Contents

0 Introduction: $x^2 + y^2 = n$ **2**
0.1 Algebraic method 2
0.2 Analytic method 2

1 Number fields and algebraic integers **2**
1.1 Algebraic integers 2
1.2 Discriminant and integral basis 2
1.2.1 Application to number fields 2
1.3 Cyclotomic fields 3

2 Dedekind domains **3**

3 Extensions of Dedekind domains **3**
3.1 Different and discriminant 4

4 Decomposition of primes in Galois extensions **4**

5 Finiteness theorems **4**
5.1 Hermite's Theorem 4
5.2 Dirichlet's Theorem 4

6 Distribution of primes **5**
6.1 Regulator 5
6.2 Infinite products 5
6.3 Applications 5
6.4 Dirichlet L-functions 5
6.5 Factorisation of the Dedekind zeta function of abelian number fields 6
6.6 Formula for $L(\chi, 1)$ 6
6.7 Class number formula for quadratic fields 6

7 p-adic numbers **6**
7.1 Structure of complete discrete valuation fields 7
7.2 Structure of $K^\times$ 7
7.3 Hensel's lemma 7
7.4 Newton polygon 7

8 Finite extensions of complete discrete valuation fields **7**
8.1 Galois extensions of complete discrete valuation fields 8

9 Global applications **8**
9.1 Comparison of local and global Galois groups 8
9.2 Product formula 8

10 Adèles and idèles **8**
10.1 Topological groups 8
10.1.1 Subgroups 8
10.1.2 Quotients 9
10.2 Adèles 9
10.3 Haar measures 9
10.4 Products and infinite products 9

10.5 Construction 9
10.6 Idèles 10
10.7 Generalisation 10
10.8 Dirichlet's theorem 10
10.9 Haar measure on $\mathbb{I}_K$ 10
10.10 Generalisation of the Pontryagin duality 10

0 Introduction: $x^2 + y^2 = n$

0.1 Algebraic method

1 Gauss integers, Eudlidean norm, the ring of Gauss integers is a PID, primitive element, unique factorisation for elements and ideals.

Prime ideals of the Gauss integers: case work based on $\mathfrak{p} \cap \mathbb{Z} = (p)$ and $p \bmod 4$.

0.2 Analytic method

$r(n)$, $\zeta_R(s)$, $\zeta(s)$, $L(\chi, s)$, $\left(\sum \frac{a_n}{n^s}\right)\left(\sum \frac{1}{n^s}\right) = \sum \left(\sum_{d|n} a_d\right) \frac{1}{n^s}$, multiplicative sequence, summation of a multiplicative sequence is multiplicative

1 Number fields and algebraic integers

1.1 Algebraic integers

2 integral element (3 equivalent properties), integral elements form a subring, transitivity of integral extension, integral closure, PIDs are integrally closed, integrality over $\mathbb{Z}$, $\mathcal{O}_K$ for quadratic number fields

1.2 Discriminant and integral basis

trace, norm, trace and norm with coefficients of the minimal polynomial and with embeddings into an algebraically closed field for separable extensions

trace is non-degenerate for separable extensions (PO), $L \cong L^\vee = \mathrm{Hom}_K(L, K)$, $(\alpha_i^\vee)$ dual basis to (α_i)

1.2.1 Application to number fields

discriminant, $\mathrm{disc} \neq 0 \Leftrightarrow$ basis, $\mathrm{disc}(AC) = \mathrm{disc}(A) \det^2 C$, $\mathrm{disc} = \det^2 \sigma_i(\alpha_j)$, discriminant of a power base, $\mathrm{sgn}\, \mathrm{disc} = (-1)^{r_2}$

$\mathcal{O}_K$ is a free $\mathbb{Z}$-module, integral basis, disc_K

3 equivalent condition for an integral basis with discriminant, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ if the minimal polynomial can be translated to an Eistenstein polynomial

1.3 Cyclotomic fields

$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$, $[\mathbb{Q}(\zeta_N):\mathbb{Q}] = \varphi(N)$, $\mathbb{Q}(\zeta_{N+M}) = \mathbb{Q}(\zeta_N)\mathbb{Q}(\zeta_M)$, $\mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_M) = Q$.

$\mathrm{disc}(1, \zeta_N, \ldots, \zeta_N^{\varphi(N)-1}) \mid N^{\varphi(N)}$, $\mathcal{O}_{\mathbb{Q}(p^N)} = \mathbb{Z}[\zeta_{p^n}]$.

