

INSTITUTE OF SCIENCE TOKYO
YOUNG SCIENCE AND ENGINEERING RESEARCHERS PROGRAM (YSEP)

**Lecture Notes on
Advanced Topics in Algebra E & F**

MOH HASBI ALFARIZI
SIT-IN STUDENT, INSTITUTE OF SCIENCE TOKYO

Version October 22, 2026

Preface

These notes are a typeset version of my handwritten notes from the graduate courses *Advanced Topics in Algebra E & F*, taught by Prof. Tadashi Ochiai at the Institute of Science Tokyo. I attended both courses as a sit-in student for two quarters (one semester, April–July 2026) during the Young Science and Engineering Researchers Program (YSEP). I joined these lectures on the suggestion of Dr. Soma Purkait, so that I could get exposure to lectures in advanced algebra alongside my research project on modular forms. The final goal of the course is to understand *Iwasawa theory*: the Iwasawa main conjecture, which relates ideal class groups along the cyclotomic tower to p -adic L -functions, and its generalisation to Selmer groups of p -adic Galois representations. To get there, the lectures start from ramification theory in number fields and a first glimpse of class field theory. They then pass through p -adic fields, zeta and L -functions and the classical class number formulas, and develop $\mathbb{Z}_p$ -extensions and the Iwasawa algebra. The second half proves Iwasawa’s class number formula, constructs the Kubota–Leopoldt p -adic L -function, formulates the main conjecture, and ends with p -adic Hodge theory, Selmer groups and elliptic curves. Part I follows my handwritten notes “Part 1” (lectures of April–June 2026), and Part II follows “Part 2” (lectures of June–July 2026).

I did not understand most of the material in these lectures. With the help of Claude Code (Opus 5.5, High-Ultracode), I could ask for clarifications of the notions I did not understand, for corrections of the slips in my handwritten notes, and for help with the proofs, for my own understanding.

In class many statements were only announced (“we can show”, “it is well known that”, “report problem”), and many proofs were omitted. Most of the proofs in these notes were not given in the original lectures and were written afterwards to complete the notes. The conversion of my handwritten notes into this L^AT_EX document, as well as several of the proofs and corrections, was produced with the help of Claude Code (Opus 5.5, High-Ultracode), in order to ease the formal write-up. Furthermore:

- boxes labelled **Notes**. make precise notions which were ambiguous or left implicit in the lectures;
- boxes labelled **Correction**. point out places where my handwritten notes contained a slip, and what the correct statement is;
- results whose proofs are far beyond the scope of the lectures (global class field theory, the Kronecker–Weber theorem, the Herbrand–Ribet theorem, p -adic Hodge theory, . . .) are stated with references; a *Proof sketch* indicates that some standard input is quoted.

Standard facts from a first course in algebraic number theory (that $\mathcal{O}_K$ is a Dedekind domain, unique factorisation of ideals, finiteness of the class group, Dirichlet’s unit theorem, . . .) are used freely; see e.g. [11, 8].

I am very grateful to Prof. Tadashi Ochiai for allowing me to sit in on his lectures for two quarters, and to Dr. Soma Purkait for suggesting it.

I would also like to give a shout-out to Orlando Ferrari’s lecture notes project, which influenced the way I make and write up these notes; see orlandoferrari.github.io.

The reader is advised to stay vigilant and verify the calculations; any remaining errors are mine. If you find a mistake or have a suggestion, please feel free to reach out to me on GitHub: github.com/Peanut2Butter9.

Contents

Preface	i
I Algebraic Number Theory, Zeta Functions and the Iwasawa Algebra	1
1 Ramification in Number Fields	2
1.1 Preliminaries	2
1.2 Ramification and decomposition of primes	4
1.3 Examples: quadratic and cyclotomic fields	5
1.4 The Hilbert class field	9
1.5 Decomposition and inertia groups; Frobenius elements	10
2 p-adic Numbers and p-adic Fields	13
2.1 Topological groups	13
2.2 The p -adic absolute value and $\mathbb{Q}_p$	13
2.3 p -adic fields	14
2.4 The structure of $\mathbb{Q}_p^\times$ and quadratic extensions	17
3 Zeta Functions of Number Fields	21
3.1 The norm of an ideal	21
3.2 The Dedekind zeta function	22
3.3 The Gamma function	22
3.4 Euler product and functional equation	23
3.5 The analytic class number formula	24
3.6 Values at negative integers	27
4 Dirichlet L-functions	28
4.1 Dirichlet characters	28
4.2 Gauss sums	29
4.3 Dirichlet L -functions	30
4.4 Generalised Bernoulli numbers and values at negative integers	31
4.5 The functional equation	33
4.6 Special values at $s = 1$ and at even positive integers	34
4.7 Non-vanishing of $L(\chi, 1)$	35
5 Class Numbers of Cyclotomic and Quadratic Fields	36
5.1 Zeta functions of abelian fields	36

5.2	The class number formula for $\mathbb{Q}(\zeta_p)$	37
5.3	Kummer's criterion	38
5.4	Eigenspaces of the class group; Herbrand–Ribet; Kronecker–Weber	40
5.5	Quadratic fields	41
6	Introduction to Iwasawa Theory	43
6.1	Gauss's conjecture and Iwasawa's class number formula	43
6.2	The analytic side: the Kubota–Leopoldt p -adic zeta function	43
6.3	The algebraic side and the Iwasawa main conjecture	44
7	$\mathbb{Z}_p$-extensions	47
7.1	Definition and the cyclotomic $\mathbb{Z}_p$ -extension	47
7.2	How many $\mathbb{Z}_p$ -extensions? Leopoldt's conjecture	48
7.3	Ramification in $\mathbb{Z}_p$ -extensions	50
8	The Iwasawa Algebra	52
8.1	Complete group algebras	52
8.2	The power series ring $\mathcal{O}[[T]]$	53
8.3	The p -adic Weierstrass preparation theorem	55
8.4	The Iwasawa–Serre isomorphism	56
8.5	Measures on Γ : the Iwasawa algebra from the analytic point of view	58
II	Iwasawa Main Conjecture and p-adic Galois Representations	60
9	Iwasawa's Class Number Formula	61
9.1	The Iwasawa module X_∞	61
9.2	The key proposition	62
9.3	Proof of the key proposition	63
10	The Kubota–Leopoldt p-adic L-function	65
10.1	Statement and interpolation property	65
10.2	Generalised Bernoulli numbers modulo p -powers	66
10.3	Stickelberger elements and the construction of $L_p(\psi)$	67
10.4	The interpolation property	68
11	The Iwasawa Main Conjecture	70
11.1	Setting	70
11.2	The $(-)$ -version	71
11.3	The module $\mathfrak{X}_\infty^{\text{cyc}}$ and the $(+)$ -version	71
11.4	Equivalence of the two versions via the Kummer pairing	72

11.5 λ - and μ -invariants and the analytic class number formula	73
11.6 Strategies of proof: Mazur–Wiles and Rubin	74
11.7 Report problem: primes in residue classes modulo 4	74
12 p-adic Hodge Theory and Selmer Groups	75
12.1 Fontaine’s rings of p -adic periods	75
12.2 Comparison theorems	75
12.3 de Rham and geometric Galois representations	76
12.4 Stable lattices and Galois cohomology	77
12.5 Local conditions H_f^1	78
12.6 Selmer groups and examples	78
13 Elliptic Curves and the Tate–Shafarevich Group	81
13.1 Elliptic curves and the Mordell–Weil theorem	81
13.2 The Tate–Shafarevich group	81
13.3 Selmer’s example	82

Part I

Algebraic Number Theory, Zeta Functions and the Iwasawa Algebra

Chapter 1

Ramification in Number Fields

Throughout, a *number field* is a finite extension of $\mathbb{Q}$, and $\mathcal{O}_K$ denotes the ring of integers of a number field K . For a nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ we write $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ for its residue field; it is a finite field.

1.1 Preliminaries

In this section K'/K is an extension of number fields of degree $n = [K' : K]$ and $\mathfrak{p} \subset \mathcal{O}_K$ is a nonzero prime ideal. The material here was used implicitly in the lecture; we collect it so that the later proofs are complete.

Lemma 1.1.1 (Localisation)

Let $S = \mathcal{O}_K \setminus \mathfrak{p}$, $A = S^{-1}\mathcal{O}_K$ and $B = S^{-1}\mathcal{O}_{K'}$. Then

- (i) A is a discrete valuation ring with maximal ideal $\mathfrak{p}A$, and $A/\mathfrak{p}A \cong k(\mathfrak{p})$;
- (ii) B is a free A -module of rank n ;
- (iii) the natural map $\mathcal{O}_{K'}/\mathfrak{p}\mathcal{O}_{K'} \rightarrow B/\mathfrak{p}B$ is an isomorphism.

Proof. (i) A is a localisation of a Dedekind domain at a prime, hence a local Dedekind domain, hence a DVR. Since $\mathcal{O}_K/\mathfrak{p}$ is already a field, every element of S is invertible modulo $\mathfrak{p}$, so $\mathcal{O}_K/\mathfrak{p} \rightarrow A/\mathfrak{p}A$ is an isomorphism.

(ii) $\mathcal{O}_{K'}$ is a finitely generated $\mathcal{O}_K$ -module, so B is a finitely generated A -module; it is torsion free, and A is a PID, so B is free. Every element of K' is of the form x/m with $x \in \mathcal{O}_{K'}$, $m \in \mathbb{Z} \setminus \{0\}$, so $B \otimes_A K = K'$ and the rank of B is $[K' : K] = n$.

(iii) *Surjective:* let $x/s \in B$ with $x \in \mathcal{O}_{K'}$, $s \in S$. Choose $t \in \mathcal{O}_K$ with $st \equiv 1 \pmod{\mathfrak{p}}$. Then $x/s - xt = x(1 - st)/s \in \mathfrak{p}B$. *Injective:* if $x \in \mathcal{O}_{K'} \cap \mathfrak{p}B$, then $sx \in \mathfrak{p}\mathcal{O}_{K'}$ for some $s \in S$; with t as before, $x = t(sx) + (1 - st)x \in \mathfrak{p}\mathcal{O}_{K'}$. ■

Since $\mathcal{O}_{K'}$ is a Dedekind domain, $\mathfrak{p}\mathcal{O}_{K'}$ factors uniquely as

$$\mathfrak{p}\mathcal{O}_{K'} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad (1.1)$$

with distinct prime ideals $\mathfrak{P}_i \subset \mathcal{O}_{K'}$ and $e_i \geq 1$. These $\mathfrak{P}_i$ are exactly the primes of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$, i.e. with $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$. We call $e_i = e(\mathfrak{P}_i|\mathfrak{p})$ the *ramification index* and $f_i = f(\mathfrak{P}_i|\mathfrak{p}) = [k(\mathfrak{P}_i) : k(\mathfrak{p})]$ the *residue degree*.

Notes. Here $\mathfrak{p}\mathcal{O}_{K'}$ denotes the ideal of $\mathcal{O}_{K'}$ generated by $\mathfrak{p}$ (the *extension* of $\mathfrak{p}$ to $\mathcal{O}_{K'}$). A prime $\mathfrak{P} \subset \mathcal{O}_{K'}$ *lies over* $\mathfrak{p}$, written $\mathfrak{P} | \mathfrak{p}$ (in my handwritten notes also $\mathfrak{P}|\mathcal{O}_K = \mathfrak{p}$), if $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. This is equivalent to $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_{K'}$, i.e. to $\mathfrak{P}$ occurring in (1.1): if $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_{K'}$, then $\mathfrak{P} \cap \mathcal{O}_K$ is a prime ideal containing the maximal ideal $\mathfrak{p}$, hence equal to it.

Proposition 1.1.2 (Fundamental identity)

With notation as in (1.1),

$$\sum_{i=1}^r e_i f_i = [K' : K].$$

In particular $1 \leq r \leq [K' : K]$.

Proof. By the Chinese remainder theorem, $\mathcal{O}_{K'}/\mathfrak{p}\mathcal{O}_{K'} \cong \prod_i \mathcal{O}_{K'}/\mathfrak{P}_i^{e_i}$. All these rings are $k(\mathfrak{p})$ -vector spaces, and by Lemma 1.1.1 the left-hand side has dimension $\dim_{k(\mathfrak{p})} B/\mathfrak{p}B = n$.

Fix $\mathfrak{P} = \mathfrak{P}_i$, $e = e_i$. In the chain $\mathcal{O}_{K'} \supset \mathfrak{P} \supset \mathfrak{P}^2 \supset \cdots \supset \mathfrak{P}^e$ every quotient $\mathfrak{P}^j/\mathfrak{P}^{j+1}$ is a vector space over $k(\mathfrak{P})$. It is nonzero (unique factorisation), and it is one-dimensional: an $\mathcal{O}_{K'}$ -submodule strictly between $\mathfrak{P}^{j+1}$ and $\mathfrak{P}^j$ would be an ideal $\mathfrak{b}$ with $\mathfrak{P}^{j+1} \subsetneq \mathfrak{b} \subsetneq \mathfrak{P}^j$, but the ideals containing $\mathfrak{P}^{j+1}$ are the divisors $\mathfrak{P}^0, \dots, \mathfrak{P}^{j+1}$ of $\mathfrak{P}^{j+1}$. Hence $\dim_{k(\mathfrak{p})} \mathcal{O}_{K'}/\mathfrak{P}^e = e \cdot [k(\mathfrak{P}) : k(\mathfrak{p})] = ef$, and summing gives the claim. ■

Lemma 1.1.3 (Trace form and reducedness)

Let k be a finite field and R a finite-dimensional commutative k -algebra. The trace form $(x, y) \mapsto \text{Tr}_{R/k}(xy)$ is nondegenerate if and only if R is reduced (has no nonzero nilpotent elements).

Proof. If $x \neq 0$ is nilpotent, then xy is nilpotent for every y , so multiplication by xy is a nilpotent endomorphism of R and $\text{Tr}_{R/k}(xy) = 0$. Thus x lies in the radical of the trace form and the form is degenerate.

Conversely let R be reduced. R is Artinian, so it has finitely many maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ and its Jacobson radical $\bigcap \mathfrak{m}_j$ is nilpotent, hence 0. By the Chinese remainder theorem $R \cong \prod_j k_j$ with $k_j = R/\mathfrak{m}_j$ finite field extensions of k , and the trace form is the orthogonal sum of the trace forms of the k_j/k . Since finite fields are perfect, k_j/k is separable, and $\text{Tr}_{k_j/k} = \sum_{\sigma} \sigma$ (sum over the distinct embeddings) is not identically zero by Dedekind's lemma on the independence of characters. If $0 \neq x \in k_j$, choose z with $\text{Tr}(z) \neq 0$ and put $y = x^{-1}z$; then $\text{Tr}(xy) \neq 0$. Hence each summand, and so the whole form, is nondegenerate. ■

Corollary 1.1.4

$\mathfrak{p}$ is unramified in K' (i.e. all $e_i = 1$) if and only if $\mathcal{O}_{K'}/\mathfrak{p}\mathcal{O}_{K'}$ is reduced.

Proof. $\mathcal{O}_{K'}/\mathfrak{p}\mathcal{O}_{K'} \cong \prod_i \mathcal{O}_{K'}/\mathfrak{P}_i^{e_i}$ is reduced iff every factor is. If $e \geq 2$ then any element of $\mathfrak{P}^{e-1} \setminus \mathfrak{P}^e$ gives a nonzero nilpotent of $\mathcal{O}_{K'}/\mathfrak{P}^e$; if $e = 1$ the factor is a field. ■

Finally we record the standard tool for computing factorisations.

Proposition 1.1.5 (Dedekind–Kummer)

Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$, let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α , and let p be a prime with $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Write

$$\bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r} \quad \text{in } \mathbb{F}_p[x]$$

with distinct monic irreducible $\bar{g}_i$, and let $g_i \in \mathbb{Z}[x]$ be monic lifts. Then $\mathfrak{P}_i = (p, g_i(\alpha))$ are distinct prime ideals of $\mathcal{O}_K$, $f(\mathfrak{P}_i|p) = \deg \bar{g}_i$, and

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

Proof. Let $m = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ and choose $u, v \in \mathbb{Z}$ with $um + vp = 1$. We claim that $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \rightarrow \mathcal{O}_K/p\mathcal{O}_K$ is an isomorphism. It is surjective because for $y \in \mathcal{O}_K$ we have $y = u(my) + p(vy)$ with $my \in \mathbb{Z}[\alpha]$. It is injective: if $x = py \in \mathbb{Z}[\alpha]$ with $y \in \mathcal{O}_K$, then $y = u(my) + vx \in \mathbb{Z}[\alpha]$, so $x \in p\mathbb{Z}[\alpha]$.

Hence $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[x]/(p, f) \cong \mathbb{F}_p[x]/(\bar{f}) \cong \prod_i \mathbb{F}_p[x]/(\bar{g}_i^{e_i})$. The maximal ideals of $\mathbb{F}_p[x]/(\bar{f})$ are the $(\bar{g}_i)$, with residue fields $\mathbb{F}_p[x]/(\bar{g}_i)$ of degree $\deg \bar{g}_i$; under the isomorphism they correspond to the ideals $\mathfrak{P}_i = (p, g_i(\alpha))$ of $\mathcal{O}_K$, which are therefore exactly the primes above p , pairwise distinct, with $f(\mathfrak{P}_i|p) = \deg \bar{g}_i$.

The image of $\prod_i \mathfrak{P}_i^{e_i}$ in $\mathbb{F}_p[x]/(\bar{f})$ is $\prod_i (\bar{g}_i)^{e_i} = (\bar{f}) = 0$, so $\prod_i \mathfrak{P}_i^{e_i} \subseteq p\mathcal{O}_K$, i.e. $p\mathcal{O}_K \mid \prod_i \mathfrak{P}_i^{e_i}$. Writing $p\mathcal{O}_K = \prod_i \mathfrak{P}_i^{a_i}$ this gives $a_i \leq e_i$. By Proposition 1.1.2, $\sum_i a_i \deg \bar{g}_i = [K : \mathbb{Q}] = \deg f = \sum_i e_i \deg \bar{g}_i$, so $a_i = e_i$ for all i . ■

1.2 Ramification and decomposition of primes

Definition 1.2.1

Let K'/K be a finite extension of number fields, $d = [K' : K]$, and $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero prime ideal with prime decomposition

$$\mathfrak{p}\mathcal{O}_{K'} = \prod_{1 \leq i \leq r} \mathfrak{P}_i^{e_i},$$

where the $\mathfrak{P}_i$ are distinct prime ideals of $\mathcal{O}_{K'}$ and the e_i are positive integers (r is a positive integer with $1 \leq r \leq [K' : K]$, by Proposition 1.1.2).

- (1) We say that $\mathfrak{p}$ is *ramified* if $e_i \geq 2$ for some i . We say that $\mathfrak{p}$ is *totally ramified* if $r = 1$ and $e_1 = d$. We say that $\mathfrak{p}$ is *unramified* if $\mathfrak{p}$ is not ramified, i.e. $e_i = 1$ for all i .
- (2) Suppose that $\mathfrak{p}$ is unramified. We say that $\mathfrak{p}$ is *decomposed* if $r > 1$, and *totally decomposed* (or *splits completely*) if $r = d$. We say that $\mathfrak{p}$ is *inert* if $r = 1$.

Notes. By the fundamental identity, an unramified $\mathfrak{p}$ is totally decomposed iff all $f_i = 1$, and is inert iff $\mathfrak{p}\mathcal{O}_{K'}$ stays prime with $f_1 = d$. Likewise, $\mathfrak{p}$ is totally ramified iff $r = 1$, $e_1 = d$, $f_1 = 1$.

Theorem 1.2.2 (Dedekind)

Let K be a number field with discriminant D_K . Then a prime ideal $(p) \subset \mathbb{Z}$ is ramified in K if and only if $p \mid D_K$.

Notes. The *discriminant* is $D_K = \det(\text{Tr}_{K/\mathbb{Q}}(\omega_i \omega_j))_{i,j}$ for a $\mathbb{Z}$ -basis $\omega_1, \dots, \omega_n$ of $\mathcal{O}_K$. Another $\mathbb{Z}$ -basis differs by a matrix $U \in GL_n(\mathbb{Z})$, which multiplies the determinant by $\det(U)^2 = 1$. So $D_K \in \mathbb{Z}$ is well defined, and $D_K \neq 0$ because $K/\mathbb{Q}$ is separable. “The prime ideal $(p) = p\mathbb{Z}$ is ramified in K ” means that $p\mathcal{O}_K$ has a repeated prime factor; we identify (p) with the prime number p .

Proof. Let $\omega_1, \dots, \omega_n$ be a $\mathbb{Z}$ -basis of $\mathcal{O}_K$, so that $D_K = \det(\text{Tr}_{K/\mathbb{Q}}(\omega_i \omega_j))$. The images $\bar{\omega}_1, \dots, \bar{\omega}_n$ form an $\mathbb{F}_p$ -basis of $R = \mathcal{O}_K/p\mathcal{O}_K$. For $x \in \mathcal{O}_K$ the matrix of multiplication by $\bar{x}$ on R in this basis is the reduction mod p of the matrix of multiplication by x on $\mathcal{O}_K$, so $\text{Tr}_{R/\mathbb{F}_p}(\bar{x}) =$

$\text{Tr}_{K/\mathbb{Q}}(x) \bmod p$. Hence $D_K \bmod p$ is the discriminant of the trace form of $R/\mathbb{F}_p$, and

$$p \mid D_K \iff \text{trace form of } R \text{ degenerate} \iff R \text{ not reduced} \iff p \text{ ramified,}$$

by Lemma 1.1.3 and Corollary 1.1.4. ■

Proposition 1.2.3

Let K'/K be a finite extension of number fields. Then only finitely many prime ideals of $\mathcal{O}_K$ are ramified in K'/K .

Correction. In my notes this was written as “only finite prime ideals are ramified”; it should read “only *finitely many* prime ideals are ramified”.

Proof. Choose a primitive element $\alpha \in \mathcal{O}_{K'}$ of K'/K with minimal polynomial $f \in \mathcal{O}_K[x]$ of degree n , and let $\delta = \text{disc}(1, \alpha, \dots, \alpha^{n-1}) = \text{disc}(f) \in \mathcal{O}_K$. Since K'/K is separable, $\delta \neq 0$. We show that every prime $\mathfrak{p}$ with $\delta \notin \mathfrak{p}$ is unramified; as $\delta \mathcal{O}_K$ has only finitely many prime factors, this proves the claim.

Let A, B be as in Lemma 1.1.1 and $\beta_1, \dots, \beta_n$ an A -basis of B . Write $\alpha^{i-1} = \sum_j M_{ij} \beta_j$ with $M \in M_n(A)$; then $\delta = \det(M)^2 \text{disc}(\beta_1, \dots, \beta_n)$. As $\delta \notin \mathfrak{p}$, δ is a unit of A , hence so is $\text{disc}(\beta) = \det(\text{Tr}_{K'/K}(\beta_i \beta_j))$. Reducing modulo $\mathfrak{p}A$ exactly as in the proof of Theorem 1.2.2, the trace form of $B/\mathfrak{p}B \cong \mathcal{O}_{K'}/\mathfrak{p}\mathcal{O}_{K'}$ over $k(\mathfrak{p})$ is nondegenerate, so this ring is reduced and $\mathfrak{p}$ is unramified by Corollary 1.1.4. ■

Notes. More precisely, one defines the relative discriminant ideal $\mathfrak{d}_{K'/K} \subseteq \mathcal{O}_K$ and the same argument shows: $\mathfrak{p}$ ramifies in K' iff $\mathfrak{p} \mid \mathfrak{d}_{K'/K}$. For $K = \mathbb{Q}$ this is Theorem 1.2.2.

1.3 Examples: quadratic and cyclotomic fields

Quadratic fields

Lemma 1.3.1

Let $m \neq 0, 1$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{m})$. Then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{m}] & m \equiv 2, 3 \pmod{4}, \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & m \equiv 1 \pmod{4}, \end{cases} \quad D_K = \begin{cases} 4m & m \equiv 2, 3 \pmod{4}, \\ m & m \equiv 1 \pmod{4}. \end{cases}$$

Proof. An element $x = a + b\sqrt{m}$ with $b \neq 0$ has minimal polynomial $X^2 - 2aX + (a^2 - mb^2)$, so $x \in \mathcal{O}_K$ iff $A := 2a \in \mathbb{Z}$ and $a^2 - mb^2 \in \mathbb{Z}$. Then $m(2b)^2 = A^2 - 4(a^2 - mb^2) \in \mathbb{Z}$; as m is squarefree, the denominator of $2b$ must be 1, so $B := 2b \in \mathbb{Z}$ and the condition becomes $A^2 \equiv mB^2 \pmod{4}$. Since squares are $0, 1 \pmod{4}$: if $m \equiv 2, 3 \pmod{4}$ this forces A, B even, and if $m \equiv 1 \pmod{4}$ it means $A \equiv B \pmod{2}$. This gives $\mathcal{O}_K$. For the discriminant: with the basis $1, \sqrt{m}$ we get $\det\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2m \end{smallmatrix}\right) = 4m$; with $1, \omega = \frac{1+\sqrt{m}}{2}$ we have $\text{Tr } \omega = 1$, $\text{Tr } \omega^2 = \frac{1+m}{2}$ and $\det\left(\begin{smallmatrix} 2 & 1 \\ 1 & (1+m)/2 \end{smallmatrix}\right) = m$. ■

Proposition 1.3.2 (Example 1 of the lecture)

Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field (m squarefree) and let $(p) \subset \mathbb{Z}$ be a nonzero prime ideal. Then:

- (a) (p) is ramified iff $p \mid D_K$;
- (b) if p is odd and $p \nmid D_K$: (p) is decomposed iff $\bar{m} \in (\mathbb{F}_p^\times)^2$, and inert iff $\bar{m} \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$;
- (c) if $p = 2 \nmid D_K$ (i.e. $m \equiv 1 \pmod{4}$): (2) is decomposed iff $m \equiv 1 \pmod{8}$, and inert iff $m \equiv 5 \pmod{8}$.

Correction. In my notes the criterion with $(\mathbb{F}_p^\times)^2$ was written for all p ; it only makes sense for odd p . The case $p = 2$ is (c).

Proof. We apply Proposition 1.1.5. Note $[\mathcal{O}_K : \mathbb{Z}[\sqrt{m}]] \in \{1, 2\}$.

p odd, $p \mid m$. Take $\alpha = \sqrt{m}$ (index prime to p). Then $x^2 - m \equiv x^2 \pmod{p}$, so $p\mathcal{O}_K = (p, \sqrt{m})^2$ is ramified.

p odd, $p \nmid m$. Again $\alpha = \sqrt{m}$. Now $x^2 - \bar{m}$ is separable over $\mathbb{F}_p$ (its roots are nonzero and $2 \neq 0$), so it is either a product of two distinct linear factors (iff $\bar{m}$ is a square) or irreducible. Accordingly (p) is decomposed or inert.

$p = 2$, $m \equiv 2, 3 \pmod{4}$. Here $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ and $x^2 - m \equiv (x + m)^2 \pmod{2}$, so (2) ramifies.

$p = 2$, $m \equiv 1 \pmod{4}$. Take $\alpha = \omega = \frac{1+\sqrt{m}}{2}$, with minimal polynomial $x^2 - x - \frac{m-1}{4}$. Modulo 2 this is $x(x+1)$ if $m \equiv 1 \pmod{8}$ (decomposed) and the irreducible $x^2 + x + 1$ if $m \equiv 5 \pmod{8}$ (inert).

Comparing with Lemma 1.3.1, p ramifies exactly when $p \mid D_K$, in accordance with Theorem 1.2.2. ■

Cyclotomic fields

Proposition 1.3.3

Let F be a field and $n \geq 1$ with $\text{char } F \nmid n$, and let ζ_n be a primitive n -th root of unity. Then $F(\zeta_n)/F$ is a Galois extension, and there is an injective group homomorphism

$$\chi : \text{Gal}(F(\zeta_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad g(\zeta_n) = \zeta_n^{\chi(g)}.$$

Proof. Since $\text{char } F \nmid n$, $x^n - 1$ is separable, and its roots form a cyclic group μ_n of order n generated by ζ_n . Thus $F(\zeta_n)$ is the splitting field of the separable polynomial $x^n - 1$, hence Galois. Any $g \in \text{Gal}$ satisfies $g(\zeta_n)^n = 1$ and maps μ_n isomorphically onto itself, so $g(\zeta_n)$ is again a generator, $g(\zeta_n) = \zeta_n^a$ with $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ well defined. Clearly $\chi(gh) = \chi(g)\chi(h)$, and χ is injective because g is determined by $g(\zeta_n)$. ■

Report Problem 1.3.4

Prove that $\text{Gal}(F(\zeta_n)/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective (hence an isomorphism) if $F = \mathbb{Q}$.

Surjectivity of χ for $F = \mathbb{Q}$ is equivalent to $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, i.e. to the irreducibility of the cyclotomic polynomial $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a) \in \mathbb{Z}[x]$.

Theorem 1.3.5

Φ_n is irreducible over $\mathbb{Q}$. Consequently $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Solution. Let $f \in \mathbb{Q}[x]$ be the minimal polynomial of $\zeta = \zeta_n$. Since ζ is an algebraic integer, $f \in \mathbb{Z}[x]$ is monic (Gauss' lemma), and $\Phi_n = fh$ with $h \in \mathbb{Z}[x]$ monic.

Claim: if $p \nmid n$ is prime and ξ is a root of f , then ξ^p is a root of f . Otherwise $h(\xi^p) = 0$ (since ξ^p is a primitive n -th root, it is a root of Φ_n). Then ξ is a root of $h(x^p)$, so $f(x) \mid h(x^p)$ in $\mathbb{Z}[x]$. Reducing mod p and using $\bar{h}(x^p) = \bar{h}(x)^p$ we get $f \mid \bar{h}^p$, so f and $\bar{h}$ have a common irreducible factor and $\bar{\Phi}_n = \bar{f}\bar{h}$ has a repeated root in $\bar{\mathbb{F}}_p$. But $\bar{\Phi}_n \mid x^n - 1$, which is separable over $\bar{\mathbb{F}}_p$ since $p \nmid n$. Contradiction.

Every $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ is represented by a product of primes not dividing n , so applying the claim repeatedly, every ζ^a is a root of f . Thus $f = \Phi_n$, and χ is surjective since $|\text{Gal}| = \deg \Phi_n = \varphi(n)$. ■

Report Problem 1.3.6

Calculate the discriminant D_K for $K = \mathbb{Q}(\zeta_n)$.

Since $\zeta_{2m} = -\zeta_m$ for odd m , we have $\mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m)$; so we may and do assume $n \not\equiv 2 \pmod{4}$. We first treat prime powers.

Proposition 1.3.7

Let p be a prime, $k \geq 1$, $\zeta = \zeta_{p^k}$, $K = \mathbb{Q}(\zeta)$, $N = \varphi(p^k)$ and $\pi = 1 - \zeta$. Then

- (i) $p\mathcal{O}_K = (\pi)^N$, and (π) is a prime ideal with residue degree 1; in particular p is totally ramified in K ;
- (ii) $\mathcal{O}_K = \mathbb{Z}[\zeta]$;
- (iii) $|D_K| = p^{p^{k-1}(kp-k-1)}$.

Proof. (i) We have $\Phi_{p^k}(x) = \sum_{j=0}^{p-1} x^{jp^{k-1}}$, so $p = \Phi_{p^k}(1) = \prod_{a \in (\mathbb{Z}/p^k)^\times} (1 - \zeta^a)$. For $p \nmid a$ the quotient $\frac{1-\zeta^a}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{a-1}$ is integral, and so is its inverse $\frac{1-\zeta}{1-\zeta^a} = \frac{1-(\zeta^a)^b}{1-\zeta^a}$ where $ab \equiv 1 \pmod{p^k}$. Hence $1 - \zeta^a = \pi \cdot (\text{unit})$ and $p\mathcal{O}_K = \pi^N \mathcal{O}_K$. Write $\pi\mathcal{O}_K = \prod_j \mathfrak{q}_j^{c_j}$; then $p\mathcal{O}_K = \prod_j \mathfrak{q}_j^{Nc_j}$, and Proposition 1.1.2 together with $[K : \mathbb{Q}] = N$ (Theorem 1.3.5) gives $\sum_j Nc_j f_j = N$. So there is one $\mathfrak{q} = \pi\mathcal{O}_K$, with $c = f = 1$.

(iii) for $\mathbb{Z}[\zeta]$. We compute $d := \text{disc}(1, \zeta, \dots, \zeta^{N-1}) = \pm N_{K/\mathbb{Q}}(\Phi'_{p^k}(\zeta))$. Differentiating $(x^{p^{k-1}} - 1)\Phi_{p^k}(x) = x^{p^k} - 1$ and setting $x = \zeta$ yields $(\zeta^{p^{k-1}} - 1)\Phi'_{p^k}(\zeta) = p^k \zeta^{p^k-1}$. Now $\eta = \zeta^{p^{k-1}}$ is a primitive p -th root of unity, $N_{\mathbb{Q}(\eta)/\mathbb{Q}}(1-\eta) = \Phi_p(1) = p$ and $[K : \mathbb{Q}(\eta)] = p^{k-1}$, so $|N_{K/\mathbb{Q}}(\eta-1)| = p^{p^{k-1}}$. Together with $N(p^k) = p^{kN}$ and $|N(\zeta)| = 1$:

$$|d| = p^{kN - p^{k-1}} = p^{p^{k-1}(kp-k-1)}.$$

(ii) Note $\mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$, and $d = [\mathcal{O}_K : \mathbb{Z}[\pi]]^2 D_K$, so the index m is a power of p . Suppose $p \mid m$. Then there is $x \in \mathcal{O}_K \setminus \mathbb{Z}[\pi]$ with $px \in \mathbb{Z}[\pi]$; write $px = \sum_{j=0}^{N-1} a_j \pi^j$ with $a_j \in \mathbb{Z}$, not all divisible by p . Let i be minimal with $p \nmid a_i$ and put $y = \sum_{j \geq i} a_j \pi^j = px - \sum_{j < i} a_j \pi^j \in p\mathcal{O}_K$. Let v be the valuation of $\mathfrak{q} = (\pi)$, so $v(\pi) = 1$, $v(p) = N$, and $v(a) = 0$ for integers a prime to p . Then $v(a_i \pi^i) = i$ and $v(a_j \pi^j) \geq j > i$ for $j > i$, so $v(y) = i < N$, contradicting $y \in p\mathcal{O}_K$. Hence $m = 1$, $\mathcal{O}_K = \mathbb{Z}[\zeta]$ and $|D_K| = |d|$. ■

Lemma 1.3.8 (Coprime discriminants)

Let K, L be number fields with $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$ and $\gcd(D_K, D_L) = 1$. Then

$$\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L \quad \text{and} \quad D_{KL} = D_K^{[L:\mathbb{Q}]} D_L^{[K:\mathbb{Q}]}.$$

Proof. Let $m = [K : \mathbb{Q}]$, $\ell = [L : \mathbb{Q}]$, and let $\alpha_1, \dots, \alpha_m$ and $\beta_1, \dots, \beta_\ell$ be integral bases of K and L . By the degree assumption, $\{\alpha_i \beta_j\}$ is a $\mathbb{Q}$ -basis of KL . Let $\alpha \in \mathcal{O}_{KL}$ and write $\alpha = \sum_{i,j} \frac{m_{ij}}{r} \alpha_i \beta_j$ with $m_{ij}, r \in \mathbb{Z}$.

Since $[KL : L] = m$, there are exactly m embeddings $\tau_1, \dots, \tau_m$ of KL into $\mathbb{C}$ fixing L ; their restrictions to K are distinct (as $KL = L(K)$), hence are all the embeddings $\sigma_1, \dots, \sigma_m$ of K . Put $x_i = \sum_j \frac{m_{ij}}{r} \beta_j \in L$. Then $\tau_k(\alpha) = \sum_i \sigma_k(\alpha_i) x_i$ for $k = 1, \dots, m$. By Cramer's rule $x_i = \gamma_i / \delta$, where $\delta = \det(\sigma_k(\alpha_i))$ satisfies $\delta^2 = D_K$ and γ_i is an algebraic integer (a determinant of algebraic integers). Thus $D_K x_i = \delta \gamma_i$ is an algebraic integer lying in L , i.e. $D_K x_i \in \mathcal{O}_L$, which means $D_K m_{ij} / r \in \mathbb{Z}$ for all i, j . By symmetry $D_L m_{ij} / r \in \mathbb{Z}$, and since $\gcd(D_K, D_L) = 1$ we get $m_{ij} / r \in \mathbb{Z}$. Hence $\alpha \in \mathcal{O}_K \mathcal{O}_L$.

For the discriminant, the $m\ell$ embeddings of KL are exactly the pairs (σ_k, ρ_l) of embeddings of K and L . With respect to the basis $\alpha_i \beta_j$, the matrix $(\sigma_k \rho_l(\alpha_i \beta_j))$ is the Kronecker product $A \otimes B$ of $A = (\sigma_k(\alpha_i))$ and $B = (\rho_l(\beta_j))$, and $\det(A \otimes B) = \det(A)^\ell \det(B)^m$. Squaring gives the formula. ■

Theorem 1.3.9 (Solution of Report problem 2)

Let $n > 2$ with $n \not\equiv 2 \pmod{4}$ and $K = \mathbb{Q}(\zeta_n)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ and

$$D_K = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Proof. Absolute value. Let $n = \prod_i p_i^{k_i}$. Rewriting Proposition 1.3.7(iii), $|D_{\mathbb{Q}(\zeta_{p^k})}| = p^{\varphi(p^k)(k - \frac{1}{p-1})}$. We induct on the number of prime factors of n . Write $n = p^k n'$ with $p \nmid n'$, $K_1 = \mathbb{Q}(\zeta_{p^k})$, $K_2 = \mathbb{Q}(\zeta_{n'})$. Then $K_1 K_2 = \mathbb{Q}(\zeta_n)$ (since $\zeta_{p^k} \zeta_{n'}$ is a primitive n -th root of unity), $[K_1 K_2 : \mathbb{Q}] = \varphi(n) = \varphi(p^k) \varphi(n')$ by Theorem 1.3.5, and by induction D_{K_2} is divisible only by primes dividing n' , so $\gcd(D_{K_1}, D_{K_2}) = 1$. Lemma 1.3.8 gives $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^k}] \mathbb{Z}[\zeta_{n'}] = \mathbb{Z}[\zeta_n]$ and

$$|D_K| = \prod_i |D_{\mathbb{Q}(\zeta_{p_i^{k_i}})}|^{\varphi(n)/\varphi(p_i^{k_i})} = \prod_i p_i^{\varphi(n) \left(k_i - \frac{1}{p_i-1} \right)} = \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Sign. For any number field, $\text{sign } D_K = (-1)^{r_2}$, where r_2 is the number of pairs of complex embeddings: indeed $D_K = \delta^2$ with $\delta = \det(\sigma_k(\omega_i))$, and complex conjugation permutes the columns by r_2 transpositions, so $\bar{\delta} = (-1)^{r_2} \delta$, i.e. δ is real or purely imaginary according to the parity of r_2 . For $n > 2$, $\mathbb{Q}(\zeta_n)$ has no real embedding, so $r_2 = \varphi(n)/2$. ■

Example 1.3.10. $D_{\mathbb{Q}(\zeta_3)} = -3$, $D_{\mathbb{Q}(\zeta_4)} = -4$, $D_{\mathbb{Q}(\zeta_5)} = 5^3$, $D_{\mathbb{Q}(\zeta_8)} = 2^8$, $D_{\mathbb{Q}(\zeta_{12})} = \frac{12^4}{2^4 \cdot 3^2} = 144$.

Theorem 1.3.11 (Example 2 of the lecture)

Let $n \not\equiv 2 \pmod{4}$, $K = \mathbb{Q}(\zeta_n)$, and let p be a prime. Then

- (a) (p) is ramified iff $(p) \mid D_K$ iff $p \mid n$;
- (b) if $p \nmid n$, let f be the order of $\bar{p}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $p\mathcal{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ with $r = \varphi(n)/f$ distinct primes, each of residue degree f . In particular

- (p) is totally decomposed iff $p \equiv 1 \pmod{n}$;
- (p) is inert iff $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group generated by $\bar{p}$.

Correction. For $n \equiv 2 \pmod{4}$ statement (a) is false for $p = 2$: e.g. $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$ and 2 is unramified there. Hence the assumption $n \not\equiv 2 \pmod{4}$.

