_2 - K_1$. We argue by induction on n. We are assuming $[K_1' : K_1(\alpha)'] \leq [K_1(\alpha) : K_1]$. Note: $K_1 \subsetneq K_1(\alpha) \subseteq K_2$ and $K_1' \supseteq K_1(\alpha)' \supseteq K_2'$. $[K_1' : K_2'] = [K_1' : K_1(\alpha)']\ [K_1(\alpha)' : K_2'] \leq [K_2 : K_1]$.
$\wedge$ (induction) $\wedge$
$[K_1(\alpha) : K_1]\ [K_2 : K_1(\alpha)]$
Back to proof of theorem when $K_2 = K_1(\alpha) = K_1[X]/\langle p(X)\rangle$. $[K_2 : K_1] = n$ = deg. of min. ploy. $p(X) \in K_1[X]$ of α over K_1. Let $\sigma \in K_1' = \mathrm{Gal}\,(K/K_1)$. It fixes K_1 so must send α to a root of $p(X)$ in K be Lemma 4.4. $\therefore$ There are $\leq n$ possibilities for $\sigma(\alpha)$. The theorem will be proved once

we show:
Lemma: Let $\sigma, \tau \in K_1'$, then $\sigma K_2' \neq \tau K_2' \implies \sigma(\alpha) = \tau(\alpha)$.
Proof: (of contrapositive). Suppose $\sigma(\alpha) = \tau(\alpha)$. Then $\tau^{-1}\sigma \in K_1' := \mathrm{Gal}\,(K/K_1)$ sends α to $\tau^{-1}\sigma(\alpha) = \tau^{-1}\tau(\alpha) = \alpha$ so fixes α and $K_1 \therefore$ it fixed $K_2 = K_1(\alpha) \therefore \tau^{-1}\sigma \in \mathrm{Gal}\,(K/K_2) = K_2' \implies \sigma K_2' = \tau K_2'$. This proves lemma. Theorem follows. □

Theorem 6.2. *Let $H_1 \leq H_2 \leq G$. Suppose $n = [H_2 : H_1] < \infty$. Then $[H_1' : H_2'] \leq [H_2 : H_1]$.*

Proof. Uses:
Lemma: Let $\sigma, \tau \in G$ be such that $\sigma H_1 = \tau H_1$. The for any $\alpha \in H_1'$ we have $\sigma(\alpha) = \tau(\alpha)$.
Proof: Let $\rho \in H_1$ be such that $\sigma = \tau\rho$. Then $\sigma(\alpha) = \tau\rho(\alpha) = \tau\alpha$ $\left(\text{since } \alpha \in H_1' = K^{H_1}\right)$.
Remark: As a result, given any left coset C of H_1 in G and $\alpha \in H_1'$ we can define (unambiguously) $C(\alpha) := \sigma(\alpha)$ where σ is any element of C. Back to the proof of theorem, by contradiction.

Let the distinct left cosets of H_1 in H_2 be $C_1 = H_1, C_2, C_3, \ldots, C_n$. Suppose $\alpha_1, \ldots, \alpha_{n+1} \in H_1'$ are linearly independent over H_2'. Consider $n \times (n+1)$ matrix over K:

$$A := \begin{pmatrix} C_1(\alpha_1) & C_1(\alpha_2) & \cdots & C_1(\alpha_{n+1}) \\ C_2(\alpha_1) & & \ddots & \vdots \\ \vdots & & & \\ C_n(\alpha_1) & \cdots & & C_n(\alpha_{n+1}) \end{pmatrix}$$

There exists non-zero solutions $\mathbf{x} \in \mathbf{K^{n+1}}$ to $A\mathbf{x} = \mathbf{0}$. Pick a non-zero solution $\mathbf{x}$ with the most number of 0 entries. We seek to construct $\mathbf{x}' \in \mathbf{K^{n+1}} - \mathbf{0}$ with $A\mathbf{x}' = \mathbf{0}$ and having more 0 entries. By scaling $\mathbf{x}$ and permuting $\alpha_1, \ldots, \alpha_n$ if necessary, we can assume $x_1 = 1$. Also $C_1(\alpha_i) = H_1(\alpha_i) = \alpha_i$. So the first row of A is $(\alpha_1, \ldots, \alpha_{n+1})$ which are linearly independent over $H_2' \therefore$ not all x_i's are in H_2' so permuting α_i's if necessary, we can assume $x_2 \notin H_2' = K^{H_2} \therefore$ can pick $\sigma \in H_2$ such that $\sigma(x_2) \neq x_2$. Let $\sigma\mathbf{x} = \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_{n+1}) \end{pmatrix}$ which is a solution to

$$\underbrace{\begin{pmatrix} \sigma\left(C_1\left(\alpha_1\right)\right) & \cdots & \sigma\left(C_1\left(\alpha_{n+1}\right)\right) \\ \vdots & \ddots & \vdots \\ \sigma\left(C_n\left(\alpha_1\right)\right) & \cdots & \sigma\left(C_n\left(\alpha_{n+1}\right)\right) \end{pmatrix}}_{\sigma A} \begin{pmatrix} \sigma(x_1) \\ \vdots \\ \sigma(x_{n+1}) \end{pmatrix} = \mathbf{0}$$

σA is A with rows permuted since $\sigma C_1, \ldots, \sigma C_n$ is just the left cosets permuted. Therefore $A\sigma\mathbf{x} = \mathbf{0} \implies \mathbf{A}\underbrace{(\mathbf{x} - \sigma\mathbf{x})}_{\mathbf{x}'} = \mathbf{0}$. Now $x_i = 0$ iff $\sigma(x_i) = 0$, so $x_i = 0 \implies x_i' = 0$. Since $x_1 = 1$, $x_1' = x_1 - \sigma(x_1) = 1 - 1 = 0$. Also $x_2' = x_2 - \sigma(x_2) \neq 0$ by choice of σ. Therefore $\mathbf{x}'$ is a non-zero solution to $A\mathbf{x}' = \mathbf{0}$ with more 0 entries than $\mathbf{x}$. This is a contradiction, and thus the theorem is proved. □

7 Galois Correspondence

Same setup as in Section 6. Recall the bijection between closed objects (Theorem 5.9). Estimates from Section 6 gives:

Corollary 7.1. (a) *Let $H_1 \leq H_2 \leq G$. If H_1 is closed and $[H_2 : H_1] < \infty$ then H_2 is closed and $[H_2 : H_1] = [H_1' : H_2']$.*

(b) *Given intermediate fields $F \subseteq K_1 \subseteq K_2 \subseteq K$, suppose K_1 is closed and $[K_2 : K_1] < \infty$. Then K_2 is closed and $[K_2 : K_1] = [K_1' : K_2']$.*

Proof. (a) Theorem 6.1 and 6.2 give $[H_2 : H_1] \geq [H_1' : H_2'] \geq [H_2'' : H_1''] = [H_2'' : H_1]$ (since H_1 is closed). Proposition 5.6 shows $H_2'' \supseteq H_2$ and so equality must hold above and so $H_2'' = H_2$.

(b) Similar. Swap H's with K's.

□

7.1 Galois Extension

Definition 7.2. *An algebraic field extension K/F is* **Galois** *if F is closed. i.e. $F = F'' = K^{\mathrm{Gal}(K/F)}$*

Example 7.3. We saw before that $\mathbb{Q}$ is not closed in $K/\mathbb{Q} = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ therefore $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

Proposition 7.4. *Let K/F be a field extension.*

1. *$G := \mathrm{Gal}\,(K/F)$ is finite.*
2. *K/F Galois $\implies [K : F] = |G|$.*
3. *If $|G| \geq [K : F]$ then K/F is Galois.*

Proof. 1. Write $K = F(\alpha_1, \ldots, \alpha_n)$. Each α_i is algebraic over F so given $\sigma \in G$ Lemma 4.4 implies there are only finitely many possibilities for $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ $\therefore |G| < \infty$.

2. K/F Galois implies F is closed. Corollary 7.1 (b) implies $[K:F] = [F':K'] = [G:1]$ (as $F' = \mathrm{Gal}\,(K/F)$ and $K' = \mathrm{Gal}\,(K/K)) = |G|$

3.

$$\begin{array}{lll} [K:F] \leq |G| & = [G:1] & \text{because } 1 \leq G \text{ is closed} \\ & = [1':G'] & \text{by part 1 and Corrolary 7.1 (a)} \\ & = [K:F''] & \text{because } G' = K^G = F \end{array}$$

Again $F'' \supseteq F$ so dimension considerations imply $F = F''$ so F is closed K/F is Galois. □

Example 7.5. We saw $K/\mathbb{Q} = \mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ has $G := \mathrm{Gal}\,(K/\mathbb{Q}) = S_3$.

$$K = \mathbb{Q}1 \oplus \mathbb{Q}\sqrt[3]{2} \oplus \mathbb{Q}\sqrt[3]{4} \oplus \mathbb{Q}\omega \oplus \mathbb{Q}\sqrt[3]{2}\omega \oplus \mathbb{Q}\sqrt[3]{4}\omega.$$

So $[K:\mathbb{Q}] = 6 = |S_3|$. Thus by Proposition 7.4 (3), $K/\mathbb{Q}$ is Galois.

Theorem 7.6 (**Fundamental Theorem of Galois Theory (Galois Correspondence)**). *Let K/F be a finite Galois extension and $G := \mathrm{Gal}\,(K/F)$.*

(a) *There are inverse bijections*

$$H \longmapsto K^H$$

$$\left\{ \begin{array}{c} \textit{subgroups} \\ \textit{of } G \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \textit{intermediate} \\ \textit{fields of } K/F \end{array} \right\}$$

$$K_0' := \mathrm{Gal}\,(K/K_0) \longleftarrow\!\shortmid K_0$$

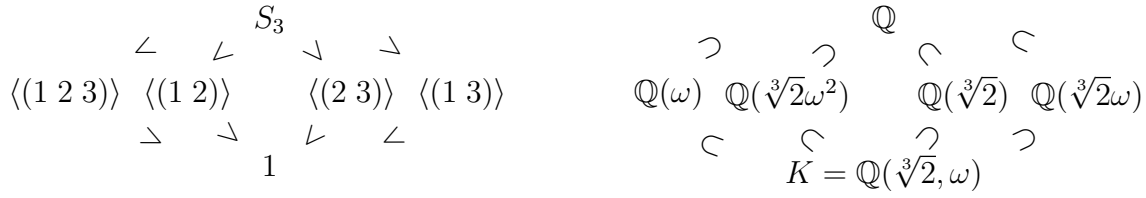
(b) *For intermediate field K_0, K/K_0 is Galois with Galois group* $\mathrm{Gal}\,(K/K_0) = K_0'$.

Proof. (a) By weak Galois correspondence suffice to show all objects are closed. Proposition 7.4 (1) implies $|G| < \infty$ so since $1 \leq G$ is closed, Corollary 7.1 (a) implies any $H \leq G$ is also closed. K/F Galois $\implies$ F is closed. Therefore any intermediate field K_0 is also closed by Corollary 7.1 (b).

(b) We need to show $K_0 = K^{\mathrm{Gal}(K/K_0)} = K_0''$ (w.r.t. K/F). This holds because K_0 is closed in K/F. Therefore K/K_0 is Galois too.

□

Example 7.5 (again). $K/\mathbb{Q} = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2)/\mathbb{Q}$, $G = \mathrm{Gal}\,(K/\mathbb{Q}) = S_3$.



Let's check $K^{\langle(1\ 2)\rangle} = \mathbb{Q}\left(\sqrt[3]{2}\omega^2\right)$. We know ($\supseteq$). Also

$$\left[K^{\langle(1\ 2)\rangle} : \mathbb{Q}\right] = \left[\mathbb{Q}' : \left(K^{\langle(1\ 2)\rangle}\right)'\right] = [S_3 : \langle(1\ 2)\rangle] = 3.$$

Since $\left[\mathbb{Q}\left(\sqrt[3]{2}\omega^2\right) : \mathbb{Q}\right] = 3$ too, we must have $K^{\langle(1\ 2)\rangle} = \mathbb{Q}\left(\sqrt[3]{2}\omega^2\right)$.

Theorem 7.7. *Let K be a field and G be a finite group of field automorphisms of K. If $K = F^G$, then K/F is Galois and its Galois group is G.*

Proof. Let $\widetilde{G} = \mathrm{Gal}\,(K/F)$ and note $G \leq \widetilde{G}$. Now

$$\begin{aligned} |\widetilde{G}| \geq |G| &= [G : 1] \\ &= [1' : G'] \quad \text{by Corollary 7.1 (a), since } 1 \leq G \text{ is closed} \\ &= \left[K : K^G\right] \\ &= [K : F] \end{aligned}$$

Therefore $[K : F] < \infty$ and so Proposition 7.4 (3) implies K/F is Galois. Also part 2 of the proposition, implies $G = \widetilde{G} = \mathrm{Gal}\,(K/F)$. □

8 Normality

Aim: Determine when intermediate field L of finite Galois extension K/F is such that L/F is Galois.

Galois $\implies$ Splitting Field

Definition 8.1. *K is a* **splitting field** *over F if it is the splitting field of some family of polynomials over F. We also say in this case that K/F is* **normal**.

Proposition 8.2. *Let K/F be a Galois extension (not necessarily finite) with Galois group G.*

1. *Let $\alpha \in K$ and $p(X) \in F[X]$ its minimal polynomial. Then $p(X)$ factors into linear factors over K.*

2. *K is the splitting field of $\{f_i\}$ over F where f_i ranges over the minimal polynomials of all $\alpha \in K$.*

Proof. (1) $\implies$ (2) is obvious. Proof of (1): Let $\alpha \in K$ and $p(X)$ its min. poly. Let $H := \{\sigma \in G \mid \sigma(\alpha) = \alpha\} \leq \mathrm{Stab}_G \alpha \leq G$. Consider

$$q(X) := \prod_{\substack{\sigma H \text{ left} \\ \text{coset}}} (X - (\sigma H)\,\alpha)\,,$$

which is well defined by the Remark from the proof of Theorem 6.2 and the product is finite because G-orbit of α is finite. But for any $\tau \in G$, $\tau q(X) = q(X)$ because it just permutes factors $(X - (\sigma H)\,(\alpha))$ since $q(X) \in K^G[X] = F[X]$ (since K/F is Galois). $\therefore p(X)|q(X)$ must factorise into linear factors over K because $q(X)$ does. □

8.1 Stability of Splitting Fields

Lemma 8.3. *Let K/F be an algebraic extension and $\sigma\colon K \to K$ be a field homomorphism over F. Then σ is an isomorphism.*

Proof. Suffice to show σ is surjective. Pick $\alpha \in K$, let $p(X) \in F[X]$ be its min. poly. and $\alpha = \alpha_1, \ldots, \alpha_r$ the roots of $p(X)$ in K. Let $L = F(\alpha_1, \ldots, \alpha_r)$. This is finite over F. But σ permutes α_i's $\implies \sigma(L) = L$. Dim. considerations $\implies \sigma|_L\colon L \hookrightarrow L$ is surjective. $\therefore \mathrm{im}\,\sigma \supseteq L \ni \alpha$. $\therefore \sigma$ is surjective. □

Proposition 8.4. *Let K be the splitting field of $\{f_i\}$ over F. Given field extension L of K and field homomorphism $\sigma : K \to L$ over F, we have $\sigma(K) = K$.*

Proof. By the previous lemma, it suffices to show $\sigma(K) \subseteq K$. Let $\{\alpha_j\}$ be the roots of all the f_i so K is generated over F by the α_j's. σ permutes these roots. So $\sigma(K) \subseteq K$. □

8.2 Galois Action on Galois Correspondence

Let K/F be a Galois extension, with $G = \mathrm{Gal}(K/F)$. G acts on:

1. $\{$intermediate fields of $K/F\}$ by $K_1 \longmapsto \sigma(K_1)$ (where $\sigma \in G$)

2. $\{$subgroups of $G\}$ by conjugation i.e. for $H \leq G$, $H \longmapsto \sigma H \sigma^{-1}$.

Galois correspondence is compatible with G-action as follows:

Proposition 8.5. *Notation as above.*

1. *If K_1 is an intermediate field $\sigma(K_1)' = \sigma K_1' \sigma^{-1}$ i.e.* $\mathrm{Gal}(K/\sigma(K_1)) = \sigma \mathrm{Gal}(K/K_1)\sigma^{-1}$.

2. *For $H \leq G$, $\sigma(H') = (\sigma H \sigma^{-1})'$*

Proof. 1. For $\tau \in G$, $\tau \in \mathrm{Gal}(K/\sigma(K_1))$ iff for any $\alpha \in K_1$, $\tau\sigma(\alpha) = \sigma(\alpha)$
$\iff$ for any $\alpha \in K_1$, $\sigma^{-1}\tau\sigma(\alpha) = \alpha$
$\iff$ $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(K/K_1)$
$\iff$ $\tau \in \sigma \mathrm{Gal}(K/K_1)\sigma^{-1}$.

2. Similar to above and is left as an exercise.

□

8.3 Normal Subgroups in Galois Correspondence

Theorem 8.6. *Let K/F be a finite Galois extension. Let $G = \mathrm{Gal}(K/F)$. If L is an intermediate field then L/F is Galois iff $L' = \mathrm{Gal}(K/L)$ is a normal subgroup. In this case* $\mathrm{Gal}(L/F) = G/L'$.

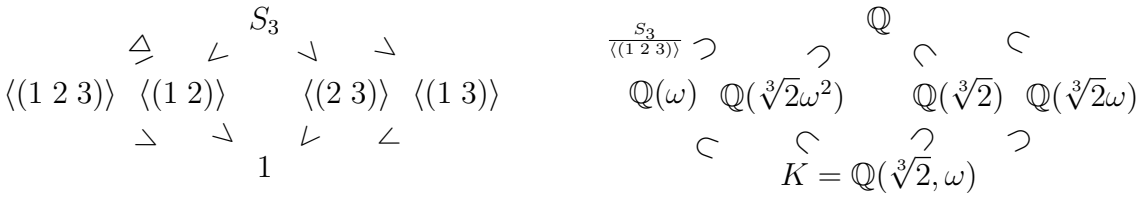
Proof. Suppose L/F is Galois so normal by Proposition 8.2. Given any $\sigma \in G$, Proposition 8.4 implies $\sigma(L) = L$. But then Proposition 8.5 $\implies$ $L' \trianglelefteq G$. Also we have a group homomorphism

$$\begin{aligned} \pi : \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}(L/F) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

Note $\ker \pi = \mathrm{Gal}(K/L) = L'$. Let $\bar{\sigma} \in \mathrm{Gal}(L/F)$. But K/L is a splitting field so uniqueness of splitting fields (Theorem 3.8) $\implies$ can extend $\bar{\sigma}$ to $\mathrm{Gal}(K/F)$ $\therefore$ π is surjective. 1st isomorphism theorem $\implies$ $\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(K/F)/\ker\pi = G/L'$.