For $K \cap L = \mathbb{Q}$, $d = \gcd(\mathrm{disc}_K, \mathrm{disc}_L)$: $\mathcal{O}_K\mathcal{O}_L \subseteq \mathcal{O}_{KL} \subseteq \frac{1}{d}\mathcal{O}_K\mathcal{O}_L$.

$\mathcal{O}_{\mathbb{Q}(\zeta_N)} = \mathbb{Z}[\zeta_N]$, $\mathrm{disc}_{\mathbb{Q}(\zeta_{p^N})} = \pm p^{p^{N-1}(pN-N-1)}$, the general formula follows from $\mathrm{disc}_{KL} = \mathrm{disc}_K^{[L:\mathbb{Q}]}\,\mathrm{disc}_L^{[K:\mathbb{Q}]}$ (holds if $\gcd(\mathrm{disc}_K, \mathrm{disc}_L) = 1$)

2 Dedekind domains

noetherian ring, Dedekind domain, PID $\Rightarrow$ Dedekind, A Dedekind $\Rightarrow S^{-1}A$ Dedekind **4**

integral closure in a field extension is Dedekind, $\mathcal{O}_K$ is Dedekind, if $A \subset B$ is integral then A field $\Leftrightarrow$ B field

fractional ideal

Dedekind domains have unique facorisation of nonzero ideals. Lemma 1: every nonzero ideal of a noetherian ring contains a product of nonzero prime ideals. Lemma 2: $\mathfrak{p} \in \mathrm{Spec}\, A \setminus (0) \Rightarrow \mathfrak{p}^{-1}$ is a fractional ideal and $\mathfrak{p}^{-1}\mathfrak{p} = A$

Dedekind $\Rightarrow$ (PID $\Leftrightarrow$ UFD), unique factorisation of factorial ideals in Dedekind domains, $v_\mathfrak{p}$, properties of $v_\mathfrak{p}$

I factorial, $\mathfrak{p}$ prime $\Rightarrow I/I\mathfrak{p}$ is a 1-dim $A/\mathfrak{p}$-vector space **5**

$\mathrm{Div}(A)$, $\mathrm{Prin}(A)$, Cl_A

Chinese Remainder Theorem for rings (for $I + J = R$, $I \cap J = IJ$) and Dedekind domains (for distinct maximal ideals), Dedekind domain with finitely many maximal ideals is PID, the localisation of a Dedekind domain at a prime is PID

localisation of Dedekind domains: prime ideals and prime decomposition of fractional ideals

3 Extensions of Dedekind domains

K/L finite separable field extension, A Dedekind with fraction field K, B the integral closure of A in L, $\mathfrak{p} \in \mathrm{Spec}\, A$, $\mathfrak{p}B = \prod Q_i^{e_i}$

$k(Q_i)/k(\mathfrak{p})$ is a finite extension with degree f_i, $\sum e_i f_i = [L:K]$

ramification index, residue degree, unramified, split, inert

Kummer's Theorem, $\mathfrak{p} \nmid N_{L/K}(f'(\alpha)) \Rightarrow B/\mathfrak{p}B = k(\mathfrak{p})[\overline{\alpha}]$

p is ramified in $\mathbb{Q}(\sqrt{D})$ iff $p \mid \mathrm{disc}_K$, $p \geq 3$ unramified prime splits iff $\left(\frac{D}{p}\right) = 1$, for $D \equiv 1 \pmod 4$ 2 splits iff $D \equiv 1 \pmod 8$ **6**

decomposition of 2, 3, 5, 7 in $\mathbb{Q}(\sqrt[3]{2})$

p unramified $\Leftrightarrow \mathcal{O}_K/p\mathcal{O}_K$ is reduced $\Leftrightarrow \overline{\mathrm{Tr}}_{K/\mathbb{Q}} : \mathcal{O}_K/p\mathcal{O}_K \times \mathcal{O}_K/p\mathcal{O}_K \to \mathbb{F}_p$ is non-degenerate $\Leftrightarrow p \nmid \mathrm{disc}_K$