Proof. (a) By Theorem 1.3.9, the exponent of p in D_K is $\varphi(n)(k - \frac{1}{p-1})$ where $p^k \parallel n$; for $k \geq 1$ this is positive unless $p^k = 2$, which is excluded. So the primes dividing D_K are exactly those dividing n , and Theorem 1.2.2 applies.

(b) Since $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, Proposition 1.1.5 applies to Φ_n . As $p \nmid n$, $x^n - 1$ is separable over $\mathbb{F}_p$, hence so is $\bar{\Phi}_n$: so $e = 1$. The roots of $x^n - 1$ in $\bar{\mathbb{F}}_p$ form a cyclic group of order n , and since $x^n - 1 = \prod_{d|n} \bar{\Phi}_d$ is separable, the roots of $\bar{\Phi}_n$ are exactly the elements ξ of exact order n . For such ξ , $[\mathbb{F}_p(\xi) : \mathbb{F}_p]$ is the least f with $\xi^{p^f} = \xi$, i.e. with $p^f \equiv 1 \pmod{n}$. So every irreducible factor of $\bar{\Phi}_n$ has degree f , and there are $\varphi(n)/f$ of them. The two special cases correspond to $f = 1$ and $f = \varphi(n)$. ■

Remark 1.3.12. The above two examples $(\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\zeta_n)$) are both *abelian* extensions of $\mathbb{Q}$. In these examples the law of decomposition of prime ideals of $\mathbb{Z}$ in $\mathcal{O}_K$ is controlled by a congruence (modulus) condition on p — for $\mathbb{Q}(\sqrt{m})$ this follows from quadratic reciprocity, since whether $\bar{m}$ is a square mod p depends only on p modulo $4|m|$. These are typical examples of the conclusion of *class field theory*.

Notes. An extension L/K is called *abelian* if it is Galois and $\text{Gal}(L/K)$ is an abelian group. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is abelian by Proposition 1.3.3, and $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$ is abelian because its Galois group has order 2. “Controlled by a modulus condition” means: there is an integer N such that, for $p \nmid N$, the decomposition type of p (here: the residue degree f) depends only on $p \bmod N$.

1.4 The Hilbert class field

Another corollary of global class field theory is as follows.

Definition 1.4.1 (Hilbert class field)

Let K be a number field. Let H_K be the largest abelian extension of K such that every prime of K is unramified in H_K . We call H_K the *maximal unramified abelian extension* of K , or the *Hilbert class field* of K .

Notes. Here “every prime” includes the *infinite* primes: a real embedding of K must stay real in H_K . If one only asks the finite primes to be unramified one obtains the (in general larger) narrow Hilbert class field, whose Galois group is the narrow class group. “Largest” means: inside a fixed algebraic closure $\bar{K}$, H_K is the compositum of all abelian extensions of K in which every prime is unramified. This makes sense because a compositum of such extensions is again abelian and unramified. That H_K is finite over K is part of class field theory.

Theorem 1.4.2 (Class field theory)

$\text{Gal}(H_K/K) \cong \text{Cl}(K)$. In particular $[H_K : K] = h_K$ is the class number.

Notes. No proof was given in the lecture; this is a consequence of the Artin reciprocity law. The isomorphism is described explicitly in Theorem 1.5.8 below.

Example 1.4.3. For $K = \mathbb{Q}(\sqrt{-5})$ one has $h_K = 2$ and $H_K = K(i) = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. Indeed $K(i) = K(\sqrt{5})$. The only primes ramified in $L = \mathbb{Q}(\sqrt{-5}, i)$ over $\mathbb{Q}$ are 2 and 5. Each of them is unramified in one of the three quadratic subfields (2 in $\mathbb{Q}(\sqrt{5})$, 5 in $\mathbb{Q}(i)$), so its ramification index in $L/\mathbb{Q}$ is 2, which is already attained in $K/\mathbb{Q}$. Hence L/K is unramified at all finite primes, and K has no real places. Since $[L : K] = 2 = h_K$, Theorem 1.4.2 gives $L = H_K$.

1.5 Decomposition and inertia groups; Frobenius elements

Let K be a number field and L/K a Galois extension. (Here L does not necessarily have to be a finite extension; $\mathcal{O}_L$ denotes the integral closure of $\mathcal{O}_K$ in L .)

Definition 1.5.1 (Decomposition group)

In the above setting, choose a prime ideal $0 \neq \mathfrak{p} \subset \mathcal{O}_K$ and a prime $\tilde{\mathfrak{p}} \subset \mathcal{O}_L$ with $\tilde{\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}$. We define a subgroup $D_{\tilde{\mathfrak{p}}} \subset \text{Gal}(L/K)$ by

$$D_{\tilde{\mathfrak{p}}} = \{ g \in \text{Gal}(L/K) \mid g(\tilde{\mathfrak{p}}) = \tilde{\mathfrak{p}} \}.$$

We call $D_{\tilde{\mathfrak{p}}}$ the *decomposition subgroup* at $\tilde{\mathfrak{p}}$ (or at $\mathfrak{p}$).

Notes. Some precisions for infinite L/K . (a) $\mathcal{O}_L = \bigcup_{L'} \mathcal{O}_{L'}$, the union over the finite subextensions L'/K . (b) A prime $\tilde{\mathfrak{p}}$ of $\mathcal{O}_L$ above $\mathfrak{p}$ always exists. The sets of primes of $\mathcal{O}_{L'}$ above $\mathfrak{p}$ are finite, nonempty and form an inverse system, so its inverse limit is nonempty. A compatible family $(\mathfrak{P}_{L'})_{L'}$ then gives $\tilde{\mathfrak{p}} = \bigcup_{L'} \mathfrak{P}_{L'}$. (c) $\text{Gal}(L/K)$ carries the *Krull topology*, in which the subgroups $\text{Gal}(L/L')$, L'/K finite Galois, form a basis of open neighbourhoods of 1. $D_{\tilde{\mathfrak{p}}}$ is a closed subgroup, being the intersection of the preimages of the $D_{\tilde{\mathfrak{p}} \cap L'} \subseteq \text{Gal}(L'/K)$. For finite L/K all of this is trivial and the topology is discrete.

Proposition 1.5.2

Let L/K be finite Galois with group G . Then G acts transitively on the set of primes of $\mathcal{O}_L$ above $\mathfrak{p}$, and $D_{g\tilde{\mathfrak{p}}} = g D_{\tilde{\mathfrak{p}}} g^{-1}$ for all $g \in G$.

Proof. Clearly g maps primes above $\mathfrak{p}$ to primes above $\mathfrak{p}$. Suppose $\mathfrak{P}'$ lies above $\mathfrak{p}$ but $\mathfrak{P}' \neq g\tilde{\mathfrak{p}}$ for all g . By the Chinese remainder theorem there is $x \in \mathcal{O}_L$ with $x \in \mathfrak{P}'$ and $x \equiv 1 \pmod{g\tilde{\mathfrak{p}}}$ for all $g \in G$. Then $N_{L/K}(x) = \prod_g g(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p} \subseteq \tilde{\mathfrak{p}}$, so $g(x) \in \tilde{\mathfrak{p}}$ for some g , i.e. $x \in g^{-1}\tilde{\mathfrak{p}}$, contradicting $x \equiv 1 \pmod{g^{-1}\tilde{\mathfrak{p}}}$.

For the second claim: $h(g\tilde{\mathfrak{p}}) = g\tilde{\mathfrak{p}} \iff g^{-1}hg \in D_{\tilde{\mathfrak{p}}}$. ■

Caution! For a given $\mathfrak{p}$, the ideal $\tilde{\mathfrak{p}} \subset \mathcal{O}_L$ with $\tilde{\mathfrak{p}} \cap \mathcal{O}_K = \mathfrak{p}$ is not unique. If we denote by $D'_{\tilde{\mathfrak{p}}}$ the decomposition subgroup defined with another $\tilde{\mathfrak{p}}'$ with $\tilde{\mathfrak{p}}' \cap \mathcal{O}_K = \mathfrak{p}$, then $D'_{\tilde{\mathfrak{p}}}$ can be different from $D_{\tilde{\mathfrak{p}}}$, but $D_{\tilde{\mathfrak{p}}} \sim D'_{\tilde{\mathfrak{p}}}$ (conjugate) in $\text{Gal}(L/K)$ by Proposition 1.5.2. In this sense

$D_{\mathfrak{p}}$ is not really “well defined”, but rather “well defined modulo conjugation”. (For infinite L/K transitivity still holds: apply the finite case to every finite Galois subextension and use a compactness argument.)

Let $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ be the residue field; it is a finite field. Similarly let $k_{\tilde{\mathfrak{p}}} = \mathcal{O}_L/\tilde{\mathfrak{p}}$ be the residue field of $\tilde{\mathfrak{p}} \subset \mathcal{O}_L$. Then $k_{\tilde{\mathfrak{p}}}$ is an algebraic extension of $k_{\mathfrak{p}}$, and it is Galois (every algebraic extension of a finite field is normal and separable).

Correction. In my notes I wrote “the residue field (not a finite field)”. In fact $k_{\mathfrak{p}}$ is always a finite field; only $k_{\tilde{\mathfrak{p}}}$ can be infinite (when L/K is infinite).

For any $g \in D_{\tilde{\mathfrak{p}}}$ and $\bar{x} \in k_{\tilde{\mathfrak{p}}}$, $g(\bar{x})$ is defined by $g(x) \bmod \tilde{\mathfrak{p}}$, where $x \in \mathcal{O}_L$ is a lift of $\bar{x}$. This is well defined because $g(\tilde{\mathfrak{p}}) = \tilde{\mathfrak{p}}$, and it fixes $k_{\mathfrak{p}}$. Thus we have a natural homomorphism

$$D_{\tilde{\mathfrak{p}}} \longrightarrow \text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}}). \quad (1.2)$$

Proposition 1.5.3

The homomorphism (1.2) is surjective.

Proof. First let L/K be finite with group G ; write $\mathfrak{P} = \tilde{\mathfrak{p}}$, $k = k_{\mathfrak{p}}$, $\ell = k_{\mathfrak{P}}$ (a finite field). Choose $\bar{\theta} \in \ell$ generating $\ell^\times$, so $\ell = k(\bar{\theta})$ and $\bar{\theta} \neq 0$. For $g \notin D_{\mathfrak{P}}$ we have $g^{-1}\mathfrak{P} \neq \mathfrak{P}$, so by the Chinese remainder theorem there is $\theta \in \mathcal{O}_L$ with $\theta \equiv \bar{\theta} \pmod{\mathfrak{P}}$ and $\theta \in g^{-1}\mathfrak{P}$ for all $g \notin D_{\mathfrak{P}}$, i.e. $g(\theta) \in \mathfrak{P}$ for $g \notin D_{\mathfrak{P}}$.

Let $F(x) = \prod_{g \in G} (x - g\theta) \in \mathcal{O}_K[x]$. Its reduction $\bar{F} = \prod_g (x - \bar{g}\bar{\theta})$ has coefficients in k and $\bar{F}(\bar{\theta}) = 0$. Given $\bar{\tau} \in \text{Gal}(\ell/k)$, $\bar{\tau}(\bar{\theta})$ is also a root of $\bar{F}$, so $\bar{\tau}(\bar{\theta}) = \bar{g}\bar{\theta}$ for some $g \in G$. If $g \notin D_{\mathfrak{P}}$ then $\bar{g}\bar{\theta} = 0$, impossible since $\bar{\theta} \neq 0$. So $g \in D_{\mathfrak{P}}$ and its image $\bar{g}$ satisfies $\bar{g}(\bar{\theta}) = \bar{g}\bar{\theta} = \bar{\tau}(\bar{\theta})$, whence $\bar{g} = \bar{\tau}$.

For infinite L/K : $D_{\tilde{\mathfrak{p}}} = \varprojlim D_{\tilde{\mathfrak{p}} \cap L'}$ and $\text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}}) = \varprojlim \text{Gal}(k_{\tilde{\mathfrak{p}} \cap L'}/k_{\mathfrak{p}})$ over the finite Galois subextensions L'/K , and an inverse limit of surjections of finite sets is surjective. ■

Definition 1.5.4 (Inertia group)

We define a subgroup $I_{\tilde{\mathfrak{p}}} \subset D_{\tilde{\mathfrak{p}}}$ to be the kernel of $D_{\tilde{\mathfrak{p}}} \rightarrow \text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}})$, and call $I_{\tilde{\mathfrak{p}}}$ the *inertia subgroup* at $\tilde{\mathfrak{p}}$.

Similarly to $D_{\tilde{\mathfrak{p}}}$, $I_{\tilde{\mathfrak{p}}} \subset \text{Gal}(L/K)$ is not necessarily well defined but “well defined up to conjugation” ($I_{g\tilde{\mathfrak{p}}} = gI_{\tilde{\mathfrak{p}}}g^{-1}$). By definition and Proposition 1.5.3,

$$D_{\tilde{\mathfrak{p}}}/I_{\tilde{\mathfrak{p}}} \cong \text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}}).$$

Proposition 1.5.5

Let L/K be finite Galois of degree n , and $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$. Then all e_i are equal to some e , all f_i are equal to some f , $n = ref$, and

$$|D_{\mathfrak{P}_i}| = ef, \quad |I_{\mathfrak{P}_i}| = e.$$

In particular, $\mathfrak{p}$ is unramified in L iff $I_{\mathfrak{P}}$ is trivial.

Proof. Applying $g \in G$ to $\mathfrak{p}\mathcal{O}_L = \prod \mathfrak{P}_i^{e_i}$ permutes the factors, and g induces $k(\mathfrak{P}) \cong k(g\mathfrak{P})$; by transitivity (Proposition 1.5.2) all e_i and all f_i agree, so $n = ref$ by Proposition 1.1.2. By

the orbit–stabiliser theorem $|D_{\mathfrak{p}}| = n/r = ef$. Since $|\text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))| = f$, surjectivity gives $|I_{\mathfrak{p}}| = ef/f = e$. ■

Let p be the prime number with $(p) = \mathfrak{p} \cap \mathbb{Z}$. Then $k_{\mathfrak{p}}$ is a finite field of characteristic p . We denote by q (a power of p) the cardinality of $k_{\mathfrak{p}}$.

Proposition 1.5.6

$\text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}})$ is (topologically) generated by

$$\text{Frob}_{\mathfrak{p}} : k_{\tilde{\mathfrak{p}}} \rightarrow k_{\tilde{\mathfrak{p}}}, \quad x \mapsto x^q.$$

Proof. $x \mapsto x^q$ is a field homomorphism (characteristic p), injective, and fixes $k_{\mathfrak{p}}$ because $x^q = x$ for all $x \in \mathbb{F}_q$. If $\ell/k_{\mathfrak{p}}$ is finite of degree f , then $\ell = \mathbb{F}_{q^f}$ and the fixed field of $\langle \text{Frob} \rangle$ consists of the roots of $x^q - x$, i.e. is $k_{\mathfrak{p}}$; by Galois theory $\text{Gal}(\ell/k_{\mathfrak{p}}) = \langle \text{Frob} \rangle$ is cyclic of order f . For infinite $k_{\tilde{\mathfrak{p}}}$, the Galois group is the inverse limit of these finite cyclic groups, and the image of $\langle \text{Frob} \rangle$ in each of them is everything, so $\langle \text{Frob} \rangle$ is dense. ■

$\text{Frob}_{\mathfrak{p}}$ is called the *Frobenius element* (of the residue extension).

Notes. A topological group G is *topologically generated* by an element g if the subgroup $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ is dense in G . If $k_{\tilde{\mathfrak{p}}}$ is finite (e.g. L/K finite), this just means that $\text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}})$ is cyclic, generated by $\text{Frob}_{\mathfrak{p}}$. In my handwritten notes the sentence reads “ x is called the Frobenius element”; what is meant is the *map* $x \mapsto x^q$.

Let us suppose that $\mathfrak{p}$ is unramified in L . Then $I_{\tilde{\mathfrak{p}}}$ is the trivial subgroup of $D_{\tilde{\mathfrak{p}}}$, so $D_{\tilde{\mathfrak{p}}} \cong \text{Gal}(k_{\tilde{\mathfrak{p}}}/k_{\mathfrak{p}})$ and $\text{Frob}_{\mathfrak{p}}$ has a unique lift $\text{Frob}_{\tilde{\mathfrak{p}}} \in D_{\tilde{\mathfrak{p}}} \subset \text{Gal}(L/K)$, characterised by

$$\text{Frob}_{\tilde{\mathfrak{p}}}(x) \equiv x^q \pmod{\tilde{\mathfrak{p}}} \quad \text{for all } x \in \mathcal{O}_L.$$

It is also called the *Frobenius element* at $\tilde{\mathfrak{p}}$.

Proposition 1.5.7

$\text{Frob}_{g\tilde{\mathfrak{p}}} = g \text{Frob}_{\tilde{\mathfrak{p}}} g^{-1}$. Hence $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(L/K)$ is well defined up to conjugation, and if L/K is an abelian extension, $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(L/K)$ is well defined.

Proof. $h = g \text{Frob}_{\tilde{\mathfrak{p}}} g^{-1}$ lies in $gD_{\tilde{\mathfrak{p}}}g^{-1} = D_{g\tilde{\mathfrak{p}}}$, and for $x \in \mathcal{O}_L$, $h(x) = g(\text{Frob}_{\tilde{\mathfrak{p}}}(g^{-1}x)) \equiv g((g^{-1}x)^q) = x^q \pmod{g\tilde{\mathfrak{p}}}$. By uniqueness of the lift, $h = \text{Frob}_{g\tilde{\mathfrak{p}}}$. As all primes above $\mathfrak{p}$ are of the form $g\tilde{\mathfrak{p}}$, the remaining claims follow. ■

Theorem 1.5.8 (Artin map for the Hilbert class field)

The isomorphism $\text{Cl}(K) \xrightarrow{\sim} \text{Gal}(H_K/K)$ of Theorem 1.4.2 sends $[\mathfrak{p}] \mapsto \text{Frob}_{\mathfrak{p}}$.

Notes. This makes sense because H_K/K is abelian and unramified, so $\text{Frob}_{\mathfrak{p}}$ is defined for every $\mathfrak{p}$. A pleasant consequence: a prime $\mathfrak{p}$ of K is principal if and only if $\text{Frob}_{\mathfrak{p}} = 1$, if and only if $\mathfrak{p}$ splits completely in H_K .

Chapter 2

p -adic Numbers and p -adic Fields

From now on, we will consider a lot of topological groups, rings and fields.

2.1 Topological groups

Definition 2.1.1

A group G equipped with a topology with which the maps

$$G \times G \rightarrow G, (x, y) \mapsto xy \quad \text{and} \quad G \rightarrow G, x \mapsto x^{-1}$$

are continuous is called a *topological group*. Topological rings and topological fields are defined in the same way (addition, multiplication, negation continuous; for fields also $x \mapsto x^{-1}$ on $K^\times$).

Correction. In my notes the second map was written $x \mapsto x$; it is the inversion $x \mapsto x^{-1}$.

Example 2.1.2. Every group with the discrete topology; $(\mathbb{R}, +)$, $(\mathbb{C}^\times, \cdot)$; profinite groups such as $\text{Gal}(L/K)$ for infinite Galois L/K (Krull topology); and, as we shall see, $\mathbb{Q}_p$, $\mathbb{Z}_p$ and $\mathbb{Q}_p^\times$.

2.2 The p -adic absolute value and $\mathbb{Q}_p$

Definition 2.2.1 (p -adic norm and distance)

Let p be a prime number. The map $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$,

$$|x|_p = \begin{cases} p^{-n}, & x = p^n \frac{b}{a} \quad (a, b \in \mathbb{Z} \text{ prime to } p), \\ 0, & x = 0, \end{cases}$$

is called the *p -adic norm*. Furthermore, $d_p(x, y) = |x - y|_p$ for $x, y \in \mathbb{Q}$ is called the *p -adic distance*. This defines the *p -adic topology* on $\mathbb{Q}$.

We write $v_p(x) = n$ for the exponent above ($v_p(0) = \infty$), so $|x|_p = p^{-v_p(x)}$.

Proposition 2.2.2

For $x, y \in \mathbb{Q}$: (i) $|x|_p = 0 \iff x = 0$; (ii) $|xy|_p = |x|_p |y|_p$; (iii) $|x + y|_p \leq \max(|x|_p, |y|_p)$, with equality if $|x|_p \neq |y|_p$. In particular d_p is a metric (even an ultrametric).

Proof. (i), (ii) follow from $v_p(xy) = v_p(x) + v_p(y)$ (unique factorisation). For (iii) let $n = \min(v_p(x), v_p(y))$; then $x = p^n x'$, $y = p^n y'$ with x', y' having no p in their denominators, so $x + y = p^n(x' + y')$ with $v_p(x' + y') \geq 0$. If, say, $v_p(x) < v_p(y)$, write $x' = a/b$ and $y' = p^k c/d$ with $k \geq 1$ and a, b, d prime to p ; then $x' + y' = (ad + p^k bc)/(bd)$ has numerator $\equiv ad \not\equiv 0 \pmod{p}$, so $v_p(x + y) = n$ and equality holds. The triangle inequality for d_p follows from (iii). ■

We denote by $\mathbb{Q}_p$ (respectively $\mathbb{Z}_p$) the completion of $\mathbb{Q}$ (resp. of $\mathbb{Z}$) with respect to the p -adic topology. The absolute value extends by continuity to $\mathbb{Q}_p$, and all properties of Proposition 2.2.2 persist. Moreover $|\mathbb{Q}_p^\times|_p = p^{\mathbb{Z}}$: if $x = \lim x_n \neq 0$, then $|x - x_n| < |x|$ for large n , and so $|x_n| = |x|$ by (iii). Since $\mathbb{Z}$ is a subset of the complete space $\mathbb{Q}_p$, its completion $\mathbb{Z}_p$ is its closure $\overline{\mathbb{Z}} \subseteq \mathbb{Q}_p$.

Notes. Precisely: $\mathbb{Q}_p$ is the set of Cauchy sequences in $(\mathbb{Q}, d_p)$ modulo the null sequences. With termwise operations it is a field containing $\mathbb{Q}$ (via constant sequences) as a dense subfield, and $|\lim x_n|_p := \lim |x_n|_p$ is well defined. “The p -adic topology” always means the metric topology defined by d_p .

Proposition 2.2.3 (i) $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.

(ii) $\mathbb{Z}_p$ is a discrete valuation ring with unit group $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}$; its only maximal ideal is $\{x \in \mathbb{Z}_p \mid |x|_p < 1\} = p\mathbb{Z}_p$, and every nonzero ideal is $p^k\mathbb{Z}_p$. Moreover $\mathbb{Q}_p = \text{Frac } \mathbb{Z}_p = \mathbb{Z}_p[1/p]$.

(iii) $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$, and $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ as topological rings.

Correction. In my notes the maximal ideal was written as $\{x \in \mathbb{Z}_p \mid |x|_p \leq 1\}$; this is all of $\mathbb{Z}_p$. The correct description is $\{x \in \mathbb{Z}_p \mid |x|_p < 1\}$ (cf. the analogous statement for $\mathcal{O}_K$ below, which I wrote correctly).

Proof. (i) The closed unit ball $B = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is closed and contains $\mathbb{Z}$, so $\mathbb{Z}_p = \overline{\mathbb{Z}} \subseteq B$. Conversely let $x \in B$ and $k \geq 1$. Choose $y \in \mathbb{Q}$ with $|x - y|_p \leq p^{-k}$; then $|y|_p \leq 1$, so $y = a/b$ with $p \nmid b$. Choose $c \in \mathbb{Z}$ with $bc \equiv a \pmod{p^k}$; then $|y - c|_p = |a - bc|_p/|b|_p \leq p^{-k}$, hence $|x - c|_p \leq p^{-k}$. So $x \in \overline{\mathbb{Z}}$.

(ii) B is a ring by the ultrametric inequality. If $|x|_p = 1$ then $|x^{-1}|_p = 1$, so $x \in \mathbb{Z}_p^\times$; conversely units have absolute value 1. Every nonzero $x \in \mathbb{Q}_p$ can be written $x = p^n u$ with $n = v_p(x)$ and $|u|_p = 1$. Hence the nonzero ideals of $\mathbb{Z}_p$ are the $p^k\mathbb{Z}_p$, so $\mathbb{Z}_p$ is a DVR with maximal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \mid |x|_p < 1\}$, and $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$.

(iii) The map $\mathbb{Z} \rightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ is surjective since $\mathbb{Z}$ is dense and $p^n\mathbb{Z}_p$ is open, and its kernel is $\mathbb{Z} \cap p^n\mathbb{Z}_p = p^n\mathbb{Z}$. The resulting map $\mathbb{Z}_p \rightarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is injective since $\bigcap_n p^n\mathbb{Z}_p = 0$, and surjective: a compatible sequence (c_n) with $c_n \in \mathbb{Z}$ is Cauchy, and its limit maps to (c_n) . Both sides carry the topology whose basic neighbourhoods of 0 are $p^n\mathbb{Z}_p$, so it is a homeomorphism. ■

2.3 p -adic fields

Definition 2.3.1

A finite extension of $\mathbb{Q}_p$ is called a *p -adic field*.

Notes. We fix an algebraic closure $\overline{\mathbb{Q}_p}$ and regard p -adic fields as subfields of it. *Warning on notation:* for a p -adic field K , $\mathcal{O}_K$ denotes the valuation ring $\{x \in K \mid |x|_p \leq 1\}$ (defined below), which is the integral closure of $\mathbb{Z}_p$ in K (Proposition 2.3.6). For a number field it denotes the ring of integers. The two notions are analogous, and the context always determines which one is meant.

To extend $|\cdot|_p$ to p -adic fields we need Hensel’s lemma. We state it for a complete discrete

valuation ring $\mathcal{O}$ with uniformiser π and residue field $\kappa = \mathcal{O}/\pi\mathcal{O}$; bars denote reduction modulo π . A polynomial in $\mathcal{O}[x]$ is *primitive* if its reduction is nonzero.

Theorem 2.3.2 (Hensel's lemma)

Let $f \in \mathcal{O}[x]$ be primitive, and suppose $\bar{f} = \bar{g}\bar{h}$ in $\kappa[x]$ with $\bar{g}, \bar{h}$ coprime. Then $f = gh$ with $g, h \in \mathcal{O}[x]$, $\deg g = \deg \bar{g}$, and g, h reducing to $\bar{g}, \bar{h}$.

Proof. Let $d = \deg f$ and $m = \deg \bar{g}$; then $\deg \bar{h} = \deg \bar{f} - m \leq d - m$. Choose lifts g_0, h_0 with $\deg g_0 = m$ (so the leading coefficient of g_0 is a unit) and $\deg h_0 \leq d - m$, and choose $a, b \in \mathcal{O}[x]$ with $ag_0 + bh_0 \equiv 1 \pmod{\pi}$.

Suppose we have g_j, h_j with $g_j \equiv g_0, h_j \equiv h_0 \pmod{\pi}$, $\deg g_j = m$ with unit leading coefficient, $\deg h_j \leq d - m$, and $f \equiv g_j h_j \pmod{\pi^{j+1}}$ (true for $j = 0$). Write $f - g_j h_j = \pi^{j+1} F$ with $F \in \mathcal{O}[x]$, $\deg F \leq d$. Divide $bF = Q_0 g_0 + P$ with $\deg P < m$ (possible since g_0 has unit leading coefficient), and let $Q \in \mathcal{O}[x]$ be obtained from $aF + h_0 Q_0$ by deleting the coefficients divisible by π . Then

$$g_0 Q + h_0 P \equiv g_0(aF + h_0 Q_0) + h_0 P = (ag_0 + bh_0)F \equiv F \pmod{\pi},$$

and comparing degrees modulo π (using $\deg \bar{g}_0 = m$, $\deg \bar{h}_0 \bar{P} < d$) gives $\deg Q \leq d - m$. Put $g_{j+1} = g_j + \pi^{j+1} P$, $h_{j+1} = h_j + \pi^{j+1} Q$. Then

$$f - g_{j+1} h_{j+1} = \pi^{j+1}(F - g_j Q - h_j P) - \pi^{2j+2} PQ \equiv \pi^{j+1}(F - g_0 Q - h_0 P) \equiv 0 \pmod{\pi^{j+2}}.$$

The coefficients of g_j and h_j form Cauchy sequences; by completeness they converge to $g, h \in \mathcal{O}[x]$ with $f = gh$, $\deg g = m$ and the right reductions. ■

Corollary 2.3.3

Let F be the fraction field of $\mathcal{O}$ with absolute value $|\cdot|$, and $f = a_n x^n + \cdots + a_0 \in F[x]$ irreducible with $a_0 a_n \neq 0$. Then $\max_i |a_i| = \max(|a_0|, |a_n|)$. In particular, if f is monic irreducible and $a_0 \in \mathcal{O}$, then $f \in \mathcal{O}[x]$.

Proof. Multiply f by a constant so that $\max_i |a_i| = 1$, i.e. $f \in \mathcal{O}[x]$ primitive. Let r be the smallest index with $|a_r| = 1$. If $0 < r < n$, then $\bar{f} = x^r \cdot (\bar{a}_r + \bar{a}_{r+1}x + \cdots)$ with coprime factors (the second does not vanish at 0), and Hensel's lemma gives $f = gh$ with $\deg g = r$ and $\deg h = n - r \geq 1$, contradicting irreducibility. Hence $r = 0$ or $r = n$, i.e. $|a_0| = 1$ or $|a_n| = 1$. ■

Lemma 2.3.4 (Equivalence of norms)

Let F be a complete valued field and V a finite-dimensional F -vector space with basis $e_1, \dots, e_n$. Every norm $\|\cdot\|$ on V is equivalent to $|\sum c_i e_i|_\infty = \max_i |c_i|$. In particular V is complete for $\|\cdot\|$.

Proof. Clearly $\|x\| \leq (\sum_i \|e_i\|) |x|_\infty$. We show $|x|_\infty \leq C \|x\|$ by induction on n ; $n = 1$ is clear. If no such C exists, there are $x^{(k)}$ with $\|x^{(k)}\| < \frac{1}{k} |x^{(k)}|_\infty$. Dividing by a coordinate of maximal absolute value and passing to a subsequence we may assume $x^{(k)} = e_i + y^{(k)}$ with $y^{(k)}$ in $W = \text{span}(e_j : j \neq i)$ and $\|x^{(k)}\| \rightarrow 0$. Then $(y^{(k)})$ is $\|\cdot\|$ -Cauchy in W ; by induction $\|\cdot\|$ is equivalent to $|\cdot|_\infty$ on W , so W is complete and $y^{(k)} \rightarrow y \in W$. Then $e_i + y = 0$, contradicting linear independence. ■

We can show that the p -adic norm $|\cdot|_p : \mathbb{Q}_p \rightarrow \mathbb{R}_{\geq 0}$ is uniquely extended to every p -adic field:

Theorem 2.3.5

Let $K/\mathbb{Q}_p$ be a finite extension of degree n . Then $|\cdot|_p$ extends in a unique way to an absolute value on K , namely

$$|x|_p = |N_{K/\mathbb{Q}_p}(x)|_p^{1/[K:\mathbb{Q}_p]} \quad (N_{K/\mathbb{Q}_p}(x) \in \mathbb{Q}_p).$$

Moreover K is complete with respect to it.

Proof. Existence. Write $|x| := |N(x)|_p^{1/n}$. It is multiplicative, $|x| = 0 \iff x = 0$, and for $a \in \mathbb{Q}_p$ we get $|a| = |a^n|_p^{1/n} = |a|_p$. For the ultrametric inequality it suffices to show $|x| \leq 1 \Rightarrow |1+x| \leq 1$ (then for $0 \neq |x| \leq |y|$ we get $|x+y| = |y||1+x/y| \leq |y|$). Let $f = x^d + \dots + a_0$ be the minimal polynomial of x over $\mathbb{Q}_p$; then $N(x) = ((-1)^d a_0)^{n/d}$, so $|x| \leq 1 \iff a_0 \in \mathbb{Z}_p$, and by Corollary 2.3.3 this means $f \in \mathbb{Z}_p[x]$. The minimal polynomial of $1+x$ is $f(X-1) \in \mathbb{Z}_p[X]$, so $N(1+x) \in \mathbb{Z}_p$ and $|1+x| \leq 1$.

Uniqueness. Let $|\cdot|_1, |\cdot|_2$ be two extensions. They are norms on the $\mathbb{Q}_p$ -vector space K , so by Lemma 2.3.4 there are $c, C > 0$ with $c|x|_1 \leq |x|_2 \leq C|x|_1$. Applying this to x^m and taking m -th roots, $c^{1/m}|x|_1 \leq |x|_2 \leq C^{1/m}|x|_1$; letting $m \rightarrow \infty$ gives $|x|_1 = |x|_2$.

Completeness follows from Lemma 2.3.4 since $\mathbb{Q}_p$ is complete. ■

We define $\mathcal{O}_K \subset K$ by $\mathcal{O}_K = \{x \in K \mid |x|_p \leq 1\}$.

Proposition 2.3.6

Let $K/\mathbb{Q}_p$ be finite of degree n .

- (i) $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}_p$ in K .
- (ii) $\mathcal{O}_K$ is a DVR and K is the field of fractions of $\mathcal{O}_K$.
- (iii) The unique maximal ideal of $\mathcal{O}_K$ is $\mathfrak{m}_K = \{x \in \mathcal{O}_K \mid |x|_p < 1\}$, and the residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ is a finite field of characteristic p .
- (iv) $\mathcal{O}_K$ is a free $\mathbb{Z}_p$ -module of rank n . If π is a uniformiser, $p\mathcal{O}_K = \pi^e \mathcal{O}_K$ and $f = [\kappa : \mathbb{F}_p]$, then $ef = n$.

Proof. (i) In the proof of Theorem 2.3.5 we saw $|x| \leq 1 \iff$ the minimal polynomial of x lies in $\mathbb{Z}_p[x]$; such x are integral. Conversely, if x is integral over $\mathbb{Z}_p$, all conjugates of x are integral, so the coefficients of its minimal polynomial are integral over $\mathbb{Z}_p$ and lie in $\mathbb{Q}_p$, hence in $\mathbb{Z}_p$ (a DVR is integrally closed).

(ii)–(iii) $\mathcal{O}_K$ is a ring by the ultrametric inequality, with units $\{|x| = 1\}$. The value group $|K^\times| \subseteq p^{\frac{1}{n}\mathbb{Z}}$ is a nontrivial discrete subgroup of $\mathbb{R}_{>0}$, hence cyclic, generated by $|\pi|$ for some π with $|\pi| < 1$ maximal. Every $x \neq 0$ is $x = \pi^k u$ with $k \in \mathbb{Z}$, $|u| = 1$. Hence the nonzero ideals of $\mathcal{O}_K$ are the $\pi^k \mathcal{O}_K$, $\mathcal{O}_K$ is a DVR with maximal ideal $\pi \mathcal{O}_K = \{|x| < 1\}$, and $K = \mathcal{O}_K[1/\pi]$ is its fraction field. κ is a quotient of $\mathcal{O}_K/p\mathcal{O}_K$, which is finite by (iv).

(iv) Choose a $\mathbb{Q}_p$ -basis $\omega_1, \dots, \omega_n$ of K in $\mathcal{O}_K$. By Lemma 2.3.4 there is C with $\max |c_i| \leq C|\sum c_i \omega_i|$, so $\mathcal{O}_K \subseteq p^{-N} \oplus \mathbb{Z}_p \omega_i$ for suitable N . As a submodule of a finitely generated free module over the PID $\mathbb{Z}_p$ which spans K , $\mathcal{O}_K$ is free of rank n . Thus $|\mathcal{O}_K/p\mathcal{O}_K| = p^n$, while the filtration by $\pi^j \mathcal{O}_K$ shows $|\mathcal{O}_K/\pi^e \mathcal{O}_K| = |\kappa|^e = p^{ef}$. ■

Notes. Terminology used from now on. A generator π of $\mathfrak{m}_K$ is called a *uniformiser*. The *normalised valuation* $v_K : K^\times \rightarrow \mathbb{Z}$ is defined by $x \in \pi^{v_K(x)} \mathcal{O}_K^\times$, so that $v_K(\pi) = 1$ and $v_K(p) = e$ (the *ramification index* of $K/\mathbb{Q}_p$). $f = [\kappa : \mathbb{F}_p]$ is the *residue degree*, $q = |\kappa| = p^f$, and $|x|_p = p^{-v_K(x)/e}$. Some texts use the *normalised absolute value* $\|x\|_K = q^{-v_K(x)} = |x|_p^{[K:\mathbb{Q}_p]}$ instead; it does not extend $|\cdot|_p$ unless $K = \mathbb{Q}_p$.

2.4 The structure of $\mathbb{Q}_p^\times$ and quadratic extensions

Lecture of 27 April 2026. Last time we explained p -adic fields. Throughout this section K is a p -adic field of degree n , $\mathcal{O}_K, \mathfrak{m}_K, \pi, \kappa, e$ are as in Proposition 2.3.6, $q = |\kappa|$, $U = \mathcal{O}_K^\times$ and $U^{(k)} = 1 + \mathfrak{m}_K^k$ ($k \geq 1$). For $K = \mathbb{Q}_p$: $U = \mathbb{Z}_p^\times$, $U^{(1)} = 1 + p\mathbb{Z}_p$.

Theorem 2.4.1 (The structure of $\mathbb{Q}_p^\times$)

We have the decomposition

$$\mathbb{Q}_p^\times = p^\mathbb{Z} \times \mathbb{Z}_p^\times, \quad p^\mathbb{Z} \cong \mathbb{Z}.$$

Moreover, for $p \neq 2$,

$$\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times (1 + p\mathbb{Z}_p), \quad 1 + p\mathbb{Z}_p \xrightarrow[\log]{\sim} p\mathbb{Z}_p \cong \mathbb{Z}_p,$$

where $\log(1+x) = \sum_{n \geq 1} (-1)^{n+1} \frac{x^n}{n}$. Hence

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \quad (p \neq 2).$$

Notes. The equality $\mathbb{Q}_p^\times = p^\mathbb{Z} \times \mathbb{Z}_p^\times$ is an *internal* direct product: the multiplication map $p^\mathbb{Z} \times \mathbb{Z}_p^\times \rightarrow \mathbb{Q}_p^\times$ is an isomorphism of topological groups ($p^\mathbb{Z}$ being discrete). The decomposition $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ below is canonical. The isomorphisms $\mu_{p-1} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ and $p\mathbb{Z}_p \cong \mathbb{Z}_p$, however, depend on choices (a generator of μ_{p-1} , division by p). So “ $\cong$ ” here means an abstract isomorphism of topological groups.

Notes. In the lecture the decomposition of $\mathbb{Z}_p^\times$ was motivated via $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and the corresponding decomposition $(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times (1 + p\mathbb{Z}/p^n\mathbb{Z})$ at finite level (the first factor being multiplicative, i.e. an “additive group” only up to isomorphism). Below we give a proof directly on $\mathbb{Z}_p$, which also works for any p -adic field.

The first decomposition is immediate: $x = p^{v_p(x)} \cdot u$ with $u \in \mathbb{Z}_p^\times$ uniquely, by Proposition 2.2.3. The rest follows from the general results below.

Lemma 2.4.2 (Teichmüller lifts)

The group μ_{q-1} of $(q-1)$ -th roots of unity is contained in K , and reduction maps it isomorphically onto $\kappa^\times$. Consequently

$$K^\times = \pi^\mathbb{Z} \times \mu_{q-1} \times U^{(1)}.$$

Proof. Over $\kappa = \mathbb{F}_q$, $x^{q-1} - 1 = \prod_{a \in \kappa^\times} (x - a)$ with pairwise coprime factors. Applying Hensel’s lemma (Theorem 2.3.2) repeatedly, $x^{q-1} - 1$ splits into linear factors over $\mathcal{O}_K$, with roots reducing

to the distinct elements of $\kappa^\times$. So the reduction map $\mu_{q-1} \rightarrow \kappa^\times$ is bijective. The reduction $U \rightarrow \kappa^\times$ is surjective with kernel $U^{(1)}$, and μ_{q-1} is a section, so $U = \mu_{q-1} \times U^{(1)}$; finally $K^\times = \pi^\mathbb{Z} \times U$ as in the proof of Proposition 2.3.6. ■

To treat $U^{(1)}$ we need to manipulate power series. Recall that in a complete non-archimedean field a family $(a_i)_{i \in I}$ (I countable) is *summable* if for every $\varepsilon > 0$ only finitely many $|a_i| \geq \varepsilon$; then $\sum_{i \in I} a_i$ converges in any order to the same value, and may be computed by first summing over the blocks of any partition of I (the partial sums over finite sets containing $\{|a_i| \geq \varepsilon\}$ differ by less than ε). Also, $|n|_p \geq 1/n$ for all $n \geq 1$, since $p^{v_p(n)} \leq n$.

