Class Field Theory

David Wiedemann

Table des matières

1 Motivation **3**

2 Interlude : Inverse Limits **5**

3 Galois Theory and profinite groups **5**

4 Local Fields **8**

List of Theorems

1 Definition . . . 3
2 Corollary . . . 3
4 Lemma . . . 4
5 Theorem (Artin Reciprocity) . . . 4
6 Theorem (Abelian polynomial theorem) . . . 4
7 Theorem . . . 5
2 Definition (Inverse System) . . . 5
10 Lemma . . . 6
3 Definition (Profinite space) . . . 6
11 Lemma . . . 6
4 Definition (Profinite group) . . . 7
5 Definition (Krull Topology) . . . 7
13 Proposition . . . 7
14 Corollary . . . 7
15 Theorem (Fundamental Theorem of Galois Theory (Cool version)) 7
6 Definition (Local Field) . . . 8
7 Definition . . . 8
8 Definition (Equivalent metrics) . . . 9
19 Proposition . . . 9
20 Theorem (Approximation Theorem) . . . 10
22 Proposition . . . 10
9 Definition (Complete Field) . . . 11

24 Theorem (Ostrowski) 11
10 Definition 12
11 Definition 12
12 Definition (Non-archimedean local field) 12
13 Definition 12
25 Proposition 12

Lecture 1: Intro

Mon 10 Oct

1 Motivation

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial and a p a prime.
Look at $f_p(x) \in \mathbb{F}_p[x]$, in general, f_p is not irreducible so we can study it's factorizations.

Definition 1
We say f splits completely mod p if f_p factors into distinct linear factors.
We write $Spl(f) = \{p | f_p = \prod (x - \alpha_i)\alpha_i \neq \alpha_j \forall i \neq j\}$

Problem
Given f, describe the factorisations behaviour of f_p as a function of p.
Or at least give a rule determining $Spl(f)$.

An answer to this illposed problem is a **Reciprocity Law**.

Example
Let $f(x) = x^2 - q$ $q > 2$ prime.
Observe that

1. $f_p(x) = (x - \alpha_p)^2$, *but this happens iff* $p = 2, q$
2. $f_p(x) = (x - \alpha_p)(x + \alpha_p)$ *iff* $p \in Spl(f)$ *iff* $(\frac{q}{p}) = 1$
3. $f_p(x)$ *is irreducible iff* $(\frac{q}{p}) = -1$

To get a rule, we need to compute $\left(\frac{q}{p}\right)$, to do so, we use quadratic reciprocity.
For us, quadratic reciprocity translates to

Corollary 2

$$(\frac{q}{p}) = \begin{cases} (\frac{p}{q}) \text{ if } p \equiv 1 \mod 4 \\ -(\frac{p}{q}) \text{ if } p \equiv 3 \mod 4 \end{cases}$$

So $Spl(X^2 - q)$ is determined by congruence conditions modula $4q$.

Example
Let Φ_n be the nth cyclotomic polynomial, then

$$Spl(\Phi_n) = \{p | p \equiv 1 \mod n\}$$

What about general polynomials?
Over $\mathbb{C}$, we can always factor polynomials and so we write $K_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$

for the splitting field of K_f over $\mathbb{Q}$.
$K_f \supset \mathbb{Q}$ is a Galois extension and $\mathcal{O} = \mathcal{O}_{K_f}$ is it's ring of integers.
As $\mathcal{O}$ is a dedekind domain, we have

$$p\mathcal{O} = \prod_{i=1}^{n} \beta_i^e, \mathcal{O}/\beta_i \supset \mathbb{Z}/(p) \text{ a finite extension of } \mathbb{Z}/p$$

We understand finite extensions of $\mathbb{F}_p$, there Galois group is generated by the Frobenius automorphism.
If p does not ramify ($e_p = 1 \iff p \nmid D_{K_f}$) then we define the Artin-Symbol $\sigma_{\beta_i} \in Galf(K_f|\mathbb{Q})$ by

$$\sigma_{\beta_i}(\alpha) \equiv \alpha^p \mod \beta_i \forall a \in \mathcal{O}$$