3.1 Different and discriminant

norm of a fractional ideal, multiplicative, transitive, $\mathrm{N}_{L/\mathbb{Q}}(I) = [J : IJ]$, $N_{K/\mathbb{Q}}$ is the absolute norm

different, $\mathrm{N}_{K/\mathbb{Q}}(\delta_K) = |\operatorname{disc}_K|$, $\delta_{M/K} = \delta_{M/L}(\delta_{L/K}\mathcal{O}_M)$

relative discriminant, $\mathfrak{p}$ unramified $\Leftrightarrow \mathfrak{p} \nmid \operatorname{disc}_{L/K}$, $|\operatorname{disc}_L| = |\operatorname{disc}_K|^{[L:K]}\,\mathrm{N}_{K/\mathbb{Q}}(\operatorname{disc}_{L/K})$

for a composite $K_1K_2/\mathbb{Q} = K_1 \cap K_2$: $\delta_{K_2}\mathcal{O}_{K_1K_2} \subseteq \delta_{K_1K_2/K_1}$, $\operatorname{disc}_L \mid \operatorname{disc}_{K_1}^{[K_2:\mathbb{Q}]}\operatorname{disc}_{K_2}^{[K_1:\mathbb{Q}]}$, $\gcd(\operatorname{disc}_{K_1}, \operatorname{disc}_{K_2}) = 1 \Rightarrow |\operatorname{disc}_L| = |\operatorname{disc}_{K_1}|^{[K_2:\mathbb{Q}]}|\operatorname{disc}_{K_2}|^{[K_1:\mathbb{Q}]}$, a rational prime p is unramified in K_1 and K_2 iff in K_1K_2

4 Decomposition of primes in Galois extensions

7 action of the Galois group is transitive, $\forall e_i = e$, $\forall f_j = f$, $efg = n$

decomposition group, $|G| = g \cdot |D(Q|\mathfrak{p})|$, $D(\sigma(Q)|\mathfrak{p}) = \sigma D(Q|\mathfrak{p})\sigma^{-1}$, inertia subgroup $1 \to I(Q|\mathfrak{p}) \to D(Q|\mathfrak{p}) \xrightarrow{\varphi_Q} \operatorname{Gal}(k(Q)/k(\mathfrak{p})) \to 1$ exact, $|D(Q|\mathfrak{p})| = ef$, $|I(Q|\mathfrak{p})| = e$

Q is the only prime above $Q' \Leftrightarrow \operatorname{Gal}(L/K') \subseteq D(Q|\mathfrak{p})$, $e(Q'|\mathfrak{p}) = \dfrac{|I(Q|\mathfrak{p})|}{|H \cap I(Q|\mathfrak{p})|}$, {primes of K' above $\mathfrak{p}$} $\leftrightarrow$ {orbits of H on $\{Q_1, \dots, Q_g\}$}

Frobenius element, $\left(\dfrac{L/K}{\sigma(Q)}\right) = \sigma\left(\dfrac{L/K}{Q}\right)\sigma^{-1}$, $\left(\dfrac{L/K}{Q}\right)\Big|_M = \left(\dfrac{M/K}{Q \cap M}\right)$, $\left(\dfrac{L/M}{Q \cap M}\right) = \left(\dfrac{L/K}{Q}\right)^{f(Q\cap M|\mathfrak{p})}$

8 $N \geq 3$ odd or $4 \mid N$: $p \in \mathbb{Z}$ ramifies in $\mathbb{Q}(\zeta_N) \Leftrightarrow p \mid N$, for $p|N$ $e = p^{v_p(N)}(p-1)$

$p \nmid N$: $\sigma_p(\zeta_N) = \zeta_N^p$, $f(\mathfrak{p}|p) =$ order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$, $g = \varphi(N)/f$

$\mathbb{Q}(p^*)$ is the unique quadratic subextension of $\mathbb{Q}(\zeta_p)$, Law of Quadratic Reciprocity

5 Finiteness theorems

(full) lattice, Minkowski's Lemma

$\operatorname{Disc}(I)$, $\operatorname{Disc}(I) = \operatorname{disc}_K \mathrm{N}_{K/\mathbb{Q}}(I)^2$, λ, for any fractional ideal I $\lambda(I) \subseteq \mathbb{R}^n$ is a lattice and $\operatorname{Vol}(\mathbb{R}^n/\lambda(I)) = \sqrt{\operatorname{Disc}(I)}/2^{r_2}$

9 $\exists\alpha \in I \setminus \{0\}$ s.t. $|\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \leq \left(\dfrac{4}{\pi}\right)^{r_2}\dfrac{n!}{n^n}\sqrt{|d_K|}\,\mathrm{N}(I)$, Minkowski Bound: every ideal class has $0 < \mathrm{N}(\mathfrak{a}) \leq \dfrac{n!}{n^n}\left(\dfrac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$, Cl_K is finite, examples: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}\sqrt{-14})$