Conversely, suppose $L' = \mathrm{Gal}(K/L) \trianglelefteq G$. Then Proposition 8.5 $\implies$ for any $\sigma \in G$, $\sigma(L) = L$. To show L/F is Galois, it suffices to show $F \supseteq L^{\mathrm{Gal}(L/F)}$. We know $F \supseteq K^{\mathrm{Gal}(K/F)}$ since K/F is Galois. Let $\alpha \in L - F$. There exists $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) \neq \alpha$. But $\sigma|_L \in \mathrm{Gal}(L/F)$ since $\sigma(L) = L$. Also, $\sigma|_L(\alpha) \neq \alpha$ so $\alpha \in L^{\mathrm{Gal}(L/F)}$ $\therefore$ $F \supseteq L^{\mathrm{Gal}(L/F)}$ and L/F is Galois too. □

Example 8.7. $K/\mathbb{Q} = \mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$, $\mathrm{Gal}\left(K/\mathbb{Q}\right) = S_3$.



9 Separability

Aim: Look at perversity in positive characteristic.

9.1 Inseparability

Let F be a field of characteristic $p \neq 0$.

Proposition/Definition 9.1. *Let K/F be a field extension. We say $\alpha \in K$ is* **purely inseparable** *over F if there is some $n \geq 1$ with $\alpha^{p^n} \in F$. In this case,* $\mathrm{Gal}\left(F\left(\alpha\right)/F\right) = 1$.

Proof. α satisfies $X^{p^n} - \alpha^{p^n} = (X - \alpha)^n \in F[X]$. Any $\sigma \in \mathrm{Gal}\left(F\left(\alpha\right)/F\right)$ sends α to α. Therefore, $\mathrm{Gal}\left(F\left(\alpha\right)/F\right) = 1$. □

Example 9.2. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $F = \mathbb{F}_p(t)$, $\alpha = \sqrt[p]{t} \notin F$, is purely inseparable over F and $F\left(\alpha\right)$ is a splitting field for $X^p - t$ over F with $\mathrm{Gal}\left(F\left(\alpha\right)/F\right) = 1$, so is Galois.

9.2 Separable Polynomials, Elements and Extensions

Let F be a field, $f(X) \in \sum_{j=0}^{n} f_j X^j \in F[X]$. We can define its derivative $f'(X) = \frac{df}{dX} = \sum j f_j X^{j-1} \in F[X]$.

Example 9.3. If F has char. $p \neq 0$ then for $a \in F$ $\frac{d}{dx}\left(X^{p^n} - a\right) = p^n X^{p^n - 1} = 0$.

Proposition 9.4. (a) $(f+g)' = f' + g'$, $(fg)' = f'g + fg'$ *for* $f, g \in F[X]$.

(b) *α is a multiple root of $f(X) \in F[X]$ iff $0 = f(\alpha) = f'(\alpha)$*

The proof is left as an exercise.

Definition 9.5. *Let K/F be a finite field extension. Its* **separable degree** *is $[K:F]_S :=$ number of field homomorphisms $\sigma: K \to \bar{K}$ over F. (Note $\bar{K} = \bar{F}$).*

Proposition/Definition 9.6. *Let $f(X) \in F[X]$ be irreducible. The following are equivalent:*

(a) *In the splitting field L of $f(X)$ over F, $f(X)$ factors into distinct linear factors;*

(b) $f'(X) \neq 0$*;*

(c) $[F(\alpha):F]_S = [F(\alpha):F]$ *where α is a root of $f(X)$.*

If these equivalent conditions hold, we say $f(X)$ and α are **separable** *over F.*

Proof. (a $\iff$ c) $[F(\alpha):F]_S =$ is the number of roots of $f(X)$ in $\bar{F}$. This is deg $f(X) = [F(\alpha):F]$ iff there is no multiple roots.
(a $\Rightarrow$ b) $f(X)$ has no multiple roots $\overset{\text{Prop 9.4 (b)}}{\Longrightarrow} f'(X) \neq 0$.
(b $\Rightarrow$ a) If (a) fails then there is a multiple root α of $f(X)$. Proposition 9.4 (b) implies $f(\alpha) = f'(\alpha) = 0$. But f is the min. poly. of α and deg $f' <$deg f so $f'(X) = 0$ so (b) fails too. □

Exercise: For field extensions K/L, L/F, if $\alpha \in K$ is separable over F, show that it is separable over L.

Definition 9.7. *A field extension K/F is* **separable** *if every $\alpha \in K$ is separable over F.*

9.3 Multiplicity of $[K:F]_S$

Theorem 9.8. *Let $K \supseteq L \supseteq F$ be a tower of finite field extensions. Then:*

(a) $[K:F]_S = [K:L]_S [L:F]_S$

(b) $[K:F]_S \leq [K:F]$ *and equality occurs iff K/F is separable.*

Proof. (a) Let $S = \{\sigma_i\}_{i=1}^{[K:L]_S}$ be distinct field homomorphisms $\sigma: K \to \bar{F}$ over L.
$T = \{\tau_j\}_{j=1}^{[L:F]_S}$ be distinct field homomorphisms $\tau: L \to \bar{F}$ over F.
Uniqueness of algebraic closure (Theorem 3.8) $\implies$ we can extend $\tau_j: L \to \bar{F}$ to field hom. $\tilde{\tau}_j: \bar{F} \to \bar{F}$. (a) follows from:
Claim: The distinct field hom. $\rho: K \to \bar{F}$ over F are the $\{\tilde{\tau}_j \sigma_i\}$. Why? If $\rho|_L = \tau_j$, then the τ_j is the unique element of T such that $\tilde{\tau}_j^{-1}\rho$ fixes L. i.e. $\tau_j^{-1}\rho \in S$. This proves claim.

(b) By induction on $[K:F]$. Pick any $\alpha \in K - F$.

$$\begin{array}{rcccc} [K:F]_S = & [K:F(\alpha)]_S & & [F(\alpha):F]_S & \\ & \wedge \,(\dagger) & & \wedge \,(*) & \\ [K:F] = & [K:F(\alpha)] & & [F(\alpha):F] & \end{array}$$

($\dagger$) holds by induction.
($*$) holds because

$$\begin{aligned} [F(\alpha):F] &= \#\text{ of roots } \alpha \text{ in } \bar{F} \\ &\leq \text{deg. of mi. poly. of } \alpha \text{ over } F \\ &= [F(\alpha):F] \end{aligned}$$

$\therefore [K:F]_S \leq [K:F]$. If K/F is separable, then by definition equality holds in $(*)$ and equality holds in $(\dagger)$ by induction.

Conversely, if $[K:F]_S = [K:F]$ then equality holds in $(*) \implies \alpha$ is separable over F. $\therefore K/F$ is separable too.

□

Corollary 9.9. (a) *Consider field extensions K/L, L/F. The K/F is separable iff K/L and L/F are separable.*

(b) *If field K is generated over F by separable elements $\{\alpha_i\}$ then K/F is separable.*

Proof. (a)

$$\begin{array}{rccc} [K:F]_S = & [K:L]_S & & [L:F]_S \\ \wedge & \wedge & & \wedge \\ [K:F] = & [K:L] & & [L:F] \end{array}$$

equality holds on LHS iff equality holds on RHS.

(b) Any $\alpha \in K$ lies in some $F(\alpha_{i_1}, \ldots, \alpha_{i_n})$. Now just apply (a) to $F \subseteq F(\alpha_{i_1}) \subseteq F(\alpha_{i_1}, \alpha_{i_2}) \subseteq \ldots$

□

10 Criterion for Galois

Aim: Show Galois extensions are separable splitting fields so separable extensions embed in Galois extensions.

10.1 Galois $\iff$ Separable Splitting field

Lemma 10.1. *Let K/F be a Galois extension. Let $L \subseteq F$ be a splitting field of some $f(X) \in F[X]$ over F. The L/F is Galois too.*

Proof. Let $\alpha \in L - F$. Since K/F is Galois, $F = K^{\mathrm{Gal}(K/F)}$ and can find $\sigma \in \mathrm{Gal}(K/F)$ with $\sigma(\alpha) \neq \alpha$. Proposition 8.4 on stability of splitting fields $\implies \sigma|_L \in \mathrm{Gal}(L/F)$. $\sigma|_L(\alpha) \neq \alpha \ \ \therefore L - F \subseteq L - L^{\mathrm{Gal}(L/F)}$ so $F \supseteq L^{\mathrm{Gal}(L/F)}$ and L/F is Galois too. □

Theorem 10.2. *K/F is a Galois extension iff K is a separable splitting field over F.*

Proof. ($\Rightarrow$) Proposition 8.2 $\implies$ K is a splitting field over F and for any $\alpha \in K$ with min. ploy. $f(X) \in F[X]$ over F, we know $f(X)$ factors into linears over K. Let $L \subseteq K$ be the splitting field of $f(X)$ over F. The above lemma $\implies$ L/F is Galois. So $[L:F] = |\mathrm{Gal}(L/F)| \leq [L:F]_S$. Theorem 9.8 $\implies$ L/F is separable $\implies$ α is separable over F. Since α was arbitrary K/F is separable.
($\Leftarrow$) Need to know $F \supseteq K^{\mathrm{Gal}(K/F)}$. Let $\alpha \in K - F$ and $f(X) \in F[X]$ its min. poly. over F. $\deg f(X) > 1$ (else $\alpha \in F$) and since α is separable there is a root α' of $f(X)$ with $\alpha \neq \alpha'$. Proposition 2.4 $\implies$ there is a field isomorphism $\tilde{\sigma}: F(\alpha) \xrightarrow{\sim} F(\alpha')$ over F such that $\tilde{\sigma}(\alpha) = \alpha'$. Uniqueness of splitting field K/F $\implies$ we can extend $\tilde{\sigma}$ to $\sigma \in \mathrm{Gal}(K/F) \ \ \therefore \sigma(\alpha) = \alpha' \neq \alpha$ and so $\alpha \notin K^{\mathrm{Gal}(K/F)}$. This shows $K - F \subseteq K - K^{\mathrm{Gal}(K/F)}$ so $F \supseteq K^{\mathrm{Gal}(K/F)}$ which shows K/F is Galois too. This proves theorem. □

Example 10.3. $\mathbb{Q}\left(\sqrt[3]{2}, \omega = e^{\frac{i2\pi}{3}}\right)/\mathbb{Q}$ is Galois and is separable (since char $= 0$) and is splitting field of $X^3 - 2$ over $\mathbb{Q}$.

10.2 Splitting Fields

Proposition 10.4. *The following are equivalent:*

(a) *K/F is a normal extension (i.e. K is a splitting field over F);*

(b) *for any $\alpha \in K$, if $f_\alpha(X)$ is its min. poly. over F, then $f_\alpha(X)$ factors into linear factors over K.*

Proof. (b $\Rightarrow$ a) K is the splitting field of $\{f_\alpha\}_{\alpha \in K}$ over F so K/F is normal. (a $\Rightarrow$ b) Let $\alpha' \in \bar{K}$ be any root of $f_\alpha(X)$. It suffice to show that $\alpha' \in K$. Proposition 2.4 $\implies$ there is a field isomorphism $\tilde{\sigma}: F(\alpha) \xrightarrow{\sim} F(\alpha')$ such that $\tilde{\sigma}(\alpha) = \alpha'$. Uniqueness of splitting fields Theorem 3.8 $\implies$ can extend

$\tilde{\sigma}$ to a field hom. $\sigma : K \to \bar{K}$. Stability of splitting fields (Proposition 8.4) $\implies \sigma(K) = K$. $\therefore \alpha' \in \sigma(K) = K$. Therefore, all roots of $f_\alpha(X)$ are in K and (b) holds. □

10.3 Normal Closure

Theorem 10.5. *Let K/F be an algebraic extension. For $\alpha \in K$, let $f_\alpha(X) \in F[X]$ be its minimal polynomial over F. Let $L \subseteq \bar{K}$ be the splitting field of $\{f_\alpha(X)\}_{\alpha \in K}$ over F, so in particular $L \supseteq K$.*

(a) *If L_1 is a subfield of $\bar{K}$ such that L_1/F is normal and $L_1 \supseteq K$ then $L_1 \supseteq L$.*

(b) *If K/F is separable, so is L/F (so L/F is Galois).*

(c) *If K/F is finite, so is L/F and L is splitting field of single polynomial $f(X) \in F[X]$ over F.*

Proof. (a) Follows from previous proposition.

(b) $\alpha \in K$ sep. over $F \implies f_\alpha(X)$ sep. poly. $\implies L$ is generated by separable elements (the roots of $f_\alpha(X)$) over F. Corollary 9.9 $\implies L/F$ is separable.

(c) Can write $K = F(\alpha_1, \ldots, \alpha_n)$. Let $f(X) = f_{\alpha_1}(X) f_{\alpha_2}(X) \ldots f_{\alpha_n}(X)$. Let $\tilde{F}$ be splitting field of $f(X)$ over F. Note $\tilde{L}/F$ is a finite normal extension. Also, it contains K since it contains $F, \alpha_1, \ldots, \alpha_n$. (a) $\implies \tilde{L} \supseteq L$. But definition shows $\tilde{L} \subseteq L$. $\therefore L/F$ is finite too.

. □

Definition 10.6. *The field L from Theorem 10.5 is called the* **normal closure** *of K (over F). If K/F is separable, we also call L the* **Galois closure** *of K (over F).*

Example 10.7. The Galois closure of $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ is $\mathbb{Q}\left(\sqrt[3]{2}, \omega = e^{\frac{i2\pi}{3}}\right)/\mathbb{Q}$.

Remark 10.8. In characteristic zero, where separability is guaranteed, can always "embed" finite extensions in finite Galois extensions.

11 Radical Extension

Aim: See what Galois correspondence reveals about radical extensions.

11.1 Radical Extensions

Recall K/F is a **radical** extension if there is tower of field extensions $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = K$, with $F_{i+1} = F_i\left(\sqrt[p_i]{\alpha_i}\right)$ for some $p_i \geq 1,\ \alpha_i \in F_i$.

N.B. If such a tower exists, can replace it with tower where all p_i are prime.

Example 11.1. $\mathbb{Q}\left(\sqrt{2+\sqrt{5}}\right)/\mathbb{Q}$ is radical.

11.2 Galois Group of Simple Radical Extension

Proposition 11.2. *Let F be a field of characteristic p and $n \geq 2$ be such that $p \nmid n$. Then the group of nth roots of unity in $\bar{F}^*$ is $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$.*

Proof. First note that $\frac{d}{dx}\left(X^n - 1\right) = nX^{n-1}$ so $X^n - 1$ has no repeated roots. So the set of roots μ_n has n distinct elements. Use structure theorem of finitely generated abelian groups to see

$$\mu_n \simeq \mathbb{Z}/h_1\mathbb{Z}\times\mathbb{Z}/h_2\mathbb{Z}\times\cdots\times\mathbb{Z}/h_r\mathbb{Z} \quad \text{where } h_1 \mid h_2 \mid \cdots \mid h_r \text{ and } h_1h_2\ldots h_r = n.$$

Now for any $z \in \mu_n$ we have $z^{h_r} = 1$. But no. of solns. to $z^{h_r} = 1$ is $\leq h_r$. $\therefore n = h_r$. Also must have then $r = 1$ so $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$. □

Lemma 11.3. *Let p be a prime and F be a field with all the pth roots of unity. For $\alpha \in F$, let $K = F\left(\sqrt[p]{\alpha}\right)$. Then:*

(i) *K/F is a splitting field for $X^p - \alpha$ over F;*

(ii) *If char $F \neq p$ and $\sqrt[p]{\alpha} \notin F$, then K/F is Galois with Galois group* $\mathrm{Gal}\left(K/F\right) \simeq \mu_p \overset{11.2}{\simeq} \mathbb{Z}/p\mathbb{Z}$;

(iii) *If char $F = p$ or $\sqrt[p]{\alpha} \in F$ then* $\mathrm{Gal}\left(K/F\right) = 1$.

Proof. (i) Proposition 11.2 $\Longrightarrow$ μ_p is a cyclic group, say generated by ω. N.B. $\mu_p = 1$ if char $F = p$ (derivative is zero) $\therefore$ the roots of $X^p - \alpha$ are $\sqrt[p]{\alpha}, \sqrt[p]{\alpha}\omega, \sqrt[p]{\alpha}\omega^2, \ldots, \sqrt[p]{\alpha}\omega^{n-1} \in F\left(\sqrt[p]{\alpha}\right) = K$. $\therefore$ K is splitting field for $X^p - \alpha$ over F.

(ii) Proposition 11.2 says if char $F \neq p$ then the roots $\sqrt[p]{\alpha}, \ldots, \sqrt[p]{\alpha}\omega^{n-1}$ are distinct. $\therefore$ $K = F\left(\sqrt[p]{\alpha}\right)/F$ is separable. Thus it is a separable splitting field and hence is Galois.

Let $\sigma \in \mathrm{Gal}\left(K/F\right)$. Then $\sigma\left(\sqrt[p]{\alpha}\right) = \sqrt[p]{\alpha}\omega^{i(\sigma)}$ for some $i\left(\sigma\right) \in \mathbb{Z}$. $\therefore \sigma\left(\sqrt[p]{\alpha}\omega^j\right) = \sqrt[p]{\alpha}\omega^{i(\sigma)}\omega^j$ and so σ just multiplies roots by $\omega^{i(\sigma)}$. Thus

we get an injective [1] group hom.

$$\begin{array}{rccc} \varphi\colon \mathrm{Gal}\,(K/F) & \hookrightarrow & \mu_p \simeq \mathbb{Z}/p\mathbb{Z} \\ \sigma & \longmapsto & \omega^{i(\sigma)} \end{array}$$

Since $\sqrt[p]{\alpha} \notin F$, $K \neq F$ and $\mathrm{Gal}\,(K/F) \neq 1$. Lagrange $\implies$ φ is an isomorphism.

(iii) Clear.