Fact :
If $\beta_i \neq \beta_j$, then there is $\zeta \in Gal(K_f|\mathbb{Q})$ such that $\zeta(\beta_i) = \beta_j$, then $\sigma_{\beta_j} = \zeta\sigma_{\beta_i}\zeta^{-1}$.
The Artin symbol of p is $\sigma_p = C_{\mathrm{Gal}}(\sigma_{\beta_i})$.
For now we suppose $Gal(K_f|\mathbb{Q})$ is an abelian group, in this case, we can turn the Artin Symbols into a map

$$\mathbb{Q}^* \supset \Gamma_{D_{K_f}} = \langle p \nmid D_{K_f} \rangle \to \mathrm{Gal}(K_f|\mathbb{Q})$$

by sending $p \to \sigma_p$

Lemma 4
If $Gal(K_f|\mathbb{Q})$ is abelian, then, up to finitely many extensions,

$$p \in Spl(f) \iff \sigma_p = 1$$

Theorem 5 (Artin Reciprocity)
For $K_f/\mathbb{Q}$ abelian, the Artin map $\sigma : \Gamma_{D_{K_f}} \to \mathrm{Gal}(K_f|\mathbb{Q})$ is surjective and it's kernel contains the "ray class group".

Here the ray class group is

$$\Gamma_a^{(ray)} = \left\{ r \in \mathbb{Q}^* | r = \frac{c}{d}(ca, d) = 1, c \equiv d \mod a \right\}$$

For a suitable a tant consists of ramified primes.
Define $\tilde{Spl}(f) = Spl(f) \setminus \{p|a\} \cup \{p \equiv 1 \mod a\}$.

Theorem 6 (Abelian polynomial theorem)
If f is abelian, then $\tilde{Spl}(f)$ can be described by congruence conditions wrt a modulus depending only on f.

Conversely, if $\tilde{Spl}(f)$ is described by congruence conditions, then $\mathrm{Gal}(K_f|\mathbb{Q})$ *is abelian.*

Theorem 7
Let f, g be polynomials (monic irreducible), then

$$K_f \subset K_g \iff Spl(g) \subset^* Spl(f)$$

This enters in the proof of the converse part of the abelian polynomail theorem.

2 Interlude : Inverse Limits

Let I be a directed ordered set ($i, j \in I \implies \exists k$ such that $i \leq k, j \leq k$)

Definition 2 (Inverse System)
A inverse system consists of data

$$\{X_i, f_{i,j} | i, j \in I, i \leq j\}$$

X_i are objects (topological spaces, groups, etc) and the $f_{i,j} : X_j \to X_i$ such that $f_{i,i} = \mathrm{Id}$ and $f_{j,k} \circ f_{k,i} = f_{j,i}$

Example
Take $X_i = {}^{\mathbb{Z}}\!/_{p^j\mathbb{Z}} \to {}^{\mathbb{Z}}\!/_{p^i\mathbb{Z}}, i \leq j$.
Then, the inverse limit is defined by

$$X = \varprojlim_{i \in I} X_i = \left\{ (x_i) \in \prod X_i | f_{ij}(x_j) = x_i \forall i \leq j \right\} \subset \prod_{i \in I} X_i$$

Lecture 2: Infinite galois theory

Thu 13 Oct

3 Galois Theory and profinite groups

Example
$\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$.
Though the extension is infinite, we can look at $\mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ *and it still contains the frobenius $\phi(x) = x^p$.*
Let $H = \{\phi^n | n \in \mathbb{Z}\} = \langle \phi_n \rangle \subset \mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$.
Note that $\overline{\mathbb{F}_p}^H = \mathbb{F}_p$ BUT $H \subsetneq \mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$

Lemma 10

Let T be a Hausdorff topological space.
The following are equivalent

- *T is an inverse limit of finite discrete spaces*
- *T is compact and every point in T has a basis of neighborhoods of subsets that are clopen*
- *T is compact and totally disconnected*

Proof (Sketch)

$1 \implies 2$ *follows from construction (exercise)*
$2 \implies 3$ *Take $x \in T$ and let C_x be the connected component of x.*
Then

$$C_x = \bigcap_{x \in U,\ clopen} U = \{x\}$$

because X is Hausdorff.
$3 \implies 1$ *Let* $I = \left\{ \text{ equivalence relation } R \subset T \times T | {}^{T}\!/_{R} \text{ is finite discrete } \right\}$
.
Then, consider $\phi : T \to \varprojlim {}^{T}\!/_{R}$, one then checks this is a homeomorphism. (exercise again) □

Definition 3 (Profinite space)

A profinite space is a totally disconnected, compact and Hausdorff space.