5.1 Hermite's Theorem

$|d_K|^{1/2} \geq \left(\dfrac{\pi}{4}\right)^{n/2}\dfrac{n!}{n^n}$, only $\mathbb{Q}$ is unramified at every prime, Hermite's Theorem

5.2 Dirichlet's Theorem

$W_K = (\mathcal{O}_K^\times)^{\text{tors}}$ is finite cyclic, for $u \in \mathcal{O}_K^\times$ $u \in W_K \Leftrightarrow \forall\sigma : K \hookrightarrow \mathbb{C} : |\sigma(u)|_{\mathbb{C}} = 1$

10 Dirichlet's Theorem, example: $\mathbb{Q}(\sqrt{2})$ has $\varepsilon = 1 + \sqrt{2}$

Lemmata: $\forall k \exists u_k : |\sigma_k(u_k)| > 1, \forall i \neq k : |\sigma_i(u_k)| < 1$; $A = (a_{ij}), a_{ii} > 0, a_{ij} < 0, \sum a_{ij} = 0 \Rightarrow \operatorname{rk} A = r - 1$

6 Distribution of primes

6.1 Regulator

Regulator, example: real quadratic number field

Artin's Theorem (PO), $\vartheta \in \mathcal{O}_K^\times, \vartheta > 1, 4\vartheta^{3/2} + 24 < |d_K|$ then ϑ is the fundamental unit of K, example: $\mathbb{Q}(\sqrt[3]{2})$

$N(t)$, examples: $\mathbb{Q}, \mathbb{Q}(i)$ 11

$N(t) = \dfrac{2^{r_1}(2\pi)^{r_2} R_K h}{w\sqrt{|d_K|}} t + O(t^{1-1/n})$, $N_C(t) = \dfrac{2^{r_1}(2\pi)^{r_2} R_K}{w\sqrt{|d_K|}} t + O(t^{1-1/n})$

$S_t = \{x \in J \mid |N_{K/\mathbb{Q}}(x)| \leq t\,\mathrm{N}(J)\}/\mathcal{O}_K^\times \longleftrightarrow \{I \subseteq \mathcal{O}_K, I \in C \mid \mathrm{N}(I) \leq t\}$

proof in the quadratic case

$(n-1)$-Lipschitz parametrisable function; Marcus' Lemma: $B \subseteq \mathbb{R}^n$ bounded, ∂B $(n-1)$-Lipschitz, $\Lambda \subset \mathbb{R}^n$ full lattice $\Rightarrow \forall a > 1$ $\#(\Lambda \cap aB) = \dfrac{\mu(B)}{\mathrm{Vol}(\mathbb{R}^n/\Lambda)} a^n + O(a^{n-1})$ (PO)

6.2 Infinite products

absolute convergent product, $\prod(1 + a_n)$ abs.conv. $\Leftrightarrow \sum a_n$ abs.conv., $\prod_p \dfrac{1}{1-p^{-s}}$ and $\zeta(s)$ are convergent for $\mathrm{Re}(s) > 1$, ζ has an analytic continuation to a meromorphic function on $\mathrm{Re}(s) > 0$ with a simple pole at 1 12

$S_t = \kappa t + O(t^{1-\delta}) \Rightarrow f$ has an analytic continuation to a meromorphic function on $\mathrm{Re}(s) > 1 - \delta$, with at most a simple pole at 1 with residue κ

6.3 Applications

Dedekind zeta $\zeta_K(s) = \prod_{\mathfrak{p}} \dfrac{1}{1 - \mathrm{N}\,\mathfrak{p}^{-s}} = \sum_{\mathfrak{a}} \dfrac{1}{(\mathrm{N}\,\mathfrak{a})^s}$ converges absolutely for $\mathrm{Re}\, s > 1$

$a_n = \#\{\mathfrak{a} \subseteq \mathcal{O}_K \mid \mathrm{N}\,\mathfrak{a} = n\}$, $\sum \dfrac{a_n}{n^s}$ has an analytic continuation with a simple pole

$\zeta_K(s)$ has an analytic continuation with a simple pole, $\mathrm{Res}_1\, \zeta_K(s) = \dfrac{2^{r_1}(2\pi)^{r_2} R_K h}{w\sqrt{|d_K|}}$