Proposition 2.4.3 (The p -adic logarithm) (i) $\log(1+x) = \sum_{n \geq 1} (-1)^{n+1} x^n / n$ converges for $x \in \mathfrak{m}_K$, and $\log : U^{(1)} \rightarrow K$ is a homomorphism: $\log(uv) = \log u + \log v$.
 (ii) If $k > e/(p-1)$, then $\log$ restricts to an isomorphism of topological groups $U^{(k)} \xrightarrow{\sim} \mathfrak{m}_K^k$ with $|\log u| = |u - 1|$.

Proof. (i) For $|x| < 1$ we have $|x^n/n| \leq n|x|^n \rightarrow 0$, so the series converges. Let $x, y \in \mathfrak{m}_K$, $\rho = \max(|x|, |y|) < 1$ and $z = x + y + xy$, so $(1+x)(1+y) = 1+z$. Expanding $\sum_n (-1)^{n+1} z^n / n$ by the multinomial theorem gives terms $c x^a y^b / n$ with $c \in \mathbb{Z}$ and $a+b \geq n$, of absolute value $\leq n\rho^n$; for each n there are finitely many, so the family is summable. Regrouping it by monomials $x^a y^b$ gives the coefficients of the formal power series $\log(1+X+Y+XY) \in \mathbb{Q}[[X, Y]]$, which equals $\log(1+X) + \log(1+Y)$ (both vanish at 0 and have the same partial derivatives, e.g. $\partial_X = \frac{1}{1+X}$). Hence $\log(1+z) = \log(1+x) + \log(1+y)$.

(ii) Let v be the normalised valuation of K , so $v(p) = e$. If $v(x) \geq k$ and $n \geq 2$, then, using $v_p(n) \leq \frac{n-1}{p-1}$ (as $p^{v_p(n)} \leq n$ and $p^s - 1 \geq s(p-1)$),

$$v\left(\frac{x^n}{n}\right) - v(x) = (n-1)v(x) - e v_p(n) > (n-1)\frac{e}{p-1} - e v_p(n) \geq 0.$$

Hence for $x \in \mathfrak{m}_K^j$, $j \geq k$: $\log(1+x) \equiv x \pmod{\mathfrak{m}_K^{j+1}}$. Consequently $\log$ maps $U^{(j)}$ into $\mathfrak{m}_K^j$ and induces isomorphisms $U^{(j)}/U^{(j+1)} \rightarrow \mathfrak{m}_K^j/\mathfrak{m}_K^{j+1}$ (both $\cong \kappa$ via $1+x \mapsto x$), and $|\log u| = |u-1|$. Injectivity: if $u \neq 1$ then $\log u \neq 0$. Surjectivity: given $a \in \mathfrak{m}_K^k$, put $a_0 = a$, $u_0 = 1 + a_0$, and inductively $a_{j+1} = a - \log(u_0 \cdots u_j) \in \mathfrak{m}_K^{k+j+1}$, $u_{j+1} = 1 + a_{j+1}$. The product $u = \prod_j u_j$ converges, and since $\log$ is an isometry on $U^{(k)}$ (as $|\log u - \log u'| = |\log(u/u')| = |u/u' - 1| = |u - u'|$), we get $\log u = \lim \log(u_0 \cdots u_j) = a$. ■

Proof of Theorem 2.4.1. Apply Lemma 2.4.2 with $K = \mathbb{Q}_p$ ($\pi = p$, $q = p$) to get $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ with $\mu_{p-1} \cong \mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ (cyclic). For $p \neq 2$ we have $e = 1 < p-1$, so Proposition 2.4.3(ii) with $k = 1$ gives $1 + p\mathbb{Z}_p \cong p\mathbb{Z}_p$, and $p\mathbb{Z}_p \cong \mathbb{Z}_p$ via multiplication by p^{-1} . ■

Notes. For $p = 2$ the same argument gives $\mathbb{Z}_2^\times = \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$ and $1 + 4\mathbb{Z}_2 \cong 4\mathbb{Z}_2 \cong \mathbb{Z}_2$ (take $k = 2 > e/(p-1) = 1$), so $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

Hence, we have $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.

Corollary 2.4.4

Assume $p \neq 2$. Then $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with representatives 1, u , p , pu , where $u \in \mathbb{Z}_p^\times \setminus (\mathbb{Z}_p^\times)^2$.

Proof. Divide each factor of $\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ by its subgroup of doubles: $\mathbb{Z}/2\mathbb{Z}$ for the first factor, $(\mathbb{Z}/(p-1)\mathbb{Z})/2 = \mathbb{Z}/2\mathbb{Z}$ since $p-1$ is even, and $\mathbb{Z}_p/2\mathbb{Z}_p = \{0\}$ since $2 \in \mathbb{Z}_p^\times$ if $p \neq 2$. For the representatives: since $1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$ is 2-divisible, a unit u is a square iff its Teichmüller component is a square iff $\bar{u} \in (\mathbb{F}_p^\times)^2$. ■

Proposition 2.4.5

Let F be a field of characteristic $\neq 2$. Then $a \mapsto F(\sqrt{a})$ is a bijection between $(F^\times / (F^\times)^2) \setminus \{1\}$ and the set of quadratic extensions of F (inside a fixed algebraic closure; equivalently, up to F -isomorphism).

Proof. If $E = F(\alpha)$ with $\alpha^2 + b\alpha + c = 0$, then $(2\alpha + b)^2 = b^2 - 4c =: a$, so $E = F(\sqrt{a})$ with a a non-square: the map is surjective. If $F(\sqrt{a}) = F(\sqrt{b}) = E$, let σ be the nontrivial element of $\text{Gal}(E/F)$; then $\sigma(\sqrt{a}) = -\sqrt{a}$, $\sigma(\sqrt{b}) = -\sqrt{b}$, so $\sqrt{a}/\sqrt{b} \in F$ and $a/b \in (F^\times)^2$. Conversely $F(\sqrt{a})$ only depends on the square class of a . Two quadratic extensions are normal, so they are F -isomorphic iff they are equal inside $\bar{F}$. ■

Thus we have proved that the number of quadratic extensions of $\mathbb{Q}_p$ (modulo isomorphism) is 3 when $p \neq 2$, namely

$$\mathbb{Q}_p(\sqrt{p}), \quad \mathbb{Q}_p(\sqrt{u}), \quad \mathbb{Q}_p(\sqrt{pu}), \quad u \in \mathbb{Z}_p^\times \setminus (\mathbb{Z}_p^\times)^2.$$

Correction. The third field was written $\mathbb{Q}(\sqrt{pu})$ in my notes; it should be $\mathbb{Q}_p(\sqrt{pu})$.

Report Problem 2.4.6

Determine the number of quadratic extensions of an arbitrary p -adic field.

Theorem 2.4.7 (Solution)

Let K be a p -adic field with $[K : \mathbb{Q}_p] = n$. Then

$$K^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^n,$$

where p^a is the number of p -power roots of unity in K . Consequently

$$\#\{\text{quadratic extensions of } K\} = |K^\times / (K^\times)^2| - 1 = \begin{cases} 3, & p \neq 2, \\ 2^{n+2} - 1, & p = 2. \end{cases}$$

For example, $\mathbb{Q}_2$ has exactly 7 quadratic extensions.

Proof. By Lemma 2.4.2 it remains to determine $U^{(1)}$.

$U^{(1)}$ is a $\mathbb{Z}_p$ -module. For $u = 1 + x \in U^{(1)}$, $|u^p - 1| \leq \max(|p||x|, |x|^p) \leq c|x|$ with $c = \max(|p|, |x|^{p-1}) < 1$, and iterating shows $u^{p^m} \rightarrow 1$. Hence for $a \in \mathbb{Z}_p$ and integers $a_m \rightarrow a$, the limit $u^a = \lim u^{a_m}$ exists, making $U^{(1)}$ a topological $\mathbb{Z}_p$ -module; $\log(u^a) = a \log u$ by continuity.

Structure. Fix $k > e/(p-1)$. By Proposition 2.4.3(ii) and Proposition 2.3.6(iv), $U^{(k)} \cong \mathfrak{m}_K^k = \pi^k \mathcal{O}_K \cong \mathcal{O}_K \cong \mathbb{Z}_p^n$ as $\mathbb{Z}_p$ -modules. Since $|U^{(j)}/U^{(j+1)}| = q$, the index $[U^{(1)} : U^{(k)}]$ is finite, so $U^{(1)}$ is a finitely generated $\mathbb{Z}_p$ -module of rank n . By the structure theorem over the PID $\mathbb{Z}_p$, $U^{(1)} \cong T \times \mathbb{Z}_p^n$ with T the (finite) torsion subgroup. T is a finite subgroup of $K^\times$, hence cyclic, of p -power order (torsion of a $\mathbb{Z}_p$ -module). Every p -power root of unity ζ lies in $U^{(1)}$ (as $\bar{\zeta}^{p^a} = 1$ in characteristic p forces $\bar{\zeta} = 1$), so $T = \mu_{p^a}(K)$.

Counting squares. Dividing each factor by squares: the factor $\mathbb{Z}$ gives $\mathbb{Z}/2\mathbb{Z}$; $(\mathbb{Z}/(q-1)\mathbb{Z})/2$ is $\mathbb{Z}/2\mathbb{Z}$ if p is odd and 0 if $p = 2$; $(\mathbb{Z}/p^a\mathbb{Z})/2$ is 0 if p is odd and $\mathbb{Z}/2\mathbb{Z}$ if $p = 2$ (then $-1 \in T$, so $a \geq 1$); and $\mathbb{Z}_p^n/2\mathbb{Z}_p^n$ is 0 if p is odd and $(\mathbb{Z}/2\mathbb{Z})^n$ if $p = 2$. So $|K^\times/(K^\times)^2| = 4$ for p odd and 2^{n+2} for $p = 2$, and Proposition 2.4.5 finishes the proof. ■

Chapter 3

Zeta Functions of Number Fields

Let K be a number field, that is, K is a finite extension of $\mathbb{Q}$, with $n = [K : \mathbb{Q}]$.

3.1 The norm of an ideal

Definition 3.1.1

For any nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$ we define the *norm* $N(\mathfrak{a}) \in \mathbb{Z}$ to be

$$N(\mathfrak{a}) = \# \mathcal{O}_K / \mathfrak{a}.$$

This is finite: $\mathfrak{a}$ contains some integer $m \neq 0$ (e.g. the norm of a nonzero element of $\mathfrak{a}$), and $|\mathcal{O}_K / m\mathcal{O}_K| = m^n$ since $\mathcal{O}_K \cong \mathbb{Z}^n$.

Lemma 3.1.2

For nonzero ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ we have $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$. In particular $N(\mathfrak{P}) = |k(\mathfrak{P})| = p^{f(\mathfrak{P}|p)}$ and $N(\prod \mathfrak{P}_i^{a_i}) = \prod N(\mathfrak{P}_i)^{a_i}$.

Proof. By unique factorisation it suffices to show $N(\mathfrak{a}\mathfrak{P}) = N(\mathfrak{a})N(\mathfrak{P})$ for a prime $\mathfrak{P}$. We have $|\mathcal{O}_K / \mathfrak{a}\mathfrak{P}| = |\mathcal{O}_K / \mathfrak{a}| \cdot |\mathfrak{a} / \mathfrak{a}\mathfrak{P}|$. The quotient $\mathfrak{a} / \mathfrak{a}\mathfrak{P}$ is a vector space over $\mathcal{O}_K / \mathfrak{P}$; it is nonzero ($\mathfrak{a}\mathfrak{P} \neq \mathfrak{a}$ by unique factorisation), and it has no proper nonzero subspaces: an ideal $\mathfrak{b}$ with $\mathfrak{a}\mathfrak{P} \subsetneq \mathfrak{b} \subsetneq \mathfrak{a}$ would give $\mathfrak{P} \subsetneq \mathfrak{a}^{-1}\mathfrak{b} \subsetneq \mathcal{O}_K$, contradicting maximality of $\mathfrak{P}$. So $\dim_{\mathcal{O}_K / \mathfrak{P}} \mathfrak{a} / \mathfrak{a}\mathfrak{P} = 1$ and $|\mathfrak{a} / \mathfrak{a}\mathfrak{P}| = N(\mathfrak{P})$. ■

Recall that a *fractional ideal* of K is a nonzero finitely generated $\mathcal{O}_K$ -submodule $\mathfrak{a} \subset K$. Choosing $0 \neq d \in \mathbb{Z}$ with $d\mathfrak{a} \subseteq \mathcal{O}_K$ we can write $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2^{-1}$ with integral ideals $\mathfrak{a}_1 = d\mathfrak{a}$ and $\mathfrak{a}_2 = d\mathcal{O}_K$; we also write $\mathfrak{a} = \mathfrak{a}_1 / \mathfrak{a}_2$.

Definition 3.1.3

For any fractional ideal $\mathfrak{a}$ of K we define the norm $N(\mathfrak{a}) \in \mathbb{Q}$ to be

$$N(\mathfrak{a}) = \frac{N(\mathfrak{a}_1)}{N(\mathfrak{a}_2)},$$

where $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq \mathcal{O}_K$ are integral ideals ($\mathfrak{a}_2$ nonzero) such that $\mathfrak{a} = \mathfrak{a}_1 / \mathfrak{a}_2$.

Proposition 3.1.4

This definition is well defined, and N is a homomorphism from the group of fractional ideals to $\mathbb{Q}_{>0}^\times$ extending the norm of integral ideals.

Proof. If $\mathfrak{a}_1\mathfrak{a}_2^{-1} = \mathfrak{b}_1\mathfrak{b}_2^{-1}$ then $\mathfrak{a}_1\mathfrak{b}_2 = \mathfrak{b}_1\mathfrak{a}_2$, so by Lemma 3.1.2 $N(\mathfrak{a}_1)N(\mathfrak{b}_2) = N(\mathfrak{b}_1)N(\mathfrak{a}_2)$, i.e. $N(\mathfrak{a}_1)/N(\mathfrak{a}_2) = N(\mathfrak{b}_1)/N(\mathfrak{b}_2)$. For integral $\mathfrak{a}$ take $\mathfrak{a}_2 = \mathcal{O}_K$. Multiplicativity follows from $(\mathfrak{a}_1\mathfrak{a}_2^{-1})(\mathfrak{b}_1\mathfrak{b}_2^{-1}) = (\mathfrak{a}_1\mathfrak{b}_1)(\mathfrak{a}_2\mathfrak{b}_2)^{-1}$ and Lemma 3.1.2. ■

3.2 The Dedekind zeta function

Definition 3.2.1

We define the *Dedekind zeta function* $\zeta_K(s)$ by the following Dirichlet series:

$$\zeta_K(s) = \sum_{\substack{\mathfrak{a} \subseteq \mathcal{O}_K \\ \mathfrak{a} \neq 0}} \frac{1}{N(\mathfrak{a})^s}, \quad s \in \mathbb{C}, \operatorname{Re}(s) > 1.$$

Notes. The sum runs over all nonzero *integral* ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ (not over fractional ideals), and $N(\mathfrak{a})^s := \exp(s \log N(\mathfrak{a}))$ with the real logarithm of the positive integer $N(\mathfrak{a})$. Since the series converges absolutely for $\operatorname{Re}(s) > 1$ (Proposition 3.2.2), its value does not depend on how the countably many ideals are ordered.

Proposition 3.2.2

This series is absolutely convergent in $\{s \in \mathbb{C} \mid \operatorname{Re}(s) > 1\}$. More precisely, for $\sigma > 1$,

$$\sum_{\mathfrak{a} \neq 0} \frac{1}{N(\mathfrak{a})^\sigma} \leq \zeta(\sigma)^n,$$

and the convergence is uniform on $\operatorname{Re}(s) \geq 1 + \delta$ for every $\delta > 0$; hence ζ_K is holomorphic there.

Proof. Let $\sigma = \operatorname{Re}(s) > 1$; then $|N(\mathfrak{a})^{-s}| = N(\mathfrak{a})^{-\sigma}$, so it suffices to bound the partial sums $S(X) = \sum_{N(\mathfrak{a}) \leq X} N(\mathfrak{a})^{-\sigma}$ of a series with positive terms.

Every prime $\mathfrak{P}$ lies over a unique rational prime p , there are at most n primes over a given p (Proposition 1.1.2), and $N(\mathfrak{P}) = p^f \geq p$. If $N(\mathfrak{a}) \leq X$, then every prime factor $\mathfrak{P}$ of $\mathfrak{a}$ has $N(\mathfrak{P}) \leq N(\mathfrak{a}) \leq X$. Expanding the finite product of geometric series below and using unique factorisation and Lemma 3.1.2, each ideal whose prime factors all have norm $\leq X$ appears exactly once, so

$$S(X) \leq \prod_{N(\mathfrak{P}) \leq X} \left(1 - N(\mathfrak{P})^{-\sigma}\right)^{-1} \leq \prod_{p \leq X} \left(1 - p^{-\sigma}\right)^{-n} \leq \left(\sum_{m \geq 1} m^{-\sigma}\right)^n = \zeta(\sigma)^n < \infty.$$

For $\operatorname{Re}(s) \geq 1 + \delta$ the terms are bounded by $N(\mathfrak{a})^{-1-\delta}$, a convergent series independent of s ; by the Weierstrass M -test the convergence is uniform, and a uniform limit of holomorphic functions is holomorphic. ■

Remark 3.2.3. When $K = \mathbb{Q}$, we have that $\zeta_{\mathbb{Q}}(s)$ coincides with the Riemann zeta function $\zeta(s)$: the nonzero ideals of $\mathbb{Z}$ are $m\mathbb{Z}$ with $m \geq 1$ unique, and $N(m\mathbb{Z}) = m$.

3.3 The Gamma function

Definition 3.3.1

Let $\Gamma(s)$ be the *Gamma function*

$$\Gamma(s) = \int_0^\infty e^{-z} z^{s-1} dz \quad \text{for } \operatorname{Re}(s) > 0.$$

The integral converges absolutely and locally uniformly on $\operatorname{Re}(s) > 0$, so Γ is holomorphic there (here $z^{s-1} = e^{(s-1)\log z}$ with the real logarithm of $z > 0$). We have the following properties of $\Gamma(s)$.

Proposition 3.3.2 (1) $\Gamma(s+1) = s\Gamma(s)$. In particular, for any positive integer n , $\Gamma(n) = (n-1)!$.

(2) $\Gamma(s)$ is meromorphically continued to the whole $\mathbb{C}$ -plane. Its poles are exactly the points $s = -n$ with $n = 0, 1, 2, \dots$; they are simple, and

$$\operatorname{Res}_{s=-n} \Gamma(s) = \frac{(-1)^n}{n!}.$$

(3) $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$. Consequently $\Gamma(s)$ has no zeros, $1/\Gamma(s)$ is an entire function with simple zeros exactly at $0, -1, -2, \dots$, and $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

Correction. My notes say that Γ has a simple pole “at the negative integer n ” with residue $(-1)^n/n!$ at $s = n$, and no zeros nor poles on $\mathbb{C} \setminus \{-1, -2, -3, \dots\}$. The point $s = 0$ is also a pole, and the residue $(-1)^n/n!$ is taken at $s = -n$ for $n \geq 0$.

Proof. (1) Integration by parts gives $\Gamma(s+1) = [-e^{-z}z^s]_0^\infty + s \int_0^\infty e^{-z}z^{s-1} dz = s\Gamma(s)$ for $\operatorname{Re}(s) > 0$, and $\Gamma(1) = \int_0^\infty e^{-z} dz = 1$.

(2) Iterating (1), $\Gamma(s) = \Gamma(s+N+1)/(s(s+1)\cdots(s+N))$ for $\operatorname{Re}(s) > 0$. The right-hand side is meromorphic on $\operatorname{Re}(s) > -N-1$ with simple poles at $0, -1, \dots, -N$, and these continuations agree for different N . At $s = -n$ ($0 \leq n \leq N$) the residue is

$$\frac{\Gamma(N-n+1)}{\prod_{0 \leq j \leq N, j \neq n} (j-n)} = \frac{(N-n)!}{(-1)^n n! (N-n)!} = \frac{(-1)^n}{n!}.$$

(3) For real $0 < s < 1$, Fubini’s theorem and the substitution $y = xt$ give

$$\Gamma(s)\Gamma(1-s) = \int_0^\infty \int_0^\infty e^{-x-y} x^{s-1} y^{-s} dy dx = \int_0^\infty t^{-s} \int_0^\infty e^{-x(1+t)} dx dt = \int_0^\infty \frac{t^{-s}}{1+t} dt.$$

With $t = e^u$ and $a = 1-s \in (0, 1)$ this is $I(a) = \int_{-\infty}^\infty \frac{e^{au}}{1+e^u} du$. Integrate $f(z) = e^{az}/(1+e^z)$ over the boundary of the rectangle $[-T, T] \times [0, 2\pi]$. The only pole inside is $z = \pi i$, with residue $e^{\pi ia}/e^{\pi i} = -e^{\pi ia}$; the vertical sides contribute $O(e^{-aT} + e^{-(1-a)T}) \rightarrow 0$; and the top side contributes $-e^{2\pi ia}I(a)$. Hence $(1 - e^{2\pi ia})I(a) = -2\pi i e^{\pi ia}$, i.e. $I(a) = \pi/\sin(\pi a) = \pi/\sin(\pi s)$. Both sides of the identity are meromorphic on $\mathbb{C}$, so it holds everywhere.

If $\Gamma(s_0) = 0$, then since $\pi/\sin(\pi s_0) \neq 0$, s_0 must be a pole of $\Gamma(1-s)$, i.e. $s_0 \in \{1, 2, 3, \dots\}$; but $\Gamma(n) = (n-1)! \neq 0$. So Γ has no zeros, and the statements about $1/\Gamma$ follow from (2). Finally $\Gamma(\frac{1}{2})^2 = \pi$ and $\Gamma(\frac{1}{2}) > 0$. ■

3.4 Euler product and functional equation

For a number field K we write $r_1(K)$ for the number of real embeddings and $r_2(K)$ for the number of pairs of complex conjugate embeddings, so $[K : \mathbb{Q}] = r_1(K) + 2r_2(K)$. We also have the following properties of $\zeta_K(s)$.

Proposition 3.4.1 (1) $\zeta_K(s)$ has the Euler product expansion

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \subset \mathcal{O}_K \\ \text{prime ideals}}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \quad \text{on } \{s \in \mathbb{C} \mid \operatorname{Re}(s) > 1\};$$

the product converges absolutely, so in particular $\zeta_K(s) \neq 0$ there.

(2) (Hecke) By defining

$$\Lambda_K(s) = A^s \Gamma(s)^{r_2(K)} \Gamma\left(\frac{s}{2}\right)^{r_1(K)} \zeta_K(s), \quad A = |D_K|^{1/2} 2^{-r_2(K)} \pi^{-[K:\mathbb{Q}]/2},$$

we have the functional equation $\Lambda_K(s) = \Lambda_K(1-s)$, and $\zeta_K(s)$ is meromorphically continued to the $\mathbb{C}$ -plane, holomorphic except for a simple pole at $s = 1$.

Correction. In my notes $A = |D_K| 2^{-r_2(K)} \pi^{-[K:\mathbb{Q}]/2}$; the discriminant must enter as $|D_K|^{1/2}$. (With $|D_K|$ the two sides of the functional equation would differ by the factor $|D_K|^{s-1/2}$.)

Notes. “ ζ_K is meromorphically continued to $\mathbb{C}$ ” means: there is a meromorphic function on $\mathbb{C}$ which agrees with the series on $\operatorname{Re}(s) > 1$. By the identity theorem such a continuation is unique, so values like $\zeta_K(0)$ or $\zeta_K(-1)$ are meaningful even though the defining series diverges there.

Proof of (1). Let $\sigma = \operatorname{Re}(s) > 1$. Every factor satisfies $|N(\mathfrak{p})^{-s}| \leq 2^{-\sigma} < 1$, and $\sum_{\mathfrak{p}} |N(\mathfrak{p})^{-s}| \leq [K:\mathbb{Q}] \sum_p p^{-\sigma} < \infty$ (at most $[K:\mathbb{Q}]$ primes lie over each p , and $N(\mathfrak{p}) \geq p$), so the product converges absolutely; as no factor vanishes, neither does the product. For $X > 0$, multiplying out the finitely many absolutely convergent geometric series and using unique factorisation and Lemma 3.1.2,

$$\prod_{N(\mathfrak{p}) \leq X} (1 - N(\mathfrak{p})^{-s})^{-1} = \sum_{\mathfrak{a} \in S_X} N(\mathfrak{a})^{-s},$$

where S_X is the set of nonzero ideals all of whose prime factors have norm $\leq X$. Since S_X contains every $\mathfrak{a}$ with $N(\mathfrak{a}) \leq X$, the difference from $\zeta_K(s)$ is bounded by $\sum_{N(\mathfrak{a}) > X} N(\mathfrak{a})^{-\sigma}$, which tends to 0 by Proposition 3.2.2. ■

Notes. Part (2) was stated without proof in the lecture. A complete proof is given below for $K = \mathbb{Q}$ (Theorem 4.5.2, with $\chi = \mathbf{1}$). For abelian fields it follows from the factorisation of ζ_K into Dirichlet L -functions (Theorem 5.1.1) together with the conductor–discriminant formula [16, Thm. 3.11]. For general K see Hecke’s proof in [11, Ch. VII, §5] or Tate’s thesis. Independently of (2), the next section shows that ζ_K continues to $\operatorname{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ with a simple pole at $s = 1$.

3.5 The analytic class number formula

We fix notation. Let $n = [K:\mathbb{Q}]$, $r_1 = r_1(K)$, $r_2 = r_2(K)$, $h_K = \#\operatorname{Cl}(K)$, and let w_K be the number of roots of unity in K . Let $\sigma_1, \dots, \sigma_{r_1}$ be the real embeddings and $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ representatives of the pairs of complex embeddings, and let

$$j: K \rightarrow K_{\mathbb{R}} := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1+r_2}(\alpha))$$

be the Minkowski embedding. We identify $\mathbb{C} = \mathbb{R}^2$ and give $K_{\mathbb{R}} \cong \mathbb{R}^n$ Lebesgue measure. For $x \in K_{\mathbb{R}}$ put $N(x) = \prod_{k \leq r_1} x_k \prod_{k > r_1} |x_k|^2$, so that $N(j(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$, and on $K_{\mathbb{R}}^{\times} = (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}$ define

$$\ell(x) = (\log |x_1|, \dots, \log |x_{r_1}|, 2 \log |x_{r_1+1}|, \dots, 2 \log |x_{r_1+r_2}|) \in \mathbb{R}^{r_1+r_2},$$

whose coordinates sum to $\log |N(x)|$. By *Dirichlet's unit theorem*, $\mathcal{O}_K^{\times} = \mu(K) \times \langle \varepsilon_1, \dots, \varepsilon_r \rangle$ with $r = r_1 + r_2 - 1$ and the ε_i of infinite order. The *regulator* R_K is the absolute value of any $r \times r$ minor of the $(r+1) \times r$ matrix with columns $\ell(j(\varepsilon_i))$; it does not depend on the deleted row because the columns sum to zero ($R_K = 1$ if $r = 0$).

Notes. The regulator does not depend on the choices made. Another basis of the free part differs by a matrix in $GL_r(\mathbb{Z})$, which changes the minor by ± 1 . Replacing a complex embedding by its conjugate does not change $|\sigma(x)|$. Multiplying the ε_i by roots of unity does not change ℓ . The factor 2 in front of $\log |x_k|$ for complex places is part of the definition: without it the formula of Theorem 3.5.1 would change by a power of 2.

Theorem 3.5.1 (Dirichlet's analytic class number formula)

$\zeta_K(s)$ has a simple pole at $s = 1$, and its residue is given by

$$\lim_{s \rightarrow 1} (s-1) \zeta_K(s) = \frac{2^{r_1(K)} (2\pi)^{r_2(K)}}{w_K |D_K|^{1/2}} \# \text{Cl}(K) R_K,$$

where w_K is the number of roots of unity in K and R_K is the regulator. More precisely, $\zeta_K(s)$ extends meromorphically to $\text{Re}(s) > 1 - \frac{1}{n}$ with only this pole.

The proof uses four auxiliary facts.

Lemma 3.5.2 (Minkowski)

For a nonzero ideal $\mathfrak{b} \subseteq \mathcal{O}_K$, $j(\mathfrak{b})$ is a lattice in $K_{\mathbb{R}}$ of covolume $2^{-r_2} N(\mathfrak{b}) |D_K|^{1/2}$.

This is standard from a first course; see [11, Ch. I, Prop. 5.2].

Lemma 3.5.3 (Lattice points)

Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $Y \subset \mathbb{R}^n$ a bounded set whose boundary is covered by the images of finitely many Lipschitz maps $[0, 1]^{n-1} \rightarrow \mathbb{R}^n$. Then for $t \geq 1$,

$$\#(\Lambda \cap tY) = \frac{\text{vol}(Y)}{\text{covol}(\Lambda)} t^n + O(t^{n-1}).$$

Proof. Let P be a fundamental parallelootope of Λ of diameter d , and tile $\mathbb{R}^n$ by the cells $\lambda + P$. Let I_t be the number of cells contained in tY and B_t the number of cells meeting $\partial(tY) = t \partial Y$. Both $\#(\Lambda \cap tY)$ and $\text{vol}(tY)/\text{covol}(\Lambda)$ lie between I_t and $I_t + B_t$, so they differ by at most B_t . Subdivide $[0, 1]^{n-1}$ into $\lceil t \rceil^{n-1}$ cubes of side $\leq 1/t$. If φ is one of the Lipschitz maps (constant L), each subcube has image under $t\varphi$ of diameter $\leq L\sqrt{n-1}$, which meets a bounded number c of cells. Hence $B_t \leq (\# \text{maps}) \cdot c \cdot \lceil t \rceil^{n-1} = O(t^{n-1})$. ■

Lemma 3.5.4

Let $(a_m)_{m \geq 1}$ be complex numbers with $A(t) = \sum_{m \leq t} a_m = \kappa t + O(t^{1-\delta})$ for some $\kappa \in \mathbb{C}$ and $0 < \delta \leq 1$. Then $\sum_m a_m m^{-s}$ converges for $\text{Re}(s) > 1$, and $\sum_m a_m m^{-s} - \kappa \zeta(s)$ extends holomorphically to $\text{Re}(s) > 1 - \delta$.

Proof. Put $b_m = a_m - \kappa$ and $B(t) = \sum_{m \leq t} b_m = A(t) - \kappa[t] = O(t^{1-\delta})$. By partial summation, $\sum_{m \leq X} b_m m^{-s} = B(X)X^{-s} + s \int_1^X B(t)t^{-s-1} dt$. For $\operatorname{Re}(s) > 1 - \delta$ the first term tends to 0, and the integral converges absolutely and locally uniformly, so $\sum_m b_m m^{-s}$ is holomorphic there. ■

Lemma 3.5.5

$\zeta(s) - \frac{1}{s-1}$ extends holomorphically to $\operatorname{Re}(s) > 0$. In particular $\zeta(s)$ has a simple pole at $s = 1$ with residue 1.

Proof. For $\operatorname{Re}(s) > 1$, $\zeta(s) - \frac{1}{s-1} = \sum_{m \geq 1} \int_m^{m+1} (m^{-s} - x^{-s}) dx$, and $|m^{-s} - x^{-s}| = |s \int_m^x u^{-s-1} du| \leq |s| m^{-\sigma-1}$ for $m \leq x \leq m+1$. So the series converges locally uniformly on $\sigma = \operatorname{Re}(s) > 0$. ■

Proof of Theorem 3.5.1. Step 1: splitting by ideal classes. For an ideal class C put $\zeta_C(s) = \sum_{\mathfrak{a} \in C} N(\mathfrak{a})^{-s}$ (sum over integral $\mathfrak{a}$), so $\zeta_K = \sum_{C \in \operatorname{Cl}(K)} \zeta_C$. We show that

$$\#\{\mathfrak{a} \in C \text{ integral} \mid N(\mathfrak{a}) \leq t\} = \kappa t + O(t^{1-1/n}), \quad \kappa = \frac{2^{r_1} (2\pi)^{r_2} R_K}{w_K |D_K|^{1/2}}. \quad (3.1)$$

Then by Lemmas 3.5.4 and 3.5.5, every $\zeta_C(s) - \frac{\kappa}{s-1}$ is holomorphic on $\operatorname{Re}(s) > 1 - \frac{1}{n}$, and summing over the h_K classes proves the theorem.

Step 2: reduction to counting elements. Fix an integral ideal $\mathfrak{b}$ in the class C^{-1} . For integral $\mathfrak{a} \in C$, the ideal $\mathfrak{a}\mathfrak{b}$ is principal, $\mathfrak{a}\mathfrak{b} = (\alpha)$ with $\alpha \in \mathfrak{b} \setminus \{0\}$, and conversely $(\alpha)\mathfrak{b}^{-1}$ is integral iff $\alpha \in \mathfrak{b}$. As $N(\mathfrak{a}) = |N(\alpha)|/N(\mathfrak{b})$, the left side of (3.1) is the number of $\alpha \in \mathfrak{b} \setminus \{0\}$ modulo units with $|N(\alpha)| \leq tN(\mathfrak{b})$.

Step 3: a fundamental domain. Let $w_0 = (1, \dots, 1, 2, \dots, 2) \in \mathbb{R}^{r+1}$ (r_1 ones and r_2 twos), so the coordinates of w_0 sum to n . Every $u \in \mathbb{R}^{r+1}$ can be written uniquely as $u = \sum_{i=1}^r c_i \ell(j(\varepsilon_i)) + c w_0/n$, with c equal to the sum of the coordinates of u . Let

$$F = \left\{ x \in K_{\mathbb{R}}^{\times} \mid \ell(x) = \sum_i c_i \ell(j(\varepsilon_i)) + c \frac{w_0}{n} \text{ with } 0 \leq c_i < 1 \right\}, \quad F(T) = \{x \in F \mid |N(x)| \leq T\}.$$

Since $\ell(j(\varepsilon)x) = \ell(j(\varepsilon)) + \ell(x)$, every orbit of $\langle \varepsilon_1, \dots, \varepsilon_r \rangle$ on $K_{\mathbb{R}}^{\times}$ meets F exactly once; and $\mu(K)$ acts freely on F (it does not change ℓ , and $\zeta x = x$ forces $\zeta = 1$). So each $\mathcal{O}_K^{\times}$ -orbit in $j(\mathfrak{b} \setminus 0)$ meets F in exactly w_K points. Moreover F is a cone ($\ell(\lambda x) = \ell(x) + (\log \lambda)w_0$ for $\lambda > 0$), hence $F(T) = T^{1/n} F(1)$. Therefore the count in (3.1) equals $\frac{1}{w_K} \#(j(\mathfrak{b}) \cap (tN(\mathfrak{b}))^{1/n} F(1))$.

Step 4: counting. $F(1)$ is bounded (on it $c \leq 0$ and the c_i are bounded, so all $\log |x_k|$ are bounded above), and its boundary is Lipschitz parametrisable [11, Ch. VII, §5]. By Lemmas 3.5.2 and 3.5.3,

$$\#(j(\mathfrak{b}) \cap (tN(\mathfrak{b}))^{1/n} F(1)) = \frac{\operatorname{vol} F(1) \cdot tN(\mathfrak{b})}{2^{-r_2} N(\mathfrak{b}) |D_K|^{1/2}} + O(t^{1-1/n}).$$

Step 5: the volume. Write the real coordinates as $x_k = \pm \rho_k$ and the complex ones as $x_k = \rho_k e^{i\theta_k}$, so the measure is $\prod_{k \leq r_1} d\rho_k \prod_{k > r_1} \rho_k d\rho_k d\theta_k$. The conditions defining $F(1)$ only involve the ρ_k , so the signs and angles contribute $2^{r_1} (2\pi)^{r_2}$. Substituting $u_k = \log \rho_k$ ($k \leq r_1$) and $u_k = 2 \log \rho_k$ ($k > r_1$), we have $d\rho_k = e^{u_k} du_k$ and $\rho_k d\rho_k = \frac{1}{2} e^{u_k} du_k$, hence

$$\operatorname{vol} F(1) = 2^{r_1} (2\pi)^{r_2} 2^{-r_2} \int_S e^{u_1 + \dots + u_{r+1}} du, \quad S = \left\{ \sum_i c_i \ell(j(\varepsilon_i)) + c \frac{w_0}{n} \mid 0 \leq c_i < 1, c \leq 0 \right\}.$$

In the coordinates $(c_1, \dots, c_r, c)$ the exponent is c , and the Jacobian is

$$|\det(\ell(j(\varepsilon_1)), \dots, \ell(j(\varepsilon_r)), w_0/n)| = R_K :$$

replacing one row by the sum of all rows produces the row $(0, \dots, 0, 1)$, and expanding along it leaves an $r \times r$ minor of the unit matrix. Thus $\operatorname{vol} F(1) = 2^{r_1} \pi^{r_2} R_K \int_{-\infty}^0 e^c dc = 2^{r_1} \pi^{r_2} R_K$, and combining Steps 2–5 gives (3.1). ■

Corollary 3.5.6

Assume Proposition 3.4.1(2). Then $\zeta_K(s)$ has a zero of order $r_1(K) + r_2(K) - 1$ at $s = 0$, and the first nonzero coefficient of its Taylor expansion at $s = 0$ is given by $\# \text{Cl}(K)$ and R_K :

$$\zeta_K(s) = -\frac{\# \text{Cl}(K) R_K}{w_K} s^{r_1(K)+r_2(K)-1} + O(s^{r_1(K)+r_2(K)}).$$

Correction. In my notes the order of vanishing was written as $r_2(K)$; it is $r_1(K) + r_2(K) - 1$, the rank of the unit group. (For $K = \mathbb{Q}$: $\zeta(0) = -\frac{1}{2} \neq 0$, and indeed $r_1 + r_2 - 1 = 0$.)

Proof. Let ρ be the residue in Theorem 3.5.1. Near $s = 0$ we have $1 - s$ near 1, so $\Lambda_K(1 - s) = A^{1-s} \Gamma(1 - s)^{r_2} \Gamma(\frac{1-s}{2})^{r_1} \zeta_K(1 - s) \sim A \pi^{r_1/2} \cdot \frac{\rho}{1-s}$, using $\Gamma(1) = 1$ and $\Gamma(\frac{1}{2}) = \sqrt{\pi}$. On the other side, $\Gamma(s) \sim \frac{1}{s}$ and $\Gamma(\frac{s}{2}) \sim \frac{2}{s}$, so $\Lambda_K(s) \sim 2^{r_1} s^{-r_1-r_2} \zeta_K(s)$. The functional equation gives

$$\begin{aligned} \zeta_K(s) &\sim -\frac{A \pi^{r_1/2} \rho}{2^{r_1}} s^{r_1+r_2-1} = -\frac{|D_K|^{1/2} 2^{-r_2} \pi^{-n/2} \pi^{r_1/2}}{2^{r_1}} \cdot \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{w_K |D_K|^{1/2}} s^{r_1+r_2-1} \\ &= -\frac{h_K R_K}{w_K} s^{r_1+r_2-1}, \end{aligned}$$

since $\pi^{-n/2+r_1/2+r_2} = 1$. ■

3.6 Values at negative integers

Further properties of $\zeta_K(s)$ are in the following.

Proposition 3.6.1 (1) For any negative integer n , $\zeta_K(n) \in \mathbb{Q}$.

(2) For any even negative integer n , $\zeta_K(n) = 0$.

(3) For any odd negative integer n , $\zeta_K(n) \neq 0 \iff r_2(K) = 0$.

More precisely, for $m \geq 1$ the order of vanishing of ζ_K at $s = -m$ is $r_1(K) + r_2(K)$ if m is even and $r_2(K)$ if m is odd.