□

Lemma 11.4. *Let p be a prime and F be a field. Let K be a splitting field of $X^p - 1$ over F. Then* $\mathrm{Gal}\,(K/F)$ *is abelian.*

Proof. If $\mathrm{char}\, F = p$ then $X^p - 1 = (X-1)^p$ so $K = F$ and $\mathrm{Gal}\,(K/F) = 1$. So assume $\mathrm{char}\, F \neq p$ and suppose $\omega \in \mu_p$ generates μ_p. Note $K = F(\omega)$. Let $\sigma \in \mathrm{Gal}\,(K/F)$ so $\sigma(\omega) = \omega^{i(\sigma)}$ for some $i(\sigma) \in \mathbb{Z}$. Thus $\sigma(\omega^j) = \sigma(\omega)^j = \omega^{ji(\sigma)}$, i.e. σ raises root ω^j to the power of $i(\sigma)$. It is left as an exercise to show that action of any $\sigma, \tau \in \mathrm{Gal}\,(K/F)$ commutes. □

11.3 Solvability

Galois correspondence and Lemma 11.4 suggests:

Definition 11.5. *Let G be a group. A* **normal chain of subgroups** *is a sequence of the form*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

We say G is **solvable** *if there exists such a normal chain of subgroups with G_{i+1}/G_i cyclic of prime order (or trivial).*

In Section 13 we will show:

Theorem 11.6. *Let K/F be a field extension such that there exists a field extension L/F with L/F separable and radical. The* $\mathrm{Gal}\,(K/F)$ *is solvable.*

The main key to the proof is:

Theorem 11.7. *Consider tower of field extensions*

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_i \subseteq F_{i+1} \subseteq \cdots \subseteq F_n = K,$$

where $F_{i+1} = F_i(\sqrt[p_i]{\alpha_i})$ for some p_i and $\alpha_i \in F_i$. Suppose K/F is Galois and F contains all p_ith roots of unity. Then $G := \mathrm{Gal}\,(K/F)$ is solvable.

[1] Proving injectivity is left as an exercise

Proof. Galois correspondence gives:

$$G = F' = F'_0 \geq F'_1 \geq \cdots \geq F'_i \geq F'_{i+1} \geq \cdots \geq F'_n = 1 \qquad (*)$$

Note K/F_i is Galois. Also F_{i+1}/F_i is a normal extension by Lemma 11.3 and separable because K/F_i is Galois. Thus F_{i+1}/F_i is Galois. Therefore Theorem 8.6 $\implies$ $\mathrm{Gal}\,(K/F_{i+1}) = F'_{i+1} \trianglelefteq F'_i$. And also $F'_i/F'_{i+1} \simeq \mathrm{Gal}\,(F_{i+1}/F_i) \overset{11.3}{\simeq} \mathbb{Z}/p_i\mathbb{Z}$. Therefore $(*)$ is a normal chain of subgroups showing $G = F'$ is solvable. □

12 Solvable Groups

Aim: Find ways to verify (not) solvable.

12.1 Basic Fact

Proposition 12.1. *Let G be a finite group and $N \trianglelefteq G$, then G is solvable iff N and G/N is solvable.*

Proof. ($\Leftarrow$) Suppose we have normal chain of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_m = N$$

$$1_{G/N} = G_0/N \trianglelefteq G_1/N \trianglelefteq \cdots \trianglelefteq G_n/N = G/N$$

and N_{i+1}/N_i and $\frac{G_{i+1}/N}{G_i/N} \simeq \frac{G_{i+1}}{G_i}$ are cyclic of prime order. Then we get a normal chain of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

($\Rightarrow$) Suppose we have normal chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_r = G$$

with G_{i+1}/G_i cyclic of prime order. If $\pi : G \to G/N$ is the quotient map $g \mapsto gN$, then consider normal chain of subgroups:
1) $1 = G_0 \cap N \trianglelefteq G_1 \cap N \trianglelefteq G_2 \cap N \trianglelefteq \cdots \trianglelefteq G_r \cap N \trianglelefteq N$
2) $1_{G/N} = \pi\,(G_0) \trianglelefteq \pi\,(G_1) \trianglelefteq \cdots \trianglelefteq \pi\,(G_r) = G/N$.
Recall that $H < G_{i+1},\ K \trianglelefteq G_{i+1} \implies \frac{H}{H\cap K} \simeq \frac{HK}{K}$. Therefore

$$\frac{G_{i+1} \cap N}{(G_{i+1} \cap N) \cap G_i} \simeq \frac{(G_{i+1} \cap N)\, G_i}{G_i} \leq \frac{G_{i_1}}{G_1}$$

Note that G_{i+1}/G_i is cyclic of prime order. Therefore Lagrange $\Longrightarrow$ $\frac{G_{i+1}\cap N}{G_i}\cap$ N is cyclic prime order or trivial. Thus N is solvable. [2] Also

$$\begin{array}{ccc} \dfrac{G_{i+1}}{G_i} & \longrightarrow & \dfrac{\pi\left(G_{i+1}\right)}{\pi\left(G_i\right)} \\ gG_i & \longmapsto & \pi(g)\,\pi\left(G_i\right) \end{array}$$

is a surjective group hom. $\pi\left(G_{i+1}\right)/\pi\left(G_i\right)$ is cyclic of prime order or trivial. Thus G/N is solvable too. This proves proposition. □

Proposition 12.2. *A finite group G is solvable iff there is a normal chain of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_r = G$ with all G_{i+1}/G_i abelian.*

Proof. ($\Rightarrow$) By definition.
($\Leftarrow$) By induction and Proposition 12.1 suffice to show G is abelian then it is solvable. Assume G is abelian and pick $g \in G - 1$. Let p be a prime dividing the order n of g. Then $\langle g^{n/p}\rangle$ is cyclic of prime order so solvable and $G/\langle g^{n/p}\rangle$ is solvable by induction, so G is solvable by Proposition 12.1. □

12.2 Derived Series

Definition 12.3. *Let G be a group and $g, h \in G$. The* **commutator** *of g and h is $[g,h] = g^{-1}h^{-1}gh$. The* **commutator subgroup** *of G is the group generated by all $[g,h]$ as g, h range over G. It is denoted by $[G,G]$.*

Proposition 12.4. *Let G be a group.*

(a) $[G,G] \trianglelefteq G$.

(b) $G/[G,G]$ *is abelian.*

(c) *Given any normal subgroup, $N \trianglelefteq G$ with G/N abelian, we have $N \supseteq [G,G]$.*

Proof. (a) Let $g, h, k \in G$. $k[g,h]k^{-1} = [kgk^{-1}, khk^{-1}] \in [G,G]$. Thus $[G,G] \trianglelefteq G$.

(b) & (c) Let $g, h \in G$. $[g,h] \in N \Leftrightarrow g^{-1}h^{-1}ghN = N \Leftrightarrow ghN = hgN \Leftrightarrow (gN)(hN) = (hN)(gN)$. $[G,G]$ contains all $[g,h]$ so $G/[G,G]$ is abelian i.e. (b) holds. Also, if $gNhN = hNgN \quad \forall g, h$ then $N \supseteq [G,G]$ giving (c).

□

[2] Note that we never used the normality of N for this. This fact will be important later.

Definition 12.5. *Let G be a finite group. Its* **derived series** *is the normal chain of subgroups*

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq \cdots \trianglerighteq G^{(r)} \trianglerighteq \ldots \qquad (*)$$

where $G^{(r+1)} = \left[G^{(r)}, G^{(r)}\right]$.

Corollary 12.6. *A finite group G is solvable iff in the derived series $(*)$, $G^{(r)} = 1$ for some $r < \infty$.*

Proof. ($\Leftarrow$) Clear by Proposition 12.4 (b) and Proposition 12.2.
($\Rightarrow$) Consider normal chain of subgroups $G = G^0 \trianglerighteq G^1 \trianglerighteq \cdots \trianglerighteq G^r = 1$ with G^i/G^{i+1} abelian. Proof by induction on r, that $G^{(r)} \subseteq G^r$, $G^{(i+1)} = \left[G^{(i)}, G^{(i)}\right] \subseteq [G^i, G^i]$ (by induction) $\subseteq G^{i+1}$ (by Proposition 12.4 (c)). □

12.3 An Insolvable Group

Let $A(n)$ be a subgroup of S_n generated by 3-cycles. Note $A(n) \trianglelefteq S_n$, $A(n) \subseteq A_n$ (in fact $A(n) = A_n$).

Theorem 12.7. *Let $n \geq 5$.*

(a) $[A(n), A(n)] = A(n)$.

(b) *$A(n)$, A_n and S_n are not solvable.*

Proof. (a)⇒(b) by 12.6.
(a) Consider $e, f, g, h, k \in \{1, \ldots, n\}$ distinct.[3]

$$\underbrace{(efg)^{-1}(ehk)^{-1}(efg)(ehk)}_{[A(n), \bigcap A(n)]} = (egk).$$

Therefore $[A(n), A(n)] = A(n)$. □

13 Solvability by Radicals

Aim: Determine solvability by radicals.

Lemma 13.1. *Let L be a Galois closure of separable radical extension. Then L is radical.*

[3] Note that we need $n \geq 5$ for this

Proof. Consider tower of field extensions $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$ where $F_i = F_{i-1}(\alpha_i)$ and $\alpha^{p_i} \in F_{i-1}$ with p_i prime. Let L_0 be subfield of L generated over F by $\{\sigma(\alpha_i) \mid \sigma \in \mathrm{Gal}(L/F)\}$. Note $L_0 \supseteq K$. Now L_0/F is a radical extension so it suffices to show that $L_0 = L$. For any $\tau \in \mathrm{Gal}(L/F)$, τ permutes generators of L_0/F so $\tau(L_0) = L$. Proposition 8.5 implies $L_0' = \mathrm{Gal}(L/L_0) \trianglelefteq \mathrm{Gal}(L/F)$. Theorem 8.6 implies L_0/F is Galois. Minimality of Galois closure $L \Rightarrow L = L_0$. □

Theorem 13.2. *Let K/F be a field extension which "embeds" in a separable radical extension L/F in the sense that we have a tower of field extensions $F \subseteq K \subseteq L$. Then $\mathrm{Gal}(K/F)$ is solvable.*

Proof. We can replace F with $K^{\mathrm{Gal}(K/F)}$ since this leaves Galois group unchanged as well as the hypothesis. Thus we can assume K/F is Galois. Lets fix an algebraic closure $\bar{L}$ of L in which to work. Lemma 13.1 implies we may replace L with Galois closure in $\bar{L}$. Therefore can also assume L/F is Galois. Theorem 8.6 gives $\mathrm{Gal}(K/F) \simeq \frac{\mathrm{Gal}(L/F)}{\mathrm{Gal}(L/K)}$. So suffices to show $\mathrm{Gal}(L/F)$ is solvable. Therefore can now also have $L = K$.

Consider the tower of field extension $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = L$, where $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{p_i} \in F_{i-1}$ for some p_i prime. Note L/F separable $\Rightarrow p_i \neq \mathrm{char}\ F$. Let F_1 be splitting field of $\{X^{p_i} - 1\}_{i=1}^r$ over F. Let L_1 be subfield of $\bar{L}$ generated over L by roots of these $X^{p_i} - 1$. Note F_1/F is a separable normal extension so is Galois. Proposition 11.2 (or rather its proof) shows $\mathrm{Gal}(F_1/F)$ is abelian and hence solvable. Claim: L_1/F is separable normal therefore Galois. Why? L_1 is generated over F by the separable generators $\alpha_1, \ldots, \alpha_r$ of L/F and roots of $X^{p_i} - 1$. Also if L and F_1 are splitting fields of $f(X), g(X) \in F[X]$ over F then L_1 is splitting field of $f(X)g(X)$ over F, proves claim.

F_1/F Galois $\Rightarrow F_1' = \mathrm{Gal}(L_1/F_1) \trianglelefteq \mathrm{Gal}(L_1/F) = G$. L_1/F Galois $\Rightarrow L_1/F_1$ Galois. Also Theorem 11.7 and fact $L_1 = F_1(\alpha_1, \ldots, \alpha_r) \Rightarrow F_1' = \mathrm{Gal}(L_1/F_1)$ is solvable, so Proposition 12.1 implies $G = \mathrm{Gal}(L_1/F)$ is solvable. But $\mathrm{Gal}(L/F)$ is a quotient of $\mathrm{Gal}(L_1/F)$ so is solvable too. Theorem is proved. □

13.1 Solvability of polynomials

Definition 13.3. *Let F be a field and $f(X) \in F[X]$. The* **Galois group** *of $f(X)$ is $\mathrm{Gal}(K/F)$ where K is the splitting field of $f(X)$ over K. We say $f(X)$ is* **solvable by radicals** *if K/F embeds in a separable radical extension L/F as in theorem above.*

13.2 General degree n monic polynomial

Let $\alpha_1, \ldots, \alpha_n$ be indeterminants representing roots. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Let

$$a_1 = -(\alpha_1 + \cdots + \alpha_n), \quad a_2 = \sum_{i<j} \alpha_i \alpha_j, \quad \ldots, \quad a_n = (-1)^n \alpha_1 \alpha_2 \ldots \alpha_n.$$

Have "general" degree n monic polynomial $p(X) = X^n + a_1 X_{n-1} + a_2 X^{n-2} + \cdots + a_n$ whose roots are $\alpha_1, \ldots, \alpha_n$. Note S_n permutes $\alpha_1, \ldots, \alpha_n$ so acts on field K. Let $F = K^{S_n}$ and note that K/F is Galois with Galois group S_n. Also $a_i \in F$ so $p(X) \in F[X]$ and K is splitting field for $p(X)$ over F.

Corollary 13.4. *For $p(X)$, F, K as above. The Galois group of $p(X)$ (over F) is $S_n = \mathrm{Gal}(K/F)$. If $n \geq 5$, $p(X)$ is not solvable by radicals.*

14 Some Applications

Aim: Give example of polynomial not solvable by radicals. Show ubiquity of simple extension.

14.1 A polynomials not solvable by radicals

Fix p a prime.

Lemma 14.1. *Let $\sigma, \tau \in S_p$ be a p-cycle and a 2-cycle respectively. Then subgroup generated by σ, τ is S_p.*

Proof. Relabelling if need be, can assume $\tau = (1\ 2)$. Taking a power of σ if necessary and relabelling further, can assume $\sigma = (1\ 2\ \ldots\ p)$. $\sigma^i(1\ 2)\sigma^{-i} = (\sigma^i(1)\ \ \sigma^i(2)) = (i+1 \quad i+2) \pmod p$. But S_p is generated by such transpositions since any permutation of a row of elements can be gotten by switching neighbouring elements. □

Proposition 14.2. *Let $f(X) \in \mathbb{Q}[X]$ be irreducible of degree p. Suppose f has exactly 2 non-real roots. Then G = Galois group of $f(X)$ is S_p. Thus $f(X)$ is not solvable by radicals if $p \neq 5$.*

Proof. Let K be splitting field of $f(X)$ over $\mathbb{Q}$. Labelling roots as usual gives monomorphism $\phi : G \hookrightarrow S_p$. Conjugation c is an element of Galois group and $\phi(c) \in S_p$ is a 2-cycle. Let α be a root of $f(X)$. Then

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \,\Big|\, [K : \mathbb{Q}] = |G|$$

also $p = \deg f(X) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Thus, Sylow's theorem implies there is a Sylow p-subgroup of G which must have order p so is say generated by $\alpha \in G$. Therefore $\phi(\alpha)$ is a p-cycle. Thus $\phi(G) = S_p$ by Lemma 14.1. $\square$

Example 14.3. $f(X) = X^5 - 6X + 3$ is irreducible over $\mathbb{Q}$ by Eisenstein criterion. $f'(X) = 5X^4 - 6$. Therefore 3 real and 2 non-real roots. Proposition 14.2 implies $f(X)$ not solvable by radicals.

14.2 Primitive element theorem

Exercise: Use argument of Proposition 11.2 to show, if F is a finite field, then F^* is a cyclic group.

Theorem 14.4. *Let K/F be a finite separable extension. Then $K = F(\alpha)$ for some $\alpha \in K$.*

Proof. If F is finite, so is K, so simply let α be a generator of the cyclic group K^*. Thus $K = F(\alpha)$.

Suppose now F is infinite. Pick $\alpha \in K$ such that $[F(\alpha) : F]$ is maximal. Suppose $F(\alpha) \subsetneq K$ so can pick $\beta \in K - F(\alpha)$. Note K/F has only finitely many intermediate fields since the same is of the Galois closure L/F by the Galois correspondence. Pigeon hole principle implies we can find distinct $c_1, c_2 \in F$ with $F(\alpha + c_1\beta) = F(\alpha + c_2\beta)$. Note $F(\alpha + c_1\beta) \ni \alpha + c_2\beta$ and therefore β and also contains α. Therefore $F(\alpha + c_1\beta) \supsetneq F(\alpha)$. This contradicts maximality of $[F(\alpha) : F]$. Hence $K = F(\alpha)$. $\square$

14.3 Fundamental theorem of algebra

Theorem 14.5. $\mathbb{C} := \mathbb{R}\left[\sqrt{-1}\right]$ *is algebraically closed.*

Proof. We use the following facts about $\mathbb{R}$:

(a) Any odd degree real polynomial has a real root.

(b) Any complex quadratic polynomial has a complex root.

Proof by contradiction. Let $K/\mathbb{C}$ be a non-trivial finite field extension. Taking Galois closure if necessary we can assume $K/\mathbb{R}$ is Galois with Galois group G. Let P be a Sylow 2-subgroup of G so $2 \nmid \frac{|G|}{|P|}$. Note $\left[K^P : \mathbb{R} = K^G\right] = [G : P]$ is odd. Any $\alpha \in K^P$ has $[\mathbb{R}(\alpha) : \mathbb{R}] \mid \left[K^P : \mathbb{R}\right]$ so min. poly. of α over $\mathbb{R}$ is odd $\overset{\text{(a)}}{\Longrightarrow}$ $\alpha \in \mathbb{R}$ so $K^P = \mathbb{R} = K^G$ so $G = P$.

Lemma 14.6. *Let P be any 2-group. There is a chain of subgroups*

$$P = P_0 \triangleright P_1 \triangleright P_2 \triangleright \dots 1$$

with $[P : P_i] = 2^i$.

Proof. By induction on $|P|$, since P is a p-group ($p = 2$ here) $Z(P) \neq 1$. It suffices by induction to first find $P_1 \triangleleft P$ with $[P : P_1] = 2$. If $Z(P) \neq P$ we are done by applying inductive hypothesis, to $P/Z(P)$, to get $P_1/Z(P)$.

If $Z(P) = P$ then P_1 is abelian so you can find P, by hand, e.g. using structure theorem for finitely generated abelian groups. This proves the lemma. □

Back to proof of theorem. Pick $P = P_0 > P_1 > P_2 \dots$ as in lemma. $[P : P_1] = 2 \Rightarrow K^{P_2}$ is a degree 2 extension of $\mathbb{C}$. This is impossible by (b). This proves theorem. □

15 Trace and Norm

Aim: Introduce two tools to study field extension trace and norm.

15.1 Trace and Norm

Let K/F be a finite field extension of degree n.