Lemma 11

Let G be a Hausdorff topological group.
Then the following are equivalent

- *G is the inverse limit of discrete finite groups*
- *G is compact and the identity in G has a basis of neighborhoods consisting of normal clopen subgroups.*
- *G is compact and totally disconnected.*

Proof

$1 \implies 3$ *see course notes*
$2 \implies 1$ *We want to show that $\phi : G \to \varprojlim {}^{G}\!/_{U}$ where the limit is taken over all normal clopen subgroups.*
$3 \implies 2$ *We take a basis for e as in the lemma above.*
We take a basis of clopen neighborhoods U and then define

$$V = \{v \in U | Uv \subset U\} \text{ and } H = \left\{h \in V | h^{-1} \in V\right\}$$

and one can show that H is a normal finite subgroup of finite index. □

Definition 4 (Profinite group)
A totally disconnected compact Hausdorff topological group is called a profinite group.

Example
— $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$
— $\hat{\mathbb{Z}} = \lim_{n\in\mathbb{N}} \mathbb{Z}/N\mathbb{Z}$ *where the inverse system is given by divisibility*

Now we try to fix the fundamental theorem of Galois theory.
Let F be a field with algebraic closur $\overline{F}$.
Write $G_E = \mathrm{Gal}(\overline{F}|E)$ for a field extension $F \subset E \subset \overline{F}$.
In particular, G_F is just the absolute Galois group of F

Definition 5 (Krull Topology)
For some element $\sigma \in G_F$, define a absis of (open) neighborhoods to be

$$\{\sigma G_E | F \subset E \text{ finite normal }\}$$

Proposition 13
G_F equipped with the Krull topology is a profinite group. We have

$$G_F = \varprojlim \mathrm{Gal}(E/F)$$

where E runs over finite Galois extensions of E

Corollary 14
$G_{\mathbb{F}_p} \simeq \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \simeq \hat{\mathbb{Z}}$

Theorem 15 (Fundamental Theorem of Galois Theory (Cool version))
The assignment

$$K \to \mathrm{Gal}(\overline{F}|K)$$

is a one-to-one correspondence between extensions $F \subset K \subset \overline{F}$ and closed subgroups of G_F.
The open subgroups of G_F correspond to finite extensions of F.

Proof
1. *First, notice that an open subgroup of G_F is closed.*
2. *Finite extensions correspond to open subgroup (essentially by definition, one needs to take the normal closure)*

3. *Now, for an arbitrary field extensionf*

$$\mathrm{Gal}(\overline{F}|K) = \bigcap_i \mathrm{Gal}(\overline{F}|K_i)$$

as K_i varies over all finite subextensions of K

4. *This assignment is injective as K is the fixed field of* $\mathrm{Gal}(\overline{F}|K)$

5. *This assignment is surjective :*
Take $H \subset G_F$ a closed subgroup and let $K = \overline{F}^H$, so that $H \subset \mathrm{Gal}(\overline{F}|K)$.
To see that this is in fact an equality, we take $\sigma \in \mathrm{Gal}(\overline{F}|K)$ and we show that $\sigma \in \overline{H} = H$.
Take some finite extension $K \subset L \subset \overline{F}$ so that $\sigma\,\mathrm{Gal}(\overline{F}|L)$ is a neighborhood of σ.
We need to show that

$$H \cap \sigma\,\mathrm{Gal}(\overline{F}|L) \neq \emptyset$$

To do this, we have to show $\tau \in H$ such that $\tau|_L = \sigma|_L$.

$$p : G_K \to \mathrm{Gal}(L/K) \qquad \square$$

is surjective and $p(H) \subset \mathrm{Gal}(L/K)$.
Since K is the fixed field of H, $L^{p(H)} = K$, we have $p|_H : H \to \mathrm{Gal}(L/K)$ is surjective.

4 Local Fields

Example

$\mathbb{R}$ *and* $\mathbb{C}$ *are local fields for us*

Definition 6 (Local Field)
A local field is a topological field which is locally compact but not discrete.