Proof of (2), (3). Assume Proposition 3.4.1(2) and let $m \geq 1$. Then $\Lambda_K(-m) = \Lambda_K(1 + m)$ is finite and nonzero, since Γ has no zeros or poles at $\frac{1+m}{2}, 1 + m$ and $\zeta_K(1 + m) \neq 0$ by the Euler product. On the other hand, by Proposition 3.3.2, $\Gamma(s)$ has a simple pole at $s = -m$, and $\Gamma(\frac{s}{2})$ has a simple pole at $s = -m$ iff m is even. So the Gamma factors of Λ_K have a pole of order $r_2 + r_1 \cdot [m \text{ even}]$ at $-m$, which ζ_K must compensate by a zero of exactly that order. Since $r_1 + r_2 \geq 1$, this gives (2); for odd m the order is r_2 , giving (3). ■

Notes. Statement (1) is the theorem of Siegel and Klingen; for fields with $r_2(K) > 0$ it is trivial by (2) and (3), so its content concerns totally real fields. We prove it for all abelian number fields in Corollary 5.1.2, where $\zeta_K(1 - m)$ is expressed through generalised Bernoulli numbers. For $K = \mathbb{Q}$: $\zeta(1 - m) = -B_m/m$ (Corollary 4.4.5).

Chapter 4

Dirichlet L -functions

Throughout we fix an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$ (and later also an embedding $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$), and regard algebraic numbers as complex numbers when convenient.

4.1 Dirichlet characters

Definition 4.1.1

Let N be a positive integer. A map $\chi : \mathbb{Z} \rightarrow \overline{\mathbb{Q}}$ is called a *Dirichlet character of modulus N* if

- (1) $\chi(ab) = \chi(a)\chi(b)$ for any $a, b \in \mathbb{Z}$;
- (2) if $a \equiv b \pmod{N}$, then $\chi(a) = \chi(b)$;
- (3) $\chi(a) \neq 0 \iff (a, N) = 1$.

Correction. In my notes the definition only says “a map $\chi : \mathbb{Z} \rightarrow \overline{\mathbb{Q}}$ is called a Dirichlet character of modulus N ”, and (1)–(3) appear afterwards as a proposition. Properties (1)–(3) are really part of the definition.

Proposition 4.1.2

We have a bijection

$$\{\text{Dirichlet characters } \chi : \mathbb{Z} \rightarrow \overline{\mathbb{Q}} \text{ of modulus } N\} \longleftrightarrow \{\text{homomorphisms } \chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \overline{\mathbb{Q}}^\times\},$$

where a homomorphism corresponds to $a \mapsto \chi(\bar{a})$ for $(a, N) = 1$ and $a \mapsto 0$ otherwise. In particular the values of χ are 0 or roots of unity, and $\chi(-1) = \pm 1$.

Proof. By (2) and (3), χ induces a map $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \overline{\mathbb{Q}}^\times$, which is a homomorphism by (1); conversely the extension by zero of a homomorphism satisfies (1)–(3) (note that ab is prime to N iff both a and b are). Values on $(\mathbb{Z}/N\mathbb{Z})^\times$ have order dividing $\varphi(N)$, and $\chi(-1)^2 = \chi(1) = 1$. ■

If χ is a Dirichlet character, we have $\chi(-1) = +1$ or $\chi(-1) = -1$. In the first case χ is called an *even* Dirichlet character, in the second an *odd* one.

If χ is a Dirichlet character with modulus N and M is a multiple of N , then χ *induces* a Dirichlet character χ_M of modulus M : $\chi_M(a) = \chi(a)$ if $(a, M) = 1$ and $\chi_M(a) = 0$ otherwise (i.e. χ_M corresponds to $(\mathbb{Z}/M\mathbb{Z})^\times \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \overline{\mathbb{Q}}^\times$). When χ is a Dirichlet character with modulus N , sometimes χ might be induced from another Dirichlet character χ' with modulus N' where $N' \mid N$. If χ is not induced from any Dirichlet character whose modulus is $< N$, then χ is called a *primitive* character.

Proposition 4.1.3

For a Dirichlet character χ of modulus N , there exist a unique $N_0 \mid N$ and a unique primitive

Dirichlet character χ_0 of modulus N_0 such that χ is induced from χ_0 .

This χ_0 is called the *primitive Dirichlet character associated to χ* , and N_0 is called the *conductor* of χ . The *trivial character* $\mathbb{1}$ is the one of conductor 1 ($\mathbb{1}(n) = 1$ for all n); we call χ *nontrivial* if its conductor is > 1 .

Correction. My notes say that χ_0 has modulus N ; it has modulus N_0 .

Notes. Two conventions to keep in mind. (a) In these notes χ_0 always denotes the *primitive* character associated to χ . Many books instead write χ_0 for the *principal* character modulo N , which we denote $\mathbb{1}_N$: $\mathbb{1}_N(a) = 1$ if $(a, N) = 1$ and 0 otherwise. (b) “Trivial” refers to the conductor. $\mathbb{1}_N$ is induced from $\mathbb{1}$, so it counts as trivial, although $\mathbb{1}_N \neq \mathbb{1}$ as functions on $\mathbb{Z}$ when $N > 1$. Their L -functions differ by finitely many Euler factors, see (4.1).

Proof. Say that $d \mid N$ is a *period* of χ if $\chi(a) = 1$ for all a with $(a, N) = 1$ and $a \equiv 1 \pmod{d}$; this means exactly that χ is induced from a character of modulus d (as $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/d\mathbb{Z})^\times$ is surjective with kernel $\{a \equiv 1 \pmod{d}\}$).

Claim: if d_1, d_2 are periods, so is $g = \gcd(d_1, d_2)$. Let $(a, N) = 1$, $a \equiv 1 \pmod{g}$. By the Chinese remainder theorem there is x with $x \equiv 1 \pmod{d_1}$ and $x \equiv a \pmod{d_2}$, unique modulo $\text{lcm}(d_1, d_2)$. Such an x is prime to every prime dividing $d_1 d_2$, and adding a suitable multiple of $\text{lcm}(d_1, d_2)$ we can make it prime to the remaining primes dividing N as well. Then $\chi(x) = 1$, and $ax^{-1} \equiv 1 \pmod{d_2}$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ gives $\chi(a) = \chi(x)\chi(ax^{-1}) = 1$.

Hence there is a smallest period N_0 , dividing all others, and χ is induced from a character χ_0 of modulus N_0 , which is primitive by minimality. If χ is induced from a primitive χ' of modulus N' , then N' is a period, so $N_0 \mid N'$, so χ' is induced from a character of modulus N_0 , and primitivity forces $N' = N_0$. Finally $\chi' = \chi_0$: every a prime to N_0 is congruent mod N_0 to some a' prime to N , and $\chi'(a) = \chi(a') = \chi_0(a)$. ■

4.2 Gauss sums

Definition 4.2.1

Let χ be a Dirichlet character of modulus N and $\zeta_N = e^{2\pi i/N}$. The *Gauss sum* of χ is $G(\chi) = \sum_{a=1}^N \chi(a) \zeta_N^a$.

Notes. $G(\chi)$ depends on the choice of the primitive N -th root of unity: with ζ_N^b instead of ζ_N , $(b, N) = 1$, the sum becomes $\bar{\chi}(b)G(\chi)$. We always take $\zeta_N = e^{2\pi i/N} \in \mathbb{C}$. For $N > 1$ the term $a = N$ vanishes, so this agrees with the sum $\sum_{a=1}^{N-1}$ in my handwritten notes.

Lemma 4.2.2

Let χ be primitive of conductor N . Then

- (i) $\sum_{a=1}^N \chi(a) \zeta_N^{an} = \bar{\chi}(n) G(\chi)$ for every $n \in \mathbb{Z}$;
- (ii) $G(\chi)G(\bar{\chi}) = \chi(-1)N$ and $|G(\chi)|^2 = N$.

Proof. (i) If $(n, N) = 1$, substitute $a \mapsto an^{-1}$. If $d = (n, N) > 1$, put $N' = N/d$; then ζ_N^{an} only depends on $a \pmod{N'}$. Since χ is primitive, N' is not a period (proof of Proposition 4.1.3), so there

is c prime to N with $c \equiv 1 \pmod{N'}$ and $\chi(c) \neq 1$. Since $(c-1)n \equiv 0 \pmod{N}$, substituting $a \mapsto ca$ gives $S = \sum_a \chi(ca) \zeta_N^{can} = \chi(c)S$ for the sum S in question, so $S = 0 = \bar{\chi}(n)G(\chi)$.

(ii) Taking absolute values squared in (i) and summing over $n \pmod{N}$:

$$\varphi(N)|G(\chi)|^2 = \sum_{a,b} \chi(a)\bar{\chi}(b) \sum_n \zeta_N^{(a-b)n} = N\varphi(N),$$

so $|G(\chi)|^2 = N$. Also $\overline{G(\chi)} = \sum_a \bar{\chi}(a) \zeta_N^{-a} = \chi(-1)G(\bar{\chi})$, whence $G(\chi)G(\bar{\chi}) = \chi(-1)|G(\chi)|^2 = \chi(-1)N$. ■

4.3 Dirichlet L -functions

Definition 4.3.1 (Dirichlet series)

Let χ be a Dirichlet character of modulus N . We define

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad s \in \mathbb{C}, \operatorname{Re}(s) > 1.$$

This series is called a *Dirichlet series* (or the Dirichlet L -function of χ). In my notes it is denoted $\zeta(\chi, s)$.

Notes. Here $n^s := e^{s \log n}$ with the real logarithm, and $\chi(n) \in \overline{\mathbb{Q}} \subset \mathbb{C}$ via the fixed embedding. In general, “Dirichlet series” means any series $\sum_n a_n n^{-s}$; the L -function is the special case $a_n = \chi(n)$.

The above series is absolutely convergent on $\operatorname{Re}(s) > 1$, since $|\chi(n)| \leq 1$. If $\chi = \mathbb{1}$ is the trivial Dirichlet character, $\mathbb{1}(n) = 1$ for all n , then $L(\mathbb{1}, s) = \zeta(s)$ is the Riemann zeta function. If χ of modulus N is induced from χ_0 , comparing Euler products (below) gives

$$L(\chi, s) = L(\chi_0, s) \prod_{p|N} (1 - \chi_0(p)p^{-s}). \quad (4.1)$$

We have the following properties of $L(\chi, s)$.

Proposition 4.3.2 (1) $L(\chi, s)$ has the Euler product $L(\chi, s) = \prod_{p \text{ prime}} (1 - \chi(p)p^{-s})^{-1}$ on $\operatorname{Re}(s) > 1$.

(2) $L(\chi, s)$ is meromorphically continued to the $\mathbb{C}$ -plane.

(3) If χ is a nontrivial Dirichlet character (conductor > 1), then $L(\chi, s)$ is holomorphic on the $\mathbb{C}$ -plane, and $L(\chi, 1) \neq 0$.

(4) Let χ be primitive of conductor N_χ and $\delta_\chi = \begin{cases} 1, & \chi \text{ odd,} \\ 0, & \chi \text{ even.} \end{cases}$ Define

$$\Lambda(\chi, s) = \left(\frac{N_\chi}{\pi}\right)^{\frac{s+\delta_\chi}{2}} \Gamma\left(\frac{s+\delta_\chi}{2}\right) L(\chi, s).$$

Then we have the functional equation

$$\Lambda(\chi, s) = W(\chi) \Lambda(\bar{\chi}, 1-s), \quad W(\chi) = \frac{G(\chi)}{i^{\delta_\chi} \sqrt{N_\chi}}, \quad |W(\chi)| = 1.$$

Correction. In my notes the functional equation reads $\Lambda(\chi, s) = w_\chi \Lambda(\chi, 1 - s)$ with $\Lambda(\chi, s) = N_\chi \pi^{-\frac{s+\delta_\chi}{2}} \Gamma(\frac{s+\delta_\chi}{2}) L(\chi, s)$, and w_χ annotated as “the number of roots of unity in K ”. Three corrections: the conductor enters as $N_\chi^{s/2}$ (up to a constant), the right-hand side involves $\bar{\chi}$, and $W(\chi)$ is the *root number* $G(\chi)/(i^{\delta_\chi} \sqrt{N_\chi})$, a complex number of absolute value 1. It has nothing to do with roots of unity in a field. Also χ must be primitive.

Proof of (1). χ is completely multiplicative and $|\chi(p)p^{-s}| < 1$, so the argument of Proposition 3.4.1(1), with unique factorisation in $\mathbb{Z}$, applies verbatim. Formula (4.1) follows since $\chi(p) = \chi_0(p)$ for $p \nmid N$ and $\chi(p) = 0$ for $p \mid N$. ■

Part (2) and the holomorphy in (3) are proved in Theorem 4.4.4, the non-vanishing in Theorem 4.7.2, and (4) in Theorem 4.5.2.

4.4 Generalised Bernoulli numbers and values at negative integers

Lecture of 18 May 2026. The values of $L(\chi, s)$ at integers can be expressed by generalised Bernoulli numbers.

Recall the usual Bernoulli numbers: $\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}$ for $|z| < 2\pi$, so $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, and $B_n = 0$ for odd $n \geq 3$ (because $\frac{z}{e^z - 1} + \frac{z}{2}$ is even).

Definition 4.4.1

Let χ be a Dirichlet character with modulus N . We define the *generalised Bernoulli numbers* $B_{n,\chi} \in \overline{\mathbb{Q}}$ by

$$F_\chi(t) := \sum_{a=1}^N \frac{\chi(a) t e^{at}}{e^{Nt} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!},$$

i.e. $B_{n,\chi}/n!$ is the n -th coefficient of the left-hand side.

Correction. In my notes the denominator is written e^{Nt} instead of $e^{Nt} - 1$, and the sum starts at $n = 1$. Also, the example “for $\chi = \mathbb{1}$, $B_{n,\mathbb{1}} = B_n$ ” needs care: with $N = 1$ we get $F_{\mathbb{1}}(t) = \frac{te^t}{e^t - 1} = \frac{-t}{e^{-t} - 1}$, so $B_{n,\mathbb{1}} = (-1)^n B_n$. This agrees with B_n except for $B_{1,\mathbb{1}} = +\frac{1}{2}$.

Since F_χ has coefficients in $\mathbb{Q}(\chi)$ (the field generated by the values of χ), we have $B_{n,\chi} \in \mathbb{Q}(\chi)$, and $\sigma(B_{n,\chi}) = B_{n,\sigma\chi}$ for $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Two simple facts are used below:

$$B_{0,\chi} = \frac{1}{N} \sum_{a=1}^N \chi(a), \quad B_{1,\chi} = \frac{1}{N} \sum_{a=1}^N \chi(a) a \quad \text{if } \sum_a \chi(a) = 0,$$

obtained from $\frac{te^{at}}{e^{Nt} - 1} = \frac{1}{N} (1 - \frac{Nt}{2} + \cdots)(1 + at + \cdots)$.

Lemma 4.4.2 (Parity)

If $N > 1$, then $B_{n,\chi} = 0$ whenever $\chi(-1) \neq (-1)^n$.

Proof. Substituting $b = N - a$ and using $\chi(N) = 0$, $F_\chi(-t) = \sum_a \chi(a) \frac{t e^{(N-a)t}}{e^{Nt}-1} = \chi(-1) F_\chi(t)$. Compare coefficients. ■

Lemma 4.4.3 (Mellin transforms)

Let $\varphi : (0, \infty) \rightarrow \mathbb{C}$ be smooth with $\varphi(t) = O(e^{-ct})$ as $t \rightarrow \infty$ for some $c > 0$, and suppose $\varphi(t) = \frac{a_{-1}}{t} + g(t)$ where g extends to a C^∞ function on $[0, \infty)$. Then

$$\Phi(s) = \frac{1}{\Gamma(s)} \int_0^\infty \varphi(t) t^{s-1} dt \quad (\operatorname{Re}(s) > 1)$$

extends meromorphically to $\mathbb{C}$, holomorphic except for at most a simple pole at $s = 1$ with residue a_{-1} , and $\Phi(-k) = (-1)^k g^{(k)}(0)$ for all integers $k \geq 0$.

Proof. Split $\int_0^\infty = \int_0^1 + \int_1^\infty$. The second integral is entire in s . Next, $\int_0^1 a_{-1} t^{s-2} dt = \frac{a_{-1}}{s-1}$. For $M \geq 1$ write $g(t) = \sum_{j < M} \frac{g^{(j)}(0)}{j!} t^j + R_M(t)$ with $R_M(t) = O(t^M)$ on $[0, 1]$; then

$$\int_0^1 g(t) t^{s-1} dt = \sum_{j < M} \frac{g^{(j)}(0)}{j! (s+j)} + \int_0^1 R_M(t) t^{s-1} dt,$$

the last term being holomorphic on $\operatorname{Re}(s) > -M$. Multiply by $1/\Gamma(s)$, which is entire with simple zeros at $0, -1, -2, \dots$ (Proposition 3.3.2); near $s = -k$ we have $1/\Gamma(s) = (-1)^k k! (s+k) + O((s+k)^2)$ by the residue computation. So all poles at $s = 0, -1, \dots$ cancel, the only possible pole is at $s = 1$ with residue $a_{-1}/\Gamma(1) = a_{-1}$, and at $s = -k$ only the term $j = k$ survives, giving $(-1)^k k! \cdot \frac{g^{(k)}(0)}{k!}$. ■

Theorem 4.4.4

Let χ be a Dirichlet character of modulus N . Then $L(\chi, s)$ continues meromorphically to $\mathbb{C}$. It is holomorphic except for a simple pole at $s = 1$ with residue $B_{0,\chi}$, which is $\varphi(N)/N$ if χ is induced from $\mathbb{1}$ and 0 otherwise. Moreover

$$L(\chi, 1-n) = -\frac{B_{n,\chi}}{n} \quad \text{for all integers } n \geq 1.$$

In particular $L(\chi, 1-n) \in \mathbb{Q}(\chi)$, and for $N > 1$ it vanishes unless $\chi(-1) = (-1)^n$.

Proof. For $\operatorname{Re}(s) > 1$, using $\int_0^\infty e^{-nt} t^{s-1} dt = \Gamma(s) n^{-s}$ and absolute convergence,

$$\Gamma(s) L(\chi, s) = \int_0^\infty \varphi_\chi(t) t^{s-1} dt, \quad \varphi_\chi(t) = \sum_{n \geq 1} \chi(n) e^{-nt} = \sum_{a=1}^N \frac{\chi(a) e^{-at}}{1 - e^{-Nt}}.$$

Now $t \varphi_\chi(t) = \sum_a \chi(a) \frac{(-t) e^{a(-t)}}{e^{N(-t)} - 1} = F_\chi(-t)$, so

$$\varphi_\chi(t) = \frac{B_{0,\chi}}{t} + g(t), \quad g(t) = \sum_{n \geq 1} (-1)^n B_{n,\chi} \frac{t^{n-1}}{n!}, \quad g^{(k)}(0) = \frac{(-1)^{k+1} B_{k+1,\chi}}{k+1}.$$

Lemma 4.4.3 gives the continuation, the pole and $L(\chi, -k) = (-1)^k \cdot \frac{(-1)^{k+1} B_{k+1,\chi}}{k+1} = -\frac{B_{k+1,\chi}}{k+1}$. The last assertion is Lemma 4.4.2. ■

Corollary 4.4.5

$\zeta(0) = -\frac{1}{2}$ and $\zeta(1-n) = -\frac{B_n}{n}$ for $n \geq 2$. In particular $\zeta(1-n) = 0$ for odd $n \geq 3$ and $\zeta(1-n) \in \mathbb{Q}^\times$ for even $n \geq 2$.

Proof. Take $\chi = \mathbb{1}$ ($N = 1$): $\zeta(1-n) = -B_{n,\mathbb{1}}/n = -(-1)^n B_n/n$, and $B_n = 0$ for odd $n \geq 3$, while $B_{1,\mathbb{1}} = \frac{1}{2}$. For even n , $B_n \neq 0$ by Corollary 4.6.1 below. ■

4.5 The functional equation

We use the Poisson summation formula $\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n)$ for Schwartz functions, where $\hat{f}(y) = \int_{\mathbb{R}} f(x) e^{-2\pi i x y} dx$, and the Fourier transforms

$$\widehat{e^{-\pi u x^2}}(y) = u^{-1/2} e^{-\pi y^2/u}, \quad \widehat{x e^{-\pi u x^2}}(y) = -i y u^{-3/2} e^{-\pi y^2/u} \quad (u > 0),$$

the second obtained by differentiating the first in y .

Lemma 4.5.1 (Theta transformation)

Let χ be primitive of conductor N and $\delta = \delta_\chi$. Put $\theta(\chi, t) = \sum_{n \in \mathbb{Z}} \chi(n) n^\delta e^{-\pi n^2 t/N}$ for $t > 0$. Then

$$\theta(\chi, 1/t) = W(\chi) t^{\delta + \frac{1}{2}} \theta(\bar{\chi}, t).$$

Proof. By Lemma 4.2.2(i) applied to $\bar{\chi}$, $\chi(n) = G(\bar{\chi})^{-1} \sum_{a=1}^N \bar{\chi}(a) e^{2\pi i a n/N}$ for all n . Apply Poisson summation to $f_a(x) = x^\delta e^{-\pi x^2 t/N} e^{2\pi i a x/N}$, i.e. to the Gaussian with $u = t/N$ shifted by a/N in frequency. For $\delta = 0$ we get $\sum_n f_a(n) = (N/t)^{1/2} \sum_{y \in \mathbb{Z}} e^{-\pi(Ny-a)^2/(Nt)}$. Multiplying by $\bar{\chi}(a)$, summing over a and writing $m = Ny - a$ (so $\bar{\chi}(a) = \bar{\chi}(-m)$), we find

$$\theta(\chi, t) = \frac{\chi(-1)}{G(\bar{\chi})} \left(\frac{N}{t}\right)^{1/2} \theta(\bar{\chi}, 1/t) = \frac{G(\chi)}{\sqrt{N}} t^{-1/2} \theta(\bar{\chi}, 1/t),$$

using $\chi(-1)/G(\bar{\chi}) = G(\chi)/N$ (Lemma 4.2.2(ii)). For $\delta = 1$ the same computation with the second Fourier transform gives $\theta(\chi, t) = \frac{-i\chi(-1)}{G(\bar{\chi})} N^{1/2} t^{-3/2} \theta(\bar{\chi}, 1/t) = \frac{G(\chi)}{i\sqrt{N}} t^{-3/2} \theta(\bar{\chi}, 1/t)$, since $\chi(-1) = -1$. In both cases $\theta(\chi, t) = W(\chi) t^{-\delta - \frac{1}{2}} \theta(\bar{\chi}, 1/t)$; now replace t by $1/t$. ■

Theorem 4.5.2

Proposition 4.3.2(4) holds. For $\chi = \mathbb{1}$ it reads: the function $\Lambda(s) = \pi^{-s/2} \Gamma(\frac{s}{2}) \zeta(s)$ satisfies $\Lambda(s) = \Lambda(1-s)$, and it is holomorphic except for simple poles at $s = 0, 1$.

Proof. Case $N > 1$. Then $\chi(0) = 0$ and $\chi(-n)(-n)^\delta = \chi(n)n^\delta$, so $\theta(\chi, t) = 2 \sum_{n \geq 1} \chi(n) n^\delta e^{-\pi n^2 t/N}$ decays exponentially as $t \rightarrow \infty$. Since $\int_0^\infty e^{-\pi n^2 t/N} t^{\frac{s+\delta}{2}} \frac{dt}{t} = (N/\pi)^{\frac{s+\delta}{2}} n^{-s-\delta} \Gamma(\frac{s+\delta}{2})$, we get for $\text{Re}(s) > 1$

$$2\Lambda(\chi, s) = \int_0^\infty \theta(\chi, t) t^{\frac{s+\delta}{2}} \frac{dt}{t} = \int_1^\infty \theta(\chi, t) t^{\frac{s+\delta}{2}} \frac{dt}{t} + W(\chi) \int_1^\infty \theta(\bar{\chi}, t) t^{\frac{1-s+\delta}{2}} \frac{dt}{t},$$

where we substituted $t \mapsto 1/t$ in $\int_0^1$ and used Lemma 4.5.1. The right-hand side is entire. Doing the same for $\bar{\chi}$ at $1-s$ and using $W(\chi)W(\bar{\chi}) = \frac{G(\chi)G(\bar{\chi})}{(-1)^\delta N} = 1$ (Lemma 4.2.2(ii)) gives $W(\chi)\Lambda(\bar{\chi}, 1-s) = \Lambda(\chi, s)$. Finally $|W(\chi)| = |G(\chi)|/\sqrt{N} = 1$.

Case $\chi = \mathbb{1}$. Here $\theta(t) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 t} = 1 + 2\omega(t)$ satisfies $\theta(1/t) = t^{1/2}\theta(t)$ (the same Poisson computation with $N = 1$). Hence $\omega(1/t) = t^{1/2}\omega(t) + \frac{t^{1/2}-1}{2}$, and for $\operatorname{Re}(s) > 1$

$$\Lambda(s) = \int_0^\infty \omega(t) t^{s/2} \frac{dt}{t} = \int_1^\infty \omega(t) (t^{s/2} + t^{(1-s)/2}) \frac{dt}{t} - \frac{1}{s} - \frac{1}{1-s},$$

because $\int_1^\infty \frac{t^{1/2}-1}{2} t^{-s/2} \frac{dt}{t} = \frac{1}{s-1} - \frac{1}{s}$. The right-hand side is meromorphic on $\mathbb{C}$ with simple poles at 0, 1 and symmetric under $s \leftrightarrow 1-s$. ■

4.6 Special values at $s = 1$ and at even positive integers

Corollary 4.6.1 (Euler)

For any even positive integer n ,

$$\zeta(n) = (-1)^{\frac{n}{2}-1} \frac{B_n}{2 \cdot n!} (2\pi)^n = -\frac{B_n}{2n!} (2\pi i)^n.$$

By the functional equation this is equivalent to $\zeta(1-n) = -B_n/n$. In particular $B_n \neq 0$, and $(-1)^{n/2-1} B_n > 0$.

Proof. Write $n = 2m$. Theorem 4.5.2 with $s = n$ gives $\zeta(n) = \pi^{n-\frac{1}{2}} \frac{\Gamma(\frac{1}{2}-m)}{\Gamma(m)} \zeta(1-n)$. From Proposition 3.3.2, $\Gamma(m) = (m-1)!$ and $\Gamma(\frac{1}{2}-m) = \frac{(-4)^m m!}{(2m)!} \sqrt{\pi}$ (induction using $\Gamma(s) = \Gamma(s+1)/s$). With $\zeta(1-n) = -B_n/n$ (Theorem 4.4.4):

$$\zeta(n) = \pi^{2m} \frac{(-4)^m m!}{(2m)! (m-1)!} \cdot \frac{-B_{2m}}{2m} = -\frac{(-4\pi^2)^m B_{2m}}{2(2m)!} = -\frac{(2\pi i)^n B_n}{2n!}.$$

Since $\zeta(n) > 0$, $B_n \neq 0$ and has sign $(-1)^{m-1}$. ■

Recall that if the conductor of χ is nontrivial, then $L(\chi, s)$ is holomorphic at $s = 1$ (Theorem 4.4.4), and $L(\chi, 1) \neq 0$ (Theorem 4.7.2 below).

Proposition 4.6.2

Let χ be a primitive Dirichlet character whose conductor N is nontrivial. Then

$$L(\chi, 1) = \begin{cases} \frac{\pi \sqrt{-1} G(\chi)}{N} B_{1, \chi^{-1}}, & \chi \text{ odd,} \\ -\frac{G(\chi)}{N} \sum_{a=1}^N \chi^{-1}(a) \log|1 - \zeta_N^a|, & \chi \text{ even,} \end{cases}$$

where $G(\chi) = \sum_{a=1}^N \chi(a) \zeta_N^a$ is the Gauss sum and $\chi^{-1} = \bar{\chi}$.

Proof. Since χ is nontrivial, the partial sums $\sum_{n \leq X} \chi(n)$ are bounded, so by partial summation the series $\sum \chi(n) n^{-s}$ converges locally uniformly on $\operatorname{Re}(s) > 0$ and equals $L(\chi, s)$ there; in particular $L(\chi, 1) = \sum_{n \geq 1} \chi(n)/n$. By Lemma 4.2.2(i) for $\bar{\chi}$, $\chi(n) = G(\bar{\chi})^{-1} \sum_a \bar{\chi}(a) \zeta_N^{an}$, so

$$L(\chi, 1) = \frac{1}{G(\bar{\chi})} \sum_{a=1}^{N-1} \bar{\chi}(a) \sum_{n \geq 1} \frac{\zeta_N^{an}}{n} = -\frac{\chi(-1) G(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log(1 - \zeta_N^a),$$

using $\sum_{n \geq 1} z^n/n = -\log(1-z)$ for $|z| = 1$, $z \neq 1$ (principal branch; Abel's theorem) and $1/G(\bar{\chi}) = \chi(-1)G(\chi)/N$. For $0 < a < N$, $1 - \zeta_N^a = 2 \sin(\frac{\pi a}{N})e^{i(\frac{\pi a}{N} - \frac{\pi}{2})}$, so $\log(1 - \zeta_N^a) = \log|1 - \zeta_N^a| + \pi i(\frac{a}{N} - \frac{1}{2})$.

If χ is even, the pairing $a \leftrightarrow N - a$ shows $\sum_a \bar{\chi}(a)(\frac{a}{N} - \frac{1}{2}) = 0$, which leaves the stated formula. If χ is odd, the same pairing shows $\sum_a \bar{\chi}(a) \log|1 - \zeta_N^a| = 0$; also $\sum_a \bar{\chi}(a) = 0$, so $L(\chi, 1) = -\frac{(-1)^{G(\chi)}}{N} \pi i \sum_a \bar{\chi}(a) \frac{a}{N} = \frac{\pi i G(\chi)}{N} B_{1, \bar{\chi}}$. ■

4.7 Non-vanishing of $L(\chi, 1)$

Lemma 4.7.1 (Landau)

Let $D(s) = \sum_{m \geq 1} a_m m^{-s}$ with $a_m \geq 0$, and let $\sigma_c \in \mathbb{R}$ be its abscissa of convergence. Then D does not extend holomorphically to any neighbourhood of $s = \sigma_c$.

Proof. Suppose D extends holomorphically to a disc around σ_c . Then it is holomorphic on a disc $|s - \sigma_1| < 1 + \varepsilon$ with $\sigma_1 = \sigma_c + 1$ (for ε small, the part of this disc with $\operatorname{Re}(s) \leq \sigma_c$ lies in a small neighbourhood of σ_c). Its Taylor series at σ_1 therefore converges at $\sigma = \sigma_c - \frac{\varepsilon}{2}$. Since $D^{(k)}(\sigma_1) = \sum_m a_m (-\log m)^k m^{-\sigma_1}$,

$$D(\sigma) = \sum_{k \geq 0} \frac{(\sigma_1 - \sigma)^k}{k!} \sum_m a_m (\log m)^k m^{-\sigma_1} = \sum_m a_m m^{-\sigma_1} e^{(\sigma_1 - \sigma) \log m} = \sum_m a_m m^{-\sigma},$$

where the interchange is allowed because all terms are ≥ 0 . So the Dirichlet series converges at $\sigma < \sigma_c$, a contradiction. ■

Theorem 4.7.2

If χ is a nontrivial Dirichlet character, then $L(\chi, 1) \neq 0$.

Proof. By (4.1) we may assume χ is a character of modulus N (not necessarily primitive), and it suffices to show $L(\chi, 1) \neq 0$ for all nontrivial characters mod N . Let $F(s) = \prod_{\chi \bmod N} L(\chi, s)$, the product over all $\varphi(N)$ characters of modulus N . For $p \nmid N$ let f_p be the order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$. As χ runs over the characters of the finite abelian group $(\mathbb{Z}/N\mathbb{Z})^\times$, $\chi(p)$ runs over the f_p -th roots of unity, each exactly $\varphi(N)/f_p$ times. Hence

$$F(s) = \prod_{p \nmid N} (1 - p^{-f_p s})^{-\varphi(N)/f_p} \quad (\operatorname{Re}(s) > 1),$$

a Dirichlet series with non-negative coefficients. Since $f_p \mid \varphi(N)$, its coefficients dominate those of $\sum_{(m, N)=1} m^{-\varphi(N)s}$, which diverges at $s = 1/\varphi(N)$.

If $L(\chi, 1) = 0$ for some $\chi \neq \mathbf{1}_N$, this zero cancels the simple pole of $L(\mathbf{1}_N, s)$ at $s = 1$, and F is entire by Theorem 4.4.4. The Dirichlet series of F converges (to F) on $\operatorname{Re}(s) > \sigma_c$, and $\sigma_c \geq 1/\varphi(N)$ is finite. This contradicts Lemma 4.7.1. ■

Chapter 5

Class Numbers of Cyclotomic and Quadratic Fields

5.1 Zeta functions of abelian fields

Recall that $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, $\sigma_a(\zeta_N) = \zeta_N^a$ (Theorem 1.3.5). Hence every subfield $K \subseteq \mathbb{Q}(\zeta_N)$ corresponds to a subgroup $H_K = \text{Gal}(\mathbb{Q}(\zeta_N)/K)$, and we let $X(K)$ be the group of Dirichlet characters of modulus N which are trivial on H_K ; it is identified with the character group of $\text{Gal}(K/\mathbb{Q})$. For $\chi \in X(K)$ we write χ_0 for the associated primitive character.

Theorem 5.1.1

For every subfield $K \subseteq \mathbb{Q}(\zeta_N)$,

$$\zeta_K(s) = \prod_{\chi \in X(K)} L(\chi_0, s).$$

In particular, it is known that $\zeta_{\mathbb{Q}(\zeta_N)}(s) = \prod_{\chi} L(\chi_0, s)$, the product over all Dirichlet characters χ of modulus N .

Correction. In the lecture the formula was written $\zeta_{\mathbb{Q}(\zeta_N)}(s) = \prod_{\chi} \zeta(\chi, s)$ over characters of modulus N . This is true only if each L -function is replaced by that of the associated *primitive* character; with imprimitive characters, Euler factors at primes dividing N are lost.

Proof. Both sides are Euler products, so we compare the factors at a prime p . Write $N = p^k M$ with $p \nmid M$, $G = \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^\times$, and fix a prime $\mathfrak{P}$ of $\mathbb{Q}(\zeta_N)$ above p with decomposition and inertia groups $D \supseteq I$.

(a) $I = \{a \in G \mid a \equiv 1 \pmod{M}\}$ and D/I is generated by the class of p in $G/I = (\mathbb{Z}/M\mathbb{Z})^\times$. The field $\mathbb{Q}(\zeta_M)$ is unramified at p (Theorem 1.3.11), so $I \subseteq \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_M))$, which is the subgroup $\{a \equiv 1 \pmod{M}\}$ of order $\varphi(p^k)$. Conversely $|I| = e(\mathfrak{P}|p) \geq \varphi(p^k)$, because p is totally ramified in $\mathbb{Q}(\zeta_{p^k}) \subseteq \mathbb{Q}(\zeta_N)$ (Proposition 1.3.7). Hence equality. $D/I \subseteq G/I = \text{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ is generated by the Frobenius, which on $\mathbb{Q}(\zeta_M)$ is σ_p , as $\sigma_p(\sum c_i \zeta_M^i) = \sum c_i \zeta_M^{p^i} \equiv (\sum c_i \zeta_M^i)^p \pmod{p}$.

(b) *Passage to K .* Let $H = H_K$, $G_K = G/H$, $\mathfrak{p} = \mathfrak{P} \cap K$. The decomposition and inertia groups of $\mathfrak{p}$ in $K/\mathbb{Q}$ are $D_K = DH/H$ and $I_K = IH/H$. Indeed, an element of G_K fixing $\mathfrak{p}$ lifts to $g \in G$ with $g\mathfrak{P}$ above $\mathfrak{p}$; by transitivity of H on the primes above $\mathfrak{p}$ (Proposition 1.5.2), some hg fixes $\mathfrak{P}$. If moreover it acts trivially on $k(\mathfrak{p})$, then $\bar{g} \in \text{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, which is the image of $D \cap H$ by Proposition 1.5.3, so adjusting by an element of $D \cap H$ we land in I . With $e_K = |I_K|$, $f_K = |D_K/I_K|$, $r_K = [G_K : D_K]$, the Euler factor of ζ_K at p is $(1 - p^{-f_K s})^{-r_K}$ (Proposition 1.5.5).

(c) *The L -side.* Let $\chi \in X(K)$. Then $\chi_0(p) \neq 0$ iff the conductor of χ is prime to p , iff χ factors through $(\mathbb{Z}/M\mathbb{Z})^\times$, iff χ is trivial on I (equivalently on I_K). In that case $\chi_0(p) = \chi(\tilde{p})$ for any $\tilde{p} \in G$ with $\tilde{p} \equiv p \pmod{M}$, i.e. $\chi_0(p) = \chi(\text{Frob}_p)$ with $\text{Frob}_p \in G_K/I_K$ of order f_K . Thus the factor at p of the right-hand side is $\prod_{\psi} (1 - \psi(\text{Frob}_p) p^{-s})^{-1}$ over the characters ψ of G_K/I_K , and as $\psi(\text{Frob}_p)$ runs over the f_K -th roots of unity, each $|G_K/I_K|/f_K = r_K$ times, this equals $(1 - p^{-f_K s})^{-r_K}$. ■

Corollary 5.1.2

Let $K \subseteq \mathbb{Q}(\zeta_N)$. Then $\zeta_K(s)$ continues meromorphically to $\mathbb{C}$, and for every integer $n \geq 1$

$$\zeta_K(1-n) = \prod_{\chi \in X(K)} \left(-\frac{B_{n,\chi_0}}{n} \right) \in \mathbb{Q}.$$

Proof. The first statement and the formula follow from Theorems 5.1.1 and 4.4.4. For $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\chi \mapsto \sigma \circ \chi$ permutes $X(K)$ and $\sigma(B_{n,\chi_0}) = B_{n,(\sigma \circ \chi)_0}$, so the product is fixed by every σ , hence rational. ■

Comparing residues at $s = 1$ (Theorem 3.5.1) with Theorem 5.1.1, and using $\lim_{s \rightarrow 1} (s-1)\zeta(s) = 1$, we get

$$\frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |D_K|^{1/2}} = \prod_{\chi \in X(K), \chi \neq 1} L(1, \chi_0) \quad (5.1)$$

($L(1, \chi_0)$ is our $L(\chi_0, 1)$). Combined with Proposition 4.6.2, this gives us a more explicit class number formula.

5.2 The class number formula for $\mathbb{Q}(\zeta_p)$

Let p be an odd prime. Fix embeddings $\overline{\mathbb{Q}} \subset \mathbb{C}$ and $\iota_p : \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$.

Definition 5.2.1 (Teichmüller character)

The *Teichmüller character* is the Dirichlet character ω of modulus p such that $\iota_p(\omega(a)) \in \mathbb{Z}_p$ is the unique $(p-1)$ -st root of unity congruent to a modulo p (Lemma 2.4.2), for $p \nmid a$.

Notes. (1) ω is defined on $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, and it is injective there, so it has order $p-1$. (2) Hence $\omega^0 = 1, \omega^1, \omega^2, \dots, \omega^{p-2}$ give the set of all Dirichlet characters modulo p . Every ω^i with $i \not\equiv 0$ is primitive of conductor p , and ω^i is odd iff i is odd, since $\omega(-1) = -1$.

Theorem 5.2.2

Let $p \neq 2$ be a prime and $K = \mathbb{Q}(\zeta_p)$. Then $r_1(K) = 0$, $r_2(K) = \frac{p-1}{2}$, $w_K = 2p$, $|D_K| = p^{p-2}$, and

$$\begin{aligned} \frac{2^{r_1(K)}(2\pi)^{r_2(K)}}{w_K |D_K|^{1/2}} \# \text{Cl}(K) R_K &= \frac{(\pi\sqrt{-1})^{\frac{p-1}{2}}}{p^{p-2}} \left(\prod_{i=1}^{p-2} G(\omega^i) \right) (-1)^{\frac{p-3}{2}} \\ &\quad \times \prod_{i \text{ odd}} B_{1,\omega^{-i}} \prod_{\substack{i \text{ even} \\ i \neq 0}} \left(\sum_{a=1}^{p-1} \omega^{-i}(a) \log |1 - \zeta_p^a| \right), \end{aligned}$$

where i runs over $1 \leq i \leq p-2$, and $|\prod_i G(\omega^i)| = p^{\frac{p-2}{2}}$. In particular, up to a complex number of absolute value 1, the right-hand side equals

$$\frac{(\pi\sqrt{-1})^{\frac{p-1}{2}}}{p^{p-2}} p^{\frac{p-2}{2}} \prod_{i \text{ odd}} B_{1,\omega^{-i}} \prod_{\substack{i \text{ even} \neq 0}} \left(\sum_{a=1}^{p-1} \omega^{-i}(a) \log |1 - \zeta_p^a| \right),$$

which is the form given in the lecture.