Definition 15.1. *Let $\alpha \in K$ and let multiplication by α be $m_\alpha : K \to K$ an F-linear map. Represent m_α with $n \times n$-matrix over $\mathbb{F}$ M_α. We define the* **trace** *of α to be* $\mathrm{tr}_{K/F}\ \alpha = \mathrm{tr}\ \alpha = \mathrm{tr}\ \mathrm{M}_\alpha$, *and the* **norm of** *α to be* $N_{K/F}\ \alpha = \mathrm{N}\ \alpha = \det \mathrm{M}_\alpha$.

Note that tr, and N are well dell-define.

Example 15.2. If $\alpha \in F$ then $M_\alpha = \begin{pmatrix} \alpha & & \\ & \ddots & \\ & & \alpha \end{pmatrix}$. Therefore $\mathrm{tr}\ \alpha = \mathrm{n}\alpha$ and $\mathrm{N}\ \alpha = \alpha^{\mathrm{n}}$.

Notation 15.3 (Only for this section)**.** For a finite field extension L/F let $G_{L/F}$ be the set of field homomorphisms $L \to \bar{L}$ over F, so $|G_{L/F}| = [L : F]_S$.

Proposition 15.4. *Let K/F be a finite separable extension. Then for $\alpha \in K$*

$$\mathrm{tr}\ \alpha = \sum_{\alpha \in \mathrm{G_{K/F}}} \sigma(\alpha) \quad \textit{and} \quad \mathrm{N}\ \alpha = \prod_{\alpha \in \mathrm{G_{K/F}}} \sigma(\alpha)$$

Proof. Easy case: Suppose first $K = F(\alpha)$. Then (as in proof of Proposition 8.2) the min. poly. of α over F is $p(X) = \prod_{\sigma \in G_{K/F}} (X - \sigma(\alpha))$ because $\sigma(\alpha)$ are certainly roots of min. poly. and deg. $p(X) = |G_{K/F}| = [K:F]_S \overset{\text{separability}}{=\!=} [F(\alpha):F] =$ deg. of min. poly. Thus $p(X)$ is also the min. poly. of M_α ($p(M_\alpha) = 0$). But the characteristic poly. of M_α has degree $[F(\alpha):F] \Rightarrow p(X)$ is char. poly. of M_α. Therefore, $\mathrm{tr}\ \alpha = \mathrm{tr}\ \mathrm{M}_\alpha = \sum_{\sigma \in \mathrm{G_{K/F}}} \sigma(\alpha)$ and $\mathrm{N}\ \alpha = \det \mathrm{M}_\alpha = \prod_{\sigma \in \mathrm{G_{K/F}}} \sigma(\alpha)$.

General case: want to reduce to easy case. Recall from proof of Theorem 9.8 the following fact. Suppose $G_{F(\alpha)/F} = \{\tau, \ldots, \tau_{[F(\alpha):F]}\}$ and let $\tilde{\tau}_j : \bar{K} \to \bar{K}$ be arbitrary extension of τ_j. Then $G_{K/F} = \{\tilde{\tau}_j \rho \mid \tau_j \in G_{F(\alpha)/F},\ \rho \in G_{K/F(\alpha)}\}$. Therefore

$$\begin{aligned}\sum_{\sigma \in G_{K/F}} \sigma(\alpha) &= [K:F(\alpha)] \sum_{\sigma \in G_{F(\alpha)/F}} \sigma(\alpha) \\ &= [K:F(\alpha)]\, \mathrm{tr}_{F(\alpha)/F}\ \alpha \\ \prod_{\sigma \in G_{K/F}} \sigma(\alpha) &= \left(\prod_{\sigma \in G_{F(\alpha)/F}} \sigma(\alpha) \right)^{[K:F(\alpha)]}\end{aligned}$$

Let $\{\alpha_i\}$ be an F-basis for $F(\alpha)$ and suppose $m_\alpha : F(\alpha) \to F(\alpha)$ is represented by $\bar{M}_\alpha$ with respect to this basis. Let $\{\beta_j\}$ be an $F(\alpha)$-basis for K. With respect to F-basis for K $\{\alpha_i \beta_j\}$, $m_\alpha : K \to K$ is represented by matrix

$$\begin{pmatrix} \bar{M}_\alpha & & & \\ & \bar{M}_\alpha & & \\ & & \ddots & \\ & & & \bar{M}_\alpha \end{pmatrix}$$

$\mathrm{tr}_{K/F}\ \alpha = [K:F(\alpha)]\, \mathrm{tr}\ \bar{\mathrm{M}}_\alpha = [\mathrm{K}:\mathrm{F}(\alpha)]\, \mathrm{tr}_{\mathrm{F}(\alpha)/\mathrm{F}}\ \alpha$
$\mathrm{N}_{K/F}\ \alpha = \left(\det \bar{M}_\alpha\right)^{[K:F(\alpha)]} = \left(\mathrm{N}_{F(\alpha)/F}\ \alpha\right)^{[K:F(\alpha)]}$ so proposition follows from easy case. □

Example 15.5. Consider $K = \mathbb{Q}\left(\sqrt{d}\right)$, d square free integer. $K/\mathbb{Q}$ is

Galois, with Galois group $G = \left\{1, \sigma \colon \sqrt{d} \to -\sqrt{d}\right\}$. For $\alpha, \beta \in \mathbb{Q}$.

$$\begin{aligned} \mathrm{tr}_{K/\mathbb{Q}}\left(\alpha + \beta\left(\sqrt{d}\right)\right) &\overset{15.4}{=} \sum_{\tau \in G} \tau\left(\alpha + \beta\sqrt{d}\right) \\ &= \alpha + \beta\sqrt{d} + \alpha - \beta\sqrt{d} \\ &= 2\alpha \\ \mathrm{N}_{K/\mathbb{Q}}\left(\alpha + \beta\sqrt{d}\right) &= \left(\alpha + \beta\sqrt{d}\right)\left(\alpha - \beta\sqrt{d}\right) \\ &= \alpha^2 - d\beta^2 \end{aligned}$$

Number theorists are often interested in solving equations like $\alpha^2 - d\beta^2 = \gamma$ for certain $\gamma, \alpha, \beta \in \mathbb{Q}$.

15.2 Linear independence of characters

Theorem 15.6 (E.Artin)**.** *Let F, K be fields. Consider the distinct linear homomorphism $\chi_1, \ldots, \chi_n : F \to K$. Then these are linearly independent over K. i.e. if there are $a_1, \ldots, a_n \in K$ with*

$$a_1\chi_1(\alpha) + a_2\chi_2(\alpha) + \cdots + a_n\chi_n(\alpha) = 0 \qquad (*)$$

for all $\alpha \in F$ then all the $a_i = 0$.

Proof. By induction. Suppose we have non-trivial relation $(*)$ and pick with as many $a_i = 0$ as possible. (Can assume $a_1, a_2 \neq 0$). Pick $0 \neq \beta \in F$ with $\chi_1(\beta) \neq \chi_2(\beta)$. $(*) \Rightarrow$

$$0 = a_1\chi_1(\beta\alpha) + \cdots + a_n\chi_n(\beta\alpha)$$

$$0 = a_1\chi_1(\beta)\chi_1(\alpha) + \cdots + a_n\chi_n(\beta)\chi_n(\alpha) \qquad (\dagger)$$

$\chi_1(\beta)(*) - (\dagger))$ gives a shorter relation and thus the theorem is proved. □

Corollary 15.7. *Let K/F be a finite separable extension. There exists an element $\alpha \in K$ with $\mathrm{tr}_{K/F}\,\alpha = 1$.*

Proof. (Obvious if char $= 0$) Linear independence of characters implies $\sum_{\sigma \in G_{K/F}} \sigma \neq 0$. Pick $\alpha' \in K$ with

$$\sum_{\sigma \in G_{K/F}} \sigma(\alpha') = \beta \neq 0.$$

If $\alpha = \frac{\alpha'}{\beta}$, tr $\alpha =$ tr $\frac{\alpha'}{\beta} = \frac{1}{\beta}$tr $\alpha' = 1$. □

16 Cyclic Extensions

Aim: Galois theory says study filed extensions via the Galois group. Study implication of cyclic Galois group.

Definition 16.1. *A Galois extension is* **cyclic** *(resp.* **abelian***) if its Galois group is cyclic or abelian.*

Example 16.2. $\mathbb{Q}\left(\sqrt[n]{2},\ e^{\frac{2\pi i}{n}}\right)/\mathbb{Q}\left(e^{\frac{2\pi i}{n}}\right)$ is cyclic. $\mathbb{Q}\left(\sqrt{2},\ \sqrt{3}\right)/\mathbb{Q}$ is abelian.

16.1 Hilbert's theorem 90

Theorem 16.3 (Hilbert's theorem 90)**.** *Let K/F be a cyclic extension of degree n and Galois group $G = \langle\sigma\rangle$. Then $\alpha \in K$ satisfies $\mathrm{N}\ \alpha = 1$ if and only if $\alpha = \frac{\beta}{\sigma(\beta)}$ for some $\beta \in K$.*

Proof. ($\Leftarrow$)

$$\mathrm{N}\left(\frac{\beta}{\sigma(\beta)}\right) = \prod_{\tau\in G}\tau\left(\frac{\beta}{\sigma(\beta)}\right) = \frac{\beta}{\sigma(\beta)}\frac{\sigma(\beta)}{\sigma^2(\beta)}\frac{\sigma^2(\beta)}{\sigma^2(\beta)}\cdots\underbrace{\frac{\sigma^{n-1}(\beta)}{\sigma^n(\beta)}}_{\beta} = 1$$

($\Rightarrow$) Linear dependence of characters implies the function $f\colon K \to K$ defined by

$$f = \mathrm{id}+\alpha\sigma+[\alpha\sigma(\alpha)]\,\sigma^2+\left[\alpha\sigma(\alpha)\,\sigma^2(\alpha)\right]\sigma^3+\cdots+\left[\alpha\sigma(\alpha)\ldots\sigma^{n-2}(\alpha)\right]\sigma^{n-1} \neq 0.$$

We can find $\gamma \in K$ with $f(\gamma) =: \beta \neq 0$.

$$\sigma(f(\gamma)) = \sigma(\gamma)+\sigma(\alpha)\,\sigma^2(\gamma)+\sigma(\alpha)\,\sigma^2(\alpha)\,\sigma^3(\gamma)+\cdots+\underbrace{\sigma(\alpha)\,\sigma^2(\alpha)\ldots\sigma^{n-1}(\alpha)\,\underbrace{\sigma^n(\gamma)}_{\gamma}}_{\mathrm{N}(\alpha)\alpha^{-1}=\alpha^{-1}}$$

$$= \alpha^{-1}f(\gamma)$$

$$\therefore \alpha = \frac{\beta}{\sigma(\beta)}$$

□

Theorem 16.4. *Let K/F be a cyclic extension of degree n. Suppose char $F \nmid n$ and F contains all n nth roots of 1. Then $K = f(\beta)$ where β has min. poly. $X^n - b$ over F.*[4]

[4]The β is not unique

Proof. Let σ generate the Galois group G and ω be a primitive nth root of 1, so $\mu_n = \{\text{id}, \omega, \ldots, \omega^{n-1}\}$. $\omega \in F$ so $\mathrm{N}\,\omega = \omega^{\mathrm{n}} = 1$ so Hilbert's theorem 90 implies there exists some $\beta \in K$ with $\omega = \frac{\beta}{\sigma(\beta)}$ so $\sigma(\beta) = \omega^{-1}\beta$. Let $f(X)$ be the min. poly. of β over F. Then

$$f(X) = \prod_{i=0}^{n-1} \left(X - \sigma^i(\beta)\right) = \prod_{i=0}^{n-1} \left(X - \omega^{-i}\beta\right)$$

since $X - \sigma^i(\beta) \mid f(X)$ and $\deg f(X) \leq [K:F] = n$. Note $[F(\beta):F] = \deg f(X) = n \Rightarrow K = F(\beta)$. Direct expansion shows $f(X) = X^n - b$ where $b = \beta^n$. □

16.2 Artin-Schreier Theory

Theorem 16.5. *Let K/F be a cyclic extension of degree n and with Galois group $G = \langle\sigma\rangle$. Then $\alpha \in K$ satisfies* $\mathrm{tr}\,\alpha = 0$ *if and only if $\alpha = \beta\sigma(\beta)$*

Proof. ($\Leftarrow$) easy as in Hilbert's theorem 90. ($\Rightarrow$) Corollary 15.7 implies there is a $\gamma \in K$ with $\mathrm{tr}\,\gamma = 1$.

$$\begin{aligned}
\beta &= \alpha\gamma + \left[\alpha + \sigma(\alpha)\right]\sigma(\gamma) + \left[\alpha + \sigma(\alpha) + \sigma^2(\alpha)\right]\sigma^2(\gamma) + \ldots \\
&\quad \cdots + \left[\alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)\right]\sigma^{n-1}(\gamma) \\
\sigma(\beta) &= \sigma(\alpha)\sigma(\gamma) + \left[\sigma(\alpha) + \sigma^2(\alpha)\right]\sigma^2(\gamma) + \cdots + \left[\underbrace{\sigma(\alpha) + \sigma^2(\alpha) + \cdots + \alpha}_{0=\mathrm{tr}\,\alpha}\right]\gamma \\
\therefore \beta - \sigma(\beta) &= \alpha\left[\sigma(\gamma) + \sigma^2(\gamma) + \cdots + \sigma^{n-1}(\gamma) + \gamma\right] \\
&= \alpha\,\mathrm{tr}\,\gamma \\
&= \alpha
\end{aligned}$$

□

Theorem 16.6. *Let K/F be a Galois extension of prime degree p =*char *F. Then $K = F(\beta)$ where β has min. poly. $X^p - X - b$ over F.*

Proof. Since $[K:F]$ is prime then the Galois group $G = \langle\sigma\rangle$ is cyclic of prime order. Note that $\mathrm{tr}\,1 = \mathrm{p} = 0$ so Theorem 16.5 implies $1 = \beta - \sigma(\beta)$ or $\sigma(\beta) = \beta - 1$ for some $\beta \in K$. Since $\sigma(\beta) \neq \beta$, $\beta \notin K^G = F$. Therefore, as $[K:F]$ is prime, $F(\beta) = K$. Let $b = \beta^p - \beta$ so that β is a root of $F(X) := X^p - X - b$. Now $\sigma(\beta) = \sigma(\beta^p) - \sigma(\beta) = (\beta - 1)^p - (\beta - 1) = (\beta^p - 1 - \beta + 1) = \beta^p - \beta = b$. By induction, $\sigma^i(\beta) \Rightarrow b \in K^G = F$. So $f(X) \in F[X]$. It has the correct degree i.e. $[K:F] = [F(\beta):F]$ so is the min. poly. of β. □

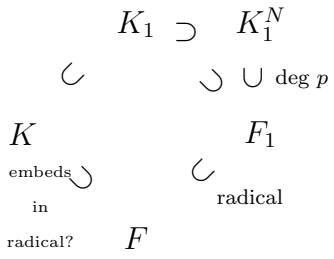
17 Solvable Extension

Aim: Study implication of a solvable Galois group.

Definition 17.1. *Let K/F be a finite separable extension. We say K/F is* **solvable** *if it is Galois closure has solvable Galois group.*

Theorem 17.2. *Let F be a field of char. 0. Then any solvable extension K/F embeds in a radical extension.*

Proof. We may pass to Galois closure of K/F and so assume K/F is Galois. Fix an algebraic closure $\bar{K}$ in which to work. Let $G = \mathrm{Gal}\,(K/F)$ and $n = |G|$. Let F_1 and K_1 be obtained from F and K respectively by adjoining all nth roots of 1. Since F_1/F is radical it satisfies to show K_1/F_1 embeds in a radical extension. As in proof of Theorem 13.2, K_1/F is Galois so K_1/F_1 is Galois too.



Now we need:

Lemma 17.3. (i) *$G_1 := \mathrm{Gal}\,(K_1/F_1)$ is isomorphic to a subgroup of G, an so*

(ii) *is solvable.*

Proof. (i)⇒(ii) by proof of Proposition 12.1. To prove (i), consider the restriction map

$$\begin{array}{rcl} \varphi\colon G_1 & \longrightarrow & \mathrm{Gal}\,(K/F) \\ \sigma & \longmapsto & \sigma|_K \end{array}$$

which is well-defined since K/F is Galois. We check injectivity of φ as follows. Suppose $\sigma \in \ker\varphi$ so fixes K. But $\sigma \in \mathrm{Gal}\,(K/F)$ so fixes also all nth roots of unity, and thus σ fixes K_1 i.e. $\sigma = 1$ in G_1. This proves lemma. □

Back to proof of theorem. Use induction on $n = |G|$ (is a multiple of $|G_1|$). Definition of solvable ⇒ there is $N \triangleleft G_1$ with G_1/N cyclic of prime order p.

Note $p \Big| |G|$. Theorem 8.6 $\Rightarrow K_1^N/F$ is Galois with Galois group G_1/N. This cyclic extension is radical by Theorem 16.4 (and the fact that $p \Big| |G|$). Also, K_1/K_1^N is Galois and has solvable Galois group N. By induction, K_1/K_1^N embeds in a radical extension. We see from the picture that K/F embeds in a radical extension. $\square$

Remark 17.4. (i) The above theorem is false in char. $= p > 0$ since there are cyclic extensions of deg p which can not be constructed by adjoining pth roots (since $X^p - a$ is not separable). But of we only assume K/F finite separable in theorem, we do have another version of the theorem provided in our tower of field extensions we allow not just nth roots but also roots of $X^p - X - a$.

(ii) In proof of theorem, it is easy to see that K_1/F_1 is in fact radical.

17.1 General cubic

Let $\omega = e^{\frac{2\pi i}{3}}$. $K + \mathbb{Q}(\omega, \alpha_1, \alpha_2, \alpha_3)$ where $\alpha_1, \alpha_2, \alpha_3$ are indeterminants. S_3 acts on K by permuting $\alpha_1, \alpha_2, \alpha_3$. Note if $F = K^{S_3}$ then K/F is a solvable Galois extension with Galois group S_3. Consider normal chain of subgroups $1 \triangleleft A_3 = \langle (1\ 2\ 3) \rangle \triangleleft S_3$. Galois correspondence gives tower of field extensions

$$K \overset{\text{Gal}}{\underset{A_3}{\supset}} K^{A_3} \overset{\text{Gal}}{\underset{S_3/A_3}{\supset}} K^{S_3} = F.$$

$\underline{K^{A_3}/F}$: is cyclic of degree 2 with Galois group $S_3/A_3 = \langle (1\ 2) A_3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Whats K^{A_3}? Let $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in K^{A_3}$. Note that the action of the Galois group of S_3/A_3 is $(1\ 2)A_3.\delta = -\delta \Rightarrow \delta \notin K^{S_3} = F$. Thus $K^{A_3} = F(\delta)$ (it's only deg. 2). Proof of Theorem 16.4 says $\delta^2 \in F$. Let's check directly: $\delta^2 \in K^{A_3}$. Also, $(1\ 2), (2\ 3), (1\ 3)$ all fixδ^2 so $\delta^2 \in K^{A_3} = F$.