Definition 7
Let F be a field. An absolute value on F is a map $|\cdot| : F \to \mathbb{R}$ such that

1. $|x| \geq 0$ *and* $|x| = 0$ *and* $|x| = 0 \iff x = 0$
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$

Example

— $\mathbb{R}$ *and* $\mathbb{C}$ *with euclidean norm*

— *If $\mathcal{O}$ is a DVR, $F = \frac{(}{\mathcal{O}})$, then $|x| = c^{-\nu(x)}$ with $c > 1$ defines an absolute value.*

—

Lecture 3: Local Fields

Mon 17 Oct

Remark

1. *On a local field, we get a metric $d(x, y) = |x - y|$ which induces a topology on our field F*
2. *We could define the discrete metric which induces the discrete topology, but we always exclude it*

Definition 8 (Equivalent metrics)

1. *We call $|\cdot|_1$ and $|\cdot|_2$ equivalent if they induce the same topology.*
2. *If $|x + y| \leq \max(|x|, |y|) \leq |x| + |y|$ holds, then we call $|\cdot|$ non-archimedean.*

Observe that, if $|\cdot|_1$ and $|\cdot|_2$ are equivalent absolute values, then

$$|x|_1 < 1 \implies x^n \to 0 \text{ in } |\cdot|_1 \implies x^n \to 0 \text{ in } |\cdot|_2 \implies |x|_2 < 1.$$

Proposition 19

Two absolute values $|\cdot|_1, |\cdot|_2$ are equivalent iff there is $s > 0$ such that

$$|\cdot|_1 = |\cdot|_2^s$$

Proof

The implication from right to left is easy.
Fix $y \in F^\times$ with $|y|_1 > 1$.
For any $x \in F^\times$ there is $\alpha \in \mathbb{R}$ such that

$$|x|_1 = |y|_1^\alpha$$

Take a rational approximation from above $\frac{m_i}{n_i} \to \alpha$, we get $|\frac{x^{n_1}}{y^{m_1}}|_1 < 1 \implies |\frac{x^{n_1}}{y^{m_1}}|_2 < 1$
Thus $|x|_2 \leq |y|_2^{\frac{m_i}{n_i}} \implies |x|_2 \leq |y|_2^\alpha$.
Doing the same with an approximation of α from below we get $|x|_2 = |y|_2^\alpha$.
Then

$$0 < s = \frac{\log |y|_1}{\log |y|_2} = \frac{\log |x|_1}{\log |x|_2}$$

□

Theorem 20 (Approximation Theorem)
Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent absolute values.
For all $a_1, \ldots, a_n \in F$ and every $\epsilon > 0$, there is $x \in F$ such that

$$|x - a_i|_i < \epsilon$$

Remark
Taking $F = \mathbb{Q}$ and p, q primes.
There are valuations v_p, v_q which induce absolute values $|\cdot|_p = p^{-v_p(\cdot)}$ which are non-archimedean and inequivalent.
A special case of the theorem above says that for each $a_1, a_2 \in \mathbb{Z}$ and all $\epsilon > 0$ there is $x \in \mathbb{Q}$ such that $|a_1 - x|_p < \epsilon$ and $|a_2 - x|_q < \epsilon$

Proof
We claim : There is $z \in F$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n$.
First, take $\alpha, \beta \in F$ such that

$$|\alpha|_1 < 1 \leq |\alpha|_n \text{ and } |\beta|_1 \geq 1 > |\beta|_n$$

Put $y = \frac{\beta}{\alpha}$.
The case $n = 2$ follows from this (with $z = y$).
By induction, for $n > 2$ we argue by induction. Say z' satisfies the claim for $n - 1$.
If $|z'|_n \leq 1$, take $z = (z')^m y$ for m large enough.
If $|z'|_n > 1$, look at

$$t_m = \frac{(z')^m}{1 + z'^m}$$

t_m will converge to 1 for $j = 1, n$ and 0 if not.
Take $z = t_m y$ for m large enough.
By the same argument we find $z_i \in F$ such that $|z_i|_i > 1$ and $|z_i|_j < 1$ for $j \neq i$.
Put $x = a_1 z_1^{m_1} + \ldots + a_n z_n^{m_n}$ for $m_1, \ldots, m_n \in \mathbb{N}$ large enough. Look at script here :

$$|x - a_1|_1 \leq |a_1|_1$$

□

Proposition 22
An absolute value $|\cdot|$ on a field F is non-archimedean iff $(|n|)_{n \in \mathbb{N}}$ is bounded.

Proof
"$\Longrightarrow$" $|n| = |1 + \ldots + 1| \leq \max(|1|, \ldots) = 1$
"$\Longleftarrow$" *Say $|n| \leq N$, look at* $|x + y|^l \leq \sum_{v=0}^{l} |\binom{l}{v}| \underbrace{|x|^v |y|^{l-v}}_{\leq \max(|x|,|y|)^l}$.
Taking l-th roots, we get $|x + y| \leq N^{\frac{1}{l}} (1 + l)^{\frac{N}{l}} \max(|x|, |y|)$ □

Definition 9 (Complete Field)
We call $(F, |\cdot|)$ complete if every Cauchy sequence has a limit in F.