Correction. Three slips in my notes: (i) the left-hand side has $|D_K|^{1/2}$, not $|D_K|$; (ii) the parities are swapped: $B_{1,\omega^{-i}}$ occurs for *odd* i (by Lemma 4.4.2, $B_{1,\chi} = 0$ for even χ), and the logarithmic sums for *even* $i \neq 0$; (iii) as corrected in red in my notes, $w_K = 2p$ (the roots of unity in $\mathbb{Q}(\zeta_p)$ are $\pm\zeta_p^k$). The lecture formula holds up to the unimodular factor $(-1)^{\frac{p-3}{2}} \prod_i G(\omega^i) / p^{\frac{p-2}{2}}$.

Proof. K is totally imaginary of degree $p-1$. Its roots of unity form μ_{2p} : if $\zeta_m \in K$, then $\mathbb{Q}(\zeta_m) \subseteq K$ is unramified outside p and has degree $\leq p-1$, which forces $m \mid 2p$ (Theorem 1.3.11). Finally $|D_K| = p^{p-2}$ by Proposition 1.3.7. By (5.1) the left side equals $\prod_{i=1}^{p-2} L(1, \omega^i)$. By Proposition 4.6.2, $L(1, \omega^i) = \frac{\pi i G(\omega^i)}{p} B_{1,\omega^{-i}}$ for odd i (there are $\frac{p-1}{2}$ of them) and $L(1, \omega^i) = -\frac{G(\omega^i)}{p} \sum_a \omega^{-i}(a) \log |1 - \zeta_p^a|$ for even $i \neq 0$ (there are $\frac{p-3}{2}$). Multiplying gives the formula, and $|G(\omega^i)| = \sqrt{p}$ by Lemma 4.2.2. ■

5.3 Kummer's criterion

Let $K = \mathbb{Q}(\zeta_p)$ and $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ its maximal real subfield. One has $h_{K^+} \mid h_K$ [16, Thm. 4.14], and $h_K^- := h_K / h_{K^+}$ is called the *relative class number*.

Theorem 5.3.1 (Relative class number formula)

$$h_K^- = 2p \prod_{i \text{ odd}} \left(-\frac{1}{2} B_{1,\omega^{-i}} \right), \text{ the product over odd } i \text{ with } 1 \leq i \leq p-2.$$

Proof sketch. Apply (5.1) to K and to K^+ (which has $r_1 = \frac{p-1}{2}$, $w = 2$, $|D_{K^+}| = p^{\frac{p-3}{2}}$ and $X(K^+) = \{\omega^i : i \text{ even}\}$) and divide: the quotient of the left sides involves R_K / R_{K^+} , which equals $2^{\frac{p-3}{2}}$ [16, Prop. 4.16], and the quotient of the right sides is $\prod_{i \text{ odd}} L(1, \omega^i)$. Inserting Proposition 4.6.2 and $|\prod_{i \text{ odd}} G(\omega^i)| = p^{\frac{p-1}{4}}$ gives $h_K^- = 2p \prod_{i \text{ odd}} |\frac{1}{2} B_{1,\omega^{-i}}|$. The sign is fixed by a separate argument [16, Thm. 4.17]. ■

From now on we regard the values of ω as elements of $\mathbb{Z}_p$ via ι_p , so that $B_{1,\omega^{-i}} = \frac{1}{p} \sum_{a=1}^{p-1} \omega^{-i}(a) a \in \mathbb{Q}_p$.

Notes. Since ω takes values in μ_{p-1} , its values can be read in $\mathbb{C}$ (for L -values and Gauss sums) and in $\mathbb{Z}_p$ (for congruences), compatibly via the fixed embeddings $\overline{\mathbb{Q}} \subset \mathbb{C}$ and $\iota_p : \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$. For $x \in \mathbb{Q}(\mu_{p-1})$ we write “ $p \mid x$ ” if $\iota_p(x) \in p\mathbb{Z}_p$. For a p -integral rational number such as B_m ($m \leq p-3$) this means that p divides its numerator. Individual values depend on ι_p , but ω itself was defined through ι_p , so all statements are consistent.

Corollary 5.3.2

$p \mid h_K^- \iff p \mid \prod B_{1,\omega^{-i}}$ (in $\mathbb{Z}_p$), the product over odd i with $3 \leq i \leq p-2$. (Recall: ω^i is odd $\iff i$ is odd.)

Correction. My notes write “ $p \mid \# \text{Cl}(\mathbb{Q}(\zeta_p)) \iff p \mid \prod_{i \text{ even}} B_{1,\omega^{-i}}$ ”. The product is over *odd* i , excluding $i = 1$. Also the precise statement is about h^- ; that $p \mid h \iff p \mid h^-$ is a further theorem of Kummer (see below).

Proof. Write $a = \omega(a)\langle a \rangle$ with $\langle a \rangle \in 1 + p\mathbb{Z}_p$ (Theorem 2.4.1). For $i = 1$: $pB_{1,\omega^{-1}} = \sum_a \langle a \rangle \equiv p - 1 \equiv -1 \pmod{p}$, so $-pB_{1,\omega^{-1}}$ is a unit. For odd $i \geq 3$: $pB_{1,\omega^{-i}} \equiv \sum_a \omega^{1-i}(a) = 0 \pmod{p}$, since $\omega^{1-i} \neq 1$; so $B_{1,\omega^{-i}} \in \mathbb{Z}_p$. Hence $h_K^- = (-pB_{1,\omega^{-1}}) \cdot \prod_{i \geq 3} (-\frac{1}{2}B_{1,\omega^{-i}})$ is a unit times the product in question. ■

By the definition of B_{n,ω^i} , we have the following lemma.

Lemma 5.3.3

For odd i with $3 \leq i \leq p - 2$, put $m = p - i$ (even, $2 \leq m \leq p - 3$). Then

$$B_{1,\omega^{-i}} \equiv \frac{B_m}{m} \pmod{p}.$$

Correction. My notes have $B_{1,\omega^{-i}} \equiv B_{p-1-i} \pmod{p}$. For odd i the index $p - 1 - i$ is odd, and then $B_{p-1-i} = 0$. The correct index is $p - i$, and there is a factor $1/(p - i)$.

Proof. Note $\omega^{-i} = \omega^{m-1}$ since $\omega^{p-1} = 1$, and $\omega^{m-1}(a)a = \omega^m(a)\langle a \rangle$. Write $\langle a \rangle = 1 + x_a$ with $x_a \in p\mathbb{Z}_p$. Since $m \not\equiv 0 \pmod{p-1}$, $\sum_a \omega^m(a) = 0$, and therefore

$$pB_{1,\omega^{m-1}} = \sum_{a=1}^{p-1} \omega^m(a)(1 + x_a) = \sum_a \omega^m(a)x_a,$$

$$\sum_{a=1}^{p-1} a^m = \sum_a \omega^m(a)(1 + x_a)^m \equiv m \sum_a \omega^m(a)x_a \pmod{p^2}.$$

On the other hand, Faulhaber's formula $\sum_{a=0}^{p-1} a^m = \frac{1}{m+1} \sum_{j=0}^m \binom{m+1}{j} B_j p^{m+1-j}$ together with the von Staudt–Clausen theorem ($pB_j \in \mathbb{Z}_p$ for all j , [16, Thm. 5.10]) gives $\sum_{a=1}^{p-1} a^m \equiv pB_m \pmod{p^2}$ (the term $j = m$ is pB_m ; the term $j = m - 1$ is 0 or p^2B_1 ; the others are divisible by p^2 because $m + 1 < p$). Hence $pB_{1,\omega^{m-1}} \equiv pB_m/m \pmod{p^2}$. ■

Hence, we have:

Theorem 5.3.4 (Kummer)

Let p be an odd prime. Then $p \mid \# \text{Cl}(\mathbb{Q}(\zeta_p))$ if and only if one of $B_2, B_4, \dots, B_{p-3}$ is divisible by p (i.e. p divides its numerator).

Correction. My notes list $B_1, B_3, B_5, \dots, B_{p-1}$. The odd-index Bernoulli numbers $B_3, B_5, \dots$ vanish. The correct list is the even-index numbers $B_2, B_4, \dots, B_{p-3}$ (B_{p-1} has p in its denominator).

Proof. By Corollary 5.3.2 and Lemma 5.3.3 (note $B_m \in \mathbb{Z}_p$ for $m \leq p - 3$ and m is a unit), $p \mid h_K^-$ iff $p \mid B_m$ for some even $2 \leq m \leq p - 3$. It remains to use Kummer's theorem that $p \mid h_{K^+} \Rightarrow p \mid h_K^-$ [16, Thm. 5.34], so that $p \mid h_K \iff p \mid h_K^-$. ■

A prime p with $p \nmid \# \text{Cl}(\mathbb{Q}(\zeta_p))$ is called *regular*, otherwise *irregular*.

Remark 5.3.5. The smallest irregular prime, i.e. the smallest p such that $p \mid \# \text{Cl}(\mathbb{Q}(\zeta_p))$, is $p = 37$; indeed 37 divides the numerator of B_{32} . The next ones are 59, 67, 101, 103, ...

Theorem 5.3.6 (Kummer)

If $p \nmid \# \text{Cl}(\mathbb{Q}(\zeta_p))$, then Fermat's Last Theorem is true for the exponent p : the equation $a^p + b^p = c^p$ has no solutions in nonzero integers a, b, c .

Notes. No proof was given in the lecture; see [16, Ch. 9].

5.4 Eigenspaces of the class group; Herbrand–Ribet; Kronecker–Weber

Note that $\Delta = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ acts on $\text{Cl}(\mathbb{Q}(\zeta_p))$. Let

$$\text{Cl}(\mathbb{Q}(\zeta_p))[p] = \{x \in \text{Cl}(\mathbb{Q}(\zeta_p)) \mid p \cdot x = 0\},$$

a finite-dimensional $\mathbb{F}_p$ -vector space with an action of Δ .

Proposition 5.4.1

Let A be a $\mathbb{Z}_p[\Delta]$ -module (e.g. $\text{Cl}(\mathbb{Q}(\zeta_p))[p]$ or the p -Sylow subgroup $\text{Cl}(\mathbb{Q}(\zeta_p))[p^\infty]$). Then we have the decomposition

$$A = \bigoplus_{i=0}^{p-2} A^{\omega^i}, \quad A^{\omega^i} = \{x \in A \mid \sigma_a x = \omega^i(a)x \text{ for all } a\},$$

the part on which $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts by ω^i . Moreover $A^{\omega^i} = \varepsilon_i A$ with the idempotents $\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^{-i}(a) \sigma_a \in \mathbb{Z}_p[\Delta]$.

Proof. Since $p-1$ is invertible in $\mathbb{Z}_p$, $\varepsilon_i \in \mathbb{Z}_p[\Delta]$. Substituting $a \mapsto ab^{-1}$ gives $\sigma_b \varepsilon_i = \omega^i(b) \varepsilon_i$. By orthogonality of characters ($\sum_a \omega^j(a) = (p-1)[j \equiv 0]$) we get $\varepsilon_i \varepsilon_j = \delta_{ij} \varepsilon_i$ and $\sum_i \varepsilon_i = \sigma_1 = 1$. Hence $A = \bigoplus \varepsilon_i A$, with $\varepsilon_i A \subseteq A^{\omega^i}$, and $\varepsilon_i x = x$ for $x \in A^{\omega^i}$. ■

Since ε_i commutes with multiplication by p , $A^{\omega^i} \neq 0$ iff $(A[p])^{\omega^i} \neq 0$; so it does not matter whether we use $\text{Cl}[p]$ or $\text{Cl}[p^\infty]$ below.

Theorem 5.4.2 (Herbrand–Ribet)

Let n be even with $2 \leq n \leq p-3$. Then

$$p \mid \# \text{Cl}(\mathbb{Q}(\zeta_p))[p]^{\omega^{1-n}} \iff p \mid B_n.$$

Correction. My notes state this for all n with $1 \leq n \leq p-1$. It should be even n with $2 \leq n \leq p-3$, i.e. $\omega^{1-n} = \omega^i$ with $i = p-n$ odd, $3 \leq i \leq p-2$. Note how this refines Theorem 5.3.4: the Bernoulli number B_n “sees” exactly the ω^{1-n} -part.

Notes. The direction $\Rightarrow$ is due to Herbrand (1932), using Stickelberger's theorem. The direction $\Leftarrow$ is due to Ribet [12], who constructs the corresponding unramified extension using modular forms (congruences between cusp forms and Eisenstein series). The same strategy, generalised by Mazur and Wiles, proves the Iwasawa main conjecture; see Chapter 11. Proofs: [16, §6.3, §15.2].

Theorem 5.4.3 (Kronecker–Weber)

Let F be an abelian number field, i.e. $F/\mathbb{Q}$ is Galois and $\text{Gal}(F/\mathbb{Q})$ is an abelian group. Then there exists a positive integer N such that $F \subseteq \mathbb{Q}(\zeta_N)$.

Notes. No proof in the lecture; see [16, Ch. 14]. Combined with Theorem 5.1.1 and Corollary 5.1.2, it shows that the zeta function of every abelian number field is a product of Dirichlet L -functions, and that $\zeta_F(1-n) \in \mathbb{Q}$ for all abelian F and $n \geq 1$.

5.5 Quadratic fields

Lemma 5.5.1

Every quadratic field F is contained in $\mathbb{Q}(\zeta_{|D_F|})$.

Proof. For an odd prime ℓ let η_ℓ be the Legendre symbol mod ℓ (the quadratic character) and $\ell^* = (-1)^{(\ell-1)/2}\ell$. By Lemma 4.2.2(ii), $G(\eta_\ell)^2 = \eta_\ell(-1)\ell = \ell^*$, so $\sqrt{\ell^*} \in \mathbb{Q}(\zeta_\ell)$. Also $\sqrt{-1} = \zeta_4$, $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ and $\sqrt{-2} = \zeta_8 + \zeta_8^3$. Writing $F = \mathbb{Q}(\sqrt{m})$ with m squarefree, a case check with Lemma 1.3.1 shows that $D_F = \prod_{\ell|m \text{ odd}} \ell^*$ times one of 1, -4 , 8 , -8 (according to $m \equiv 1 \pmod{4}$, $m \equiv 3 \pmod{4}$, and $m = 2m'$ with $m' \equiv \pm 1 \pmod{4}$). Hence $\sqrt{D_F} \in \mathbb{Q}(\zeta_{|D_F|})$. ■

Let F be a quadratic field. Composing $(\mathbb{Z}/|D_F|\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(\zeta_{|D_F|})/\mathbb{Q}) \rightarrow \text{Gal}(F/\mathbb{Q}) \cong \{\pm 1\}$, we have the following Dirichlet character $\chi_F : \mathbb{Z} \rightarrow \{0, \pm 1\}$ with modulus $|D_F|$.

Proposition 5.5.2

For a prime ℓ ,

$$\chi_F(\ell) = \begin{cases} 1 & \text{if } \ell \text{ is unramified and decomposed in } F/\mathbb{Q}, \\ -1 & \text{if } \ell \text{ is unramified and not decomposed (inert) in } F/\mathbb{Q}, \\ 0 & \text{if } \ell \text{ is ramified in } F/\mathbb{Q}. \end{cases}$$

Moreover χ_F is even iff F is real, and we have $\zeta_F(s) = \zeta(s)L(\chi_F, s)$.

Correction. In my notes the values 1 and -1 are interchanged (1 for “not decomposed”, -1 for “decomposed”). With that convention the factorisation $\zeta_F = \zeta \cdot L(\chi_F, \cdot)$ would fail.

Proof. If $\ell \mid D_F$, then ℓ ramifies (Proposition 1.3.2) and $\chi_F(\ell) = 0$ by definition. If $\ell \nmid D_F$, the Frobenius of ℓ in $\text{Gal}(\mathbb{Q}(\zeta_{|D_F|})/\mathbb{Q})$ is σ_ℓ (proof of Theorem 5.1.1(a)), and its restriction to F is the Frobenius of ℓ in $F/\mathbb{Q}$, as both are characterised by $x \mapsto x^\ell$ modulo a prime above ℓ . It is trivial iff the decomposition group is trivial, iff $f = 1$, iff ℓ splits. Also $\chi_F(-1)$ is the restriction of complex conjugation σ_{-1} to F , which is trivial iff F is real. The factorisation is Theorem 5.1.1 with $X(F) = \{1, \chi_F\}$, using that χ_F is primitive of conductor $|D_F|$ [16, Thm. 3.11]. ■

In this case, we have an explicit class number formula.

Theorem 5.5.3

Let F be a quadratic field with discriminant D_F , $\chi = \chi_F$.

(a) If F is imaginary, then $R_F = 1$ and

$$\# \text{Cl}(F) = \frac{w_F |D_F|^{1/2}}{2\pi} L(\chi_F, 1), \quad L(\chi_F, 1) = -\frac{\pi}{|D_F|^{3/2}} \sum_{a=1}^{|D_F|} \chi_F(a) a,$$

$$\text{hence } \# \text{Cl}(F) = -\frac{w_F}{2|D_F|} \sum_{a=1}^{|D_F|} \chi_F(a) a.$$

(b) If F is real with fundamental unit $\varepsilon > 1$, then $R_F = \log \varepsilon$, $w_F = 2$, and

$$\# \text{Cl}(F) = \frac{D_F^{1/2}}{2R_F} L(\chi_F, 1), \quad L(\chi_F, 1) = -\frac{1}{D_F^{1/2}} \sum_{a=1}^{D_F} \chi_F(a) \log \left(\sin \frac{\pi a}{D_F} \right),$$

$$\text{hence } \# \text{Cl}(F) = -\frac{1}{2 \log \varepsilon} \sum_{a=1}^{D_F-1} \chi_F(a) \log \sin \frac{\pi a}{D_F}.$$

Correction. My notes give the single formula $\# \text{Cl}(F) = \frac{w_F |D_F|^{1/2}}{2R_F} L(\chi_F, 1)$ for both cases. From Theorem 3.5.1 the correct constants are $\frac{w_F |D_F|^{1/2}}{2\pi}$ (imaginary: $r_1 = 0, r_2 = 1, R_F = 1$) and $\frac{D_F^{1/2}}{2R_F}$ (real: $r_1 = 2, r_2 = 0, w_F = 2$). The factor π in $L(\chi_F, 1)$ for imaginary F , which I marked with “?”, is correct.

Proof. By Proposition 5.5.2 and Theorem 3.5.1, $L(\chi_F, 1)$ is the residue of ζ_F at $s = 1$, which gives the first formula in each case. For the values of $L(\chi_F, 1)$ apply Proposition 4.6.2 with $N = |D_F|$, $\bar{\chi} = \chi$, and Gauss's evaluation of the sign of the quadratic Gauss sum: $G(\chi_F) = \sqrt{D_F}$ if $D_F > 0$ and $G(\chi_F) = i\sqrt{|D_F|}$ if $D_F < 0$ [3, Ch. 2 and 9]. (Lemma 4.2.2 alone gives $G(\chi_F)^2 = D_F$, so only this sign is extra input.) In the imaginary case, $L = \frac{\pi i \sqrt{|D|}}{|D|} B_{1,\chi}$ with $B_{1,\chi} = \frac{1}{|D|} \sum \chi(a) a$. In the real case, use $|1 - \zeta_D^a| = 2 \sin \frac{\pi a}{D}$ and $\sum_a \chi(a) = 0$. ■

If F is an imaginary quadratic field, then we can calculate $\# \text{Cl}(F)$ easily by hand.

Example 5.5.4. Let $F = \mathbb{Q}(\sqrt{-5})$, so $|D_F| = 20$. Thus χ_F is a Dirichlet character modulo 20, and $w_F = 2$. By Proposition 5.5.2 and Proposition 1.3.2, $\chi_F(\ell) = 1$ iff -5 is a nonzero square mod ℓ : this holds for $\ell = 3, 7$ ($-5 \equiv 1 \pmod{3}$, $-5 \equiv 3^2 \pmod{7}$) and fails for $\ell = 11, 13, 17, 19$. Hence $\chi_F(a) = 1$ for $a = 1, 3, 7, 9$ and $\chi_F(a) = -1$ for $a = 11, 13, 17, 19$, and

$$\# \text{Cl}(F) = -\frac{2}{2 \cdot 20} (1 + 3 + 7 + 9 - 11 - 13 - 17 - 19) = -\frac{1}{20} \cdot (-40) = 2.$$

Correction. In my notes the minus sign in front is missing; without it the sum gives -2 .

Example 5.5.5. For $F = \mathbb{Q}(\sqrt{5})$: $D_F = 5$, $\varepsilon = \frac{1+\sqrt{5}}{2}$, $\chi_F(1) = \chi_F(4) = 1$, $\chi_F(2) = \chi_F(3) = -1$, and $\# \text{Cl}(F) = -\frac{1}{2 \log \varepsilon} \cdot 2 \log \frac{\sin 36^\circ}{\sin 72^\circ} = \frac{\log(2 \cos 36^\circ)}{\log \varepsilon} = 1$, since $2 \cos 36^\circ = \varepsilon$.

Chapter 6

Introduction to Iwasawa Theory

Throughout this chapter p is an odd prime. For a number field F we write $\text{Cl}(F)[p^\infty]$ for the p -Sylow subgroup of $\text{Cl}(F)$, i.e. the elements of p -power order.

6.1 Gauss's conjecture and Iwasawa's class number formula

Conjecture 6.1.1 (Gauss)

There are infinitely many real quadratic fields F such that $\text{Cl}(F) = \{1\}$.

Notes. This is still open. For imaginary quadratic fields the opposite holds: by the work of Heegner, Baker and Stark there are exactly nine with class number one. The conjecture is mentioned as an illustration of how badly understood individual class groups are. Iwasawa's idea is to study class groups not one field at a time, but along a tower of fields, where they behave regularly.

We fix a prime number p . We consider a family of cyclotomic fields $\mathbb{Q}(\zeta_{p^n})$, $n \geq 1$. The first interesting result for $\text{Cl}(\mathbb{Q}(\zeta_{p^n}))$ is the following theorem.

Theorem 6.1.2 (Iwasawa's class number formula)

Let p be a prime number. Then there exist $\lambda_p \in \mathbb{Z}_{\geq 0}$, $\mu_p \in \mathbb{Z}_{\geq 0}$ and $\nu_p \in \mathbb{Z}$ such that

$$\# \text{Cl}(\mathbb{Q}(\zeta_{p^n}))[p^\infty] = p^{\lambda_p n + \mu_p p^n + \nu_p} \quad \text{for } n \gg 0.$$

Proof. Later, for an arbitrary $\mathbb{Z}_p$ -extension, in Part II (Chapter 9). ■

Notes. (a) “ $n \gg 0$ ” means: for all n larger than some n_0 ; the formula need not hold for small n . (b) The invariants depend on p (and, in general, on the tower). Shifting the index ($\mathbb{Q}(\zeta_{p^{n+1}})$ instead of $\mathbb{Q}(\zeta_{p^n})$) only changes ν_p . (c) For the cyclotomic tower, Ferrero and Washington proved $\mu_p = 0$ [7].

6.2 The analytic side: the Kubota–Leopoldt p -adic zeta function

The analytic side of Iwasawa theory is a p -adic analogue of the zeta function. The guiding dictionary is

$$\begin{array}{ccc} \text{holomorphic (meromorphic)} & & \text{“bounded” “analytic” functions on the} \\ \text{functions on } \mathbb{C} & \longleftrightarrow & \text{open unit disc in } \overline{\mathbb{Q}_p} \text{ around 1,} \end{array}$$

where the open unit disc around 1 is

$$U(1; 1) = \{x \in \overline{\mathbb{Q}_p} \mid |x - 1|_p < 1\} = 1 + \mathfrak{m}_{\overline{\mathbb{Q}_p}},$$

with $\mathfrak{m}_{\overline{\mathbb{Q}_p}}$ the maximal ideal of the valuation ring of $\overline{\mathbb{Q}_p}$.

Correction. On one page of my notes the disc is written with ≤ 1 ; it is the *open* disc $|x - 1|_p < 1$, as on the next page.

Notes. “Bounded analytic function on $U(1; 1)$ ” means a function of the form $x \mapsto G(x - 1)$ with $G(T) = \sum_{n \geq 0} c_n T^n$, where the c_n lie in a finite extension E of $\mathbb{Q}_p$ and $\sup_n |c_n|_p < \infty$. Such series converge on $U(1; 1)$, since $|x - 1|_p < 1$ and the coefficients are bounded. Up to scaling, they are exactly the elements of $\mathcal{O}_E[[T]]$, and Chapter 8 studies this ring in detail. By the p -adic Weierstrass preparation theorem (Corollary 8.3.5), a nonzero such function has only finitely many zeros in $U(1; 1)$. So the “number of zeros” below is meaningful, and such a function is determined by its values on any subset of $U(1; 1)$ with an accumulation point in $U(1; 1)$.

Lecture of 25 May 2026: a brief review of the Iwasawa main conjecture for ideal class groups.

Theorem 6.2.1 (Kubota–Leopoldt)

Let p be an odd prime. For every odd i with $3 \leq i \leq p - 2$ there exists a unique bounded p -adic analytic function $\zeta_p^{(i)}$ on $U(1; 1)$ such that

$$\zeta_p^{(i)}((1 + p)^{1-r}) = (1 - p^{r-1}) \zeta(1 - r)$$

for every positive integer r with $r \equiv 1 - i \pmod{p - 1}$.

Correction. My notes state this “for all $0 < i < p - 1$ ”. For even i the integers $r \equiv 1 - i$ are odd, so $\zeta(1 - r) = 0$ for $r \geq 3$ (Corollary 4.4.5) and the function is identically zero. For $i = 1$ the right-hand side has p in the denominator ($r \equiv 0 \pmod{p - 1}$, von Staudt–Clausen), and $\zeta_p^{(1)}$ is only *meromorphic*, with a simple pole at $x = 1 + p$ (the p -adic analogue of the pole of $\zeta(s)$ at $s = 1$). So the interesting cases are the odd i with $3 \leq i \leq p - 2$.

Notes. Note: if i is odd, then r is even, so $1 - r$ is an odd negative integer, and $\zeta(1 - r) = -B_r/r \in \mathbb{Q}^\times$ (Corollaries 4.4.5 and 4.6.1). Since $\mathbb{Q} \subset \mathbb{Q}_p$ and $\mathbb{Q} \subset \mathbb{C}$, these rational numbers can be read both complex-analytically and p -adically: this is the bridge between the two worlds. The factor $1 - p^{r-1}$ is the Euler factor at p of $\zeta(s)$ evaluated at $s = 1 - r$; it has to be removed to obtain a p -adically continuous family. Uniqueness: as r runs through $r_0 + (p - 1)p^k$, $k \rightarrow \infty$, the points $(1 + p)^{1-r}$ converge to $(1 + p)^{1-r_0} \in U(1; 1)$, so the interpolation points accumulate, and the preceding note applies. In modern notation $\zeta_p^{(i)}((1 + p)^s) = L_p(s, \omega^{1-i})$ is a branch of the Kubota–Leopoldt p -adic L -function. Its construction is the subject of Chapter 10.

6.3 The algebraic side and the Iwasawa main conjecture

Let $A_n = \text{Cl}(\mathbb{Q}(\zeta_{p^n}))[p^\infty]$ and

$$V = \left(\varprojlim_n A_n \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Each A_n carries an action of $\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$.

Notes. The inverse limit is taken with respect to the norm maps $A_{n+1} \rightarrow A_n$, induced by $N_{\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_{p^n})}$ on ideals (equivalently, via class field theory, by restriction between the Galois groups of the maximal unramified abelian p -extensions). The norm commutes with the Galois action, so the actions are compatible. Each A_n is a finite abelian p -group, hence a $\mathbb{Z}_p$ -module, and $\varprojlim A_n$ is a compact $\mathbb{Z}_p$ -module.

V is a $\mathbb{Q}_p$ -vector space on which

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$$

acts naturally, where $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_n \mathbb{Q}(\zeta_{p^n})$ (see §7.1), and $\mu_{p-1} \cong (\mathbb{Z}/p\mathbb{Z})^\times$ by Lemma 2.4.2.

Correction. In my notes $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is identified with $(\mathbb{Z}/p^n\mathbb{Z})^\times$; it is the inverse limit, $\mathbb{Z}_p^\times$.

Proposition 6.3.1 (Iwasawa)

The vector space V is finite dimensional.

Notes. This follows from the structure theory of modules over the Iwasawa algebra (Chapter 8 and Part II): $\varprojlim A_n$ is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$ -module, and $\dim_{\mathbb{Q}_p} V = \lambda_p$ is the λ -invariant of Theorem 6.1.2.

Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mu_{p-1}$ acts on V through the factor $\mu_{p-1} \subset \mathbb{Z}_p^\times$, Proposition 5.4.1 gives

$$V \cong \bigoplus_{i=0}^{p-2} V^{\omega^i},$$

with ω the Teichmüller character. The group

$$\Gamma := \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)) \cong 1 + p\mathbb{Z}_p$$

acts on each V^{ω^i} , because $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is abelian.

Correction. My notes write $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)) \cong 1 + \mathbb{Z}_p$; it is $1 + p\mathbb{Z}_p$, the kernel of $\mathbb{Z}_p^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$.

We choose a *topological generator* $\gamma \in \Gamma$, i.e. the subgroup $\langle \gamma \rangle = \{\gamma^n \mid n \in \mathbb{Z}\}$ is dense in Γ (for example the element corresponding to $1 + p$, see Proposition 8.1.3). We denote by $p^{(i)}(x)$ the characteristic polynomial

$$p^{(i)}(x) = \det(1 - \gamma x \mid V^{\omega^i}).$$

Notes. This is the “reversed” characteristic polynomial: a polynomial in x with constant term 1 and degree $\dim_{\mathbb{Q}_p} V^{\omega^i}$, whose zeros are the inverses of the eigenvalues of γ on V^{ω^i} (in $\overline{\mathbb{Q}_p}$). The eigenvalues are $\equiv 1$ modulo $\mathfrak{m}_{\overline{\mathbb{Q}_p}}$, because $\gamma^{p^n} \rightarrow 1$, so the zeros lie in $U(1; 1)$. The same convention appears in the Weil conjectures (Remark below).

Theorem 6.3.2 (Mazur–Wiles; Iwasawa main conjecture)

For every odd $i \in \mathbb{Z}$ with $3 \leq i \leq p-2$,

$$\#\{\text{zeros of } \zeta_p^{(i)} \text{ in } U(1;1)\} = \#\{\text{zeros of } p^{(i)}\},$$

where zeros are counted with multiplicity.

Correction. My notes have the range “ $0 < i < p-i$ ”; it should be $0 < i < p-1$ (and, as explained above, the statement is meaningful for odd $i \geq 3$).

Notes. This counting statement is the form given in the lecture. The main conjecture proper (proved by Mazur and Wiles [10]) is the finer statement that the characteristic power series of the ω^i -part of $\varprojlim A_n$ and the power series attached to $\zeta_p^{(i)}$ generate the same ideal of $\mathbb{Z}_p[[T]]$. The counting statement follows from it by Corollary 8.3.5. The precise formulations are given in Part II (Chapter 11).

- Remark 6.3.3.** (1) According to the philosophy of the analogy between function fields of one variable over finite fields and number fields, the Iwasawa main conjecture is an analogue of the Weil conjecture for the congruence zeta function of curves over a finite field. For a smooth projective curve $C/\mathbb{F}_q$ one has $Z(C, t) = \frac{P(t)}{(1-t)(1-qt)}$ with $P(t) = \det(1 - \text{Frob } t \mid V_\ell(\text{Jac } C))$. Here the tower $\mathbb{F}_q \subset \mathbb{F}_{q^2} \subset \cdots$ corresponds to the cyclotomic tower, Frob to γ , and the Tate module of the Jacobian to V .
- (2) The proof of Mazur–Wiles uses the theory of modular curves, modular forms, and arithmetic geometry (generalising Ribet’s method for the Herbrand–Ribet theorem).
- (3) There is another proof by Karl Rubin [13], using the theory of Euler systems of cyclotomic units (due to Kolyvagin and Thaine).

Chapter 7

$\mathbb{Z}_p$ -extensions

For simplicity, we assume that the prime p is > 2 .

7.1 Definition and the cyclotomic $\mathbb{Z}_p$ -extension

Definition 7.1.1

Let K be a number field. If L is a Galois extension of K such that $\text{Gal}(L/K) \cong \mathbb{Z}_p$, then we say L is a $\mathbb{Z}_p$ -extension of K .

Notes. Here L/K is in general infinite, $\text{Gal}(L/K)$ carries the Krull topology, and “ $\cong$ ” means an isomorphism of *topological* groups, with $\mathbb{Z}_p$ carrying the p -adic topology.

Lemma 7.1.2

The closed subgroups of $\mathbb{Z}_p$ are 0 and $p^n\mathbb{Z}_p$ ($n \geq 0$). The open subgroups are exactly the $p^n\mathbb{Z}_p$ with $n \geq 0$, and $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Consequently a $\mathbb{Z}_p$ -extension L/K has exactly one intermediate field K_n with $[K_n : K] = p^n$ for each $n \geq 0$, these are all the intermediate fields other than L , and $L = \bigcup_n K_n$.

Proof. Let $H \neq 0$ be a closed subgroup and $n = \min\{v_p(x) \mid x \in H\}$. Then $H \subseteq p^n\mathbb{Z}_p$. Pick $x = p^n u \in H$ with $u \in \mathbb{Z}_p^\times$. Since H is a closed subgroup, it contains the closure of $\mathbb{Z}x$, which is $\mathbb{Z}_p x = p^n\mathbb{Z}_p$ (as $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and multiplication is continuous). So $H = p^n\mathbb{Z}_p$. Open subgroups are closed and nonzero; conversely $p^n\mathbb{Z}_p$ is open. The rest follows from infinite Galois theory (closed subgroups $\leftrightarrow$ intermediate fields) and Proposition 2.2.3(iii). ■

Correction. My notes say “the only open subgroups of $\mathbb{Z}_p$ are $\{p^n\mathbb{Z}_p\}_{n \in \mathbb{Z}_{\geq 1}}$ ”; $n = 0$ (the whole group) must be included.

$\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_n \mathbb{Q}(\zeta_{p^n})$ is a Galois extension of $\mathbb{Q}$. By the report problem (Theorem 1.3.5),

$$\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p^n\mathbb{Z})^\times, \quad \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times.$$

The second isomorphism is the *cyclotomic character* χ_{cyc} : $\sigma(\zeta) = \zeta^{\chi_{\text{cyc}}(\sigma)}$ for every p -power root of unity ζ .

Notes. The Galois group of a union of a tower of finite Galois extensions is the inverse limit of the finite Galois groups (this is how the Krull topology arises), and the isomorphisms for the different n are compatible with the reductions $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$.

We have a decomposition (as multiplicative groups)

$$\mathbb{Z}_p^\times \xrightarrow{\sim} \mu_{p-1} \times (1 + p\mathbb{Z}_p), \quad \mu_{p-1} \cong (\mathbb{Z}/p\mathbb{Z})^\times,$$

where μ_{p-1} is a closed (finite) subgroup, and

$$\log : 1 + p\mathbb{Z}_p \xrightarrow{\sim} p\mathbb{Z}_p \cong \mathbb{Z}_p$$

from a multiplicative group to an additive group (Theorem 2.4.1).

Correction. My notes write $1 + p\mathbb{Z}_p \xrightarrow{\log} p\mathbb{Z}$; the target is $p\mathbb{Z}_p$.

Let $\mathbb{Q}_\infty = \mathbb{Q}(\zeta_{p^\infty})^{\mu_{p-1}}$ be the fixed field of the closed subgroup of $\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ corresponding to μ_{p-1} :

$$\begin{array}{ccc} & \mathbb{Q}(\zeta_{p^\infty}) & \\ \mathbb{Z}_p^\times \swarrow & & \searrow \mu_{p-1} \\ \mathbb{Q} & \xrightarrow{\quad} & \mathbb{Q}_\infty \end{array}$$

According to Galois theory for infinite algebraic extensions, $\mathbb{Q}_\infty$ is a Galois extension of $\mathbb{Q}$ such that

$$\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p^\times / \mu_{p-1} \cong 1 + p\mathbb{Z}_p \cong \mathbb{Z}_p.$$

So $\mathbb{Q}_\infty/\mathbb{Q}$ is a $\mathbb{Z}_p$ -extension. Its n -th layer $\mathbb{Q}_n$ is the unique subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$ of degree p^n over $\mathbb{Q}$.

Let K be a number field. We define $K_\infty^{\text{cyc}} = K\mathbb{Q}_\infty$.

Proposition 7.1.3

K_∞^{cyc}/K is a $\mathbb{Z}_p$ -extension.

Proof. $K_\infty^{\text{cyc}} = K\mathbb{Q}_\infty$ is Galois over K , and restriction gives an isomorphism of topological groups $\text{Gal}(K\mathbb{Q}_\infty/K) \cong \text{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$. (This is the usual theorem on translations of Galois extensions; it holds for infinite ones as well, since a continuous bijection between compact Hausdorff groups is a homeomorphism.) $K \cap \mathbb{Q}_\infty$ is a finite extension of $\mathbb{Q}$, so $\text{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}_\infty)$ is an open subgroup of $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p$. By Lemma 7.1.2 it is $p^n\mathbb{Z}_p$ for some n , and $p^n\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}_p$, $x \mapsto p^{-n}x$. Hence K_∞^{cyc}/K is a $\mathbb{Z}_p$ -extension. ■

Definition 7.1.4

We call K_∞^{cyc} the *cyclotomic $\mathbb{Z}_p$ -extension* of K .

7.2 How many $\mathbb{Z}_p$ -extensions? Leopoldt's conjecture

Questions. (1) Are there any $\mathbb{Z}_p$ -extensions of a number field other than the cyclotomic $\mathbb{Z}_p$ -extension? (2) “How many” $\mathbb{Z}_p$ -extensions do we have for a given number field? Class field theory partially answers these.

Lemma 7.2.1

Let $K_\infty^{(1)}, \dots, K_\infty^{(d)}$ be $\mathbb{Z}_p$ -extensions of a number field K . Then their composite $K_\infty^{(1)} \cdots K_\infty^{(d)}$ is a Galois extension of K , and its Galois group is isomorphic to a free $\mathbb{Z}_p$ -module of finite rank $\leq d$.

Proof. A composite of Galois extensions is Galois. Restriction gives a continuous injective homomorphism $\text{Gal}(K_\infty^{(1)} \cdots K_\infty^{(d)}/K) \hookrightarrow \prod_i \text{Gal}(K_\infty^{(i)}/K) \cong \mathbb{Z}_p^d$, whose image H is compact, hence

closed. A closed subgroup of $\mathbb{Z}_p^d$ is stable under multiplication by $\mathbb{Z}$, hence by continuity under $\mathbb{Z}_p$; so H is a $\mathbb{Z}_p$ -submodule of the free module $\mathbb{Z}_p^d$ over the PID $\mathbb{Z}_p$, hence free of rank $\leq d$. ■

For a number field K , we denote by $\widetilde{K}_\infty$ the composite of all $\mathbb{Z}_p$ -extensions of K .

Theorem 7.2.2

Let K be a number field. Then $\text{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p^\rho$ is a free $\mathbb{Z}_p$ -module of finite rank, and we have

$$r_2(K) + 1 \leq \rho = \text{rank}_{\mathbb{Z}_p} \text{Gal}(\widetilde{K}_\infty/K) \leq [K : \mathbb{Q}].$$

Proof sketch. (Omitted in the lecture: a corollary of class field theory.) Let M be the maximal abelian pro- p extension of K unramified outside p . Every $\mathbb{Z}_p$ -extension is contained in M (Theorem 7.3.1(1)), so $\text{Gal}(\widetilde{K}_\infty/K)$ is the maximal torsion-free quotient of $\text{Gal}(M/K)$, and both have the same $\mathbb{Z}_p$ -rank. Let $U_1 = \prod_{v|p} U_v^{(1)}$ (principal units of the completions at the primes above p); by Theorem 2.4.7 it has $\mathbb{Z}_p$ -rank $\sum_v [K_v : \mathbb{Q}_p] = [K : \mathbb{Q}]$. Let $\overline{E}_1$ be the closure of the image of the global units congruent to 1. Class field theory gives $\text{Gal}(M/H) \cong U_1/\overline{E}_1$, where H is the p -Hilbert class field, and $[H : K] < \infty$. So

$$\text{rank Gal}(M/K) = [K : \mathbb{Q}] - \text{rank}_{\mathbb{Z}_p} \overline{E}_1.$$

Since $\text{rank}_{\mathbb{Z}_p} \overline{E}_1 \leq r_1 + r_2 - 1$ (see below), the rank is $\geq [K : \mathbb{Q}] - (r_1 + r_2 - 1) = r_2 + 1$; trivially it is $\leq [K : \mathbb{Q}]$. See [16, §13.1]. ■

Conjecture 7.2.3 (Leopoldt)

$$\text{rank}_{\mathbb{Z}_p} \text{Gal}(\widetilde{K}_\infty/K) = r_2(K) + 1.$$

Correction. In my notes: “ $\text{Gal}(\widetilde{K}_\infty/K) \cong r_2(K) + 1$ ”. What is meant is the *rank* (equivalently $\text{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p^{r_2(K)+1}$).