$\underline{K/K^{A_3}}$: is cyclic of degree 3 with Galois group $A_3 = (1\ 2\ 3)$. From proof of Theorem 16.4 we know $K = K^{A_3}(\epsilon)$ with $\epsilon^3 \in K^{A_3}$ and ϵ can be any element of K with $(1\ 2\ 3).\epsilon = \omega^{\pm 1}\epsilon$. We may as well take $\epsilon = \alpha_1 + \omega\alpha_1 + \omega^2\alpha_2$ or $\alpha_1 + \omega^2\alpha_1 + \omega\alpha_2$. Now go back and look at first section of these notes.

$\underline{\text{What's } F\text{:}}$ Let $a_1 = -(\alpha_1 + \alpha_2 + \alpha_3)$ $a_2 = \alpha_1\alpha_2 + \alpha_2\alpha_2 + \alpha_3\alpha_1$ $a_3 = -\alpha_1\alpha_2\alpha_3$ all in $K^{S_3} = F$. In fact, one can show $F = \mathbb{Q}(\omega, a_1, a_2, a_3)$. Also, $K = F(\delta, \epsilon)$ so in principle you can solve the general cubic $X^3 + a_1X^2 + a_2X + a_3 = 0$.

18 Finite Fields

Aim: Classify and study finite fields via Galois theory.

Proposition 18.1. *Let K be a field.*

(i) *char* $K = p > 0$

(ii) $|K| = p^{[K:\mathbb{F}_p]}$

(iii) *K is a subfield of* $\bar{\mathbb{F}}_p$.

Proof. (i) Pigeon hole principle.

(ii) K is a $[K : \mathbb{F}_p]$-dim space over $\mathbb{F}_p$.

(iii) $K \subseteq \bar{K} \subseteq \mathbb{F}_p$ since $K/\mathbb{F}_p$ is algebraic.

□

18.1 Frobenius Homomorphism

Fix a prime p.

Proposition/Definition 18.2. *Let K be a field of char. p. The* **Frobenius homomorphism** *is the map*

$$\begin{aligned} \varphi\colon K &\longrightarrow K \\ x &\longmapsto x^p \end{aligned}$$

(i) *This is a field homomorphism.*

(ii) *If K is finite or is $\overline{\mathbb{F}_p}$, then φ is an automorphism.*

Proof. (i) $1^p = 1$, $(xy)^p = x^p y^p$ and $(x + y)^p = x^p + y^p$ since char. $= p$.

(ii) φ fixes 1 and therefore fixes all of $\mathbb{F}_p$. But in both cases of (ii) $K/\mathbb{F}_p$ is algebraic so Lemma 8.3 implies φ is an automorphism.

□

18.2 Classification of finite fields

Lemma 18.3. *Let K be a field with p^n elements, n a positive integer. Then any $\alpha \in K$ is a root of $X^{p^n} - X = 0$. Equivalently, if φ the Frobenius homomorphism $\varphi^n(\alpha) = \alpha$. In particular, φ^n is the identity on K.*

Proof. $\alpha = 0$ satisfies $X^{p^n} - X = 0$. On the other hand, if $\alpha \in K^*$, since K^* is a group of order $(p^n - 1)$ α has order dividing $p^n - 1$. i.e. $\alpha^{p^n} - 1 = 1 \ \therefore \alpha^{p^n} = \alpha$. This proves the lemma. □

Theorem 18.4. *Let $\phi\colon \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ be the Frobenius homomorphism.*

1. *The fixed field $\mathbb{F}_{p^n} := \overline{\mathbb{F}_p}^{\langle \varphi^n \rangle}$ is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.*
2. *$|\mathbb{F}_{p^n}| = p^n$.*
3. *If K is a subfield of $\overline{\mathbb{F}_p}$ with p^n elements, then $K = \mathbb{F}_{p^n}$.*
4. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic of degree n and Galois group $\langle \varphi|_{\mathbb{F}_{p^n}} \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.*
5. *$\overline{\mathbb{F}_p}/\mathbb{F}_p$ is Galois.*

Proof.

1. The elements fixed by φ^n are precisely the roots of $X^{p^n} - X$. Hence, $\mathbb{F}_{p^n}$ is the smallest field containing roots of $X^{p^n} - X$ so is the splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$.
2. $\mathbb{F}_{p^n}$ is the set of roots of $X^{p^n} - X$ and $X^{p^n} - X$ is separable over $\mathbb{F}_p$ so there are p^n roots.
3. Lemma 18.3.
4. Note $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Also, φ restricts to Frob. hom. on $\mathbb{F}_{p^n}$ i.e. $\varphi|_{\mathbb{F}_{p^n}} \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. So it suffices to show $\varphi|_{\mathbb{F}_{p^n}}$ has order n. Note by definition in (1) $\varphi|^n_{\mathbb{F}_{p^n}} = 1$. Suppose $\varphi|^m_{\mathbb{F}_{p^n}} = 1$. So φ^m fixes $\mathbb{F}_{p^n}$ and (1) $\Rightarrow$ $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}^{\langle \varphi^m \rangle} = \mathbb{F}_{p^m}$. Therefore $m \geq n$ and n must be the order of $\varphi|_{\mathbb{F}_{p^n}}$. Thus (4) holds.
5. $\mathbb{F}_p$ is closed in $\overline{\mathbb{F}_p}$ since the only elements fixed by $\varphi \in \mathrm{Gal}\left(\overline{\mathbb{F}_p}/\mathbb{F}_p\right)$ is $\mathbb{F}_p$ by (1) and (2).

□

Warning: Galois group of $\overline{\mathbb{F}_p}/\mathbb{F}_p$ is not φ.

18.3 Lattice of finite fields

Let p be a prime.

Corollary 18.5. (i) *The subfields of $\mathbb{F}_{p^n}$ are those of the form $\mathbb{F}_{p^d}$, $d|n$.*

(ii) *$\mathbb{F}_{p^n}/\mathbb{F}_{p^d}$ is cyclic of degree $\frac{n}{d}$.*

Proof. Let $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the Frobenius hom. which generates $\mathrm{Gal}\,(\mathbb{F}_{p^n}/\mathbb{F}_p)$ by Theorem 18.4 (4). Now any subfield K of $\mathbb{F}_{p^n}$ contains $\mathbb{F}_p$ so Galois correspondence says it corresponds to a subgroup of $\langle\varphi\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. These have form $\langle\varphi^d\rangle$ where $d|n$. Corresponding intermediate field is $\mathbb{F}_{p^n}^{\langle\varphi^d\rangle} \overset{\text{ex}}{\simeq} \mathbb{F}_{p^d}$. Also $\langle\varphi^d\rangle \trianglelefteq \langle\varphi\rangle$ so $\mathbb{F}_{p^n}/\mathbb{F}_{p^d}$ is a cyclic extension of degree $\frac{n}{d}$. □

Remark 18.6. The lattice of finite subfields of of $\overline{\mathbb{F}_p}$ is just the lattice of positive integers ordered by divisibility. E.g. if n, l are positive integers with l.c.m. m and g.c.d $= d$ then smallest subfield containing $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^l}$ is $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^l} = \mathbb{F}_{p^d}$.

18.4 Some examples

$\mathbb{F}_4/\mathbb{F}_2$: $\mathbb{F}_4$ is splitting field of $X^4 - X$ over $\mathbb{F}_2$ and $X^4 - X = X(X^3 - 1) = X(X-1)(X^2+X+1)$ and so $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/\langle X^2 \pm X + 1\rangle = \mathbb{F}_2(\alpha)$. This is an ""Artin-Schreier" extension of degree 2. Non-trivial element of Galois group is φ is Frob. hom. $\varphi(\alpha) = \alpha^2 = \alpha + 1$ which agrees with Artin-Schreier theory.

$\mathbb{F}_{2^6}/\mathbb{F}_{2^2}$: Cyclic degree 3. Now $\mathbb{F}_{2^2}$ has all 3 roots of 1 $\therefore \mathbb{F}_{2^6} = \mathbb{F}_{2^2}\left(\sqrt[3]{2}\right)$.

19 Pro-Finite Groups

Aim: Infinite Galois groups are best studied in the context of pro-finite groups which we introduce today.

19.1 Topological groups

Definition 19.1. *A* **topological group** *is a group G endowed with a topology such that:*

(i) *multiplication map $\mu\colon G \times G \to G$ is continuous;* [5]

(ii) *the inverse map $\eta\colon G \to G : g \mapsto g^{-1}$ is also continuous.*

[5] $G \times G$ is endowed with the product topology coming from G.

Example 19.2. $\mathbb{R}$ is a group with usual Euclidean topology is a topological group because $(a, b) \mapsto a + b$ and $a \mapsto -a$ are both continuous.

Exercise 19.3. A subgroup of a topological group with the subspace topology is a topological group.

Proposition 19.4. *Let G be a topological group.*

1. *For $g \in G$, left and right multiplication by g are continuous.*
2. *If $U \subseteq G$ is open and $g \in G$ then gU is open.*
3. *Let $U \leq G$ be an open subgroup. Then U is closed.*

Proof. 1. $G \longrightarrow G \times G \xrightarrow{\text{mult.}} G$ is continuous.
$h \longmapsto (g, h)$

2. Follows from (1).

3. $G - U = \bigcup_{g \notin U} gU$ is open.

□

Proposition 19.5. *Let $\{G_\alpha\}_{\alpha \in A}$ be a set of topological groups. Then $G := \prod_{\alpha \in A} G_\alpha$ endowed with the product topology is a topological group.*

Proof. $G \times G \longrightarrow G_\alpha \times G_\alpha \xrightarrow{\text{mult.}} G_\alpha$ is continuous, so $G \times G \to G$ is continuous. Similarly the inverse map is continuous. □

19.2 Inverse limits

Consider data of:

(i) a partially ordered set, $A, \leq$;

(ii) for each $\alpha \in A$ a group G_α;

(iii) for each $\alpha, \beta \in A$ with $\alpha \leq \beta$ a group homomorphism $\varphi_{\alpha\beta} \colon G_\alpha \to G_\beta$ such that for all $\alpha \leq \beta \leq \gamma$

$$G_\alpha \xrightarrow{\varphi_{\alpha\beta}} G_\beta \xrightarrow{\varphi_{\beta\gamma}} G_\gamma, \qquad G_\alpha \xrightarrow{\varphi_{\alpha\gamma}} G_\gamma$$

$\varphi_{\alpha\gamma} = \varphi_{\beta\gamma} \circ \varphi_{\alpha\beta}$

Definition 19.6. *These data are said to be:*

(i) *an* **inverse system of groups** *if for any $\beta, \gamma \in A$, there is some $\alpha \in A$ with $\alpha \leq \beta$ and $\alpha \leq \gamma$;*

(ii) *a* **direct system** *if for any $\beta, \gamma \in A$ there is some $\delta \in A$ with $\delta \geq \beta$ and $\delta \geq \gamma$.*

Proposition/Definition 19.7. *Let $\{G_\alpha\}$ be an inverse system of groups as above. Let*

$$G = \left\{ (g_\alpha) \in \prod_{\alpha \in A} G_\alpha \;\middle|\; \varphi_{\alpha\beta}(g_\alpha) = g_\beta \right\}.$$

Then G is a subgroup of $\prod G_\alpha$ called the **inverse limit** *of the inverse system $\{G_\alpha\}$. It is denoted $\varprojlim_{\alpha \in A} G_\alpha$.*

Example 19.8. Fix a prime number p. Let $A = \{\ldots, -3, -2, -1\}$ ordered by $\leq$.

$$\begin{array}{ccccccccc} & & G_{-4} & & G_{-3} & & G_{-2} & & G_{-1} \\ & & \| & & \| & & \| & & \| \\ \cdots & \longrightarrow & \mathbb{Z}/p^4\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^3\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & & & & a + p^3\mathbb{Z} & \longmapsto & a + p^2\mathbb{Z} & \longmapsto & a + p\mathbb{Z} \end{array}$$

This inverse system has an inverse limit denoted $\hat{\mathbb{Z}}_p$ called the **ring of p-adic integers**. Consider a formal power series in p, $q = \sum_{i=0}^{\infty} a_i p^i$ where $a_i \in \{0, 1, \ldots, p-1\}$. Then q represents an element of $\hat{\mathbb{Z}}_p$ as follows:

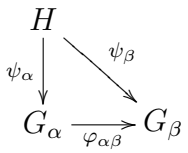
$$\begin{array}{ccccccc} \cdots & \longrightarrow & \mathbb{Z}/p^3\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ \cdots & \longmapsto & a_0 + a_1 p + a_2 p^2 + p^3\mathbb{Z} & \longmapsto & a_0 + a_1 p + p^2\mathbb{Z} & \longmapsto & a_0 + p\mathbb{Z} \\ & & \| & & \| & & \| \\ & & q + p^3\mathbb{Z} & & q + p^2\mathbb{Z} & & q + p\mathbb{Z} \end{array}$$

Example 19.9. Let A be the set of positive integers. We order A by $m \preceq n$ if $n|m$. Define inverse system as follows: $G_n := \mathbb{Z}/n\mathbb{Z}$ and if $m \preceq n$ so $n|m$ we define

$$\begin{array}{rccc} \varphi_{mn} \colon & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & Z/n\mathbb{Z} \\ & a + m\mathbb{Z} & \longmapsto & a + n\mathbb{Z}. \end{array}$$

Note that this is well-defined as $m\mathbb{Z} \subseteq n\mathbb{Z}$. The corresponding inverse limit is denoted $\hat{\mathbb{Z}}$.

Proposition 19.10 (Universal property of inverse limits)**.** *Let* $\{G_\alpha, \varphi_{\alpha\beta}\}$ *be an inverse system of groups and* $G = \varprojlim G_\alpha \leq \prod G_\alpha$*. Let* $\pi_\alpha : G \to G_\alpha$ *be the natural projection. Suppose* H *is a group and for each* $\alpha \in A$ *we have a group homomorphism* $\psi_\alpha : H \to G_\alpha$



satisfying $\psi_\beta = \varphi_{\alpha\beta} \circ \psi_\alpha$ *whenever* $\alpha \leq \beta$*. Then there is a unique group homomorphism* $\psi : H \to \varprojlim G_\alpha$ *such that* $\pi_\alpha \circ \psi = \psi_\alpha$

The proof is left as an (easy) exercise.

19.3 Pro-finite groups

Definition 19.11. *A* **pro-finite group** G *is a group that is (isomorphic to) an inverse limit of an inverse system* $\{G_\alpha\}$ *of finite groups, i.e. all the* G_α *are finite. Put discrete topology on the* G_α *which makes* $\prod G_\alpha$ *a topological group and hence* G *is also a topological group.*

Lemma 19.12. *Let* $G = \varprojlim G_\alpha$ *be a profinite group with* $G+_\alpha$ *finite.*

(i) $G \leq \prod G_\alpha$ *is closed.*

(ii) G *is compact.*

(iii) *The open subgroups are the closed subgroups of finite index.*

Proof. (i) Let $(g_\alpha) \in \prod G_\alpha - G$. So for some $\beta \leq \gamma$, $\varphi_{\beta\gamma}(g_\beta) \neq g_\gamma$.Then $U = \left\{(h_\alpha) \in \prod G_\alpha \;\middle|\; h_\beta = g_\beta,\ h_\gamma = g_\gamma\right\}$ is an open neighbourhood of (g_α) disjoint from G.

(ii) Follows from (i) and Tychoroff.

(iii) Suppose $U \leq G$ is open. Then disjoint cosets form an open open cover which is finite by compactness. Therefore $[G : U] < \infty$. Conversely, if $U \leq G$ is closed and $[G : U] < \infty$ the complement is a finite union of closed cosets, so is closed.

□

20 Infinite Galois Groups

Aim: View Galois groups as pro-finite groups.

20.1 Inverse system of finite Galois groups

Lemma 20.1. *Let K/F be a Galois extension (not necessarily finite) with Galois group G. Let L be an intermediate field with L/F Galois too. Then the restriction map*

$$\begin{array}{rcl} \rho\colon G & \longrightarrow & \mathrm{Gal}\,(L/F) \\ \sigma & \longmapsto & \sigma|_L \end{array}$$

is a well defined group homomorphism with kernel $L' := \mathrm{Gal}\,(K//)\,L$. Also ρ is surjective.

Proof. This is half of Theorem 8.6 which was stated with the additional hypothesis K/F finite. Proof doesn't require this hypothesis. □

Consider the following set up: let K/F be a Galois field extension with Galois group G.

(i) $A =$ set of subfields K_α of K such that K_α/F is finite Galois. Order A by inclusion; i.e. A is "like":

$$\begin{array}{ccccc} & & K_\beta & \cdots & \\ & \subsetneq & & \subsetneq & \\ F \subseteq K_\alpha & & & & K_\delta \cdots \\ & \subsetneq & & \subsetneq & \\ & & K_\gamma & \cdots & \end{array}$$

This is a direct system. Why? Let L be the smallest field containing $K_\beta, K_\gamma \in A$. Then L is finite over F being finitely generated by algebraic elements, and Galois closure of L is also finite over F.

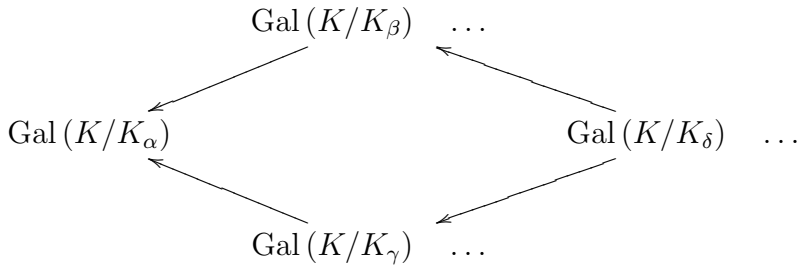
(ii) Apply Galois correspondence.

$$\begin{array}{ccccc} & & N_\beta := \mathrm{Gal}\,(K/K_\beta) & & \cdots \\ & \supsetneq & & \subsetneq & \\ N_\alpha := \mathrm{Gal}\,(K/K_\alpha) & & & & N_\delta := \mathrm{Gal}\,(K/K_\delta) \ldots \\ & \subsetneq & & \supsetneq & \\ & & N_\gamma := \mathrm{Gal}\,(K/K_\gamma) & & \cdots \end{array}$$

If $N_\beta \subseteq N_\alpha$ as above there's a natural map

$$\begin{array}{ccc} gN_\beta & \longmapsto & gN_\alpha \\ \varphi_{\alpha\beta}\colon G/N_\beta & \longrightarrow & G/N_\alpha \\ \wr\downarrow & & \wr\downarrow \\ \mathrm{Gal}\,(K_\beta/F) & \longrightarrow & \mathrm{Gal}\,(K_\alpha/F) \\ \sigma & \longmapsto & \sigma|_{K_\alpha} \end{array}$$

Note $\mathrm{Gal}\,(K_\alpha/F)$ is finite so get



This is an inverse system of finite groups.