$\sum_{\mathfrak{p}} \dfrac{1}{\mathrm{N}\,\mathfrak{p}^s} \sim \sum_{\deg \mathfrak{p} = 1} \dfrac{1}{\mathrm{N}\,\mathfrak{p}^s} \sim \log \dfrac{1}{s-1}$

Dirichlet and natural density, $\pi(x)$, $\pi_S(x)$

6.4 Dirichlet L-functions

character group, $\widehat{G} \cong G$ non-canonical, $\widehat{\cdot}$ is exact, $\widehat{\widehat{G}} \cong G$ canonical (Pontryagin duality), $\sum_g \chi(g) = 0$ or $|G|$, $\sum_\chi \chi(g) = 0$ or $|G|$ 13

Dirichlet character, conductor, primitive character, examples on $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ and the Legendre symbol

$L(\chi, s)$, has an analytic continuation if $\chi \neq \chi_0$

6.5 Factorisation of the Dedekind zeta function of abelian number fields

$\zeta_K(s) = \prod_\chi L(\chi, s)$

$\prod_{\chi \neq \chi_0} L(\chi, 1) = \dfrac{2^{r_1}(2\pi)^{r_2} R_k h}{w\sqrt{|d_K|}}$

$p \geq 3$, $K = \mathbb{Q}(\sqrt{p^*}) \Rightarrow L(\chi, 1) = \dfrac{2\log \varepsilon_K h}{\sqrt{p}}$ or $\dfrac{2\pi h}{|\mathcal{O}_K^\times|\sqrt{p}}$

14 Dirichlet's theorem: $p \equiv a \pmod N$ have Dirichlet density $1/\varphi(N)$. Generalisation: Chebotarev density theorem (PO), examples

6.6 Formula for $L(\chi, 1)$

Gauss sums, $\tau_a(\chi) = \overline{\chi}(a)\tau(\chi)$, $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)f$, $|\tau(\chi)| = \sqrt{f}$

$L(\chi, s) = -\dfrac{\tau(\chi)}{f}\sum_a \overline{\chi}(a)\log\sin\dfrac{\pi a}{f}$ or $\dfrac{\tau(\chi)\pi i}{f^2}\sum_a \overline{\chi}(a)a$

6.7 Class number formula for quadratic fields

15 χ_K, $K \leq \mathbb{Q}(\zeta_{|d_K|}$, identifying χ_K with χ_{d_K}, properties of χ_{d_K}, $\tau(\chi_{d_K}) = \sqrt{|d_K|}$ or $i\sqrt{|d_K|}$ (PO)

Dirichlet class number formula, corollary for $d_K < -4$ even, example: $\mathbb{Q}(\sqrt{-56})$

7 p-adic numbers

$\mathbb{Z}_p$ as an inverse limit, local integral domain, $\mathbb{Q}_p$ as a fraction field, the fundamental system $(a + p^n\mathbb{Z}_p)$ defines a topology, $\mathbb{Z}_p$ is complete, $\mathbb{Z} \subset \mathbb{Z}_p$ is dense

$|\cdot|_p$ absolute value, v_p, $\mathbb{Q}_p$ as a completion of $\mathbb{Q}$

16 examples for calculations in $\mathbb{Q}_p$

valuation field, (non-)archimedean valuation, examples: $\mathbb{Q}$ with the standard and the p-adic valuations, $v_\mathfrak{p}$, $k(x)$ with $v_{p(x)}$

additive valuation, equivalence of additive valuations

non-archimedean $\Leftrightarrow$ bounded on $\mathbb{Z}$, $x \neq y \Rightarrow |x + y| = \max(|x|, |y|)$

completion: unique, $K \subset \widehat{K}$ dense, an embedding of normed fields extends uniquely to the completion

valuation ring, discrete valuation ring, normalised additive valuation, examples: $\mathbb{Q}_p$, $k(x)$, $\mathbb{C}\{\{z\}\}$

equivalence of non-archimedean norms $\Leftrightarrow$ valuation rings are the same

$\mathcal{O}_K$ is an integrally closed local domain, $\mathfrak{m}_K$ maximal ideal, $\mathcal{O}_{\widehat{K}} \cong \varprojlim \mathcal{O}_K/(\pi^n)$, $\mathcal{O}_K$ DVR $\Leftrightarrow$ $\mathcal{O}_K$ local Dedekind domain