By Dirichlet’s unit theorem, $\text{rank}_{\mathbb{Z}} \mathcal{O}_K^\times = r_1(K) + r_2(K) - 1$. We consider the image of the (finitely generated abelian) group $\mathcal{O}_K^\times$ under

$$\mathcal{O}_K^\times \longrightarrow \varprojlim_n (\mathcal{O}_K/p^n \mathcal{O}_K)^\times \cong (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \cong \prod_{v|p} \mathcal{O}_{K_v}^\times.$$

Let $\overline{\mathcal{O}_K^\times}$ be the closure of the image of $\mathcal{O}_K^\times$ in $(\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$.

Correction. My notes call $\mathcal{O}_K^\times$ a “finite dim. abelian group”; it is a *finitely generated* abelian group (infinite in general).

Proposition 7.2.4

A priori, $\text{rank}_{\mathbb{Z}_p} \overline{\mathcal{O}_K^\times} \leq r_1(K) + r_2(K) - 1$, and

$$\text{Leopoldt's conjecture for } K \text{ and } p \iff \text{rank}_{\mathbb{Z}_p} \overline{\mathcal{O}_K^\times} = r_1(K) + r_2(K) - 1.$$

Proof. U_1 is open of finite index in $(\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ and is a $\mathbb{Z}_p$ -module (as in the proof of Theorem 2.4.7). $E_1 = \mathcal{O}_K^\times \cap U_1$ has finite index in $\mathcal{O}_K^\times$, so it is free of rank $r = r_1 + r_2 - 1$ modulo torsion, say generated by $\varepsilon_1, \dots, \varepsilon_r$ and torsion. The $\mathbb{Z}_p$ -span $\sum \mathbb{Z}_p \varepsilon_i$ is compact (a continuous

image of $\mathbb{Z}_p^r$), contains E_1 , and is contained in its closure; so it equals $\overline{E}_1$, which has rank $\leq r$. Since $\overline{\mathcal{O}_K^\times}$ contains $\overline{E}_1$ with finite index, it has the same rank. The equivalence follows from the rank formula in the proof of Theorem 7.2.2. ■

Notes. The rank of $\overline{\mathcal{O}_K^\times}$ can be smaller than r only if there is a nontrivial $\mathbb{Z}_p$ -linear relation $\prod \varepsilon_i^{a_i} = 1$ with $a_i \in \mathbb{Z}_p$ not all in $\mathbb{Q}$ -proportion to an integral relation. Equivalently, the p -adic regulator (the determinant of p -adic logarithms of units) vanishes. So Leopoldt's conjecture is a conjecture on p -adic transcendental numbers. By this translation and a p -adic version of Baker's theorem on linear forms in logarithms, Brumer [2] proved Leopoldt's conjecture when K is a finite abelian extension of $\mathbb{Q}$ or of an imaginary quadratic field.

Correction. My notes say “a finite abelian extension of $\mathbb{Q}$ of a finite abelian extension of an imaginary quadratic field”; it should be “or”.

Example 7.2.5. In particular:

- (1) If K is a real quadratic field, then $r_2(K) + 1 = 1$, and Leopoldt's conjecture holds ($K/\mathbb{Q}$ is abelian). Hence $\text{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p$, and K does not have a $\mathbb{Z}_p$ -extension other than K_∞^{cyc} .
- (2) If K is an imaginary quadratic field, then $r_2(K) + 1 = 2 = [K : \mathbb{Q}]$, so $\text{rank}_{\mathbb{Z}_p} \text{Gal}(\widetilde{K}_\infty/K) = 2$ unconditionally. Since $\mathbb{Z}_p^2$ has infinitely many quotients isomorphic to $\mathbb{Z}_p$, K has infinitely many $\mathbb{Z}_p$ -extensions, e.g. the cyclotomic one and the *anticyclotomic* one (on which complex conjugation acts by -1).

Notes. My notes write “ $\text{rank}_{\mathbb{Z}_p}(\widetilde{K}_\infty)$ ”; this means the rank of $\text{Gal}(\widetilde{K}_\infty/K)$. In (1), the claim that there is no other $\mathbb{Z}_p$ -extension uses that any $\mathbb{Z}_p$ -extension is a quotient of $\text{Gal}(\widetilde{K}_\infty/K) \cong \mathbb{Z}_p$, hence equal to $\widetilde{K}_\infty$.

7.3 Ramification in $\mathbb{Z}_p$ -extensions

Theorem 7.3.1

Let K be a number field and let K_∞ be a $\mathbb{Z}_p$ -extension of K .

- (1) Let λ be a prime ideal of $\mathcal{O}_K$ with $\lambda \nmid p$. Then K_∞/K is unramified at λ .
- (2) There is at least one prime $\mathfrak{p} \subset \mathcal{O}_K$ above p (i.e. dividing $p\mathcal{O}_K$) which is ramified in K_∞/K .

Correction. My notes have “a prime $\mathfrak{p} \subset \mathcal{O}_K$ divisible by (p) ”; it should be a prime *dividing* (p) , i.e. $\mathfrak{p} \supseteq p\mathcal{O}_K$.

Notes. “ K_∞/K is unramified at λ ” means that λ is unramified in every finite layer K_n/K , equivalently that the inertia group $I_\lambda \subseteq \text{Gal}(K_\infty/K)$ is trivial. Since $\text{Gal}(K_\infty/K)$ is abelian, I_λ does not depend on the choice of a prime above λ . The infinite places are automatically unramified: their decomposition groups have order ≤ 2 , and $\mathbb{Z}_p$ (p odd) has no element of order 2.

Proof. (The lecture omitted the proof: it is also a corollary of class field theory and the compatibility of global and local class field theory.)

(1) Suppose $I = I_\lambda \neq 0$; then $I = p^m \mathbb{Z}_p$ for some m (Lemma 7.1.2). For $n > m$, the inertia group of λ in K_n/K is the image of I in $\mathbb{Z}_p/p^n \mathbb{Z}_p$, cyclic of order p^{n-m} . As the residue characteristic ℓ of λ is different from p , this ramification is tame. For a tamely ramified Galois extension of local fields, the inertia group embeds into the multiplicative group of the residue field of the top field, via $\sigma \mapsto \sigma(\Pi)/\Pi \bmod \Pi$ ([14, Ch. IV, §2]). Moreover the Frobenius acts on it by $x \mapsto x^q$, $q = N(\lambda)$. In an abelian extension this action is trivial, so the order of the inertia group divides $q - 1$. Hence $p^{n-m} \mid q - 1$ for all $n > m$, which is absurd.

(2) If no prime above p ramifies, then by (1) and the preceding note every K_n/K is an abelian extension of degree p^n , unramified at all primes, finite and infinite. By Definition 1.4.1 and Theorem 1.4.2, $K_n \subseteq H_K$, so $p^n \leq h_K$ for all n , a contradiction. ■

Chapter 8

The Iwasawa Algebra

Recall that for any $\mathbb{Z}_p$ -extension K_∞/K , $\Gamma = \text{Gal}(K_\infty/K)$ acts on K_∞ and on $\text{Cl}(K_\infty)[p^\infty]$, which is a $\mathbb{Z}_p$ -module and a Γ -module. Hence it is important to recall the general theory of Γ -modules.

Notes. Here $\text{Cl}(K_\infty)[p^\infty] := \varinjlim_n \text{Cl}(K_n)[p^\infty]$ (direct limit along the maps induced by extension of ideals). In practice one mostly works with the inverse limit $X = \varprojlim_n \text{Cl}(K_n)[p^\infty]$ along norm maps, as in §6.3. The two are related by Pontryagin duality and class field theory (Part II).

8.1 Complete group algebras

Lecture of 8 June 2026.

Throughout, K is a finite extension of $\mathbb{Q}_p$, $\mathcal{O} \subset K$ is the ring of integers of K , ϖ is a uniformiser, and $\mathbb{F}_q = \mathcal{O}/\varpi\mathcal{O}$. Note that $\mathcal{O}$ is a complete discrete valuation ring whose residue field is finite (Proposition 2.3.6). Let G be a profinite group.

Correction. My notes say “ G : a profinite ring”; it is a profinite *group*.

Notes. A *profinite group* is a topological group isomorphic to an inverse limit of finite (discrete) groups; equivalently, a compact Hausdorff totally disconnected group. Galois groups with the Krull topology, $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ are examples. Note that if $U \subseteq G$ is an open normal subgroup, then G/U is a finite group: the cosets of U form an open cover of the compact group G by disjoint sets.

Definition 8.1.1

We define the *complete group algebra* $\mathcal{O}[[G]]$ to be

$$\mathcal{O}[[G]] := \varprojlim_{\substack{U \trianglelefteq G \\ \text{open normal}}} \mathcal{O}[G/U],$$

where $\mathcal{O}[G/U]$ is the (usual) group algebra of the finite group G/U over $\mathcal{O}$, and for $U' \subseteq U$ the transition map $\mathcal{O}[G/U'] \rightarrow \mathcal{O}[G/U]$ is induced by $G/U' \twoheadrightarrow G/U$.

Notes. Each $\mathcal{O}[G/U] \cong \mathcal{O}^{|G/U|}$ (as $\mathcal{O}$ -modules) carries the ϖ -adic topology, and $\mathcal{O}[[G]]$ the inverse limit topology. It is compact. G embeds into $\mathcal{O}[[G]]^\times$ via $g \mapsto (gU)_U$, and the group algebra $\mathcal{O}[G]$ is dense in $\mathcal{O}[[G]]$.

If G is an abelian profinite group, then $\mathcal{O}[[G]]$ is a commutative $\mathcal{O}$ -algebra.

From now on, we restrict ourselves to the case where G is isomorphic to $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$; we set $\Gamma = G$ with a fixed isomorphism $\kappa : \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$.

Definition 8.1.2

Classically, $\Lambda_{\mathcal{O}} := \mathcal{O}[[\Gamma]]$ is called the *Iwasawa algebra*; for $\mathcal{O} = \mathbb{Z}_p$ we write $\Lambda = \mathbb{Z}_p[[\Gamma]]$.

- Proposition 8.1.3** (1) Γ is a topologically cyclic profinite group: there exists $\gamma \in \Gamma$, called a *topological generator*, with $\Gamma = \overline{\langle \gamma \rangle}$ (closure). For example $\kappa(\gamma) = 1 + p$ works: $\overline{(1+p)^{\mathbb{Z}}} = 1 + p\mathbb{Z}_p$.
- (2) $(1 + p\mathbb{Z}_p)^{p^n} = 1 + p^{n+1}\mathbb{Z}_p$.
- (3) A subgroup $U \subseteq \Gamma$ is open (normal) iff $U = \Gamma^{p^n}$ for some $n \in \mathbb{Z}_{\geq 0}$, and $\Gamma_n := \Gamma/\Gamma^{p^n} \cong (1 + p\mathbb{Z}_p)/(1 + p^{n+1}\mathbb{Z}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$, generated by the image of γ .

Correction. My notes write $\overline{(1+p)^{\mathbb{Z}}} = 1 + p\mathbb{Z}$ (it is $1 + p\mathbb{Z}_p$), the range $n \in \mathbb{Z}_{\geq 1}$ in (3) (it should include $n = 0$), and “ $\Gamma^{p^n} \cong (1 + p\mathbb{Z})/(1 + p\mathbb{Z}_p)^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ ”. The last one is the *quotient* Γ/Γ^{p^n} .

Proof. By Proposition 2.4.3 (p odd, $e = 1$), $\log : 1 + p^k\mathbb{Z}_p \rightarrow p^k\mathbb{Z}_p$ is an isomorphism for all $k \geq 1$, transforming $x \mapsto x^{p^n}$ into $y \mapsto p^n y$. Hence (2): $\log((1 + p\mathbb{Z}_p)^{p^n}) = p^{n+1}\mathbb{Z}_p = \log(1 + p^{n+1}\mathbb{Z}_p)$. Since $v_p(\log(1 + p)) = 1$, $\log(1 + p)$ generates $p\mathbb{Z}_p$ as a $\mathbb{Z}_p$ -module, and $\mathbb{Z}\log(1 + p)$ is dense in $p\mathbb{Z}_p$; this gives (1). Under $\Gamma \cong p\mathbb{Z}_p \cong \mathbb{Z}_p$, (3) is Lemma 7.1.2; all subgroups are normal since Γ is abelian. ■

Hence

$$\mathcal{O}[[\Gamma]] = \varprojlim_n \mathcal{O}[\Gamma_n], \quad \Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Example 8.1.4. Let $\Gamma = \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)) \cong 1 + p\mathbb{Z}_p$. Then $\Gamma/\Gamma^{p^n} = \text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_p))$ acts on $\text{Cl}(\mathbb{Q}(\zeta_{p^{n+1}}))[p^\infty]$, which is therefore a $\mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$ -module. The norm maps are compatible with these actions. Hence $X = \varprojlim_n \text{Cl}(\mathbb{Q}(\zeta_{p^n}))[p^\infty]$ is naturally regarded as a $\mathbb{Z}_p[[\Gamma]]$ -module: $(\lambda_n)_n \in \varprojlim_n \mathbb{Z}_p[\Gamma_n]$ acts on $(x_n)_n$ by $(\lambda_n x_n)_n$.

8.2 The power series ring $\mathcal{O}[[T]]$

In general, for a domain R and a prime ideal $P \subset R$, the maximum of the lengths n of chains of prime ideals of R

$$P = P_0 \supsetneq P_1 \supsetneq \cdots \supsetneq P_n$$

is called the *height* of P , $\text{ht } P$. The supremum of $\text{ht } P$ over all prime ideals $P \subset R$ is called the *Krull dimension* of R .

Notes. For a domain the chain can always be extended to end at $P_n = (0)$, so $\text{ht } P = 1$ means: $P \neq 0$ and there is no prime strictly between 0 and P . Heights may in general be infinite; for Noetherian rings they are finite (Krull’s principal ideal theorem).

- Proposition 8.2.1** (1) (Report problem.) Let $f(T) = \sum_{n \geq 0} a_n T^n \in \mathcal{O}[[T]]$. Then $f(T) \in \mathcal{O}[[T]]^\times \iff a_0 \in \mathcal{O}^\times$.
- (2) $\mathcal{O}[[T]]$ is a local ring with maximal ideal $\mathfrak{m} = (\varpi, T)$, and $\mathcal{O}[[T]]/\varpi\mathcal{O}[[T]] \cong \mathbb{F}_q[[T]]$.
- (3) The $\mathfrak{m}$ -adic topology on $\mathcal{O}[[T]]$ coincides with the topology of coefficientwise conver-

gence; $\mathcal{O}[[T]]$ is compact and complete, and $\bigcap_N \mathfrak{m}^N = 0$.

(4) $\mathcal{O}[[T]]$ is a complete local Noetherian ring of Krull dimension 2, and $\text{ht } \mathfrak{m} = 2$.

Proof. (1) If $fg = 1$, then $a_0b_0 = 1$. Conversely, if $a_0 \in \mathcal{O}^\times$, define $b_0 = a_0^{-1}$ and recursively $b_n = -a_0^{-1} \sum_{i=1}^n a_i b_{n-i}$; then $g = \sum b_n T^n$ satisfies $fg = 1$.

(2) By (1) the non-units are exactly the f with $a_0 \in \varpi\mathcal{O}$, i.e. $f \in (\varpi, T)$; these form an ideal, so $\mathcal{O}[[T]]$ is local with maximal ideal (ϖ, T) . Reduction of coefficients gives $\mathcal{O}[[T]]/\varpi \cong \mathbb{F}_q[[T]]$.

(3) Let $U_N = \{f : a_i \in \varpi^N \mathcal{O} \text{ for } i < N\}$; these form a basis of neighbourhoods of 0 for the coefficientwise topology. An element of $\mathfrak{m}^{2N}$ is a sum of terms $\varpi^a T^b h$ with $a + b = 2N$, so its coefficient of T^i is divisible by ϖ^{2N-i} ; hence $\mathfrak{m}^{2N} \subseteq U_N$. Conversely, an element of U_N is $\sum_{i < N} a_i T^i + T^N(\dots) \in \mathfrak{m}^N$. So the topologies agree. $\mathcal{O}[[T]] \cong \prod_{i \geq 0} \mathcal{O}$ with the product topology is compact (Tychonoff) and complete, and $\bigcap_N \mathfrak{m}^N \subseteq \bigcap_N U_N = 0$.

(4) Noetherianity is the power series version of Hilbert's basis theorem, and $\dim R[[T]] = \dim R + 1$ for Noetherian R [9, Thm. 3.3 and Thm. 15.4]; here $\dim \mathcal{O} = 1$. The chain $\mathfrak{m} \supsetneq (\varpi) \supsetneq 0$ (primes, since $\mathcal{O}[[T]]/\mathfrak{m} = \mathbb{F}_q$ and $\mathcal{O}[[T]]/(\varpi) = \mathbb{F}_q[[T]]$ are domains) shows $\text{ht } \mathfrak{m} \geq 2$, hence $= 2$. ■

Definition 8.2.2

A polynomial $F(T) = \sum_{i=0}^n a_i T^i \in \mathcal{O}[T]$ of degree n is called a *distinguished polynomial* if $a_n = 1$ and $a_{n-1}, \dots, a_1, a_0 \in (\varpi)$, i.e. it is monic and all coefficients other than the leading one are non-units.

Remark 8.2.3. If $F(T)$ is a distinguished polynomial of degree $n \geq 1$, then $F(T)$ is a non-unit of $\mathcal{O}[[T]]$ (its constant term lies in (ϖ)).

Correction. In my notes the definition says “all coefficients other than a_0 are non-unit”, which should read “other than the leading coefficient a_n ”. In the remark one needs $n \geq 1$: the constant polynomial 1 is distinguished of degree 0 and is a unit.

Let $F(T) \in \mathcal{O}[T]$ be monic of degree n . Then

$$F(T) = \prod_{i=1}^n (T - \alpha_i) \in \overline{\mathcal{O}}[T],$$

where $\overline{\mathcal{O}}$ is the ring of integers of $\overline{\mathbb{Q}_p}$ (the valuation ring $\{|x|_p \leq 1\}$), since the roots of a monic polynomial over $\mathcal{O}$ are integral over $\mathcal{O}$.

Proposition 8.2.4 (Report problem)

A monic $F(T) \in \mathcal{O}[T]$ is distinguished $\iff \alpha_1, \dots, \alpha_n$ are all non-units of $\overline{\mathcal{O}}$, i.e. $|\alpha_i|_p < 1$ for all i .

Notes. In my notes the roots carry a bar, $\bar{\alpha}_i$. Since α_i already lies in $\overline{\mathcal{O}}$, the bar is not needed. Read with the bar meaning “reduction modulo $\mathfrak{m}_{\overline{\mathcal{O}}}$ ”, the condition becomes $\bar{\alpha}_i = 0$, which is equivalent.

Proof. The coefficients are $a_{n-k} = (-1)^k e_k(\alpha_1, \dots, \alpha_n)$, with e_k the elementary symmetric polynomials. If all $|\alpha_i|_p < 1$, then $|e_k|_p < 1$ for $k \geq 1$ by the ultrametric inequality, so $a_{n-k} \in \mathcal{O} \cap \mathfrak{m}_{\overline{\mathcal{O}}} = \varpi\mathcal{O}$. Conversely, if F is distinguished, then reducing modulo $\mathfrak{m}_{\overline{\mathcal{O}}}$ gives $\prod_i (T - \bar{\alpha}_i) = \bar{F} = T^n$ in $\overline{\mathbb{F}_p}[T]$, so all $\bar{\alpha}_i = 0$, i.e. $|\alpha_i|_p < 1$. ■

8.3 The p -adic Weierstrass preparation theorem

For $f = \sum a_i T^i \in \mathcal{O}[[T]]$ with $f \not\equiv 0 \pmod{\varpi}$, let $\lambda(f) = \min\{i \mid a_i \in \mathcal{O}^\times\}$ (the *Weierstrass degree*).

Theorem 8.3.1 (Division theorem)

Let $g \in \mathcal{O}[[T]]$ with $g \not\equiv 0 \pmod{\varpi}$ and $n = \lambda(g)$. Then every $f \in \mathcal{O}[[T]]$ can be written uniquely as $f = qg + r$ with $q \in \mathcal{O}[[T]]$ and $r \in \mathcal{O}[T]$ of degree $< n$.

Proof. Let $\tau(\sum b_i T^i) = \sum_{i \geq n} b_i T^{i-n}$; τ is $\mathcal{O}$ -linear, $\tau(T^n h) = h$, and $\tau(h) = 0$ iff h is a polynomial of degree $< n$. Write $g = \varpi Q + T^n u$ with $Q \in \mathcal{O}[T]$ of degree $< n$ (the first n coefficients of g are divisible by ϖ) and $u = \tau(g) \in \mathcal{O}[[T]]^\times$ (its constant term a_n is a unit). Then $f = qg + r$ with $\deg r < n$ iff $\tau(f) = \tau(qg) = qu + \varpi\tau(qQ)$. Putting $h = qu$, this reads

$$(1 + \varpi S)(h) = \tau(f), \quad S(h) := \tau(hu^{-1}Q).$$

S is $\mathcal{O}$ -linear with $S(\mathcal{O}[[T]]) \subseteq \mathcal{O}[[T]]$, so $\sum_{k \geq 0} (-\varpi S)^k \tau(f)$ converges coefficientwise and solves the equation. If $(1 + \varpi S)h = 0$ with $h \neq 0$, let k be maximal with $\varpi^k \mid h$; then $h = -\varpi S(h)$ is divisible by ϖ^{k+1} , a contradiction. So h , hence $q = hu^{-1}$ and $r = f - qg$, are unique. ■

Theorem 8.3.2 (p -adic Weierstrass preparation theorem)

Let $F(T) \in \mathcal{O}[[T]]$, $F \neq 0$. Then there exist a unique $m \in \mathbb{Z}_{\geq 0}$, a unique $U(T) \in \mathcal{O}[[T]]^\times$ and a unique distinguished polynomial $P(T)$ such that

$$F(T) = \varpi^m U(T) P(T).$$

Moreover $\deg P = \lambda(\varpi^{-m} F)$.

Correction. The statement in my notes omits $F \neq 0$ (for $F = 0$ there is no such decomposition).

Proof. Let m be the largest integer such that ϖ^m divides all coefficients of F (it exists since $F \neq 0$), and $g = \varpi^{-m} F$, $n = \lambda(g)$. Divide T^n by g (Theorem 8.3.1): $T^n = qg + r$, $\deg r < n$. Reducing mod ϖ , $\bar{g} = T^n \bar{u}$ with $\bar{u} \in \mathbb{F}_q[[T]]^\times$, so $\bar{r} = T^n(1 - \bar{q}\bar{u})$ has degree $< n$ and is divisible by T^n . Hence $\bar{r} = 0$ and $\bar{q}\bar{u} = 1$, so q is a unit and $r \in \varpi\mathcal{O}[T]$. Then $P := T^n - r$ is distinguished of degree n , and $P = qg$, i.e. $F = \varpi^m q^{-1} P$.

Uniqueness: if $F = \varpi^m U P$, then ϖ^m is the exact power dividing F , because $U P \not\equiv 0 \pmod{\varpi}$ ($\bar{U}\bar{P} = \bar{U}T^{\deg P}$). Comparing reductions gives $\deg P = \lambda(g)$. Then $T^n = U^{-1}g + (T^n - P)$ is a division of T^n by g with remainder $T^n - P$ of degree $< n$, so P , and then U , are unique by Theorem 8.3.1. ■

Remark 8.3.3 (Remarks from the lecture). The lecture omitted the proof but gave several remarks, which amount to another proof. *How to determine m :* if some coefficient a_i of F is a unit, then $m = 0$; in general m is the largest nonnegative integer such that ϖ^m divides all coefficients of F . Put $F'(T) = \varpi^{-m} F(T) = \sum_{i \geq 0} a'_i T^i \in \mathcal{O}[[T]]$; by definition some a'_i is a unit, and let n be the minimum of such i . Since $\mathcal{O}[[T]] = \varprojlim_k (\mathcal{O}/\varpi^k)[[T]]$, one constructs the decomposition modulo ϖ^k for each k . For $k = 1$, $F'_1(T) = \bar{a}'_n T^n + \bar{a}'_{n+1} T^{n+1} + \dots = T^n U_1(T)$ with $U_1 \in \mathbb{F}_q[[T]]^\times$, and $P_1(T) = T^n$. Then one lifts this decomposition inductively to $F'_k = P_k U_k$ in $(\mathcal{O}/\varpi^k)[[T]]$ such that F'_k, P_k, U_k reduce modulo ϖ^{k-1} to $F'_{k-1}, P_{k-1}, U_{k-1}$. (In my notes the sum defining F' starts at 1, and the lifting index is n instead of k ; both are slips.)

Definition 8.3.4

For $0 \neq F \in \mathcal{O}[[T]]$ as in Theorem 8.3.2, we put $\mu(F) = m$ and $\lambda(F) = \deg P$.

Corollary 8.3.5

A nonzero $F \in \mathcal{O}[[T]]$ has exactly $\lambda(F)$ zeros (with multiplicity) in the open unit disc $\{t \in \overline{\mathbb{Q}_p} \mid |t|_p < 1\}$. Equivalently, $x \mapsto F(x-1)$ has $\lambda(F)$ zeros in $U(1; 1)$.

Proof. For $|t|_p < 1$ all three factors converge. $\varpi^m \neq 0$. For a unit $U = \sum u_i T^i$ we have $|u_0|_p = 1 > |\sum_{i \geq 1} u_i t^i|_p$, so $|U(t)|_p = 1$ and U has no zeros. The zeros of P all lie in the open disc by Proposition 8.2.4, and there are $\deg P = \lambda(F)$ of them. ■

Proposition 8.3.6

Let $\mathfrak{P} \subset \mathcal{O}[[T]]$ be a prime ideal of height one. Then $\mathfrak{P}$ is either $\varpi \mathcal{O}[[T]]$ or $F(T) \mathcal{O}[[T]]$, where $F(T)$ is an irreducible distinguished polynomial.

Proof. (The proof was omitted in the lecture.) Pick $0 \neq f \in \mathfrak{P}$ and write $f = \varpi^m U P$ (Theorem 8.3.2). Factor $P = \prod P_j$ into monic irreducible factors in $\mathcal{O}[T]$; each P_j is distinguished by Proposition 8.2.4, since its roots are among those of P . Since $\mathfrak{P}$ is prime and $U \notin \mathfrak{P}$, either $\varpi \in \mathfrak{P}$ or some $P_j \in \mathfrak{P}$.

(ϖ) is prime because $\mathcal{O}[[T]]/(\varpi) = \mathbb{F}_q[[T]]$ is a domain. For an irreducible distinguished F , Theorem 8.3.1 gives $\mathcal{O}[[T]]/(F) \cong \mathcal{O}[T]/(F)$. This is a domain because $\mathcal{O}[T]$ is a UFD and F is irreducible, so (F) is prime. In either case we have a nonzero prime contained in $\mathfrak{P}$, which equals $\mathfrak{P}$ since $\text{ht } \mathfrak{P} = 1$. ■

Notes. The picture drawn in my notes is the poset of primes of $\mathcal{O}[[T]]$. At the bottom is (0) . In the middle are the height-one primes (ϖ) and (F) , for F irreducible distinguished, e.g. $(F_1), (F_2)$. At the top is $\mathfrak{m} = (\varpi, T)$, of height two.

Notes. Another remark in my notes (partly in Japanese) says that in the end $\mathcal{O}$ will be the ring of integers of a finite extension of K . I understand it as follows: in applications $\mathcal{O}$ is enlarged to contain the values of the characters involved, e.g. $\mathbb{Z}_p[\psi]$ in Part II. The Weierstrass preparation theorem and Corollary 8.3.5 hold for any such $\mathcal{O}$.

8.4 The Iwasawa–Serre isomorphism

Theorem 8.4.1 (Iwasawa–Serre)

Let γ be a topological generator of Γ . Then there exists a unique (non-canonical) isomorphism of topological $\mathcal{O}$ -algebras

$$\mathcal{O}[[\Gamma]] \xrightarrow{\sim} \mathcal{O}[[T]], \quad \gamma \mapsto 1 + T.$$

Notes. “Non-canonical” means that the isomorphism depends on the choice of γ . “Unique” means that, once γ is fixed, there is only one continuous $\mathcal{O}$ -algebra isomorphism with $\gamma \mapsto 1 + T$. Another choice $\gamma' = \gamma^a$, $a \in \mathbb{Z}_p^\times$, changes it by the automorphism $1 + T \mapsto (1 + T)^a$ of $\mathcal{O}[[T]]$.

For $n \geq 0$ let $\omega_n(T) = (1 + T)^{p^n} - 1$ and $\omega_n(\gamma) = \gamma^{p^n} - 1$.

Lemma 8.4.2 (i) ω_n is a distinguished polynomial of degree p^n , $\omega_n \mid \omega_{n+1}$, and $\omega_n \in \mathfrak{m}^{n+1}$.
 (ii) $\mathcal{O}[[\Gamma]]/(\omega_n(\gamma)) \cong \mathcal{O}[\Gamma_n] \cong \mathcal{O}[T]/(\omega_n(T))$, with $\gamma \leftrightarrow 1 + T$.

Correction. My notes write $\mathcal{O}[[\Gamma]]/(\omega_n(\gamma)) \cong \mathbb{Z}/p^n\mathbb{Z}$. The correct statement is $\mathcal{O}[[\Gamma]]/(\omega_n(\gamma)) \cong \mathcal{O}[\Gamma_n]$, the group algebra of $\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$.

Proof. (i) $\omega_n \equiv T^{p^n} \pmod{p}$ (Frobenius), so it is distinguished. We have $\omega_{n+1} = \omega_n \nu_n$ with $\nu_n = \sum_{j=0}^{p-1} (1 + T)^{jp^n}$. Modulo p , $\nu_n \equiv \frac{(1+T^{p^n})^p - 1}{T^{p^n}} \equiv T^{(p-1)p^n}$, so $\nu_n \in (p, T) = \mathfrak{m}$. Since $\omega_0 = T \in \mathfrak{m}$, induction gives $\omega_n \in \mathfrak{m}^{n+1}$.

(ii) The second isomorphism: $\mathcal{O}[\Gamma_n] = \mathcal{O}[X]/(X^{p^n} - 1)$ for the cyclic group Γ_n generated by $X = \bar{\gamma}$, and substitute $X = 1 + T$. For the first one, the kernel of $\mathcal{O}[[\Gamma]] \rightarrow \mathcal{O}[\Gamma_n]$ contains $\omega_n(\gamma)$. Conversely, $\mathcal{O}[[\Gamma]] = \varprojlim_k \mathcal{O}[\Gamma_k]$, and for $k \geq n$ the kernel of $\mathcal{O}[\Gamma_k] \rightarrow \mathcal{O}[\Gamma_n]$ is $\omega_n(\gamma)\mathcal{O}[\Gamma_k]$ (by the same identification with $\mathcal{O}[T]/(\omega_k) \rightarrow \mathcal{O}[T]/(\omega_n)$, $\omega_n \mid \omega_k$). Passing to the limit, using compactness to lift compatible families of preimages, gives the claim. ■

Proof of Theorem 8.4.1. (The lecture sketched exactly this argument.) Consider in $\mathcal{O}[T]$ the two families of ideals

$$I_{m,n} = (\varpi^m, T^n), \quad J_{m,n} = (\varpi^m, \omega_n(T)) \quad (m, n \geq 1).$$

On the one hand, $\mathcal{O}[[T]] = \varprojlim_n \mathcal{O}[T]/(T^n) = \varprojlim_{m,n} \mathcal{O}[T]/(\varpi^m, T^n)$. On the other hand, by Lemma 8.4.2(ii), $\mathcal{O}[T]/J_{m,n} \cong (\mathcal{O}/\varpi^m)[\Gamma_n]$, so

$$\varprojlim_{m,n} \mathcal{O}[T]/J_{m,n} \cong \varprojlim_n \varprojlim_m (\mathcal{O}/\varpi^m)[\Gamma_n] = \varprojlim_n \mathcal{O}[\Gamma_n] = \mathcal{O}[[\Gamma]],$$

with $1 + T \mapsto \gamma$. If we show that the two families are cofinal in each other, then the two inverse limits are canonically isomorphic (as topological rings), and we are done. We can check that:

- (1) for each (m, n) we can find (m', n') with $J_{m',n'} \subseteq I_{m,n}$, i.e. a surjection $\mathcal{O}[T]/J_{m',n'} \twoheadrightarrow \mathcal{O}[T]/I_{m,n}$. Indeed, take $m' = m$ and n' with $n' + 1 \geq m + n$: then $\omega_{n'} \in \mathfrak{m}^{n'+1} \subseteq (\varpi^m, T^n)$, since every monomial $\varpi^a T^b$ with $a + b \geq m + n$ lies in (ϖ^m, T^n) ;
- (2) for each (m', n') we can find (m, n) with $I_{m,n} \subseteq J_{m',n'}$, i.e. a surjection $\mathcal{O}[T]/I_{m,n} \twoheadrightarrow \mathcal{O}[T]/J_{m',n'}$. Indeed, $T^{p^{n'}} \equiv \omega_{n'} \pmod{\varpi}$ gives $T^{p^{n'}} \in (\varpi, \omega_{n'})$, hence $T^{p^{n'}m'} \in (\varpi, \omega_{n'})^{m'} \subseteq (\varpi^{m'}, \omega_{n'})$; take $m = m'$, $n = p^{n'}m'$.

The resulting isomorphism sends γ to $1 + T$. Uniqueness: a continuous $\mathcal{O}$ -algebra homomorphism on $\mathcal{O}[[\Gamma]]$ is determined by the image of γ , because $\mathcal{O}[\langle \gamma \rangle]$ is dense in $\mathcal{O}[[\Gamma]]$. ■

8.5 Measures on Γ : the Iwasawa algebra from the analytic point of view

Definition 8.5.1

A measure μ on Γ with values in $\mathcal{O}$ is an $\mathcal{O}$ -linear function

$$\mu : \{\mathcal{O}\text{-valued locally constant functions on } \Gamma\} \longrightarrow \mathcal{O}.$$

We write $\int_{\Gamma} u(g) d\mu = \mu(u)$ for any such measure μ and any locally constant function u on Γ .

Notes. Since Γ is compact, a locally constant function $u : \Gamma \rightarrow \mathcal{O}$ takes finitely many values and factors through Γ/Γ^{p^n} for some n . Thus $u = \sum_j c_j \mathbf{1}_{g_j \Gamma^{p^n}}$, and μ is determined by the values $\mu(g\Gamma^{p^n}) := \mu(\mathbf{1}_{g\Gamma^{p^n}})$. These are finitely additive: $\mu(g\Gamma^{p^n}) = \sum_{h \in g\Gamma^{p^n}/\Gamma^{p^{n+1}}} \mu(h\Gamma^{p^{n+1}})$. Such a μ is automatically bounded: if $u \in \varpi^k \cdot \{\mathcal{O}\text{-valued}\}$, then $\mu(u) \in \varpi^k \mathcal{O}$.

If $u(g)$ is a continuous $\mathcal{O}$ -valued function on Γ , not necessarily locally constant, then $u(g)$ is uniformly approximated by a sequence of locally constant functions $u_i(g)$ on Γ (e.g. $u_i = u \bmod \varpi^i$, lifted via fixed representatives; it is locally constant by uniform continuity on the compact Γ). We can consider the integral

$$\int_{\Gamma} u(g) d\mu = \lim_{i \rightarrow \infty} \int_{\Gamma} u_i(g) d\mu.$$

Notes. The limit exists and does not depend on the approximating sequence. Indeed, if $u_i - u_j \in \varpi^k \mathcal{O}$ everywhere, then $\int u_i d\mu - \int u_j d\mu \in \varpi^k \mathcal{O}$ by the boundedness above, so the integrals form a Cauchy sequence in the complete ring $\mathcal{O}$.

We denote by $\text{Meas}(\Gamma; \mathcal{O})$ the $\mathcal{O}$ -module of $\mathcal{O}$ -valued measures on Γ .

Notes. My handwritten notes for Part 1 end here. The following two results are the natural continuation: they explain why measures are “the Iwasawa algebra from the analytic point of view”. They are used in Part II, e.g. in the notation $\kappa^{1-r} \phi(L_p(\psi))$.

Proposition 8.5.2

The map $\text{Meas}(\Gamma; \mathcal{O}) \rightarrow \mathcal{O}[[\Gamma]]$,

$$\mu \longmapsto \left(\sum_{g \in \Gamma_n} \mu(g\Gamma^{p^n}) g \right)_{n \geq 0} \in \varprojlim_n \mathcal{O}[\Gamma_n],$$

is an isomorphism of $\mathcal{O}$ -modules. The Dirac measure δ_g ($u \mapsto u(g)$) corresponds to $g \in \Gamma \subset \mathcal{O}[[\Gamma]]$.

Proof. The components are compatible by finite additivity, so the map is well defined; it is clearly $\mathcal{O}$ -linear. Conversely, a compatible family $(\sum_g a_{n,g} g)_n$ defines $\mu(\mathbf{1}_{g\Gamma^{p^n}}) = a_{n,g}$ consistently on all locally constant functions. These constructions are mutually inverse. ■

Under this isomorphism, the multiplication of $\mathcal{O}[[\Gamma]]$ corresponds to convolution of measures.

Proposition 8.5.3

Let $\chi : \Gamma \rightarrow \mathcal{O}^\times$ be a continuous character, let $\mu \in \text{Meas}(\Gamma; \mathcal{O}) = \mathcal{O}[[\Gamma]]$, and let $f_\mu \in \mathcal{O}[[T]]$ be its image under Theorem 8.4.1. Then $\chi(\gamma) - 1 \in \varpi\mathcal{O}$, and

$$\int_{\Gamma} \chi(g) d\mu = f_\mu(\chi(\gamma) - 1).$$

In particular, $\mu \mapsto \int_{\Gamma} \chi d\mu$ is the continuous $\mathcal{O}$ -algebra homomorphism $\mathcal{O}[[\Gamma]] \rightarrow \mathcal{O}$ extending χ .

Proof. Since $\gamma^{p^n} \rightarrow 1$, also $\chi(\gamma)^{p^n} \rightarrow 1$. As $\mathbb{F}_q^\times$ has order prime to p , this forces $\chi(\gamma) \equiv 1 \pmod{\varpi}$. Put $u_n = \chi(\gamma)^{p^n} - 1 \rightarrow 0$. For $y = \gamma^{p^n a} \in \Gamma^{p^n}$, $a \in \mathbb{Z}_p$, we have $\chi(y) - 1 = (1 + u_n)^a - 1 = \sum_{k \geq 1} \binom{a}{k} u_n^k \in u_n \mathcal{O}$. Hence, approximating χ on each coset $g\Gamma^{p^n}$ by its value $\chi(g)$ at a representative,

$$\int_{\Gamma} \chi d\mu \equiv \sum_{g \in \Gamma_n} \chi(g) \mu(g\Gamma^{p^n}) \pmod{u_n \mathcal{O}}.$$

The right-hand side is the image of the n -th component of μ under the ring homomorphism $\mathcal{O}[\Gamma_n] \rightarrow \mathcal{O}/u_n \mathcal{O}$, $g \mapsto \chi(g)$. So $\mu \mapsto \int \chi d\mu$ is a ring homomorphism (a limit of compatible ring homomorphisms, with $\bigcap_n u_n \mathcal{O} = 0$), continuous, and $\gamma \mapsto \chi(\gamma)$. Also $f \mapsto f(\chi(\gamma) - 1)$ is a continuous ring homomorphism $\mathcal{O}[[T]] \rightarrow \mathcal{O}$ (the series converges since $\chi(\gamma) - 1 \in \varpi\mathcal{O}$) with $1 + T \mapsto \chi(\gamma)$. Two continuous $\mathcal{O}$ -algebra homomorphisms agreeing on $\gamma \leftrightarrow 1 + T$ coincide, by density of $\mathcal{O}[\langle \gamma \rangle]$. ■

Part II

Iwasawa Main Conjecture and p -adic Galois Representations

Chapter 9

Iwasawa's Class Number Formula

Throughout Part II, p is an odd prime, $\Lambda = \mathbb{Z}_p[[\Gamma]]$, and for a ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_p$ we write $\Lambda_{\mathcal{O}} = \mathcal{O}[[\Gamma]]$. We identify $\Lambda_{\mathcal{O}} \cong \mathcal{O}[[T]]$ via Theorem 8.4.1, after fixing a topological generator γ .