20.2 Infinite Galois groups

Theorem 20.2. *Let K/F be a Galois extension with Galois group G. Then*

$$G \simeq \varprojlim \mathrm{Gal}\,(K_\alpha/F)$$

where the limit is taken over all the K_α subfields of K such that K_α/F is a finite Galois extension. In particular, G is pro-finite.

Proof. We consider the restriction map in Lemma 20.1

$$\rho_\alpha \colon G \longrightarrow \mathrm{Gal}\,(K_\alpha/F)\,.$$

Also, if $K_\alpha \subseteq K_\beta$ are finite Galois "sub-extensions "

$$\begin{array}{ccc} \mathrm{Gal}\,(K/F) = G & & \\ {\scriptstyle \rho_\beta}\downarrow & \searrow^{\rho_\alpha} & \\ \mathrm{Gal}\,(K_\beta/F) & \xrightarrow{\varphi_{\alpha\beta}} & \mathrm{Gal}\,(K_\alpha/F) \end{array}$$

$$\therefore \rho_\alpha = \varphi_{\alpha\beta} \circ \rho_\beta.$$

So by the universal property of inverse limits we have a group homomorphism

$$\begin{array}{rcl} \rho \colon G & \longrightarrow & \varprojlim \mathrm{Gal}\,(K_\alpha/F) \\ \sigma & \longmapsto & \sigma|_{K_\alpha} \end{array}$$

To show that ρ is injective, suppose $\rho\,(\sigma) = 1$. Thus for any finite Galois sub extension K_α/F, $\sigma_{K_\alpha} = \mathrm{id}_{K_\alpha}$. But $K = \bigcup K_\alpha$ where the union is taken over all finite Galois sub-extensions K_α so $\sigma = \mathrm{id}_K$, so ρ is injective.

To show that ρ is surjective consider $(\sigma_\alpha) \in \varprojlim \mathrm{Gal}\,(K_\alpha/F)$. We wish to find $\sigma \in G$ with $\rho\,(\sigma) = (\sigma_\alpha)$. Pick $\epsilon \in K$. There exists a finite Galois

sub-extension K_β/F with $\epsilon \in K_\beta$. We define $\sigma(\epsilon) = \sigma_\beta(\epsilon) \in K_\beta \subseteq K$. This is well-defined, for if $\epsilon \in K_\gamma$ there is another finite Galois sub extension K_δ containing K_β and K_γ.

$$\begin{array}{ccc} \sigma_\beta(\epsilon) = \sigma_\delta\big|_{K_\beta}(\epsilon) & = & \sigma_\delta(\epsilon) \\ & \diagup\!\diagup & \\ \sigma_\gamma(\epsilon) & & \end{array}$$

Note that $\sigma_\delta\big|_{K_\beta} = \sigma_\beta$. Therefore, σ is well-defined. A similar argument shows it is a field automorphism of K fixing F. Clearly $\rho(\sigma) = (\sigma_\alpha)$. Hence ρ is surjective and theorem is proved. □

20.3 Absolute Galois group

Proposition/Definition 20.3. *Let F be a field and F^{sep} be the set of elements in $\overline{F}$ which are separable over F*

(i) *F^{sep} is a field.*

(ii) *F^{sep}/F is Galois.*

F^{sep} is called the **separable closure** *of F.*

Proof. (i) Essentially because fields generated by separable elements are separable.

(ii) We need only show F^{sep} is normal over F. But any separable polynomial (over F) has all roots separable so if $f(X) \in F[X]$ has a root in F^{sep} then all roots are in F^{sep}.

□

Definition 20.4. *Let F be a field. The* **absolute Galois group of** *F is* $\text{Gal}(F^{\text{sep}}/F)$.

Example 20.5. Fix a prime p. What is the absolute Galois group of $\mathbb{F}_p$? Answer: $\text{Gal}\left(\mathbb{F}_p^{\text{sep}}/\mathbb{F}_p\right) \simeq \hat{\mathbb{Z}}$. Why? The finite Galois sub-extensions are $\mathbb{F}_{p^n}/\mathbb{F}_p$ which has Galois group $\mathbb{Z}/n\mathbb{Z}$. Lattice of finite fields is positive integers reverse ordered by divisibility. Hence the inverse system of finite Galois groups is $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ with $n|m$ and $\mathbb{Z}/n\mathbb{Z} \leftarrow \mathbb{Z}/m\mathbb{Z}$. This is the inverse system we used to define $\hat{\mathbb{Z}}$.

21 Infinite Galois Theory

Aim: Exhibit the Galois correspondence in the infinite case by determining closed objects.

21.1 Basic facts about pro-finite groups

Let $G = \varprojlim_{\alpha \in A} G_\alpha$ be a pro-finite group with all G_α finite. Let $\pi_\alpha : G \to G_\alpha$ be natural projection map. Note $\{1_{G_\alpha}\} \subseteq G_\alpha$ is open. Hence $U_\alpha := \ker \pi_\alpha = \pi_\alpha^{-1}(1)$ is an open subgroup of G. It is often called a **fundamental open neighbourhood of** 1.

Proposition 21.1. *With the above notation:*

1. *The U_α form a basis of open nbhds of 1 i.e. if U is an open nbhd of 1 then, $U \supseteq U_\alpha$ for some α.*
2. *If $\sigma \in G$, then $\{\sigma U_\alpha\}$ form a basis of open nbhds of σ.*
3. *G is a Hausdorff so in particular points are closed.*

Proof. 1. Note that $\left\{\pi_\beta^{-1}(g_\beta) \subseteq G \;\middle|\; \text{for some } \beta \in A,\ g_\beta \in G_\beta\right\}$ is a subbase for the topology on G. Note $\pi_\beta^{-1}(g_\beta) \ni 1_G$ iff $g_\beta = 1$. $\therefore$ it suffices to show that any finite intersection $\bigcap_{j=1}^{n} U_{\alpha_j} \supseteq U_\alpha$ for some α. But the $\{G_\alpha\}$ form an inverse system so you can find $\alpha \in A$ with $\alpha \leq \alpha_j$ for $j = 1, \ldots, n$. But now

$$\begin{array}{ccc} G & & \\ \downarrow{\scriptstyle \pi_\alpha} & \searrow^{\pi_{\alpha_j}} & \\ G_\alpha & \xrightarrow{\varphi_{\alpha\alpha_j}} & G_{\alpha_j} \end{array}$$

$$\begin{array}{ccc} \pi_\alpha^{-1}(1) & \subseteq & \pi_{\alpha_j}^{-1}(1) \\ \| & & \| \\ U_\alpha & & U_{\alpha_j} \end{array}$$

$$\therefore U_\alpha \subseteq \bigcap_{j=1}^{n} U_{\alpha_j}$$

2. (1)$\Rightarrow$(2) since multiplication by σ is bicontinous.

3. Suppose $(g_\alpha), (h_\alpha)$ are distinct elements of G so say $g_\beta \neq h_\beta$ for some $\beta \in A$. Then $\pi_\beta^{-1}(g_\beta), \pi_\beta^{-1}(h_\beta)$ are disjoint open nbhds of (g_α) and (h_α).

□

21.2 Infinite Galois correspondence

Let K/F be a Galois extension with Galois group G. We wish to show topologically closed subgroups of G are precisely the subgroups which are closed a la Section 5.

Lemma 21.2. *With notation as above, let L be an intermediate field of K/F.*

1. *The $L' := \mathrm{Gal}(K/L) \leq G$ is a topologically closed.*
2. *The subspace topology on L' is the same as that coming from its structure as a pro-finite group.*

Proof. 1. We first prove the case where L/F is finite. Pick $\tilde{L} \subseteq K$ a Galois closure of L/F. Note $\tilde{L}/F$ is finite. $\left(F \subset L \subset \tilde{L} \subset K\right)$. Have restriction map:

$$\begin{aligned} \pi \colon G = \mathrm{Gal}(K/F) &\longrightarrow \mathrm{Gal}\left(\tilde{L}/F\right) \\ H := \pi^{-1}\left(\mathrm{Gal}\left(\tilde{L}/L\right)\right) &\longmapsto \mathrm{Gal}\left(\tilde{L}/L\right) \end{aligned}$$

Now $\mathrm{Gal}\left(\tilde{L}/F\right)$ has discrete topology so $\mathrm{Gal}\left(\tilde{L}/L\right) \subseteq \mathrm{Gal}\left(\tilde{L}/F\right)$ is topologically closed. Therefore, $H := \pi^{-1}\left(\mathrm{Gal}\left(\tilde{L}/L\right)\right) \subseteq G$ is also topologically closed. It suffices thus to show $H = \mathrm{Gal}(K/L)$. But π is restriction so $H \leq \mathrm{Gal}(K/L)$ as $\sigma \in H \Rightarrow \sigma|_{\tilde{L}} \in \mathrm{Gal}\left(\tilde{L}/L\right)$ so fixes L. Similarly, $\mathrm{Gal}(K/L) \subseteq H$.

Now if L/F is infinite, write $L = \bigcup L_\alpha$ where $L - \alpha/F$ are finite subextensions. If $\sigma \in G$, then to be in $\mathrm{Gal}(K/L)$ means σ fixes every L_α. $\mathrm{Gal}(K/L) = \bigcap \mathrm{Gal}(K/L_\alpha)$ so it topologically closed by the L/K finite case.

2. Left as an exercise. Hint: Let $f(X) \in F[X]$ and $\tilde{F}, \tilde{L} \subseteq K$ be the splitting fields of f over F and L respectively. Then $U_1 := \ker\left(G \to \mathrm{Gal}\left(\tilde{F}/F\right)\right)$

is a fundamental open neighbourhood of G and $U_2 := \ker\left(\mathrm{Gal}\,(K/L) \to \mathrm{Gal}\left(K/\tilde{L}\right)\right)$ is a fund. open nbhd. of $1_{\mathrm{Gal}(K/F)}$ and observe $U_2 = \mathrm{Gal}\,(K/L) \bigcap U_1$. □

Theorem 21.3. *Let K/F be a Galois extension with Galois group G. There are inverse bijections*

$$H \longmapsto H' := K^H$$

$$\left\{\begin{array}{c}\text{top. closed} \\ \text{subgroups } H \leq G\end{array}\right\} \begin{array}{c}\longrightarrow \\ \longleftarrow\end{array} \left\{\begin{array}{c}\text{intermediate field} \\ L\end{array}\right\}$$

$$L' := \mathrm{Gal}\,(K/L) \longleftarrow L$$

Proof. Use weak Galois correspondence. We first show any intermediate field L is closed. K/F is separable and normal $\Rightarrow$ K/L is also such. Thus K/L is Galois i.e. $L = K^{\mathrm{Gal}(K/L)} = L''$. So L is closed a la Section 5.

Let $H \leq G$ be a top. closed subgroup. We wish to show it is closed a la Section 5 i.e. $H \supseteq H'' = \mathrm{Gal}\left(K/K^H\right)$. Of course $H'' \supseteq H$ so by Lemma 21.2 we may assume $F = K^H$. Let $\sigma \in \mathrm{Gal}\left(K/K^H\right)$ and L/K^H a finite Galois sub-extension of K/K^H. Consider fundamental open nbhd of 1.

$$U := \ker\left(\mathrm{Gal}\left(K/K^H\right) \xrightarrow{\pi} \mathrm{Gal}\left(L/K^H\right)\right)$$

σU is a basic open nbhd of σ. Now by finite Galois theory we have $\pi(\sigma) \in \mathrm{Gal}\left(L/L^H\right) = \pi(H)$. But $\mathrm{Gal}\left(L/K^H\right) = L/L^H = L/L^{\pi(H)}$. Therefore $\sigma^{-1}(H) \cap \ker\pi = U \neq \emptyset$. Thus $H \cap \sigma U \neq \emptyset$. Since σU runs through basic open nbhds of σ and H is top. closed $\sigma \in H$. Therefore $H = \mathrm{Gal}\left(K/K^H\right)$. This proves the theorem. □

22 Inseparability

Aim: See what Galois group tells us about inseparable (i.e. not separable) extensions.

22.1 Purely inseparable extensions

Proposition 22.1. *Let K/F be a field extension where char $F = p \geq 0$.*

(i) *The following are equivalent:*

(a) *$\alpha \in K$ is purely inseparable over F i.e. $\alpha^{p^n} \in F$ for some $n \geq 0$.*

(b) *α is the only root of its minimal polynomial $f(X) \in F[X]$.*

(c) $[F(\alpha) : F]_S = 1$.

(ii) *In particular, if $\alpha \in K$ is both separable and purely inseparable over F then $\alpha \in F$.*

Proof. (i) (b) $\Leftrightarrow$ (c) easy.

(a) $\Rightarrow$ (b): α is a root of $X^{p^n} - \alpha^{p^n} \in F[X]$ so $f(X) \big| X^{p^n} - \alpha^{p^n} = (X-\alpha)^{p^n}$. Therefore the only root of $f(X)$ is α.

(b) $\Leftarrow$ (a): By induction on deg f. If deg f=1 then $\alpha \in F$ so (a) holds. Assume $\alpha \notin F$ so no separable over F. $f(X) = (X-\alpha)^n$. Have $p \big| n$ otherwise $f'(X) \neq 0$ so f is separable. Write $m = \frac{n}{p} \in \mathbb{Z}$. $f(X) = (X-\alpha)^{pm} = (X^p - \alpha^p)^m$. $\therefore$ α^p satisfies a polynomial in $F[X]$ of degree m whose only roots is α^p. By induction, α^p is purely inseparable over F. Thus α is purely inseparable over F too.

(ii) $1 \overset{\text{(c)}}{=} [F(\alpha) : F]_S \overset{\alpha \text{ sep.}}{=} [F(\alpha) : F]$. Therefore $\alpha \in F$.

□

22.2 Maximal separable and purely inseparable extensions

Let F be a field, which characteristic $p > 0$.

Proposition/Definition 22.2. *Let K/F be a field extensions. The intermediate field $L := K \cap F^{\text{sep}}$ of all elts in K which are separable over F is such that K/L is purely inseparable. L is called the* **maximal separable sub-extension**.

Proof. Let $\alpha \in K$ and $f(X)$ be its min. poly. over L. Argue by induction on deg $f(x)$. As before deg $f(X) = 1 \Rightarrow \alpha \in L$. Suppose deg $f(X) > 1$, so $\alpha \notin L$. Note α is not separable over F $\therefore$ not separable over L $\therefore$ $f'(x) = 0 \Rightarrow f(X) = g(X^p)$. Thus α^p has min. poly. over L of smaller degree so is purely insep. over L and hence α is purely insep. over L. □

Proposition/Definition 22.3. *Let K/F be a field extension. The set of elements in K which are purely inseparable over F forms a field, say L, called the* **maximal purely inseparable sub-extension**.

Proof. Left as an easy exercise. □

Example 22.4. If $\phi : K \to K$ is Frobenius then L is just the union of increasing chain of subfields $\phi^{-n}(F)$, $n = 1, 2, \ldots$

22.3 Normal extensions

Theorem 22.5. *Let F be a field of char. $p > 0$ and K/F a normal extension with Galois group G. Let L_{sep} be the maximal separable sub-extension and L_{pi} be the maximal purely inseparable sub-extension. Then:*

(i) *K/K^G is Galois with Galois group G.*

(ii) *$L_{\text{pi}} = K^G$ is Galois.*

(iii) *L_{sep}/F is Galois.*

(iv) *$L_{\text{sep}} \cap L_{\text{pi}} = F$.*

(v) *The smallest subfield $\tilde{L}$ containing L_{sep} and L_{pi} is K.*

(vi) *The restriction map $\rho\colon \text{Gal}\,(K/L_{\text{pi}}) \to \text{Gal}\,(L_{\text{sep}}/F)$ is a well-defined group isomorphism.*

Proof. (i) $G \leq \text{Gal}\left(K/K^G\right) \leq \text{Gal}\,(K/F) = G$. Therefore, $K^{\text{Gal}\left(K/K^G\right)} = K^G$ and thus K/K^G is Galois with Galois group G.

(ii) Since K/F is normal, the G-orbits of any $\alpha \in K$ is precisely the set of roots of its min. poly. $f\,(X)$ over F. But $\alpha \in K^G$ iff the G-orbit of α is 1 element iff (by Proposition 22.1) α is purely inseparable over F.

(iii) Same as for F^{sep}. If $\alpha \in L_{\text{sep}}$ then its min. poly. $f(X)$ is separable and K/F normal $\Rightarrow$ all roots of $f(X)$ lie in L_{sep}. Therefore L_{sep}/F is normal too and hence Galois.

(iv) Proposition 22.1 (ii).

(v) K purely inseparable over L_{sep} so K is purely inseparable over $\tilde{L}$. (i) and (ii) $\Rightarrow$ K is separable over L_{pi} so K is separable over $\tilde{L}$. Therefore $K/\tilde{L}$ is separable and purely inseparable so by Proposition 22.1 $K = \tilde{L}$.

(vi) Let $\sigma \in \text{Gal}\left(K/K^G\right)$. It must permute separable elements so $\sigma\,(L_{\text{sep}}) = L_{\text{sep}}$ so ρ is a well-defined group homomorphism.

To see that ρ is injective, note that if $\rho\,(\sigma) = 1$ then σ fixes L_{sep} and L_{pi} and by (v) K. Thus $\sigma = 1$ and hence ρ is on-to-one.

Also, any $\bar{\sigma} \in \text{Gal}\,(L_{\text{sep}}/F)$ can by uniqueness of splitting fields be lifted to $\text{Gal}\,(K/F) = \text{Gal}\left(K/K^G\right)$ so ρ is surjective and the theorem is proved.

□

Corollary/Definition 22.6. *A field F of char $p > 0$ is* **perfect** *is Frob $F \to F$ is surjective. (Also fields of characteristic 0 are said to be prefect too). Any finite extension K/F of a prefect field is separable.*

Proof. Let $\phi : K \to K$ be the Frobenius map. We can assume K/F is normal. The maximal purely inseparable sub extension is $\bigcup_{n\in\mathbb{N}} \phi^{-n}(F) = F$. So result follows from theorem. □

23 Duality

Aim: Prepare for classification of finite abelian extension in the next section.