Any valued field has a completion $(\hat{F}, |\cdot|)$.

Example
$(\mathbb{Q}, |\cdot|) \xrightarrow{completion} (\mathbb{R}, |\cdot|_\infty)$.
We can do the same for the p-adic absolute values $(\mathbb{Q}, |\cdot|_p) \xrightarrow{completion} (\mathbb{Q}_p, |\cdot|_p)$.

Theorem 24 (Ostrowski)
Let F be a complete valued field such that $|\cdot|$ is archimedean.
Then there is an isomorphism $\sigma : F \to \mathbb{R}$ or $\mathbb{C}$ such that $|x| = |\sigma(x)|_\infty^s \forall x \in F$

Proof
As $|\cdot|$ is archimedean, the sequence (n) is unbounded and hence $char(F) = 0$.
Hence $\mathbb{Q} \to \hat{\mathbb{Q}} \to F$ and thus $\mathbb{R} \subset F$.
Take $a \in F$, we want to find a quadratic polynomial in $\mathbb{R}[x]$ that a satisfies.
Define $f(z) = |a^2 - Tr_{\mathbb{C}|\mathbb{R}}(z)a + Nr_{\mathbb{C}|\mathbb{R}}(z)$ for $z \in \mathbb{C}$.
Note that $f : \mathbb{C} \to [0, \infty)$ and $f(z) \to \infty$ as $|z| \to \infty$.
So $m = \min_{z\in\mathbb{C}} f(z)$ is attained in $S = \{z \in \mathbb{C} | f(z) = m\}$.
We claim $m = 0$.
Take $z_0 \in S$ and suppose $m = f(z_0) > 0$, consider

$$g(x) = x^2 - Tr_{\mathbb{C}|\mathbb{R}}(z_0)x + Nr_{\mathbb{C}|\mathbb{R}}(z_0) + \epsilon \in \mathbb{R}[x]$$

Let z_1, z_1' be complex roots of g, we must have

$$z_1 z_1' = Nr_{\mathbb{C}|\mathbb{R}}(z_0) + \epsilon$$

and in particular $|z_1| > |z_0|$.
Consider $G(x) = [g(x) - \epsilon]^n - (-\epsilon)^n = \prod_{i=1}^n (x - \alpha_i)$ and assume $\alpha_1 = z_1$

$$|G(a)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(z_1)|m|^{2n-1}$$

and

$$|G(a)| \leq f(z_0)^n + \epsilon^n = m^n + \epsilon^n$$

Rearranging

$$\frac{f(z_1)}{m} \leq (1 + (\frac{\epsilon}{m})^n)^2 \to 1$$

as $n \to \infty$.
Rearranging $f(z_1) \leq m = f(z_0)$ □

Definition 10
The fields $\mathbb{R}$ and $\mathbb{C}$ are called archimedean local fields.

Let $|\cdot|$ be non-archimedean

Definition 11
Let $\mathcal{O} = \{x \in F || x| \leq 1\}$ be the " valuation ring ".
Then

$$p = \{x \in F || x| < 1\}$$

is the unique maximal ideal of p.
Then $\mathcal{O}^\times = \{x \in F || x| = 1\}$ are the units and $k = \mathcal{O}/p$ is the residue field.

Definition 12 (Non-archimedean local field)
A non-archimedean local field is a complete valued field such that $|\cdot|$ is non-archimedean and k is finite.

Definition 13
The valuation v defined by $v(x) = -\log(|x|)$ is called discrete if there is a $s > 0$ such that $v(F^\times) \subset s\mathbb{Z}$.
We say v is normalized if $v(F^\times) = \mathbb{Z}$

Proposition 25
Let $(F, |\cdot|)$ be a non-archimedean valued field with completion $(\hat{F}, |\cdot|)$, then

$$\hat{\mathcal{O}}/\hat{p} \simeq \mathcal{O}/p$$

Further, if $|\cdot|$ has discrete valuation then

$$\hat{\mathcal{O}}/\hat{p}^n \simeq \mathcal{O}/p^n \text{ and } \hat{\mathcal{O}} = \lim \mathcal{O}/p^n$$

Similarly

$$\hat{\mathcal{O}}^\times = \lim \mathcal{O}^\times/U^n$$

for $U^n = 1 + p^n$