9.1 The Iwasawa module X_{∞}

Lecture of 29 June 2026.

Let us recall the following theorem (Theorem 6.1.2), now for an arbitrary $\mathbb{Z}_p$ -extension.

Theorem 9.1.1 (Iwasawa's class number formula)

Let K be a finite extension of $\mathbb{Q}$ and K_{∞}/K a $\mathbb{Z}_p$ -extension. Then there exist $\lambda, \mu \in \mathbb{Z}_{\geq 0}$ and $\nu \in \mathbb{Z}$ such that

$$\# \text{Cl}(K_n)[p^{\infty}] = p^{\lambda n + \mu p^n + \nu} \quad \text{for } n \gg 0,$$

where K_n is the unique intermediate field in K_{∞}/K with $[K_n : K] = p^n$ (Lemma 7.1.2).

Let L_{∞} be the maximal unramified abelian p -extension of K_{∞} , and let

$$X_{\infty} = \text{Gal}(L_{\infty}/K_{\infty}), \quad \Gamma = \text{Gal}(K_{\infty}/K).$$

$$\begin{array}{c} L_{\infty} \\ |_{X_{\infty}} \\ K_{\infty} \\ | \\ K_n \\ | \\ K \end{array}$$

Notes. “Maximal unramified abelian p -extension” means: inside a fixed algebraic closure, the compositum of all abelian extensions of K_{∞} of p -power degree that are unramified at all primes. Equivalently, L_{∞} is the union of the maximal unramified abelian p -extensions of the finite subfields K_n , composed with K_{∞} . L_{∞} is Galois over K : any embedding of L_{∞} over K maps K_{∞} to itself, and hence maps L_{∞} to a maximal unramified abelian p -extension of K_{∞} , i.e. to L_{∞} . X_{∞} is an abelian pro- p group, hence a compact $\mathbb{Z}_p$ -module.

By definition, we have the following exact sequence:

$$1 \longrightarrow X_{\infty} \longrightarrow \text{Gal}(L_{\infty}/K) \longrightarrow \Gamma \longrightarrow 1.$$

Let $x \in X_{\infty}$ and $g \in \Gamma$. We define an action $g \cdot x = \hat{g}x\hat{g}^{-1}$, where $\hat{g} \in \text{Gal}(L_{\infty}/K)$ is a lift of $g \in \Gamma$.

Lemma 9.1.2

This action is well defined. Hence X_∞ is a compact $\mathbb{Z}_p$ -module with a continuous action of Γ , and therefore a compact Λ -module.

Proof. Let $\hat{g}'$ be another lift of g . Then there exists $h \in X_\infty$ with $\hat{g}' = \hat{g}h$. Thus

$$\hat{g}'x\hat{g}'^{-1} = (\hat{g}h)x(\hat{g}h)^{-1} = \hat{g}h x h^{-1} \hat{g}^{-1} = \hat{g}x\hat{g}^{-1},$$

since X_∞ is abelian. Continuity is clear. Since $X_\infty = \varprojlim_U X_\infty/U$ over open Γ -stable subgroups U , and on each finite p -group X_∞/U the action factors through some Γ/Γ^{p^n} , the module structures over the $\mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$ assemble to a continuous $\Lambda = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$ -module structure. ■

9.2 The key proposition

From now on, we agree to the following assumptions:

- (a) there exists exactly one prime $\mathfrak{p}$ of K above (p) (i.e. with $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$);
- (b) K_∞/K is totally ramified at $\mathfrak{p}$.

Example 9.2.1. The following satisfy (a) and (b):

- (1) $K_\infty/K = \mathbb{Q}_\infty/\mathbb{Q}$;
- (2) $K_\infty/K = \mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$;
- (3) $K_\infty = K\mathbb{Q}_\infty$, where $K/\mathbb{Q}$ is a quadratic extension such that (p) is inert or ramified in K .

Verification. (1), (2): p is totally ramified in every $\mathbb{Q}(\zeta_{p^n})$ (Proposition 1.3.7), hence in every subfield. (3): (p) has a unique prime $\mathfrak{p}$ above it in K . Since $[K \cap \mathbb{Q}_\infty : \mathbb{Q}]$ divides both 2 and a power of p , $K \cap \mathbb{Q}_\infty = \mathbb{Q}$ and $[K_n : K] = p^n$. The ramification index of p in $K_n = K\mathbb{Q}_n$ is divisible by p^n (from $\mathbb{Q}_n$) and by $e(\mathfrak{p}|p)$, and is at most $[K_n : \mathbb{Q}] = 2p^n$. If p is inert ($e = 1$, $f = 2$), then $f \geq 2$ in K_n forces $e(K_n/\mathbb{Q}) = p^n$. If p ramifies, $e(K_n/\mathbb{Q}) = 2p^n$. In both cases $e(K_n/K) = p^n$, so $\mathfrak{p}$ is totally ramified. ■

Correction. My notes also list “(4) for $p \neq 2$, $K_\infty/K = \mathbb{Q}_\infty K/K$ satisfies (a) and (b)”. This is only true under a hypothesis like (3) on K ; e.g. for a quadratic field in which p splits, (a) fails.

Proposition 9.2.2

Under the assumptions (a) and (b), we have

$$X_\infty/(\gamma^{p^n} - 1)X_\infty \cong \text{Cl}(K_n)[p^\infty],$$

where γ is a fixed topological generator of $\Gamma = \text{Gal}(K_\infty/K)$.

Correction. In the margin of my notes, Γ is annotated as $\text{Gal}(K_\infty/K)$. This is indeed the group here; it is not the group $\text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p))$ of Part I unless $K = \mathbb{Q}(\zeta_p)$.

What was used from “last week”. The lecture refers to “the theorem describing the behaviour of $\#(M/\omega_n(\gamma)M)$ last week”. That lecture is not contained in my notes, so we recall the two results needed ([16, §13.2]). A *pseudo-isomorphism* is a homomorphism of Λ -modules with finite kernel and cokernel.

- *Structure theorem.* A finitely generated $\Lambda_{\mathcal{O}}$ -module M is pseudo-isomorphic to $\Lambda_{\mathcal{O}}^r \oplus \bigoplus_i \Lambda_{\mathcal{O}}/(\varpi^{m_i}) \oplus \bigoplus_j \Lambda_{\mathcal{O}}/(F_j^{n_j})$ with F_j irreducible distinguished polynomials (compare Proposition 8.3.6). If M is torsion ($r = 0$), one defines $\mu(M) = \sum m_i$, $\lambda(M) = \sum n_j \deg F_j$, and the *characteristic ideal* $\text{char}(M) = (\varpi^{\mu(M)} \prod_j F_j^{n_j})$.
- *Growth.* If M is a finitely generated torsion Λ -module with $M/\omega_n M$ finite for all n , then $\#M/\omega_n M = p^{\lambda(M)n + \mu(M)p^n + \nu}$ for $n \gg 0$.

Corollary 9.2.3

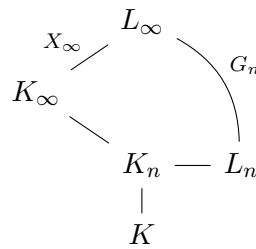
Under (a) and (b), X_{∞} is a finitely generated torsion Λ -module, and Theorem 9.1.1 holds with $\lambda = \lambda(X_{\infty})$, $\mu = \mu(X_{\infty})$.

Proof. Since $\text{Cl}(K)[p^{\infty}]$ is a finite abelian group, Proposition 9.2.2 with $n = 0$ shows that X_{∞}/TX_{∞} is finite, so $X_{\infty}/\mathfrak{m}X_{\infty}$ is finite ($\mathfrak{m} = (p, T)$). By the topological Nakayama lemma for compact Λ -modules [16, Lemma 13.16], X_{∞} is finitely generated. If its rank r were ≥ 1 , then $X_{\infty}/\omega_n X_{\infty}$ would be infinite ($\Lambda/\omega_n \cong \mathbb{Z}_p^n$). So X_{∞} is torsion, and the growth theorem applies. ■

Notes. Without (a) and (b) Theorem 9.1.1 still holds: one replaces ω_n by ω_n/ω_e and X_{∞} by a suitable submodule, for some e beyond which all ramified primes are totally ramified [16, Thm. 13.13].

9.3 Proof of the key proposition

Below, we explain the proof of Proposition 9.2.2. For each $n \geq 0$ let L_n be the maximal unramified abelian p -extension of K_n , and let $G_n = \text{Gal}(L_{\infty}/K_n)$.



By (a) and (b), K_n has a unique prime $\mathfrak{p}_n$ above p , and $\mathfrak{p}_n$ is totally ramified in K_{∞}/K_n . Let $I_n \subseteq G_n$ be the inertia subgroup of a prime of L_{∞} above $\mathfrak{p}_n$.

Notes. $L_n \subseteq L_{\infty}$: $L_n K_{\infty}$ is an unramified abelian p -extension of K_{∞} . By unramified global class field theory (Theorem 1.4.2, restricted to p -parts), $\text{Gal}(L_n/K_n) \cong \text{Cl}(K_n)[p^{\infty}]$. Hence it suffices to show that

$$X_{\infty}/(\gamma^{p^n} - 1)X_{\infty} \cong \text{Gal}(L_n/K_n).$$

Lemma 9.3.1 (i) $I_n \cap X_\infty = \{1\}$, and the restriction $I_n \hookrightarrow G_n \twoheadrightarrow G_n/X_\infty = \text{Gal}(K_\infty/K_n)$ is an isomorphism. Hence $G_n = I_n \ltimes X_\infty$.
 (ii) $\text{Gal}(L_n/K_n) \cong G_n/I_n \overline{[G_n, G_n]}$, where the bar denotes closure.

Proof. (i) $I_n \cap X_\infty$ is the inertia group in L_∞/K_∞ , which is trivial. The image of I_n in $\text{Gal}(K_\infty/K_n)$ is the inertia group of $\mathfrak{p}_n$ in K_∞/K_n , which is everything by total ramification.

(ii) L_n is the largest subextension of L_∞/K_n that is abelian over K_n and unramified at all primes. Being abelian means being fixed by $\overline{[G_n, G_n]}$. Primes not above p are unramified in L_∞/K_n (Theorem 7.3.1(1), and L_∞/K_∞ is unramified). The inertia groups of the primes of L_∞ above $\mathfrak{p}_n$ are the conjugates of I_n ; modulo $\overline{[G_n, G_n]}$ they all coincide with the image of I_n . Hence L_n is the fixed field of $I_n \overline{[G_n, G_n]}$. ■

Lemma 9.3.2

We have the following equality of subgroups of G_n :

$$(\gamma^{p^n} - 1)X_\infty = \overline{[G_n, G_n]}.$$

Proof. Write X_∞ additively, with $g \cdot x = \hat{g}x\hat{g}^{-1}$. Fix a generator σ of I_n (a topological generator lifting γ^{p^n} , by Lemma 9.3.1(i)). Every element of G_n is $\sigma^a x$ with $a \in \mathbb{Z}_p$, $x \in X_\infty$. Put $s = \gamma^{p^n a}$, $t = \gamma^{p^n b}$ (acting on X_∞). A direct computation in the semidirect product gives

$$[\sigma^a x, \sigma^b y] = (s - 1)t \cdot y - (t - 1)s \cdot x \quad (\text{in } X_\infty),$$

and $s - 1 = (1 + \omega_n(\gamma))^a - 1$ lies in $\omega_n(\gamma)\Lambda = (\gamma^{p^n} - 1)\Lambda$ (binomial series), likewise $t - 1$. So $\overline{[G_n, G_n]} \subseteq (\gamma^{p^n} - 1)X_\infty$. The latter is compact (a continuous image of X_∞), hence closed, so it also contains the closure. Conversely $[\sigma, x] = (\gamma^{p^n} - 1)x$. ■

Notes. The lecture proves Lemma 9.3.2 with Galois theory. Put $L'_n = L_\infty^{(\gamma^{p^n} - 1)X_\infty}$ and $L''_n = L_\infty^{\overline{[G_n, G_n]}}$. Then L'_n is the largest intermediate field of L_∞/K_∞ on which γ^{p^n} acts trivially (by conjugation), and L''_n is the largest intermediate field of L_∞/K_∞ which is abelian over K_n . These two descriptions coincide, so $L'_n = L''_n$, and the lemma follows by Galois theory. The computation above is the group-theoretic content of “these descriptions coincide”.

Proof of Proposition 9.2.2. By Lemma 9.3.1(ii) we have

$$\text{Gal}(L_n/K_n) \cong G_n/I_n \overline{[G_n, G_n]}. \quad (1)$$

By Lemma 9.3.2 and $G_n = I_n X_\infty$,

$$G_n/I_n \overline{[G_n, G_n]} = I_n X_\infty / I_n (\gamma^{p^n} - 1)X_\infty \cong X_\infty / (\gamma^{p^n} - 1)X_\infty, \quad (2)$$

where the last isomorphism is induced by $X_\infty \rightarrow G_n$. It is surjective since $G_n = I_n X_\infty$. Its kernel is $X_\infty \cap I_n (\gamma^{p^n} - 1)X_\infty = (\gamma^{p^n} - 1)X_\infty$, because $I_n \cap X_\infty = 1$. Therefore (1) and (2) complete the proof. ■

Chapter 10

The Kubota–Leopoldt p -adic L -function

10.1 Statement and interpolation property

Analytic aspect of Iwasawa theory.

Let N be a positive integer with $(N, p) = 1$. Let

$$\Gamma = \text{Gal}(\mathbb{Q}(\zeta_{Np^\infty})/\mathbb{Q}(\zeta_{Np})) \cong \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}), \quad \chi_{\text{cyc}} : \text{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times$$

(the cyclotomic character). Restricted to Γ , it gives the canonical isomorphism $\kappa = \kappa_{\text{cyc}} : \Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p \subset \mathbb{Q}_p^\times$, and $\chi_{\text{cyc}} = \kappa_{\text{cyc}} \cdot \omega$, with ω the Teichmüller character.

Notes. Notation. For a Dirichlet character ψ , $\mathbb{Z}_p[\psi]$ is the ring generated over $\mathbb{Z}_p$ by the values of ψ (via ι_p); it is the ring of integers of $\mathbb{Q}_p(\psi)$, a DVR. A *finite character* ϕ of Γ is a continuous homomorphism $\phi : \Gamma \rightarrow \overline{\mathbb{Q}_p}^\times$ of finite order. It factors through some Γ/Γ^{p^n} . Via $\text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}) \twoheadrightarrow \Gamma/\Gamma^{p^n}$, we regard ϕ as an even Dirichlet character of p -power conductor. For $\lambda \in \Lambda_{\mathcal{O}}$ and a continuous character $\chi : \Gamma \rightarrow \mathcal{O}^\times$, we write $\chi(\lambda) := \int_{\Gamma} \chi d\lambda$ (Proposition 8.5.3). In particular $\kappa^{1-r}\phi(\lambda)$ is the evaluation of λ at the character $g \mapsto \kappa(g)^{1-r}\phi(g)$; under $\gamma \leftrightarrow 1 + T$ this is $f_{\lambda}(\kappa(\gamma)^{1-r}\phi(\gamma) - 1)$.

Theorem 10.1.1 (Kubota–Leopoldt, Iwasawa, Coleman)

Let ψ be an even Dirichlet character of conductor Np^e ($e = 0$ or 1), i.e. $\psi(-1) = 1$. Then there exists a unique

$$L_p(\psi) \in \begin{cases} \mathbb{Z}_p[\psi][[\Gamma]], & \psi \neq \mathbf{1}, \\ \frac{1}{\gamma - \kappa(\gamma)} \mathbb{Z}_p[[\Gamma]], & \psi = \mathbf{1}, \end{cases}$$

such that, for every $r \in \mathbb{Z}_{\geq 1}$ and every finite character ϕ of Γ ,

$$\kappa^{1-r}\phi(L_p(\psi)) = \left(1 - \frac{(\psi\omega^{-r}\phi^{-1})(p)}{p^{1-r}}\right) L(\psi\omega^{-r}\phi^{-1}, 1-r), \quad (\star)$$

where $L(\eta, s)$ is the Dirichlet L -function of the primitive character η (Chapter 4).

Notes. (a) Uniqueness follows from the “coincidence theorem” on the Iwasawa algebra, i.e. from Corollary 8.3.5. If two candidates differ by δ , then for $\psi \neq \mathbf{1}$, $\delta \in \Lambda_{\mathcal{O}}$ vanishes at the infinitely many distinct points $\kappa(\gamma)^{1-r} - 1$ ($r \geq 1$) of the open unit disc, so $\delta = 0$. For $\psi = \mathbf{1}$ apply this to $(\gamma - \kappa(\gamma))\delta$, and use that Λ is a domain. (b) The denominator $\gamma - \kappa(\gamma)$ reflects the pole of $\zeta(s)$: the character κ^{1-r} sends it to $\kappa(\gamma)^{1-r} - \kappa(\gamma)$, which vanishes exactly at $r = 0$, i.e. at “ $s = 1$ ”. (c) With $N = 1$ and $\psi = \omega^{1-i}$ (i odd), $\phi = \mathbf{1}$ and $r \equiv 1 - i \pmod{p-1}$, the right side of $(\star)$ is $(1 - p^{r-1})\zeta(1-r)$. So $\zeta_p^{(i)}(x) = f_{L_p(\omega^{1-i})}(x-1)$ recovers Theorem 6.2.1 when $\kappa(\gamma) = 1 + p$.

Recall: let η be a Dirichlet character and $L(\eta, s)$ the associated Dirichlet L -function, $L(\eta, s) = \sum_{n \geq 1} \eta(n)n^{-s}$ on $\text{Re}(s) > 1$. Then (Theorem 4.4.4, Proposition 4.3.2):

- $L(\eta, 1-r) = -\frac{1}{r}B_{r,\eta} \in \mathbb{Q}(\eta)$ for any $r \in \mathbb{Z}_{\geq 1}$;
- for primitive $\eta \neq \mathbb{1}$, $L(\eta, 1-r) \neq 0 \iff (-1)^r = \eta(-1)$. (“ $\Leftarrow$ ”: by the functional equation, $L(\eta, 1-r)$ is a nonzero multiple of $L(\bar{\eta}, r) \neq 0$; for $\eta = \mathbb{1}$: $\zeta(1-r) \neq 0 \iff r$ even.)

Correction. My notes then say “hence the RHS of $(\star)$ is nonzero for all $r \geq 1$ ”. The L -value is indeed nonzero: ϕ and ψ are even, so $\eta = \psi\omega^{-r}\phi^{-1}$ satisfies $\eta(-1) = (-1)^r$. But the Euler factor $1 - \eta(p)p^{r-1}$ vanishes if $r = 1$ and $\eta(p) = 1$ (this can happen when η has conductor prime to p : an “exceptional zero”). So the correct statement is: the RHS is nonzero except possibly for $r = 1$ and $\eta(p) = 1$.

Notes. On the Euler factor. Write $\eta = \psi\omega^{-r}\phi^{-1}$. If ϕ has order p^n with $n \geq 1$, then ϕ has conductor $p^{n+1} \geq p^2$, while $\psi\omega^{-r}$ has p -part of conductor $\leq p$. So η has conductor divisible by p^2 and $\eta(p) = 0$: the Euler factor is 1. (My notes: “conductor of $\eta\eta'$ divides $\text{lcm}(N, N')$; $n \geq 2 \Rightarrow$ the conductor of $\psi^{-1}\omega^{-r}\phi$ is divisible by $p^n \Rightarrow (\psi^{-1}\omega^{-r}\phi)(p) = 0$.”) For $\phi = 1$ the factor is $1 - (\psi\omega^{-r})(p)p^{r-1}$, which removes the Euler factor at p .

10.2 Generalised Bernoulli numbers modulo p -powers

Let us recall that we defined the generalised Bernoulli numbers $B_{r,\eta}$ by

$$\sum_{i=1}^M \frac{\eta(i) z e^{iz}}{e^{Mz} - 1} = \sum_{r=0}^{\infty} B_{r,\eta} \frac{z^r}{r!}$$

for a character η of modulus M . If η is regarded as a character of modulus M (not necessarily its conductor), we write $B_{r,\eta}^{(M)}$ for the resulting number. Then $L(\eta_M, 1-r) = -\frac{1}{r}B_{r,\eta}^{(M)}$ for the imprimitive L -function (Theorem 4.4.4), so by (4.1)

$$B_{r,\eta}^{(M)} = B_{r,\eta_0} \prod_{\ell|M} (1 - \eta_0(\ell)\ell^{r-1}). \quad (10.1)$$

Correction. In my notes the conductor of ψ is written under “ $e^{Nz} - 1$ ”. The denominator involves the *modulus* used in the sum, which must match the upper limit of summation.

Lemma 10.2.1 (Key fact)

Let $q_n = Np^{n+1}$ and let η be a Dirichlet character of modulus q_n with $\eta(-1) = (-1)^r$. Then, in $\mathbb{Z}_p[\eta]$,

$$B_{r,\eta}^{(q_n)} \equiv \frac{1}{q_n} \sum_{i=1}^{q_n} \eta(i) i^r \pmod{p^n}.$$

Proof. With the Bernoulli polynomials $\frac{ze^{xz}}{e^z - 1} = \sum_r B_r(x) \frac{z^r}{r!}$ we get, substituting $z \mapsto qz$, $B_{r,\eta}^{(q)} = q^{r-1} \sum_{i=1}^q \eta(i) B_r(i/q)$. With $B_r(x) = \sum_j \binom{r}{j} B_j x^{r-j}$:

$$B_{r,\eta}^{(q)} = \frac{1}{q} \sum_i \eta(i) i^r - \frac{r}{2} \sum_i \eta(i) i^{r-1} + \sum_{j \geq 2} \binom{r}{j} B_j q^{j-1} \sum_i \eta(i) i^{r-j}.$$

Pairing $i \leftrightarrow q - i$ and using $\eta(-1) = (-1)^r$ shows $\sum_i \eta(i) i^{r-1} \equiv 0 \pmod{q}$ (2 is a unit). For $j \geq 2$, $pB_j \in \mathbb{Z}_p$ (von Staudt–Clausen), so the j -th term lies in $q^{j-1}p^{-1}\mathbb{Z}_p[\eta] \subseteq p^n\mathbb{Z}_p[\eta]$. ■

Notes. This is the precise form of the “Key fact” of the lecture, which is stated there modulo “ q_n/p ” (i.e. modulo p^n , as N is a unit). The parity assumption is satisfied in all cases used below. The motivation in the lecture: the power sums $1^r + 2^r + \cdots + n^r$ are described by Bernoulli numbers (Faulhaber’s formula).

10.3 Stickelberger elements and the construction of $L_p(\psi)$

We denote by $\langle \cdot \rangle$ the projection $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p) \rightarrow 1 + p\mathbb{Z}_p$, so $\langle i \rangle = i\omega^{-1}(i)$. For $i \in \mathbb{Z}$ with $(i, p) = 1$ we denote by $\gamma(i) \in \Gamma$ the element $\kappa^{-1}(\langle i \rangle)$, so $\kappa(\gamma(i)) = \langle i \rangle = i\omega^{-1}(i)$. Let $\gamma_n(i)$ be its image under $\Gamma \rightarrow \Gamma_n = \Gamma/\Gamma^{p^n}$; it only depends on $i \bmod p^{n+1}$.

Definition 10.3.1

We define the *Stickelberger element* $\Xi_n(\psi) \in \mathbb{Q}_p(\psi)[\Gamma_n]$ by

$$\Xi_n(\psi) = -\frac{1}{q_n} \sum_{\substack{i=1 \\ (i,p)=1}}^{q_n} \langle i \rangle \psi(i) \gamma_n(i)^{-1}.$$

Lemma 10.3.2

Let ψ be even of conductor Np^e ($e \leq 1$), and put $c = 1 + Np$. Then:

- (1) $(\gamma_n(c) - c) \Xi_n(\psi) \in \mathbb{Z}_p[\psi][\Gamma_n]$;
- (2) if $\psi \neq \mathbf{1}$, then $\Xi_n(\psi) \in \mathbb{Z}_p[\psi][\Gamma_n]$;
- (3) $\Xi_{n+1}(\psi)$ is mapped to $\Xi_n(\psi)$ by $\mathbb{Q}_p(\psi)[\Gamma_{n+1}] \rightarrow \mathbb{Q}_p(\psi)[\Gamma_n]$. That is, $\{\Xi_n(\psi)\}_n$ is a projective system.

Proof. (The lecture omitted the proof.) Let $q = q_n$.

A general identity. Let $c \in \mathbb{Z}$ with $(c, Np) = 1$. As j runs over $1 \leq j \leq q$, $(j, p) = 1$, so does the representative $i \in [1, q]$ of $cj \bmod q$; write $cj = i + qt_j$ with $t_j \in \mathbb{Z}$. Then $\psi(i) = \psi(c)\psi(j)$, $\omega(i) = \omega(c)\omega(j)$, $\gamma_n(i) = \gamma_n(c)\gamma_n(j)$ (as $\langle i \rangle \equiv \langle c \rangle \langle j \rangle \bmod p^{n+1}$), and $\langle i \rangle = \omega^{-1}(c)\omega^{-1}(j)(cj - qt_j)$. Substituting into Ξ_n and using $c\omega^{-1}(c) = \langle c \rangle$:

$$\Xi_n = \psi(c)\langle c \rangle \gamma_n(c)^{-1} \Xi_n + \psi(c)\omega^{-1}(c)\gamma_n(c)^{-1} \sum_j (\psi\omega^{-1})(j) t_j \gamma_n(j)^{-1},$$

$$\text{i.e.} \quad (\gamma_n(c) - \psi(c)\langle c \rangle) \Xi_n = \psi(c)\omega^{-1}(c) \Theta_n(c), \quad \Theta_n(c) := \sum_j (\psi\omega^{-1})(j) t_j \gamma_n(j)^{-1} \in \mathbb{Z}_p[\psi][\Gamma_n]. \quad (10.2)$$

(1) For $c = 1 + Np$ we have $\psi(c) = 1$ (as $c \equiv 1 \bmod Np$), $\omega(c) = 1$ and $\langle c \rangle = c$.

(2) $\mathbb{Z}_p[\psi][\Gamma_n] \cong \mathbb{Z}_p[\psi][T]/(\omega_n)$ is local with maximal ideal (π, T) , and $\gamma_n(c) - \psi(c)\langle c \rangle \equiv 1 - \psi(c)$ modulo it. If some value $\psi(c)$ is a root of unity of order not a power of p (in particular if $\psi \neq \mathbf{1}$ has order prime to p), then $1 - \psi(c)$ is a unit, and (10.2) shows $\Xi_n \in \mathbb{Z}_p[\psi][\Gamma_n]$. For $\psi \neq \mathbf{1}$ of p -power order a finer argument is needed; see [16, Thm. 7.10 and §12.2].

(3) Group the $i \bmod q_{n+1}$ by their residue $i \bmod q_n$: $i' = i + kq_n$, $0 \leq k < p$. Then $\psi(i') = \psi(i)$ (the conductor of ψ divides q_n), $\omega(i') = \omega(i)$ and $\gamma_n(i') = \gamma_n(i)$, while $\sum_k \langle i + kq_n \rangle = \omega^{-1}(i)(pi +$

$q_n^{\frac{p(p-1)}{2}}$). Hence the image of Ξ_{n+1} is

$$\Xi_n - \frac{p-1}{2} \sum_i (\psi\omega^{-1})(i) \gamma_n(i)^{-1}.$$

Since ψ is even, $\psi\omega^{-1}$ is odd, while $\gamma_n(-i) = \gamma_n(i)$ ($\langle -i \rangle = \langle i \rangle$). So the terms for i and $q_n - i$ cancel, and the last sum is 0. ■

Notes. This is where the hypothesis $\psi(-1) = 1$ enters: it makes the Stickelberger elements compatible.

By admitting this lemma, we define

$$L_p(\psi) = \varprojlim_n \Xi_n(\psi) \in \begin{cases} \mathbb{Z}_p[\psi][[\Gamma]], & \psi \neq \mathbb{1}, \\ \frac{1}{\gamma(c) - c} \mathbb{Z}_p[[\Gamma]], & \psi = \mathbb{1}. \end{cases}$$

Precisely, $\Theta(c) := \varprojlim_n (\gamma_n(c) - c) \Xi_n \in \Lambda_{\mathcal{O}}$ (compatible by (3)), and $L_p(\psi) := \Theta(c)/(\gamma(c) - c)$ in the fraction field of $\Lambda_{\mathcal{O}}$. It lies in $\Lambda_{\mathcal{O}}$ when $\psi \neq \mathbb{1}$, by (2).

Notes. For $N = 1$ we have $c = 1 + p$. If γ is chosen with $\kappa(\gamma) = 1 + p$, then $\gamma(c) = \gamma$, so the denominator $\gamma(c) - c = \gamma - \kappa(\gamma)$ agrees with Theorem 10.1.1 (which my notes write as $\kappa_{\text{cyc}}(\gamma) - \gamma$, the same up to sign).

10.4 The interpolation property

Proposition 10.4.1

The element $L_p(\psi)$ satisfies $(\star)$. Hence Theorem 10.1.1 holds (for $\psi \neq \mathbb{1}$ of p -power order modulo the integrality quoted in Lemma 10.3.2(2)).

Correction. The sketch in my notes evaluates Ξ_n directly: “ $\kappa^{1-r}\phi(L_p(\psi)) = \lim(\kappa_n^{1-r}\phi)\Xi_n \equiv -\frac{1}{rq_n} \sum \psi\omega^{-r}\phi^{-1}(i)i^r$ ”. A direct evaluation of Ξ_n gives $-\frac{1}{q_n} \sum \psi\omega^{-r}\phi^{-1}(i)i^r$, *without* the factor $1/r$. Moreover, because of the denominator $1/q_n$, the congruence obtained this way only holds modulo a bounded power of p , so one cannot pass to the limit. The factor $1/r$ appears through the regularised elements $\Theta_n(c)$, as follows.

Proof. Fix $r \geq 1$ and ϕ , put $\eta = \psi\omega^{-r}\phi^{-1}$ (of modulus q_n for n large), $\chi = \kappa^{1-r}\phi$ and $u_n = \chi(\gamma)^{p^n} - 1 \rightarrow 0$. Let $c = 1 + Np$. Since $\Theta_n(c)$ is integral, the ring homomorphism $\mathcal{O}[\Gamma_n] \rightarrow \mathcal{O}/u_n$, $g \mapsto \chi(g)$ (proof of Proposition 8.5.3), gives

$$\chi(\Theta(c)) \equiv \sum_j (\psi\omega^{-1})(j) t_j \chi(\gamma(j))^{-1} = \sum_j \eta(j) t_j j^{r-1} \pmod{u_n},$$

since $\chi(\gamma(j))^{-1} = \langle j \rangle^{r-1} \phi^{-1}(j)$ and $\omega^{-1}(j) \langle j \rangle^{r-1} = \omega^{-r}(j) j^{r-1}$. Now compute $\sum_j \eta(j) (cj)^r$ in two ways. Since $j \mapsto i$ is a permutation and $\eta(j) = \eta(c)^{-1} \eta(i)$,

$$\sum_j \eta(j) (cj)^r - \eta(c)^{-1} \sum_i \eta(i) i^r = \sum_j \eta(j) [(i + qt_j)^r - i^r] \equiv rq c^{r-1} \sum_j \eta(j) j^{r-1} t_j \pmod{q^2}$$

(using $i \equiv cj \pmod{q}$). The left side is $(c^r - \eta(c)^{-1}) \sum_j \eta(j) j^r$. By Lemma 10.2.1 (note $\eta(-1) = (-1)^r$), $\sum_j \eta(j) j^r \equiv q B_{r,\eta}^{(q)} \pmod{qp^n}$. Dividing by $r q c^{r-1}$:

$$\sum_j \eta(j) j^{r-1} t_j \equiv \frac{(c^r - \eta(c)^{-1})}{r c^{r-1}} B_{r,\eta}^{(q)} \pmod{p^{n-v_p(r)}}.$$

Here $\eta(c)^{-1} = \phi(c)$, since $\psi(c) = \omega(c) = 1$. On the other side, $\chi(\gamma(c) - c) = c^{1-r} \phi(c) - c = -c^{1-r}(c^r - \phi(c))$, which is nonzero for $r \geq 1$ (c^r is not a root of unity). Letting $n \rightarrow \infty$ and dividing,

$$\chi(L_p(\psi)) = \frac{\chi(\Theta(c))}{\chi(\gamma(c) - c)} = \frac{(c^r - \phi(c)) B_{r,\eta}^{(q)}}{r c^{r-1}} \cdot \frac{-1}{c^{1-r}(c^r - \phi(c))} = -\frac{1}{r} B_{r,\eta}^{(q)}.$$

Finally, by (10.1), $-\frac{1}{r} B_{r,\eta}^{(q_n)} = (1 - \eta_0(p) p^{r-1}) L(\eta_0, 1 - r)$. The only prime dividing q_n but not the conductor of η_0 can be p , because the N -part of the conductor of ψ is all of N . This is $(\star)$. ■

Example 10.4.2. Take $p = 3$, $N = 5$, $\psi = (\frac{\cdot}{5})$ (even, of conductor 5), $n = 0$, so $q_0 = 15$ and $\Gamma_0 = 1$. A direct computation gives

$$\Xi_0(\psi) = -\frac{1}{15}(1 + 2 + 4 - 7 + 8 - 11 - 13 - 14) = 2.$$

For $r = 2$, $\phi = 1$: $\eta = \psi \omega^{-2} = \psi$, $B_{2,\psi} = \frac{4}{5}$, and the right side of $(\star)$ is $-\frac{1}{2}(1 - \psi(3) \cdot 3) B_{2,\psi} = -\frac{8}{5}$. Since $u_0 = \kappa(\gamma)^{-1} - 1$ has valuation 1, the prediction is $2 \equiv -\frac{8}{5} \pmod{3}$, which is true: $-8 \cdot 5^{-1} \equiv -8 \cdot 2 \equiv 2 \pmod{3}$. The version without $1/r$ would give $-\frac{16}{5} \equiv 1 \pmod{3}$, which is not congruent to 2.

Chapter 11

The Iwasawa Main Conjecture

11.1 Setting

We go back again to the algebraic side of Iwasawa theory for ideal class groups.

- (1) Let us fix a positive integer N with $(N, p) = 1$.
- (2) Let ψ be an even Dirichlet character of conductor Np^e ($e = 0$ or 1).
- (3) We set $K = \mathbb{Q}(\zeta_{Np})$, so $\Delta := \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/Np\mathbb{Z})^\times$.
- (4) Let $K_\infty^{\text{cyc}} = \mathbb{Q}(\zeta_{Np^\infty})$ be the cyclotomic $\mathbb{Z}_p$ -extension of K .
- (5) Let $\Gamma = \text{Gal}(K_\infty^{\text{cyc}}/K)$.
- (6) Let L_∞ be the maximal unramified abelian p -extension of K_∞^{cyc} .
- (7) We set $X_\infty^{\text{cyc}} = \text{Gal}(L_\infty/K_\infty^{\text{cyc}})$.

$$\begin{array}{c} L_\infty \\ | X_\infty^{\text{cyc}} \\ K_\infty^{\text{cyc}} \\ | \Gamma \\ \mathbb{Q} \xrightarrow{\Delta} K \end{array}$$

Correction. In my notes, item (6) calls the maximal unramified abelian p -extension “ Γ_∞ ”; it is L_∞ , as in item (7).

Notes. $\text{Gal}(K_\infty^{\text{cyc}}/\mathbb{Q}) \cong (\mathbb{Z}/Np\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) = \Delta \times \Gamma$ canonically, so Δ acts on X_∞^{cyc} (by conjugation, as in Chapter 9), commuting with Γ . Recall that X_∞^{cyc} is a finitely generated torsion Λ -module. For $K = \mathbb{Q}(\zeta_{Np})$ assumption (a) of Chapter 9 may fail when $N > 1$, and the general version is [16, Thm. 13.31].

Definition 11.1.1

For a character η of Δ and a $\mathbb{Z}_p[\Delta]$ -module M , M_η denotes the largest quotient of M on which Δ acts by η , i.e. $M_\eta = M \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p[\eta]$, where Δ acts on $\mathbb{Z}_p[\eta]$ through η . In particular we define $(X_\infty^{\text{cyc}})_{\omega\psi^{-1}}$ to be the largest quotient of X_∞^{cyc} on which $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/Np\mathbb{Z})^\times$ acts by $\omega\psi^{-1}$: g acts as multiplication by $\omega\psi^{-1}(g)$.

Notes. If $p \nmid |\Delta|$, then M_η is also the η -eigenspace, cut out by an idempotent as in Proposition 5.4.1. In general (when $p \mid \varphi(N)$) the quotient is the correct notion. Note that $\omega\psi^{-1}$ is odd. In one place my notes write $(X_\infty^{\text{cyc}})_{\psi\omega^{-1}}$; this should be $(X_\infty^{\text{cyc}})_{\omega\psi^{-1}}$ throughout.

Then, it is easy to see that $(X_\infty^{\text{cyc}})_{\omega\psi^{-1}}$ is a finitely generated torsion $\mathbb{Z}_p[\psi][[\Gamma]]$ -module. (It is a quotient of $X_\infty^{\text{cyc}} \otimes \mathbb{Z}_p[\psi]$.)

11.2 The $(-)$ -version

Theorem 11.2.1 (Iwasawa main conjecture, $(-)$ -version; Mazur–Wiles)

For every even Dirichlet character ψ of conductor Np^e ($e = 0, 1$) we have

$$\text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}(X_\infty^{\text{cyc}})_{\omega\psi^{-1}} = \begin{cases} (L_p(\psi)), & \psi \neq \mathbb{1}, \\ ((\kappa_{\text{cyc}}(\gamma) - \gamma)L_p(\psi)), & \psi = \mathbb{1}. \end{cases}$$

Notes. char is the characteristic ideal defined in Chapter 9 (structure theorem). For $\psi = \mathbb{1}$ the left side concerns X_ω , and the pole of $L_p(\mathbb{1})$ is removed by the factor $\kappa_{\text{cyc}}(\gamma) - \gamma$. In fact $X_\omega = 0$, consistent with $(\kappa(\gamma) - \gamma)L_p(\mathbb{1})$ being a unit. Comparing λ -invariants and using Corollary 8.3.5 gives the counting statement of Theorem 6.3.2.

11.3 The module $\mathfrak{X}_\infty^{\text{cyc}}$ and the $(+)$ -version

Let M_∞ be the maximal abelian p -extension of K_∞^{cyc} unramified outside p , and define

$$\mathfrak{X}_\infty^{\text{cyc}} = \text{Gal}(M_\infty/K_\infty^{\text{cyc}}).$$

$$\mathfrak{X}_\infty^{\text{cyc}} \begin{pmatrix} M_\infty \\ | \\ L_\infty \\ | \\ K_\infty^{\text{cyc}} \\ | \Gamma \\ K \end{pmatrix}$$

By the same argument as for X_∞^{cyc} , $\mathfrak{X}_\infty^{\text{cyc}}$ is a compact $\mathbb{Z}_p[[\Gamma]]$ -module.

Proposition 11.3.1

$\mathfrak{X}_\infty^{\text{cyc}}/(\gamma - 1)\mathfrak{X}_\infty^{\text{cyc}}$ is a finitely generated $\mathbb{Z}_p$ -module (but not finite). By Nakayama's lemma, $\mathfrak{X}_\infty^{\text{cyc}}$ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$ -module, but not a torsion one. For a Dirichlet character η modulo Np , $(\mathfrak{X}_\infty^{\text{cyc}})_\eta$ is torsion over $\mathbb{Z}_p[[\Gamma]]$ iff $\eta(-1) = 1$.