23.1 The dual group

Definition 23.1. *Let A be an abelian group and m be a positive integer. An element $a \in A$ is m-***torsion** *if $ma = 0$. We say A is m-***torsion** *if every element in A is m-torsion. We say A is* **torsion** *if every element of A has finite order.*

Example 23.2. $\mathbb{Q}/\mathbb{Z}$ is torsion since $\frac{p}{q} + \mathbb{Z}$ is q-torsion.

Proposition/Notation 23.3. *Let G be a group and A be an abelian group. Let $\mathrm{Hom}(G, A)$ be the set of group homomorphisms $\varphi : G \to A$. This is an abelian group when endowed with addition $(\varphi_1 + \varphi_2)(g) := \varphi_1(g) + \varphi_2(g)$.*

Proof. Easy. □

Definition 23.4. *Let G be a torsion abelian group. The* **dual** *of G is $G^\wedge := \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$.*

Example 23.5. $(\mathbb{Z}/n\mathbb{Z})^\wedge \simeq \mathbb{Z}/n\mathbb{Z}$. Why? Any group homomorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/n\mathbb{Z}$ is determined by $a := \varphi(1 + n\mathbb{Z}) \in \mathbb{Q}/\mathbb{Z}$. This can be any n-torsion element of $\mathbb{Q}/\mathbb{Z}$ i.e. $0+\mathbb{Z}, \frac{1}{n}+\mathbb{Z}, \frac{2}{n}+\mathbb{Z}, \ldots, \frac{n-1}{n}+\mathbb{Z}$. One easily verifies that the hom. $\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/n\mathbb{Z}$ mapping $i + n\mathbb{Z} \mapsto \frac{i}{n} + \mathbb{Z}$ is the generator of $(\mathbb{Z}/n\mathbb{Z})^\wedge$.

Exercise 23.6. Let A, B be torsion abelian groups. Show

$$\begin{array}{rcl} A^\wedge \times B^\wedge & \xrightarrow{\sim} & (A \times B)^\wedge \\ (\varphi, \psi) & \longmapsto & ((a, b) \mapsto \varphi(a) + \psi(b)) \end{array}$$

is a group isomorphism. Hence by Example 23.5 and structure theorem for finitely generated abelian groups, $A \simeq A^\wedge$ for A finite abelian.

23.2 Perfect pairings

Let A, B be torsion abelian groups.

Definition 23.7. *A* **pairing** *between A and B is a function $\psi\colon A \times B \to \mathbb{Q}/\mathbb{Z}$ such that:*

(i) *$\psi(a,-)$, $\psi(-,b)$ are group homomorphisms for all $a \in A, b \in B$. We say ψ is* **perfect** *if:*

(ii) *$\psi(a,-) = 0 \Rightarrow a = 0$ and $\psi(-,b) = 0 \Rightarrow b = 0$.*

Exercise 23.8. For a finite abelian group A, show

$$\begin{array}{rcl} A \times A^\wedge & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ (a, \varphi) & \longmapsto & \varphi(a) \end{array}$$

is a perfect pairing. Conversely, we have:

Proposition 23.9. *Let A, B be finite abelian groups and $\psi\colon A \times B \to \mathbb{Q}/\mathbb{Z}$ is a perfect pairing between them, then $A \simeq B^\wedge$.*

Proof. Let $\Psi : A \to B^\wedge$ be the map $a \mapsto \psi(a,-)$. It is a group homomorphism by Definition 23.7 and injective by part (ii). Therefore, $|A| \leq |B^\wedge| = |B|$. Switching roles of A and B shows $|B| \leq |A|$ so Ψ is an isomorphism. $\square$

23.3 Some abelian extensions

Fix positive integer m. Let F be a field of characteristic not dividing m and such that $F \supseteq \mu_m$ (note $|\mu_m| = m$). Kummer theory classifies abelian extensions of F with m-torsion Galois groups. Here we construct some examples.
F^*/F^{*m}: Let $F^{*m} = \{\alpha^m \mid \alpha \in F^*\}$. F^* abelian $\Rightarrow F^{*m} \leq F^*$ and F^*/F^{*m} is m-torsion abelian group.
$\sqrt[m]{\alpha F^{*m}}$: Let $a \in F^*/F^{*m}$, say $a = \alpha F^{*m}$. We "define" $\sqrt[m]{a}$ to be any m-th root of α. Fact: $\sqrt[m]{a}$ is well defined up to scalar multiple by some scalar $\beta \in F^*$. Why? Changing choice of m-th root of α, changes $\sqrt[m]{a}$ by an element of $\mu_m \subseteq F^*$. Changing α to $\alpha\beta^m$ where $\beta \in F^*$ changes $\sqrt[m]{\alpha}$ by β.
$F\left(\sqrt[m]{J}\right)$: Let $J \leq F^*/F^{*m}$. Define $F\left(\sqrt[m]{J}\right)$ to be the splitting field over F of the family of polynomials

$$\{X^m - \alpha \mid \alpha F^{*m} \in J\}.$$

This is generated over F by the $\sqrt[m]{a}, a \in J$.

Proposition 23.10. *For $J \leq F^*/F^{*m}, F\left(\sqrt[m]{J}\right)/F$ is Galois.*

Proof. For $\alpha F^{*m} \in J$, $X^m - \alpha$ has m distinct roots which must be separable over F. Therefore, $F\left(\sqrt[m]{J}\right)$ is generated by separable elements over F. Since it is also normal, it's Galois. □

Proposition 23.11. *Let $J \leq F^*/F^{*m}$. Let $\sigma \in \mathrm{Gal}\left(F\left(\sqrt[m]{J}\right)/F\right), a \in J$. Then $\psi(\sigma, a) = \frac{\sigma\left(\sqrt[m]{a}\right)}{\sqrt[m]{a}} \in \mu_m$ and is independent of choice of m-th root of a.*

Proof. Suppose $\sqrt[m]{a} = \sqrt[m]{\alpha}$, where $\alpha \in F^{*m}$. Then σ maps $\sqrt[m]{\alpha}$ to some other root of $X^m - \alpha$. $\psi(\sigma, a) = \frac{\sigma\left(\sqrt[m]{a}\right)}{\sqrt[m]{a}} \in \mu_m$. Also, for $\beta \in F^*$ $\frac{\sigma\left(\sqrt[m]{a}\beta\right)}{\sqrt[m]{a}\beta} = \frac{\sigma\left(\sqrt[m]{a}\right)\sigma(\beta)}{\sqrt[m]{a}\beta}$ so independence of choice of $\sqrt[m]{a}$ follows from this fact. □

Proposition 23.12. *For $J \leq F^*/F^{*m}, G := \mathrm{Gal}\left(F\left(\sqrt[m]{J}\right)/F\right)$ is m-torsion abelian group.*

Proof. The action of $\sigma, \tau \in G$ on $F\left(\sqrt[m]{J}\right)$ is determined by its action on the generators $\{\sqrt[m]{a} \mid a \in J\}$ of $F\left(\sqrt[m]{J}\right)/F$. Just as in the case of cyclic extension Proposition 23.11 implies σ, τ act on $\sqrt[m]{a}$ by multiplication by $\psi(\sigma, a), \psi(\tau, a)$ and the fact that $F \supseteq \mu_m \Rightarrow$ these actions commute. Therefore, G is abelian. Finally, $\psi(\sigma, a) \in \mu_m$ implies σ^m acts as identity so G is also m-torsion. □

24 Kummer Theory

Aim: Classify abelian extensions a la Kummer.

Fix for this section a positive integer m and field F of characteristic not dividing m such that F contains all m, m-th roots of 1.

24.1 A perfect pairing

Let $J \leq F^*/F^{*m}$ and $G = \mathrm{Gal}\left(F\left(\sqrt[m]{J}\right)/F\right)$. Recall from propositions in section 23, we have a well-defined map

$$\begin{aligned} \psi\colon G \times J &\longrightarrow \mu_m \\ (\sigma, a) &\longmapsto \frac{\sigma\left(\sqrt[m]{a}\right)}{\sqrt[m]{a}} \end{aligned}$$

Note also that $\mu_m \simeq \frac{1}{m}\mathbb{Z}/\mathbb{Z} < \mathbb{Q}/\mathbb{Z}$.

Theorem 24.1. *The map* $G \times J \xrightarrow{\psi} \mu_m \hookrightarrow \mathbb{Q}/\mathbb{Z}$ *is a prefect pairing. If* J *is finite then* $\mathrm{Gal}\left(F\left(\sqrt[m]{J}\right)/F\right) \simeq J^\wedge$.

Proof. We first check ψ is a paring. Let $\sigma, \tau \in G\,, a, b \in J$.

$$\psi(\sigma, ab) := \frac{\sigma(\sqrt[m]{ab})}{\sqrt[m]{ab}} = \frac{\sigma\left(\sqrt[m]{a}\right)\sigma(\sqrt[m]{b})}{\sqrt[m]{a}\,\sqrt[m]{b}} = \psi\left(\sigma, a\right)\psi\left(\sigma, b\right)$$

thus $\psi\left(\sigma, -\right)$ is a homomorphism. Also,

$$\psi\left(\sigma, \tau, a\right) := \frac{(\sigma\tau)(\sqrt[m]{a})}{\sqrt[m]{a}} = \frac{\sigma(\psi(\tau, a))\,\sqrt[m]{a}}{\sqrt[m]{a}} = \psi(\tau, a)\psi(\sigma, a)$$

so $\psi(-, a)$ is multiplicative.

We now check that ψ is perfect. If $\psi(\sigma, -)$ is 1, then σ acts as the identity on the generator $\sqrt[m]{a}, a \in J$ if $F\left(\sqrt[m]{J}\right)/F \;\; \therefore\; \sigma = 1$. Suppose now that $a \in J - 1_J$. So $\alpha \notin F^{*m} \;\therefore\; \sqrt[m]{a} \notin F$ so as $\mathbb{F}\left(\sqrt[m]{J}\right)/F$ is Galois (by Proposition 23.10) there exists $\sigma \in G$ such that $\sigma(\sqrt[m]{a}) \neq \sqrt[m]{a}$ and so $\psi(\sigma, a) = \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}} \neq 1$. Therefore $\psi(-, a) = 1 \Rightarrow a = 1$. Thus ψ is perfect too. Now Proposition 23.9 shows if J is finite (so is Galois too) then $G \simeq J^\wedge$. This proves theorem. □

24.2 Classification of abelian extensions

Theorem 24.2. *For a positive integer* m*,* F *a field of characteristic not dividing* m *containing primitive* m*-th root of unity, then:*

(i) *There is a bijection*

$$\left\{\begin{array}{c}\textit{subgroups}\\ J \leq F^*/F^{*m}\end{array}\right\} \xrightarrow{\Psi} \left\{\begin{array}{c}\textit{Abelian extensions}\\ \textit{of } F \textit{ with } m\textit{-torsion}\\ \textit{Galois group}\end{array}\right\}$$
$$J \longmapsto F(\sqrt[m]{J})$$

(ii) *Finite subgroups correspond to finite extensions.*

Proof. (ii) Do finite case first.

Ψ injective: Let $J_1, J_2 \leq F^*/F^{*m}$ be finite and J_1J_2 be the groups generated by J_1 and J_2 (which is still finite). Suppose $F(\sqrt[m]{J_1}) = F(\sqrt[m]{J_2})$. Then $F(\sqrt[m]{J_1J_2}) = F(\sqrt[m]{J_1})$ since J_1J_2 consists of products

of elements of J_1 and J_2. Thus it suffices to show $J_1 = J_1J_2$ for then by symmetry $J_2 = J_1J_2$. By Theorem 24.1

$$J_1^\wedge \simeq \mathrm{Gal}\left(F(\sqrt[m]{J_1})/F\right) = \mathrm{Gal}\left(F(\sqrt[m]{J_1J_2})/F\right) \simeq (J_1J_2)^\wedge.$$

Therefore $|J_1| = |J_1^\wedge| = |\,(J_1J_2)^\wedge\,| = |J_1J_2|$ so $J_1 = J_1J_2$.

Ψ surjective: Suppose K/F is a finite abelian extension with $m$torsion Galois group say $G \simeq G_1 \times G_2 \times \cdots \times G_r$ where G_i is a cyclic group of order $n_i|m$. Let $\pi_i : G = G_1 \times \cdots \times G_r \to G_i$ be the natural projection and $H_i = \ker \pi \triangleleft G$. Note, $H_i \triangleleft G \Rightarrow K^{H_i}/F$ is a Galois extension with Galois group $G/H^i \simeq G_i$ i.e. is a cyclic extension of degree n_i. The theory of cyclic extensions (Theorem 16.4) tells us $K^{H_i} = F(\sqrt[m]{a_i})$ for some $a_i \in F^*/F^{*m}$. Let $J = \langle a_1, \ldots, a_r\rangle$. Then $F(\sqrt[m]{J}) = F(\sqrt[m]{a_1}, \sqrt[m]{[a_2]}, \ldots, \sqrt[m]{[a_r]}) \subseteq K$. We wish to show equality by computing $\mathrm{Gal}\left(K/F(\sqrt[m]{J})\right)$. Now $F(\sqrt[m]{J})$ is the smallest subfield containing $K^{H_1}, \ldots, K^{H_r}$ therefore by Galois correspondence $\mathrm{Gal}\left(K/F(\sqrt[m]{J})\right)$ is $H_1 \cap H_2 \cap \cdots \cap H_r = 1$. Thus $K = F(\sqrt[m]{J})$ and Ψ is surjective.

(i) do now infinite case. As before, suffice to show if $J_1 \leq J_2 \leq F^*/F^{*m}$ with $F(\sqrt[m]{J_1}) = F(\sqrt[m]{J_2})$ then $J_1 = J_2$. Let $a \in J_2$. Then there exists $a_1, \ldots, a_n \in J$, such that $\sqrt[m]{a} \in F(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_n})$. If $J_1^0 = \langle a_1, \ldots, a_n\rangle$ and $J_2^0 = \langle a, a_1, \ldots, a_n\rangle$ and $F(\sqrt[m]{J_1^0}) = F(\sqrt[m]{J_2^0})$. So by finite case $J_1^0 = J_2^0$ so $a \in J_1$). Thus $J_1 = J_2$ and so Ψ is injective.

To Ψ is surjective: let K/F be an abelian extension with m-torsion Galois group G. Write $K = \cap K_i$ where K_i/F are finite Galois extensions. These must have Galois groups which are quotients of G so are m-torsion abelian. Thus $K = F(\sqrt[m]{J_i})$ for some $J_1 \leq F^*/F^{*m}$¿ if J is a subgroups generated by all the J_i then $F(\sqrt[m]{J}) = K$.

□

25 Galois Correspondence in Topology

In this section all topological spaces X will satisfy the following.

$$(*)\begin{cases} X \text{ is path connected} \\ X \text{ is locally contractible. i.e for all } x \in X \text{ there exists open nbhd } U_x \\ \quad \text{and continous function } \kappa_x \colon U_x \times [0,1] \to U_x \text{ such that } \kappa_x(-,0) = \mathrm{id}_{U_x} \\ \quad \kappa_x(-,1) \text{ is constant.} \end{cases}$$

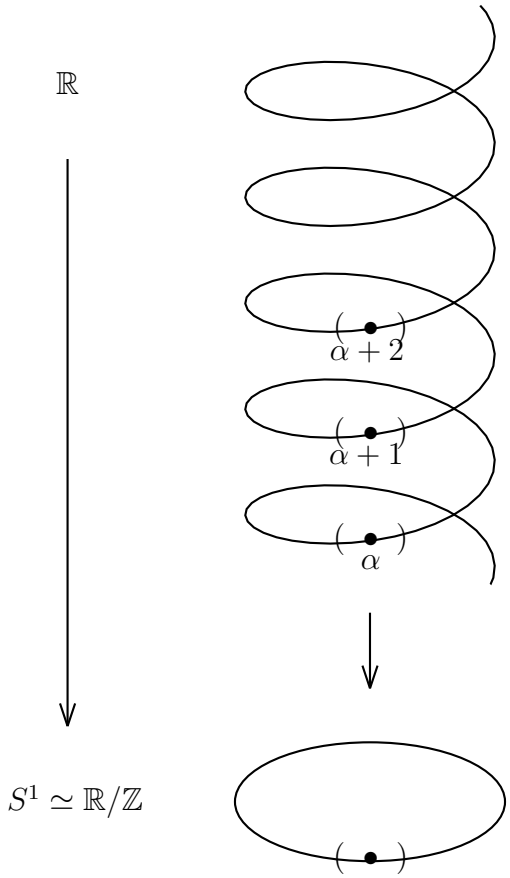
Example 25.1. X is a manifold.

25.1 (Unramified) covers

Definition 25.2. *Let X be a topological space satisfying $(*)$. A* **cover** *of X is a continuous map of topological spaces $\pi Y \to X$ such that for any $x \in X$ there is an open nbhd U of x with the property that any component V of $\pi^{-1}(U)$ is open and $\pi|_V : V \to U$ is a homeomorphism.*

Example 25.3.

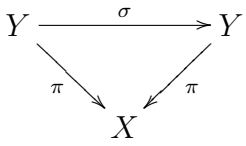
$$\begin{array}{rcl} \pi : \mathbb{R} & \longrightarrow & \mathbb{R}/\mathbb{Z} \simeq S^1 \\ \alpha & \longmapsto & \alpha + \mathbb{Z} \end{array}$$



25.2 Galois correspondence

Proposition/Definition 25.4. *Let $\pi : Y \to X$ be a cover. A* **deck transformation** *of π is a homeomorphism $\sigma : Y \to Y$ such that the following*

diagram commutes



In other words, $\pi \circ \sigma = \pi$. The set of deck transformations of π is called the **Galois group** *of π and is denoted* $\mathrm{Gal}\,(Y/X)$*. It's a group under composition.*

Remark 25.5. (i) Deck transformation σ preserves fibres of π since $y \in \pi^{-1}(x) \Rightarrow \pi(\sigma(y)) = \pi(y) = x$.

(ii) X is path connected means cardinality of fibres is constant and is called the **degree** of the cover.

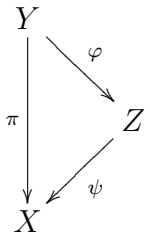
Example 25.6 (Continued from previous example)**.** For $n \in \mathbb{Z}$, we can define $\sigma_n \colon \mathbb{R} \to \mathbb{R}$ with $\sigma_n(\alpha) = \alpha + n$. In fact, $\mathrm{Gal}\,(\mathbb{R}/S) \simeq \mathbb{Z}$

Definition 25.7. *A cover $\pi \colon Y \to X$ is* **Galois** *if* $\mathrm{Gal}\,(Y/X)$ *acts transitively on every fibre of π.*

Example 25.8. From before $\mathbb{R} \to S$ is a Galois cover.