17 $\mathcal{O}_K$ has a "thick" boundary

7.1 Structure of complete discrete valuation fields

unique writing as a Laurent series

For $k = \mathbb{F}_q$: $(1+\pi^n x)^p \in 1 + \pi^{\min(v(p)+1,np)\mathcal{O}_K}$, $(1+\pi^n x)^{q^n} \in 1+\pi^{n+1}\mathcal{O}_K$, $\forall a \in k \exists! [a] \in \mathcal{O}_K : [a]^q = [a]$ Teichmüller lift

7.2 Structure of $K^\times$

U_K^n separated and exhausted filtration

7.3 Hensel's lemma

Gauss norm, primitive polynomial, Hensel's lemma

$f(\alpha_0) \equiv 0 \pmod{\mathfrak{m}_K}, f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{m}_K} \Rightarrow f(\alpha) = 0, \alpha \equiv \alpha_0 \pmod{\mathfrak{m}_K}$, example: $x^2 - a$

$\|f\| = \max(|a_0|, |a_n|)$ for irreducible polynomials

norm on a vector space, equivalence of norms, any two norms are equivalent over finite dimensional vector spaces and the space is complete

a norm extends uniquely as $|x|_L = |\mathrm{N}_{L/K}(x)|^{1/n}$ **18**

7.4 Newton polygon

$\mathrm{NP}(f)$, there are exactly m_j roots in $\overline{K}$ with valuation s_j

f irreducible $\Rightarrow \mathrm{NP}(f)$ has only one slope, if $\mathrm{NP}(f)$ has only one slope and it is of the form $s = t/n$ with $\gcd(t,n) = 1 \Rightarrow f$ is irreducible, example

8 Finite extensions of complete discrete valuation fields

$\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L:K]$, a basis over $\mathcal{O}_K$ reduces to a basis over k **19**

ramification index, residue degree, unramified and totally ramified extension

$e(L|K)f(L|K) = [L:K]$, $\{\overline{\alpha_i} \mid i\}$ k-basis $\Rightarrow \{\alpha_i \pi_L^{j-1} \mid i,j\}$ form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$

$\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ in the totally ramified case

k'/k finite separable $\Rightarrow \exists K'/K$ unramified with $k_{K'} = k$, K' is unique, K'/K is Galois iff k'/k is. For L/K finite $\mathrm{Hom}_{K\text{-alg}}(K', L) \cong \mathrm{Hom}_{k\text{-alg}}(k', k_L)$

L/K finite, k_L/k separable $\Rightarrow \exists! L_0 \subseteq L$ so that L_0/K is unramified and $k_{L_0} = k_L$, L_0 contains all unramified extensions. Example: $\overline{\mathbb{F}_p}$

$v_L(\mathfrak{a})$, $\mathrm{N}_{L/K}(\mathfrak{a})$, $v_K(\mathrm{N}_{L/K}(\mathfrak{a})) = f(L|K)v_L(\mathfrak{a})$

ϑ dual lattice of $\mathcal{O}_L$, $\delta_{L/K}$ different, $\mathfrak{d}_{L/K}$ discriminant, behaviour for subextensions, $\delta_{L/K} = (f'(\alpha))$

Totally ramified $\Rightarrow v_L(\delta_{L/K}) \geq e(L|K) - 1$, equality in the tamely ramified case. Unramified $\Leftrightarrow v_L(\delta_{L/K}) = 0$

maximal unramified and tamely ramified extensions, these are infinite Galois extensions, $K^{\mathrm{tr}} = K^{\mathrm{un}} \cdot \bigcup_{(n,p)=1} K(\sqrt[n]{\pi_K})$

8.1 Galois extensions of complete discrete valuation fields

20 $I_{L/K}$ inertia subgroup, G_n filtration, U_L^n, equivalent definition of G_n

$\operatorname{char} k = 0 \Rightarrow G_1 = 1$, G_0/G_1 cyclic finite. $\operatorname{char} k = p > 0 \Rightarrow G_1$ finite group of p-power order, G_0/G_1 finite cyclic group of order prime to p, example: $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$

9 Global applications

Ostrowski's theorem

place, $|\cdot|_{\sigma_i}$, $v_\mathfrak{p}$, $|\cdot|_\mathfrak{p}$, $|\cdot|_v \not\sim |\cdot|_w$ and any non-trivial norm is equivalent to one of these

21 weak approximation: $K \hookrightarrow \prod K_{v_i}$ has dense image

$L \otimes_K K_v \cong \prod_{w|v} L_w$, a new proof of the fundamental equation, $\mathrm{Tr}_{L/K}(x) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x)$, same for norm, example for computing a prime decomposition