Proof sketch. (No proof in the lecture.) $\mathfrak{X}_\infty^{\text{cyc}}/(\gamma - 1)$ surjects with finite kernel onto the Galois group of the maximal abelian pro- p extension of K unramified outside p . That group has $\mathbb{Z}_p$ -rank $r_2(K) + 1$, since Leopoldt holds for the abelian field K (Theorem 7.2.2 and Brumer), and this is finite but positive. More precisely, Iwasawa showed that $\text{rank}_\Lambda \mathfrak{X}_\infty^{\text{cyc}} = r_2(K)$, and that the rank is concentrated in the odd η -parts, each of rank one [16, §13.5]. ■

Correction. My notes say $\mathfrak{X}/(\gamma - 1)\mathfrak{X}$ is a finitely generated $\mathbb{Z}_p[[\Gamma]]$ -module. It is finitely generated over $\mathbb{Z}_p$, which is what Nakayama's lemma needs.

For any $\mathbb{Z}_p[[\Gamma]]$ -module M , we denote by

- M^* the module M whose Γ -action is twisted by the involution $\Gamma \rightarrow \Gamma$, $g \mapsto g^{-1}$;
- $M \otimes \kappa_{\text{cyc}}$ the module M whose action is twisted by $\gamma \mapsto \kappa_{\text{cyc}}(\gamma)\gamma$.

For example, writing $M_\chi = M/(\chi(\gamma) - \gamma)M$ for a character χ of Γ :

$$(M^*)_{\kappa_{\text{cyc}}} = M^*/(\kappa_{\text{cyc}}(\gamma) - \gamma)M^* = M/(\kappa_{\text{cyc}}(\gamma) - \gamma^{-1})M = M_{\kappa_{\text{cyc}}^{-1}}, \quad (M \otimes \kappa_{\text{cyc}})_{\kappa_{\text{cyc}}^r} = M_{\kappa_{\text{cyc}}^{r-1}}.$$

Correction. For the first example: $\kappa(\gamma) - \gamma^{-1} = \gamma^{-1}\kappa(\gamma)(\gamma - \kappa(\gamma)^{-1})$ and $\gamma^{-1}\kappa(\gamma)$ is a unit, which gives the last equality. For the second: γ acts on $M \otimes \kappa$ as $\kappa(\gamma)\gamma$, so $\kappa(\gamma)^r - \kappa(\gamma)\gamma = \kappa(\gamma)(\kappa(\gamma)^{r-1} - \gamma)$, and with the twist $\gamma \mapsto \kappa(\gamma)\gamma$ one gets $(M \otimes \kappa_{\text{cyc}})_{\kappa_{\text{cyc}}^r} = M_{\kappa_{\text{cyc}}^{r-1}}$. My notes have $M_{\kappa^{r+1}}$, which corresponds to the opposite convention $\gamma \mapsto \kappa(\gamma)^{-1}\gamma$. The point is only that twisting by κ shifts the evaluation point by one power of κ .

Theorem 11.3.2 (Iwasawa main conjecture, (+)-version; Rubin)

For any even Dirichlet character ψ of conductor Np^e ($e = 0$ or 1),

$$\text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}(\mathfrak{X}_\infty^{\text{cyc}})_\psi^* \otimes \kappa_{\text{cyc}} = \begin{cases} (L_p(\psi)), & \psi \neq \mathbb{1}, \\ ((\kappa_{\text{cyc}}(\gamma) - \gamma)L_p(\psi)), & \psi = \mathbb{1}. \end{cases}$$

Correction. In my notes the subscript of char is $\mathbb{Z}_p[\psi]$; it should be the Iwasawa algebra $\mathbb{Z}_p[\psi][[\Gamma]]$.

11.4 Equivalence of the two versions via the Kummer pairing

Proposition 11.4.1

For any even Dirichlet character ψ of conductor Np or N , we have

$$\text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}(\mathfrak{X}_\infty^{\text{cyc}})_\psi^* \otimes \kappa_{\text{cyc}} = \text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}(X_\infty^{\text{cyc}})_{\psi^{-1}\omega}.$$

That is, the Iwasawa main conjecture ((-)-version) for ψ holds iff the Iwasawa main conjecture ((+)-version) for ψ holds.

Proof sketch. (As in the lecture.) Since $\mu_{p^\infty} \subset K_\infty^{\text{cyc}}$, Kummer theory describes M_∞ as $K_\infty^{\text{cyc}}(\sqrt[p^\infty]{\mathcal{A}})$ for a suitable group $\mathcal{A}$ of p -units, and yields the “Kummer pairing”

$$(\mathfrak{X}_\infty^{\text{cyc}})_\psi \times \text{Cl}(K_\infty^{\text{cyc}})[p^\infty]^{\psi^{-1}\omega} \longrightarrow \mu_{p^\infty},$$

between a compact $\mathbb{Z}_p$ -module and a discrete $\mathbb{Z}_p$ -module. Here μ_{p^∞} is the group of p -power roots of unity, and $\text{Cl}(K_\infty^{\text{cyc}})[p^\infty] = \varinjlim_n \text{Cl}(K_n)[p^\infty]$. The pairing is equivariant w.r.t. the action of Γ , where Γ acts on μ_{p^∞} through κ_{cyc} . Up to finite modules, it gives an isomorphism of $\mathbb{Z}_p[\psi][[\Gamma]]$ -modules

$$(\mathfrak{X}_\infty^{\text{cyc}})_\psi \cong \left(\text{Cl}(K_\infty^{\text{cyc}})[p^\infty]^{\psi^{-1}\omega} \right)^\vee \otimes \kappa_{\text{cyc}},$$

where $^\vee$ is the Pontryagin dual. We also have Iwasawa’s theorem relating the inverse and direct limits of class groups:

$$\text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}(\text{Cl}(K_\infty^{\text{cyc}})[p^\infty]^{\psi^{-1}\omega})^\vee = \text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}((X_\infty^{\text{cyc}})_{\psi^{-1}\omega})^*.$$

Combining (and noting $(M^*)^* = M$) gives the proposition. Details: [16, §15.4–15.5]. ■

Notes. The Pontryagin dual of a discrete (or compact) abelian group A is $A^\vee = \text{Hom}_{\text{cont}}(A, \mathbb{Q}_p/\mathbb{Z}_p)$, with Γ acting by $(gf)(a) = f(g^{-1}a)$. This inversion of the action is why the involution $*$ appears.

11.5 λ - and μ -invariants and the analytic class number formula

Lecture of 13 July 2026. Recall: the Iwasawa main conjecture ((-)-version) for ψ holds iff the ((+)-version) for ψ holds (Proposition 11.4.1). For $0 \neq f \in \Lambda_{\mathcal{O}}$ we write $\lambda(f), \mu(f)$ for the invariants of Theorem 8.3.2 (with μ normalised so that $\mu(p) = 1$).

Theorem 11.5.1 (Analytic class number formula, Iwasawa-theoretic form)

Let N be a positive integer with $(N, p) = 1$ and $K = \mathbb{Q}(\zeta_{Np})$. Then

$$\sum_{\psi} \lambda((X_{\infty}^{\text{cyc}})_{\omega\psi-1}) = \sum_{\psi} \lambda(L_p(\psi)), \quad \sum_{\psi} \mu((X_{\infty}^{\text{cyc}})_{\omega\psi-1}) = \sum_{\psi} \mu(L_p(\psi)),$$

where ψ runs through the nontrivial even Dirichlet characters with conductor N or Np . Similar statements hold for $\lambda((\mathfrak{X}_{\infty}^{\text{cyc}})_{\psi}^* \otimes \kappa_{\text{cyc}})$ and $\mu((\mathfrak{X}_{\infty}^{\text{cyc}})_{\psi}^* \otimes \kappa_{\text{cyc}})$.

Proof sketch. The proof reduces to the classical analytic class number formula for $\zeta(K, s)$ explained in the first-quarter lecture (Theorem 3.5.1, in the form of Theorem 5.3.1). For the layers $K_n = \mathbb{Q}(\zeta_{Np^{n+1}})$, the relative class number is $h^-(K_n) = Q_n w_n \prod_{\chi \text{ odd}} (-\frac{1}{2} B_{1, \chi})$, the product over the odd characters of $\text{Gal}(K_n/\mathbb{Q})$, with $Q_n \in \{1, 2\}$ [16, Thm. 4.17]. Every odd χ can be written as $\chi = \psi\omega^{-1}\phi^{-1}$ with ψ even of conductor N or Np and ϕ a finite character of Γ of order dividing p^n . By Proposition 10.4.1 with $r = 1$, $-B_{1, \chi} = (1 - \chi(p))^{-1} \phi(L_p(\psi))$, up to the harmless Euler factor. For $f \in \Lambda_{\mathcal{O}}$ and ζ a primitive p^m -th root of unity with m large, Theorem 8.3.2 gives $v_p(f(\zeta - 1)) = \mu(f) + \lambda(f)/(p^{m-1}(p-1))$. Summing over the $p^m - p^{m-1}$ such ζ and over $m \leq n$ shows

$$v_p(h^-(K_n)) = \left(\sum_{\psi} \lambda(L_p(\psi)) \right) n + \left(\sum_{\psi} \mu(L_p(\psi)) \right) p^n + O(1).$$

On the other hand, by the growth theorem of Chapter 9 applied to the minus parts, $v_p(h^-(K_n)) = (\sum_{\psi} \lambda(X_{\omega\psi-1}))n + (\sum_{\psi} \mu(X_{\omega\psi-1}))p^n + O(1)$. Comparing coefficients gives the theorem. See [16, §7.4, §13.6]. ■

By using this analytic class number formula, it suffices to prove either (A) or (B):

- (A) show $\text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}((X_{\infty}^{\text{cyc}})_{\omega\psi-1}) \subseteq (L_p(\psi))$ for every even Dirichlet character $\psi \neq 1$ with conductor N or Np ;
- (B) show $\text{char}_{\mathbb{Z}_p[\psi][[\Gamma]]}((X_{\infty}^{\text{cyc}})_{\omega\psi-1}) \supseteq (L_p(\psi))$ for every such ψ ; i.e. X_{∞}^{cyc} is “small enough” compared to $L_p(\psi)$.

For (B) it is equivalent to show $\lambda((X_{\infty}^{\text{cyc}})_{\omega\psi-1}) \leq \lambda(L_p(\psi))$ and $\mu((X_{\infty}^{\text{cyc}})_{\omega\psi-1}) \leq \mu(L_p(\psi))$ together with the divisibility. A similar strategy also holds for the (+)-version.

Notes. Why (A) or (B) suffices (I put question marks here in my notes). Suppose (B) holds for every ψ : $\text{char}(X_{\psi}) \mid L_p(\psi)$, where $X_{\psi} := (X_{\infty}^{\text{cyc}})_{\omega\psi-1}$. Then $\lambda(X_{\psi}) \leq \lambda(L_p(\psi))$ and $\mu(X_{\psi}) \leq \mu(L_p(\psi))$ for each ψ . By Theorem 11.5.1 the sums over ψ agree, so equality holds

for each ψ . A divisibility $f \mid g$ in $\Lambda_{\mathcal{O}}$ with $\lambda(f) = \lambda(g)$ and $\mu(f) = \mu(g)$ forces g/f to have $\lambda = \mu = 0$, i.e. to be a unit (Theorem 8.3.2); so the ideals are equal. The same argument works for (A) with the inequalities reversed. Hence one divisibility for *all* ψ simultaneously implies the main conjecture.

11.6 Strategies of proof: Mazur–Wiles and Rubin

Mazur–Wiles. Mazur and Wiles proved the Iwasawa main conjecture in the mid 1980s [10], specifically the $(-)$ -version with strategy (A). They show that $(X_{\infty}^{\text{cyc}})_{\omega\psi-1}$ is large enough, using the étale cohomology of the modular curves $X_1(Np^r)$ and the congruences between cusp forms and Eisenstein series. This is a generalisation of Ribet’s proof of the Herbrand–Ribet theorem (Chapter 5).

Rubin. The $(+)$ -version was proven using strategy (B) by K. Rubin in the late 1980s [13]. He showed that $(\mathfrak{X}_{\infty}^{\text{cyc}})_{\psi}^* \otimes \kappa_{\text{cyc}}$ is small enough, using the Euler system of cyclotomic units (Thaine, Kolyvagin).

11.7 Report problem: primes in residue classes modulo 4

Report Problem 11.7.1

Show that there are infinitely many prime numbers congruent to 1 mod 4, and infinitely many congruent to 3 mod 4, without using the Dirichlet L -functions $L(\chi, s)$.

Solution. 3 mod 4. Suppose $p_1, \dots, p_k$ are all the primes $\equiv 3 \pmod{4}$, and let $M = 4p_1 \cdots p_k - 1 \equiv 3 \pmod{4}$. M is odd and not a product of primes $\equiv 1 \pmod{4}$ only (such a product is $\equiv 1 \pmod{4}$), so some prime $q \equiv 3 \pmod{4}$ divides M . But $q = p_i$ for some i , and then $p_i \mid M + 1 = 4p_1 \cdots p_k$, i.e. $p_i \mid 1$. Contradiction.

1 mod 4. Suppose $p_1, \dots, p_k$ are all the primes $\equiv 1 \pmod{4}$, and let $M = (2p_1 \cdots p_k)^2 + 1$. Let q be a prime divisor of M . Then q is odd, and $x = 2p_1 \cdots p_k$ satisfies $x^2 \equiv -1 \pmod{q}$. So x has order 4 in $\mathbb{F}_q^{\times}$, hence $4 \mid q - 1$, i.e. $q \equiv 1 \pmod{4}$. Thus $q = p_i$ for some i , but $p_i \mid x$ so $p_i \nmid x^2 + 1$. Contradiction. ■

Notes. The hint in my notes, “ $p = 4n + 1, (4n_1 + 1)(4n_2 + 1) \cdots (4n_k + 1)$ ”, is the observation used in the first part: a product of numbers $\equiv 1 \pmod{4}$ is again $\equiv 1 \pmod{4}$. The second part is the special case $f = 4$ of the fact that every prime divisor of $\Phi_f(x)$, not dividing f , is $\equiv 1 \pmod{f}$, which is Theorem 1.3.11 in disguise.

Chapter 12

p -adic Hodge Theory and Selmer Groups

Iwasawa theory is generalised to more general Galois representations and motives. In this chapter we recall the necessary input from p -adic Hodge theory; proofs are beyond the scope of the lectures (cf. [4]).

12.1 Fontaine's rings of p -adic periods

Let $G_{\mathbb{Q}_p} = \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Fontaine defines the rings of p -adic periods

$$B_{\text{cris}} \subset B_{\text{st}} \subset B_{\text{dR}}.$$

B_{cris} is a topological $\mathbb{Q}_p$ -algebra with a continuous action of $G_{\mathbb{Q}_p}$, and with a Frobenius operator $\varphi : B_{\text{cris}} \rightarrow B_{\text{cris}}$ commuting with $G_{\mathbb{Q}_p}$.

Let $\hat{\mathbb{Q}}_p^{\text{ur}}$ be the completion of the maximal unramified extension $\mathbb{Q}_p^{\text{ur}}$ of $\mathbb{Q}_p$.

Notes. $\hat{\mathbb{Q}}_p^{\text{ur}}$ is a complete discretely valued field with residue field $\overline{\mathbb{F}_p}$. It carries the action of $\text{Gal}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p) \cong \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$, generated by the arithmetic Frobenius. Note that $G_{\mathbb{Q}_p}$ acts on $\hat{\mathbb{Q}}_p^{\text{ur}}$ through the surjection $G_{\mathbb{Q}_p} \twoheadrightarrow \text{Gal}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p)$, by continuity.

We use an injection $\hat{\mathbb{Q}}_p^{\text{ur}} \hookrightarrow B_{\text{cris}}$ compatible with the $G_{\mathbb{Q}_p}$ -action (and with φ , which is the Frobenius of $\hat{\mathbb{Q}}_p^{\text{ur}}$). There exists a special element $t \in B_{\text{cris}}$ (the p -adic analogue of $2\pi i \in \mathbb{C}$) such that $G_{\mathbb{Q}_p}$ acts on t through the cyclotomic character: $G_{\mathbb{Q}_p}$ acts on t through the surjection $G_{\mathbb{Q}_p} \twoheadrightarrow \text{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$, and

$$g \cdot t = \chi_{\text{cyc}}(g) t \quad \text{for } g \in \text{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p).$$

Moreover $\varphi(t) = pt$.

Notes. Heuristically, $t = \log[\varepsilon]$, where $\varepsilon = (1, \zeta_p, \zeta_{p^2}, \dots)$ is a compatible system of p -power roots of unity. Just as $2\pi i$ is a period of dz/z (the integral over a loop), t is the p -adic period of the multiplicative group.

12.2 Comparison theorems

Theorem 12.2.1 (Crystalline comparison; Faltings, Tsuji, Nizioł)

Let X be a proper smooth variety over $\mathbb{Q}_p$ which has good reduction, i.e. it extends to a proper smooth scheme $\mathcal{X}$ over $\mathbb{Z}_p$ with special fibre $X_{\mathbb{F}_p}$. Then we have a natural isomorphism, compatible with $G_{\mathbb{Q}_p}$ and φ (and filtrations after extending scalars to B_{dR}),

$$H_{\text{cris}}^i(X_{\mathbb{F}_p}/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} B_{\text{cris}} \cong H_{\text{et}}^i(X_{\overline{\mathbb{Q}_p}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{cris}}.$$

Correction. In my notes the right-hand side reads $H_{\text{st}}^i(X_{\overline{\mathbb{Q}_p}}, \mathbb{Q}_p)$; it is *étale* cohomology $H_{\text{ét}}^i(X_{\overline{\mathbb{Q}_p}}, \mathbb{Q}_p)$. Also, φ acts on the left through both factors, and $G_{\mathbb{Q}_p}$ only through B_{cris} ; on the right $G_{\mathbb{Q}_p}$ acts on both factors.

This is a p -adic analogue of the following classical theorem.

Theorem 12.2.2 (de Rham)

Let K be a subfield of $\mathbb{C}$ and X a proper smooth variety over K . Then

$$H_{\text{dR}}^i(X/K) \otimes_K \mathbb{C} \cong H^i(X(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}.$$

In this sense, B_{cris} is the ring of p -adic periods for proper smooth varieties with good reduction. We have injections

$$B_{\text{cris}} \hookrightarrow B_{\text{st}} \hookrightarrow B_{\text{dR}},$$

where B_{cris} carries φ , B_{st} carries φ and the monodromy operator N (with $N\varphi = p\varphi N$ and $B_{\text{cris}} = B_{\text{st}}^{N=0}$). B_{dR} has neither φ nor N , but B_{dR} is a complete discrete valuation field with uniformiser t (and residue field $\mathbb{C}_p$, the completion of $\overline{\mathbb{Q}_p}$). For any finite extension k of $\mathbb{Q}_p$ (with $G_k = \text{Gal}(\overline{\mathbb{Q}_p}/k)$),

$$(B_{\text{cris}})^{G_k} = (B_{\text{st}})^{G_k} = k_0, \quad (B_{\text{dR}})^{G_k} = k,$$

where k_0 is the largest subextension of $k/\mathbb{Q}_p$ which is unramified over $\mathbb{Q}_p$.

We have similar comparison theorems of p -adic Hodge theory with B_{st} and B_{dR} : B_{st} (resp. B_{dR}) is the ring of p -adic periods for proper smooth varieties with semistable reduction (resp. for all proper smooth varieties, e.g. those with potentially semistable reduction).

Correction. My notes say “stable reduction” for B_{st} ; the standard term is *semistable* reduction (C_{st} -conjecture, proved by Tsuji). For B_{dR} the comparison (C_{dR} , Faltings) holds for every proper smooth variety over k .

12.3 de Rham and geometric Galois representations

Let $V \cong \mathbb{Q}_p^{\oplus n}$, with a continuous linear action of G_k , be a p -adic Galois representation, where k is a finite extension of $\mathbb{Q}_p$. Then

$$\dim_k(V \otimes_{\mathbb{Q}_p} B_{\text{dR}})^{G_k} \leq \dim_{\mathbb{Q}_p} V.$$

Definition 12.3.1

When we have equality $\dim_k(V \otimes_{\mathbb{Q}_p} B_{\text{dR}})^{G_k} = \dim_{\mathbb{Q}_p} V$, we say that V is B_{dR} -*admissible* (or *de Rham*). Similarly with B_{cris} (dimension over k_0): *crystalline*.

Correction. In my notes the definition of B_{dR} -admissibility is written with “ $\leq$ ”. That inequality holds for *every* V ; admissibility means equality. Also, $(V \otimes B_{\text{dR}})^{G_k}$ is a k -vector space (as $B_{\text{dR}}^{G_k} = k$), so the dimension on the left is over k , not over $\mathbb{Q}_p$.

Definition 12.3.2

Let K be a number field and $V \cong \mathbb{Q}_p^{\oplus n}$ a continuous p -adic representation of $G_K = \text{Gal}(\overline{K}/K)$. We say that V is *geometric* if

- (i) the action of $G_{K_v} := D_v$ on V is unramified (i.e. I_v acts trivially) for all but finitely many primes v of K , and
- (ii) for the primes v of K above (p) , the action of G_{K_v} on V is B_{dR} -admissible.

Notes. Here $G_{K_v} = \text{Gal}(\overline{K}_v/K_v)$ is identified with the decomposition group $D_v \subseteq G_K$ of a prime of $\overline{K}$ above v , by choosing an embedding $\overline{K} \hookrightarrow \overline{K}_v$. Changing the choice conjugates D_v and does not affect the conditions. The Fontaine–Mazur conjecture predicts that geometric representations are exactly those that “come from geometry”.

By the comparison theorems of p -adic Hodge theory, $H_{\text{et}}^i(X_{\overline{K}}, \mathbb{Q}_p)$ is geometric for any proper smooth variety X over K and any i with $0 \leq i \leq 2 \dim X$. (Condition (i) holds outside the primes of bad reduction and those above p , by smooth and proper base change; condition (ii) is C_{dR} .)

Correction. My notes write “ $0 \leq i \leq \dim K$ ”; the cohomological degrees range over $0 \leq i \leq 2 \dim X$.

12.4 Stable lattices and Galois cohomology

Lecture of 23 July 2026. From now on, K denotes a finite extension of $\mathbb{Q}_p$ (the *coefficient field*) with ring of integers $\mathcal{O}$ and uniformiser ϖ , and F denotes a number field. A p -adic representation is a finite-dimensional K -vector space $V \cong K^{\oplus d}$ with a continuous K -linear action of G_F .

Definition 12.4.1

An $\mathcal{O}$ -submodule $T \subset V$ is called a G_F -stable $\mathcal{O}$ -lattice if

- (i) T is stable under the G_F -action, i.e. $gT \subseteq T$ for all $g \in G_F$;
- (ii) T is a finitely generated $\mathcal{O}$ -module with $T \otimes_{\mathcal{O}} K \cong V$ (equivalently, T is free of rank d and spans V).

Notes. My notes have a “?” at “stable”. It means *invariant*: $g(T) \subseteq T$, hence $g(T) = T$ since g^{-1} also preserves T . It does not mean that each element is fixed.

Lemma 12.4.2

Let V be a continuous p -adic representation of $G_F = \text{Gal}(\overline{F}/F)$. Then there exists a G_F -stable lattice $T \subset V$.

Proof. Take any lattice T_0 (e.g. $\mathcal{O}^{\oplus d}$ in a basis). Its stabiliser $H = \{g \in G_F \mid gT_0 = T_0\}$ is open: $GL(T_0) = GL_d(\mathcal{O})$ is open in $GL_d(K)$, and the action map $G_F \rightarrow GL_d(K)$ is continuous. So H has finite index in the compact group G_F . Then $T = \sum_{g \in G_F/H} gT_0$ is a finite sum of lattices, hence a lattice, and it is G_F -stable. ■

Let T be a G_F -stable lattice of V . Then we set

$$A = V/T \cong T \otimes_{\mathcal{O}} K/\mathcal{O} \cong (K/\mathcal{O})^{\oplus d},$$

a finite number of copies of $K/\mathcal{O}$ on which G_F acts continuously (for the discrete topology), and $T = \varprojlim_n A[\varpi^n]$, where ϖ is a uniformiser of $\mathcal{O}$.

Let k be a field and $G_k = \text{Gal}(k^{\text{sep}}/k)$. We denote the continuous Galois cohomology $H^i(G_k, M)$ of a (topological) G_k -module M by $H^i(k, M)$. Let F be a number field and v a finite prime of F . We denote by D_v (resp. I_v) the decomposition subgroup (resp. inertia subgroup) at v . For a G_F -module M , we have

$$H^i(D_v, M) \cong H^i(F_v, M), \quad H^i(I_v, M) \cong H^i(F_v^{\text{ur}}, M),$$

where F_v^{ur} is the maximal unramified extension of F_v .

12.5 Local conditions H_f^1

Definition 12.5.1 (Bloch–Kato)

Let $V \cong K^{\oplus d}$ be a continuous p -adic representation of G_F , F a number field, and v a finite prime of F . We define a subspace $H_f^1(F_v, V)$ of the finite-dimensional K -vector space $H^1(F_v, V)$ as follows:

$$H_f^1(F_v, V) = \begin{cases} \ker(H^1(F_v, V) \xrightarrow{\text{res}} H^1(F_v^{\text{ur}}, V)) \cong H^1(D_v/I_v, V^{I_v}), & v \nmid p, \\ \ker(H^1(F_v, V) \rightarrow H^1(F_v, V \otimes_{\mathbb{Q}_p} B_{\text{cris}})), & v \mid p. \end{cases}$$

Notes. For $v \nmid p$, the isomorphism is the inflation–restriction exact sequence $0 \rightarrow H^1(D_v/I_v, V^{I_v}) \rightarrow H^1(D_v, V) \rightarrow H^1(I_v, V)$. These are the *unramified* classes. For $v \mid p$, the classes are called *crystalline*: they correspond to extensions $0 \rightarrow V \rightarrow E \rightarrow \mathbb{Q}_p \rightarrow 0$ with E crystalline. $H^1(F_v, V)$ is finite dimensional by the local Euler characteristic formula (Tate).

Let $\phi : H^1(F_v, V) \rightarrow H^1(F_v, A)$ be the morphism of Galois cohomology induced by the continuous map of G_F -modules $V \twoheadrightarrow A$. We define

$$H_f^1(F_v, A) = \phi(H_f^1(F_v, V)) \subseteq H^1(F_v, A).$$

Correction. My notes use the letter p (looking like “ $\not p$ ”) for this map; I renamed it ϕ to avoid a clash with the prime p .

12.6 Selmer groups and examples

Definition 12.6.1

Assume $p \neq 2$. Let $V \cong K^{\oplus d}$ be a geometric p -adic Galois representation of G_F , $T \subset V$ a G_F -stable lattice, and $A = V/T = T \otimes_{\mathcal{O}} K/\mathcal{O}$. We define the *Selmer group* $\text{Sel}_A(F)$ by

$$\text{Sel}_A(F) = \ker \left(H^1(G_F, A) \longrightarrow \prod_{v \text{ finite}} \frac{H^1(F_v, A)}{H_f^1(F_v, A)} \right),$$

the product over all finite primes v of F .

Notes. At the infinite places there is no condition. For p odd, $H^1(\mathbb{R}, A)$ is killed by 2 and is a p -primary group, so it vanishes. This is one reason for the assumption $p \neq 2$.

Example 12.6.2 ($A = \mathbb{Q}_p/\mathbb{Z}_p$). Let F be a number field, $V \cong \mathbb{Q}_p$ the trivial Galois representation, $T \cong \mathbb{Z}_p$ a G_F -stable lattice and $A = V/T \cong \mathbb{Q}_p/\mathbb{Z}_p$. By the well-known fact from Galois cohomology (cohomology of a trivial module),

$$H^1(F, \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}_{\text{cont}}(G_F, \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}_{\text{cont}}(G_F^{\text{ab}}, \mathbb{Q}_p/\mathbb{Z}_p).$$

Similarly $H^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}(G_{F_v}^{\text{ab}}, \mathbb{Q}_p/\mathbb{Z}_p)$, and one shows that

$$H_f^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}(D_v/I_v, \mathbb{Q}_p/\mathbb{Z}_p)$$

consists of the unramified homomorphisms (for $v \mid p$ this uses that crystalline classes in $H^1(F_v, \mathbb{Q}_p)$ are unramified). Hence $\text{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p}(F)$ consists of the homomorphisms $G_F^{\text{ab}} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ that are unramified everywhere, i.e. that factor through the Galois group of the Hilbert class field. By class field theory (Theorem 1.4.2),

$$\text{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p}(F) \cong \text{Hom}(\text{Cl}(F), \mathbb{Q}_p/\mathbb{Z}_p) = \text{Cl}(F)[p^\infty]^\vee,$$

the Pontryagin dual of the p -part of the ideal class group of F .

Notes. In my notes this line reads “ $\text{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p}(F) = \text{Cl}(F)[p^\infty]$ ”, with a circled “ $\vee$?” added and a “?” next to it. The answer: yes, the dual $\vee$ belongs there. Since $\text{Cl}(F)[p^\infty]$ is a finite abelian group, it is (non-canonically) isomorphic to its dual, so both versions are true as abstract groups. But the natural isomorphism is with the dual, and the dual is also what is compatible with Galois actions.

The next example. Let $\mu_{p^n} = \{x \in \overline{F}^\times \mid x^{p^n} = 1\}$. Let us define

$$\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}, \quad \mathbb{Q}_p(1) = \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \quad \mathbb{Q}_p/\mathbb{Z}_p(1) = \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = \varprojlim_n \mu_{p^n}.$$

We will discuss $\text{Sel}_A(F)$ for $A = \mathbb{Q}_p/\mathbb{Z}_p(1)$.

By Kummer theory in Galois cohomology (Hilbert’s Theorem 90),

$$H^1(F, \mu_{p^n}) \cong F^\times / (F^\times)^{p^n}, \quad H^1(F_v, \mu_{p^n}) \cong F_v^\times / (F_v^\times)^{p^n}.$$

Hence

$$H^1(F, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \varprojlim_n H^1(F, \mu_{p^n}) \cong F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \quad H^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong F_v^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p.$$

For each finite prime v we have the exact sequence $1 \rightarrow \mathcal{O}_{F_v}^\times \rightarrow F_v^\times \rightarrow \varpi_v^\mathbb{Z} \cong \mathbb{Z} \rightarrow 1$, where ϖ_v is a uniformiser of $\mathcal{O}_{F_v}$. We can show that

$$H_f^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) \subseteq H^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong F_v^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$$

is the image of $\mathcal{O}_{F_v}^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$ [1, Example 3.9]. Hence, for each finite prime v , the map

$$H^1(F, \mathbb{Q}_p/\mathbb{Z}_p(1)) \rightarrow H^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) \rightarrow \frac{H^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1))}{H_f^1(F_v, \mathbb{Q}_p/\mathbb{Z}_p(1))} \cong \mathbb{Q}_p/\mathbb{Z}_p$$

sends $x \otimes a \in F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$ to $v(x)a$, where $v = \text{val}_v$.

Proposition 12.6.3

We have the following exact sequence:

$$0 \longrightarrow \mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \text{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p(1)}(F) \longrightarrow \text{Cl}(F)[p^\infty] \longrightarrow 0.$$

In particular $\text{Sel}_{\mathbb{Q}_p/\mathbb{Z}_p(1)}(F)$ has corank $r_1(F) + r_2(F) - 1$ over $\mathbb{Z}_p$.

Correction. My notes write $\mathcal{O}_F \otimes \mathbb{Q}_p/\mathbb{Z}_p$; it is the *unit group* $\mathcal{O}_F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$. The crossed-out recollection $\mathcal{O}_F^\times \cong \mathbb{Z}^{r_1+r_2-1} \oplus (\text{finite})$ in my notes is still relevant: tensoring with $\mathbb{Q}_p/\mathbb{Z}_p$ kills the finite part, so $\mathcal{O}_F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{r_1+r_2-1}$.

Proof. (By this observation and the snake lemma, as in the lecture.) Let $I_F = \bigoplus_v \mathbb{Z}$ be the group of fractional ideals and P_F the subgroup of principal ideals. By the observation, $\text{Sel} = \ker(F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\text{div}} I_F \otimes \mathbb{Q}_p/\mathbb{Z}_p)$. Tensor the exact sequences

$$1 \rightarrow \mathcal{O}_F^\times \rightarrow F^\times \rightarrow P_F \rightarrow 1, \quad 0 \rightarrow P_F \rightarrow I_F \rightarrow \text{Cl}(F) \rightarrow 0$$

with $\mathbb{Q}_p/\mathbb{Z}_p$. Since P_F and I_F are free abelian groups, all Tor terms vanish except

$$\text{Tor}_1^{\mathbb{Z}}(\text{Cl}(F), \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Cl}(F)[p^\infty],$$

and $\text{Cl}(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ ($\text{Cl}(F)$ is finite). We get exact sequences

$$\begin{aligned} 0 \rightarrow \mathcal{O}_F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p &\rightarrow F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow P_F \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow 0, \\ 0 \rightarrow \text{Cl}(F)[p^\infty] &\rightarrow P_F \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow I_F \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow 0. \end{aligned}$$

The map div is the composite $F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \twoheadrightarrow P_F \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow I_F \otimes \mathbb{Q}_p/\mathbb{Z}_p$. So its kernel Sel contains $\mathcal{O}_F^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p$, and the quotient is the kernel of the second map, $\text{Cl}(F)[p^\infty]$. The corank statement follows from Dirichlet's unit theorem. $\blacksquare$

Chapter 13

Elliptic Curves and the Tate–Shafarevich Group

13.1 Elliptic curves and the Mordell–Weil theorem

Definition 13.1.1

Let k be a field. A proper smooth curve E over k of genus 1 such that $E(k) \neq \emptyset$, together with a chosen point $O \in E(k)$, is called an *elliptic curve* over k .

Notes. The base point O is part of the data. It becomes the neutral element of the group law; the same curve with a different base point is isomorphic as an elliptic curve via a translation. A genus one curve without rational points is *not* an elliptic curve: such curves are exactly what the Tate–Shafarevich group measures (§13.2).

For an elliptic curve E over k and any (finite) extension k' of k , $E(k')$ naturally becomes an abelian group (chord–tangent law with neutral element O).

Example 13.1.2. Let $\text{char } k \neq 2$, and consider the affine curve in $\mathbb{A}^2$ defined by the equation

$$y^2 = f(x),$$

where $f(x)$ is a cubic polynomial with no double roots. The Zariski closure E of this affine curve in $\mathbb{P}^2$ is an elliptic curve, with $O = [0 : 1 : 0]$ the unique point at infinity. Conversely, every elliptic curve over k has such a (Weierstrass) model [15, Ch. III].

Recall the following well-known theorem.

Theorem 13.1.3 (Mordell–Weil)

Let E be an elliptic curve over a number field F . Then $E(F)$ is a finitely generated abelian group. That is, there exists $r_F(E) \in \mathbb{Z}_{\geq 0}$ (the *Mordell–Weil rank*) such that

$$E(F) \cong \mathbb{Z}^{\oplus r_F(E)} \oplus (\text{finite abelian group}).$$

Proof sketch. *Weak Mordell–Weil:* $|E(F)/nE(F)| < \infty$ for $n \geq 2$. One embeds $E(F)/nE(F)$ into the n -Selmer group, a subgroup of $H^1(F, E[n])$ unramified outside a finite set of primes, which is finite. Then an argument using the theory of heights (a quadratic function $\hat{h}$ on $E(F)$ with finitely many points of bounded height) gives finite generation by descent. See [15, Ch. VIII]. ■

13.2 The Tate–Shafarevich group

Definition 13.2.1

Let E be an elliptic curve over a number field F . We define an abelian group

$$\text{III}_F(E) = \ker \left[H^1(F, E(\overline{F})) \longrightarrow \prod_v H^1(F_v, E(\overline{F}_v)) \right]$$

and call it the *Tate–Shafarevich group* of E .

Correction. In my notes the product runs over the finite primes only. The standard definition runs over *all* places v of F , including the infinite ones; the two versions differ at most by a finite 2-group, so they agree on p -parts for p odd.

Conjecture 13.2.2

For all elliptic curves E/F , $\text{III}_F(E)$ is a finite abelian group.

Notes. Only partial results are known: Kolyvagin [6] and Kato [5] (Euler system method). For example, for $E/\mathbb{Q}$ with analytic rank ≤ 1 , $\text{III}_{\mathbb{Q}}(E)$ is finite (Gross–Zagier and Kolyvagin). Kato’s Euler system gives one divisibility in the Iwasawa main conjecture for elliptic curves. This links Chapter 11 to this chapter. The finiteness of III is also part of the Birch–Swinnerton-Dyer conjecture.

By definition, $\text{III}_F(E)$ becomes nontrivial iff there is a proper smooth curve C over F with genus 1 such that $C(F_v) \neq \emptyset$ for all places v , $C(F) = \emptyset$, and $C \cong E$ over $\overline{F}$ in a way compatible with the action of E .

Notes. Precisely: $H^1(F, E)$ classifies *principal homogeneous spaces* (torsors) C for E , i.e. curves C/F with a simply transitive action $E \times C \rightarrow C$ defined over F ; such C is isomorphic to E over $\overline{F}$. The class of C is trivial iff $C(F) \neq \emptyset$, and its restriction to F_v is trivial iff $C(F_v) \neq \emptyset$. So nontrivial elements of III are curves that violate the Hasse principle. My notes write “ $C \cong E(\overline{F})$ ”; it should be “ $C \cong E$ over $\overline{F}$ ”.

13.3 Selmer’s example

Example 13.3.1 (Selmer). Let C be the proper smooth curve in $\mathbb{P}^2$ defined by

$$3x^3 + 4y^3 = 5z^3.$$

Then the genus of C is 1 (a smooth plane cubic), and $C(\mathbb{Q}) = \emptyset$, but $C(\mathbb{Q}_\ell) \neq \emptyset$ for all finite primes ℓ of $\mathbb{Q}$ (and $C(\mathbb{R}) \neq \emptyset$). Thus C is a counterexample to the Hasse principle. It is a torsor under its Jacobian, the elliptic curve $E : x^3 + y^3 + 60z^3 = 0$, and it gives a nontrivial element of $\text{III}_{\mathbb{Q}}(E)$.

Notes. Selmer’s original equation is $3x^3 + 4y^3 + 5z^3 = 0$; replacing z by $-z$ gives the form above. Local solubility is elementary. For $\ell \nmid 60$, the reduction is a smooth cubic with points by the Hasse bound, and Hensel’s lemma lifts a smooth point; for $\ell \in \{2, 3, 5\}$ one exhibits explicit ℓ -adic solutions. Real points obviously exist. The absence of rational points is Selmer’s theorem (1951), proved by a descent; see [15, §X.6] or Cassels’ *Lectures on Elliptic Curves*.

Bibliography

- [1] S. Bloch and K. Kato, L -functions and Tamagawa numbers of motives, in *The Grothendieck Festschrift*, Vol. I, Progr. Math. 86, Birkhäuser, 1990, 333–400.
- [2] A. Brumer, On the units of algebraic number fields, *Mathematika* 14 (1967), 121–124.
- [3] H. Davenport, *Multiplicative Number Theory*, 3rd ed., Graduate Texts in Mathematics 74, Springer, 2000.
- [4] J.-M. Fontaine (ed.), *Périodes p -adiques*, Astérisque 223, 1994.
- [5] K. Kato, p -adic Hodge theory and values of zeta functions of modular forms, *Astérisque* 295 (2004), 117–290.
- [6] V. A. Kolyvagin, Euler systems, in *The Grothendieck Festschrift*, Vol. II, Progr. Math. 87, Birkhäuser, 1990, 435–483.
- [7] B. Ferrero and L. C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, *Ann. of Math.* 109 (1979), 377–395.
- [8] D. A. Marcus, *Number Fields*, 2nd ed., Universitext, Springer, 2018.
- [9] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, 1986.
- [10] B. Mazur and A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* 76 (1984), 179–330.
- [11] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften 322, Springer, 1999.
- [12] K. A. Ribet, A modular construction of unramified p -extensions of $\mathbb{Q}(\mu_p)$, *Invent. Math.* 34 (1976), 151–162.
- [13] K. Rubin, The main conjecture, Appendix to S. Lang, *Cyclotomic Fields I and II*, Graduate Texts in Mathematics 121, Springer, 1990.
- [14] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer, 1979.
- [15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics 106, Springer, 2009.
- [16] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics 83, Springer, 1997.