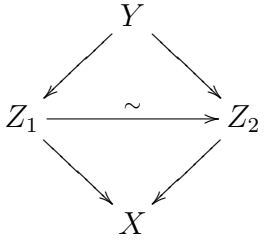
25.3 Galois correspondence

Definition 25.9. *Let $\pi \colon Y \to X$ be a cover. An* **intermediate cover** *is a factorisation of π i.e. commutative diagram*



such that ψ is a cover (and therefore φ is a cover too).

Two intermediate covers $Y \to Z_1 \to X$ and $Y \to Z_2 \to X$ are **equivalent** *if there exists a homeomorphism $h :! \xrightarrow{\sim} Z_2$ such that the following diagram commutes*



Theorem 25.10. *Let $\pi : Y \to X$ be a Galois cover with Galois group G. There is a lattice anti-isomorphism*

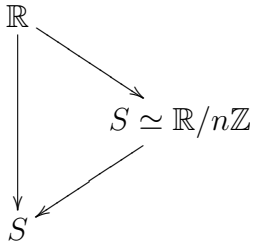
$$H \longmapsto (Y \to Y/H \to X)$$

$$\left\{ \begin{matrix} \textit{subgroups} \\ \textit{of } G \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \textit{intermediate} \\ \textit{covers of } \pi \end{matrix} \right\}$$

$$\operatorname{Gal}(Y/Z) \longmapsfrom (Y \to Z \to X)$$

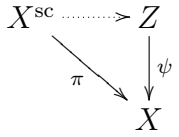
The normal subgroups correspond to intermediate covers $Y \to Z \to X$ where $Z \to X$ is Galois.

Example 25.11 (Continuing from all previous examples)**.** $0 \supseteq n\mathbb{Z} \supseteq \mathbb{Z} = \operatorname{Gal}(\mathbb{R}/S)$ corresponds to



25.4 Simply connected cover

Theorem 25.12. *Let X be a topological space satisfying $(*)$. Then there is a unique cover $\pi : X^{\text{sc}} \to X$ with X^{sc} simply connected*[6]*. This is called the* **simply connected cover of** X*. It satisfies the following universal property: Consider any cover $\psi : Z \to X$, then there is a commutative diagram of continuous maps:*



Corollary 25.13. *Any cover $\pi : Y \to X$ of a simply connected space X is trivial. i.e. $\pi = \mathrm{id}$.*

Theorem 25.14. *Let X be a topological space. Then $X^{\text{sc}} \to X$ is Galois and $\operatorname{Gal}(X^{\text{sc}}/X)$ is isomorphic to the fundamental group of X, $\pi_1(X)$.*

[6] i.e. all loops in X^{sc} are contractile to a point.

26 Riemann Surfaces

Aim: See how field extensions arise in the theory of Riemann surfaces.

26.1 Riemann surfaces

Definition 26.1. *A Riemann surface is a* 1 *dimensional complex manifold i.e. a Hausdorff topological space* X *with an atlas*

$$\left\{U_\alpha \xrightarrow{\phi_\alpha} V_\alpha \subseteq \mathbb{C}\right\}$$

where $X = \cup U_\alpha$ *is an open cover such that the transition functions* $\pi_\alpha \circ \pi_\beta^{-1}$ *are holomorphic.*

Example 26.2. Riemann sphere of complex projection line $\mathbb{P}^1_{\mathbb{C}} = X$. As a topological space, X = spheres $S^2 = 1-$pt compactification of C. Atlas given by identifying

(i) $X - \infty$ with $\mathbb{C}$ (with complex variable z);

(ii) $X - 0$ with $\mathbb{C}$ (with complex variable y)

and transition function $y = z^{-1}$.

Example 26.3. Elliptic curve. Pick $\tau \in \mathbb{C}$ with im $z > 0$. Consider lattice $\Lambda := \mathbb{Z} + \mathbb{Z}\tau < \mathbb{C}$. Let $X = \mathbb{C}/\Lambda$. This a Riemann surface.

26.2 Field of meromorphic functions

Definition 26.4. *Let* X *be a Riemann surface. The* **field of meromorphic functions** $\mathbb{C}(X)$ *is the set of meromorphic functions on* X *i.e. functions which are holomorphic except for a finite number of poles.*

Note that meromorphic functions on X are just holomorphic functions $X \to \mathbb{P}^1_{\mathbb{C}}$.

Example 26.5. The meromorphic functions on $X = \mathbb{P}^1_{\mathbb{C}}$ are the meromorphic functions on C which are neither holomorphic at ∞ or have a pole there. Thus meromorphic functions are just rational functions. Therefore $\mathbb{C}\left(\mathbb{P}^1_{\mathbb{C}}\right) = \mathbb{C}\left(z\right)$.

Example 26.6. As before $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ is a lattice in $\mathbb{C}$ and $X = \mathbb{C}/\Lambda$. A meromorphic functions on X is a meromorphic function $f(x)$ on $\mathbb{C}$ which double periodic with periods $1, \tau$ i.e. $f(z+1) = f(z), f(z+\tau) = f(z)$.

Proposition/Definition 26.7. *The Weierstrass $\wp$ function*

$$\wp(z) := \frac{1}{z^2} + \sum_{w \in \Lambda - 0} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

is meromorphic on $\mathbb{C}$ and doubly periodic. Therefore $\mathbb{C}(\wp(z)) = \subseteq \mathbb{C}(X)$.

Facts:

(i) $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for some $g_2, g_3 \in \mathbb{C}$ depending on Λ.

(ii) $\mathbb{C}(X) = \mathbb{C}(\wp(z), \wp'(z)) \simeq \mathbb{C}(t, \sqrt{4t^3 - g_2 t - g_3})$. In fact,

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow \mathbb{P}^2_{\mathbb{C}} \\ z + \Lambda &\longmapsto (\wp(z) : \wp : (z) : 1) \end{aligned}$$

embeds $\mathbb{C}/\Lambda$ into $\mathbb{P}^2_{\mathbb{C}}$ as the the curve $y^2 = 4x^3 - g_2 x - g_3$

26.3 Functoriality

Proposition 26.8. *Let $\sigma : X \to Y$ be a non-constant map of Riemann surfaces.*

(i) *Let $f : Y \to \mathbb{P}^1_{\mathbb{C}}$ be a meromorphic function Y. Then $\sigma^* f := f \circ \sigma$ is meromorphic on X. We thus obtain a field homomorphism $\sigma^* : \mathbb{C}(Y) \to \mathbb{C}(X)$. This is the pull back of functions.*

(ii) *If we have another non-constant holomorphic map $\tau : W \to X$ of Riemann surfaces then $(\sigma \circ \tau)^* = \tau^* \circ \sigma^* : \mathbb{C}(Y) \to \mathbb{C}(W)$.*

(iii) $(\mathrm{id}_Y)^* = \mathrm{id}_{\mathbb{C}(Y)}$.

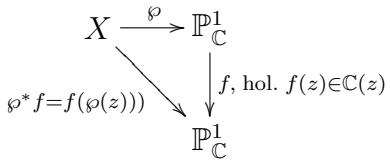
Proof. (i) Clear.

(ii) $(\sigma \circ \tau)^* (f) = \tau^*(\sigma^* f)$.

(iii) Clear.

□

Example 26.9. Elliptic curve $X = \mathbb{C}/\Lambda$



Therefore, writing t for $\wp(z)$

$$\begin{aligned} \wp* \colon \mathbb{C}(\mathbb{P}^1_{\mathbb{C}}) &\longrightarrow \mathbb{C}\,(\mathbb{C}/\Lambda) \\ \mathbb{C}(t) &\hookrightarrow \mathbb{C}\left(t, \sqrt{4t^3 - g_2 - g_3}\right) \\ t &\longmapsto t \end{aligned}$$

26.4 Riemann's Theorem

Theorem 26.10. *Let K be a finite extension of $\mathbb{C}(z)$. Then there is a unique compact Riemann surface with $\mathbb{C}(X) \simeq K$. Furthermore, if L/K is a finite extension and Y is the compact Riemann surface with $\mathbb{C}(Y) \simeq L$, then there is a non-constant holomorphic map $\sigma \colon Y \to X$ such that $\sigma^*\mathbb{C}(X) \to \mathbb{C}(Y)$ is the original field inclusion $K \subseteq L$.*

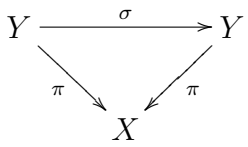
27 Geometric examples of field automorphisms

Proposition 27.1. *Let X, Y be a Riemann surfaces and $\pi : Y \to XX$ be an unramified cover. Then Y has a unique structure as a Riemann surface in such a way that π is holomorphic.*

27.1 Galois groups

Proposition 27.2. *Let $\pi : Y \to X$ be a non-constant holomorphic map of compact Riemann surfaces. We will use $\pi^* \colon \mathbb{C}(X) \to \mathbb{C}(Y)$ to identify $\mathbb{C}(X)$ with a subfield of $\mathbb{C}(Y)$.*

(i) *Let $\sigma \colon Y \to Y$ be a biholomorphic map such that*



commutes $\pi \circ \sigma = \pi$. Then $\sigma^* \colon \mathbb{C}(Y) \to \mathbb{C}(Y) \in \mathrm{Gal}\,(\mathbb{C}(Y)/\mathbb{C}(X))$.

(ii) *The elements of $\mathrm{Gal}\,(\mathbb{C}(Y)/\mathbb{C}(X))$ are the σ^* where σ is as in (i).*

(iii) *Let G be the pro-finite completion $\pi_1(X)$ i.e.*

$$G = \varprojlim_{\substack{N \trianglelefteq \pi_1(X) \\ [\pi_1(X) \,:\, N] \leq \infty}} \pi_1(X)/N \triangleleft \widehat{\pi_1(X)}$$

Then G is a quotient of the absolute Galois group $\mathrm{Gal}\left(\overline{\mathbb{C}(X)}/\mathbb{C}(X)\right)$ *corresponds to the "maximal unramified extension".*

Proof. (i) Functoriality implies $\sigma^* \circ \pi^* = \pi^*$. Thus σ^* fixes $\mathbb{C}(X)$.

(ii) This follows from Riemann's theorem.

(iii) Any finite Galois unramified cover $X^{\mathrm{sc}} \to Y \to X$ corresponds to $N \triangleleft \pi_1(X)$, Proposition 27.1 implies Y is a Riemann surface. Parts (i) and (ii) give $\mathrm{Gal}\,(\mathbb{C}(Y)/\mathbb{C}(X)) \simeq \mathrm{Gal}\,(Y/X) \simeq \pi_1(X)/N$.

□

27.2 Unramified covers of elliptic curves

Consider lattice in $\mathbb{C}$, $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\mathrm{im}\,\tau > 0$. Elliptic curve $X = \mathbb{C}/\Lambda$. $\mathbb{C}$ is simply connected so $\mathbb{C} \to \mathbb{C}/\Lambda$ is the simply connected cover. Translation by $\lambda \in \mathbb{C}$ is a deck transformation. We see that $\pi_1(\mathbb{C}/\Lambda) \simeq \Lambda \simeq \mathbb{Z}^2$. Therefore by Proposition 27.2 (iii) the absolute Galois group $\mathrm{Gal}\,(\mathbb{C}(X)/\mathbb{C}(X))$ has a quotient corresponding to $\widehat{\pi_1(G/\Lambda)} \simeq \widehat{\mathbb{Z}}^2$. What are finite unramified covers of $X = \mathbb{C}/\Lambda$? Pick $\Lambda' < \Lambda$ of finite index $Y = \mathbb{C}/\Lambda' \to \mathbb{C}/\Lambda = X$. Note Λ' is still a Riemann surface, in fact an elliptic curve. Also $\mathrm{Gal}\,(Y/X) = \mathrm{Gal}\,(\mathbb{C}(Y)/\mathbb{C}(X)) = \Lambda/\Lambda'$.

27.3 Ramified Cyclic Covers of $\mathbb{P}^1_{\mathbb{C}}$

Definition 27.3. *Let $\pi Y \to X$ be a non-constant holomorphic map of compact Riemann surfaces. If is surjective, so we will call it a* **ramified cover** *if it not unramified. We will say it is* **Galois** *or* **cyclic** *if $\mathbb{C}(Y)/\mathbb{C}(X)$ is.*

Now $\mathbb{P}^1_{\mathbb{C}} \overset{\text{top. sp.}}{\simeq} S^2$ which is simply connected so any unramified cover is trivial. Let's find all ramified cyclic covers using Kummer theory, say with Galois group $G \simeq \mathbb{Z}/m\mathbb{Z}, m > 0$. Recall, $\mathbb{C}(\mathbb{P}^1_{\mathbb{C}}) \simeq \mathbb{C}(Z)$. Need to know $\mathbb{C}(z)^*/\mathbb{C}(z)^{*m}$.

Fact:

(i) $\varphi\colon \mathbb{C}^* \oplus \left(\bigoplus_{\lambda\in\mathbb{C}} \mathbb{Z}\right) \xrightarrow{\sim} \mathbb{C}(z)^*$.

(ii) $\mathbb{C}(z)^*/\mathbb{C}(z)^{*m} \simeq \bigoplus_{\lambda\in\mathbb{C}} \mathbb{Z}/m\mathbb{Z}$.

Why?

$$\varphi\colon \alpha + n_{\lambda_1} + \cdots + n_{\lambda_r} \mapsto \alpha\,(z-\lambda)^{n_{\lambda_1}} \ldots (z-\lambda_1)^{n_{\lambda_r}}$$

Need cyclic, order m subgroups of $\bigoplus_{\lambda\in\mathbb{C}} \mathbb{Z}/m\mathbb{Z}$. Pick some $(n_{\lambda_1},\dots,n_{\lambda_r}) \in \mathbb{Z}^r$ which is order m, modulo m. Kummer theory says if $f(z) = (z-\lambda_1)^{n_{\lambda_1}}\dots(z-\lambda_r)^{n_{\lambda_r}}$ then $\mathbb{C}\left(z, \sqrt[m]{f(z)}\right)/\mathbb{C}(z)$ is a cyclic extension of degree m.

What's happening geometrically? Let $X \to \mathbb{P}^1_{\mathbb{C}}$ be corresponding map of compact Riemann surfaces. Then away from $\lambda_1, \lambda_2, \dots \lambda_r$ π is unramified, $\lambda_1,\dots,\lambda_r$ (and maybe ∞) are ramified points.

Example 27.4. If $X \to \mathbb{P}^1_{\mathbb{C}}$ corresponds to $\mathbb{C}\left(z, \sqrt{z(z-10(z-\lambda)}\right)/\mathbb{C}(z)$ then X is essentially zeroes of $y^2 = z(z-1)(z-\lambda)$ in $\mathbb{C}^2$ compactified in $\mathbb{P}^2_{\mathbb{C}}$.

28 Ramification Theory

28.1 Discrete valuation rings

Proposition/Definition 28.1. *A* **discrete valuation ring** *(DVR) is a PID R which is not a field and has a unique maximal ideal (i.e. a* **local ring***) $tR = \langle t\rangle$. In this case, any non-zero ideal I has form $\langle t^n\rangle$, for some $n \in \mathbb{N}$.*

This is not the standard definition, but is equivalent to it.

Example 28.2. Let F be a field. Then $F[\![t]\!] = \left\{\sum_{i\geq 0}\alpha_i t^i \mid \alpha_i \in F\right\}$ which is the ring of formal power series in t with coefficients in F. This is a DVR with maximal ideal $\langle t\rangle$. Why? Given $a(t) = \sum_{i\geq 0}\alpha_i t^i$ where $\alpha_0 \neq 0$ then $a(t)$ is invertible. This means that any element $a(t) = \sum_{i\geq n}\alpha_i t^i$ with $\alpha_n \neq 0$ is an associate of t^n and so any non-zero ideal has form $\langle t^n\rangle$ for some $n \in \mathbb{N}$.

Example 28.3. $\mathbb{C}\{t\} < \mathbb{C}[\![t]\!]$ is the subring of convergent power series. This is a DVR $\mathbb{C}\{t\} \simeq$ ring of germs of holomorphic functions at some point of a Riemann surface.

Example 28.4. $\hat{\mathbb{Z}}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is a DVR, with maximal ideal $\langle p\rangle$.

28.2 Motivation for Ramification

Let $\pi : Y \to Z$ be a (un)ramified cover of a Riemann surface. Essentially, ramification is where the sheets come together. Lets study π locally at $y_0 \in Y$ and $z_0 \in \pi(y_0)$. Using charts we may identify open nbhds of y_0 with open an nbhd U of 0 in $\mathbb{C}$ with variable y and open nbhd of z_0 with open nbhd of 0 in $\mathbb{C}$ with variable z. Then π is given by some holomorphic $f : U \to \mathbb{C}$ say with $f(0) = 0$. There are 2 cases:

Unramified case: $f'(0) = 0$ i.e. $f(y) = \alpha_1 y + \alpha_2 y^2 + \dots$ where $\alpha_1 \neq 0$. Inverse function theorem implies that f is a local isomorphism.

Ramified case: $f'(0) = 0$ so $f(y) = \alpha_n y^n + \alpha_{n+1} y^{n+1} + \dots$ with $\alpha_n \neq 0$, $n \geq 2$. Locally at $y = 0$, f behaves like $f(y) \approx \alpha_n y^n$.

Generically in nbhd of 0, f is $n : 1$. But at $y = 0$, the n sheets come together. Can't possibly be unramified there. The upshot is $\pi : Y \to Z$ is unramified everywhere except a finite number of points.

28.3 Ring-Theoretic Reformulation

Let $\pi \colon Y \to Z$ be a non-constant map of Riemann surfaces and $y_0 \in Y$. Let $z_0 = \pi(y_0) \in Z$. Write $\mathbb{C}\{y\}, \mathbb{C}\{z\}$ for the ring of germs of holomorphic functions at y_0 and z_0. Consider

$$\begin{aligned} \pi^* \colon \mathbb{C}\{z\} &\longrightarrow \mathbb{C}\{y\} \\ z &\longmapsto \alpha_n y^n + \alpha_{n+1} y^{n+1} + \dots, n \geq 1, \alpha_n \neq 0. \end{aligned}$$

$\pi^*(z)\mathbb{C}\{y\} = \langle y^n \rangle$. π is unramified at y_0 iff $\pi^*(z)$ generates the maximal ideal of $\mathbb{C}\{y\}$.

Definition 28.5. *Let R, S be DVRs with maximal ideals tR and uS. Suppose $\varphi \colon R \to S$ is a ring homomorphism such that $\varphi^{-1}(uS) = tR$. We say φ is unramified if*

(i) *$\pi^*(t)$ generates the maximal ideal uS of S and*

(ii) *S/uS is a separable field extension of R/tR*