9.1 Comparison of local and global Galois groups

i_w induced map, i_w induces $\mathrm{Gal}(L_w/K_v) \xrightarrow{\sim} D_{w|v}$, $I(L_w|K_v) \xrightarrow{\sim} I$, example: computing a Galois group

9.2 Product formula

$\prod_v |x|_v = 1$, lemma: $|\,\mathrm{N}_{K/\mathbb{Q}}(x)|_p = \prod_{v|p} |x|_v$

10 Adèles and idèles

10.1 Topological groups

22 topological group, examples, T2 $\Leftrightarrow$ T1 $\Leftrightarrow$ e is closed

locally compact topological group, examples

$\varprojlim X_i \subset \prod X_i$ compact

10.1.1 Subgroups

$H \le G \Rightarrow \overline{H}$ is a topological group

every locally closed subgroup is closed, every locally compact of a T2 group is closed, any discrete subgroup is closed

in locally compact groups: a subgroup is closed $\Leftrightarrow$ locally compact

10.1.2 Quotients

the quotient map is open, $G \rhd H \Rightarrow G/H$ is a topological group and the quotient map is continuous

$H \subseteq G$ closed $\Leftrightarrow G/H$ T2, $H \subseteq G$ open $\Leftrightarrow G/H$ discrete, G locally compact and H closed $\Rightarrow G/H$ locally compact, example

$f : G \twoheadrightarrow H$ continuous map induces $f' : G/\ker f \to H$ continuous bijection, if f is open then f' is a homeomorphism, example

10.2 Adèles

restricted product, V, V_∞, V_f

G_v locally compact $\Rightarrow \prod'_v G_v$ locally compact

$\mathbb{A}_K$ adèle ring locally compact, $K_v \hookrightarrow \mathbb{A}_K$ closed

$K \hookrightarrow \mathbb{A}_K$ (diagonal embedding) discrete hence closed subgroup, $\mathbb{A}_K/K$ compact T2

$\mathbb{A}_K = K + K_\infty \times \prod_{v \in V_f} \mathcal{O}_{K_v}$

$K_\infty \times \prod_{v \in V_f} \mathcal{O}_{K_v} \hookrightarrow \mathbb{A}_K$ induces $\left(K_\infty \times \prod_{v \in V_f} \mathcal{O}_{K_v}\right) / \mathcal{O}_K \xrightarrow{\sim} \mathbb{A}_K/K$

$\left(\sum_i [0,1)\iota_\infty(\alpha_i)\right) \times \prod_v \mathcal{O}_{K_v}$ is a fundamental domain for $\mathbb{A}_K/K$ **23**

10.3 Haar measures

$C_c(X, \mathbb{R})$, positive Radon measure, $C_c(X, \mathbb{R}) = \bigcup_K C_K(X, \mathbb{R})$, topology on these

$(L_g f)(x)$ left inverse, $(L_g \Lambda)(f)$, left Haar measure, Haar's theorem about the existence and uniqueness of left Haar measures (PO)

$\mu(U) > 0$ if U is open and $0 \geq f \in C_c(X, \mathbb{R}), f \not\equiv 0 \Rightarrow \int_G f \, \mathrm{d}\mu > 0$

examples: $\mathbb{R}, \mathbb{R}^\times, \mathbb{Q}_p \supset \mathbb{Z}_p, K/\mathbb{Q}_p, \mathbb{Q}_p^\times, \mathbb{C}$

$\mathrm{mod}(\varphi)$ modulus, examples

G compact or discrete $\Rightarrow \mathrm{mod}(\varphi) = 1$

10.4 Products and infinite products

Fubini's theorem (PO)

$\prod_i \mu_i(X_i)$ converges $\Rightarrow \exists! \mu : \forall J \subseteq I, \#J < \infty : \int_X f_J \circ \mathrm{pr}_J \, \mathrm{d}\mu = \prod_{i \notin J} \mu_i(X_i) \int_{X_J} f_J \, \mathrm{d}\mu_J$

Stone–Weierstrass theorem (PO)

10.5 Construction

unique left Haar measure on a restricted product, application for number fields: induced Haar measure on $\mathbb{A}_K$ and $\mathbb{A}_K/K$

$\mu(\mathbb{A}_K/K) = \sqrt{|\operatorname{disc}_K|}$, Minkowski's theorem: $\prod_v C_v > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\operatorname{disc}_K|} \Rightarrow \exists a \in K^\times, \forall v \in V : |a|_v < C_v$

24 strong approximation: $K \hookrightarrow \mathbb{A}_K^{(v_0)} = \prod'_{v \neq v_0} K_v$ is dense

$\mathbb{A}_K/K$ is connected

10.6 Idèles

$\mathbb{I}_K$ idèle group, definition as a restricted product, $\mathbb{I}_K = \mathbb{A}_K^\times$, $\mathbb{I}_K$ has a finer topology

norm on $\mathbb{A}_K$, $x \in \mathbb{I}_K \Leftrightarrow |x| > 0$, $|\cdot|$ is an open continuous surjective homomorphism with a continuous section

$\mathbb{I}_K^1$, $\mathbb{I}_K^1 \subset \mathbb{I}_K$ is a closed subgroup, $\mathbb{I}_K/\mathbb{I}_K^1 \xrightarrow{\sim} \mathbb{R}_{>0}$ is canonical, $\mathbb{I}_K \cong \mathbb{I}_K^1 \times s(\mathbb{R}_{>0})$ non-canonical

$K^\times \subset \mathbb{I}_K$ discrete subgroup, $\mathbb{I}_K^1/K^\times$ is compact, $\mathbb{I}_K^1 \subset \mathbb{A}_K$ closed and the topology coincides with the induced one

application: $\operatorname{div} : \mathbb{I}_K \to \operatorname{Div}(\mathcal{O}_K)$ divisor map, div is surjective, $\ker \operatorname{div} = \prod_{v \in V_\infty} K_v^\times \prod_{v \notin V_\infty} \mathcal{O}_{K_v}$, $\operatorname{div}(K^\times)$ is the subgroup of principal fractional ideals, $\operatorname{Cl}_K = \dfrac{\mathbb{I}_K}{K^\times \left(K_\infty \times \prod_{v \notin V_\infty} \mathcal{O}_{K_v}\right)}$, corollary: Cl_K is finite

10.7 Generalisation

25 modulus for K, equivalent to a pair $(I, V_\mathbb{R}^+)$, $\mathcal{I}_K(m), \mathcal{P}_K(m), \operatorname{Cl}_K(m)$, special cases: $m = 0$ yields the classical notions, narrow class group

$\operatorname{Cl}_K(m)$ is finite

$0 \to \dfrac{K^\times U_K^1}{K^\times U_{K,m}} \to \operatorname{Cl}_K(m) \to \operatorname{Cl}_K \to 0$ exact, $\dfrac{K^\times U_K^1}{K^\times U_{K,m}} \cong \left(\pi_0(\mathbb{R})^{V_\mathbb{R}^+} \times \prod_{v \in V_f, m_v > 0} \dfrac{\mathcal{O}_{K,v}^\times}{1 + \mathfrak{p}_v^{m_v}}\right) / \mathcal{O}_K^\times$

examples: $\mathbb{Q}$, quadratic real field

10.8 Dirichlet's theorem

C_v, $C = \prod C_v$, $C \cap K^\times = \mu_K$

S-integers $\mathcal{O}_{K,S}$, S-units $\mathcal{O}_{K,S}^\times$, examples

Dirichlet's theorem: $\mathcal{O}_{K,S}^\times \cong \mu_K \times L$

10.9 Haar measure on $\mathbb{I}_K$

$\mathrm{d}\mu_v$ normalised on K_v, $\mathrm{d}\mu = \prod \mathrm{d}\mu_v$

26 $\operatorname{Vol}(\mathbb{I}_K/K^\times) = \dfrac{2^{r_1}(2\pi)^{r_2} R_K h}{w}$

10.10 Generalisation of the Pontryagin duality

unitary character, compact-open topology, $W(K, U)$ base

$e(x), U(\varepsilon)$

$\widehat{G}$ T2, G discrete $\Rightarrow \widehat{G}$ compact, G compact $\Rightarrow \widehat{G}$ discrete

Functoriality: $f : G_1 \to G_2$ induces $\widehat{f} : \widehat{G_2} \to \widehat{G_1}$

$\widehat{G} \xrightarrow{\sim} \varprojlim \widehat{G_n}$ canonical, examples: $\mathbb{Z}, S^1, \mathbb{R}$, finite dimensional $\mathbb{R}$-vector space, $p^{-n}\mathbb{Z}/\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$

Pontryagin' theorem (PO), a short exact sequence induces a short exact sequence of dual groups