Math 538: Algebraic Number Theory
Lecture Notes

Lior Silberman

These are rough notes for the Spring 2017 course. Problem sets and solutions were posted on an internal website.

Contents

Introduction (Lecture 1)

Lior Silberman, lior@Math.UBC.CA, http://www.math.ubc.ca/~lior
Office: Math Building 229B
Phone: 604-827-3031

0.1. Administrivia

- Problem sets will be posted on the course website.
  - To the extent I have time, solutions may be posted on Connect.
  - I will do my best to mark regularly.
- Textbooks
  - Lang, *Algebraic Number Theory*
  - Neukirch, *Algebraic Number Theory*
  - Borevich–Shafarevich, *Algebraic Number Theory*
  - Weil, *Basic Number Theory*

0.2. Course plan (subject to revision)

- Number fields, rings of integers, ideals and unique factorization. Finiteness of the class group.
- Valuations and completions; local fields.
- Ramification theory, the different and discriminant.
- Geometry of numbers: Dirichlet's Unit Theorem and discriminant bounds.
- Other topics if time permits.

0.3. Review of $\mathbb{Z}$

- Classification of elements
  - Zero
  - Units: ± 1
  - Primes: $2, 3, 5, 7, \ldots,$
  - Composite numbers
- Euclidean domain, hence a UFD
- Remarks
  - Every non-trivial ideal is of finite index
  - Every prime is maximal

0.4. Motivating examples

DEFINITION 1 (Caricature). Number Theory tries to find integer solutions to polynomial equations.

- Algebraic Number Theory: study individual solutions.
- Analytic Number Theory: count the solutions.

0.4.1. The equation $x^2+y^2=z^2$, solution 1: May assume x,y,z pairwise relatively prime. Now z is odd, wlog x is odd. Then $y^2=(z-x)(z+x)$ with $\frac{z-x}{2}, \frac{z+x}{2}$ relatively prime. Thus each is a square and we have $x=n^2-m^2$, $y=2mn$, $z=n^2+m^2$.

For a solution by the methods of this course see the

0.4.2. Primes representable as a sum of two squares.

PROBLEM 2. For which integers n does the equation $n=x^2+y^2$ have integer solutions?

FACT 3. *We have the following identity in $\mathbb{Z}[x,y,z,w]$:*

$$\left(x^2+y^2\right)\left(z^2+w^2\right)=(xz-yw)^2+(xw+yz)^2 \tag{0.4.1}$$

so it is natural to understand prime n first.

PROPOSITION 4 (Fermat). *$p=x^2+y^2$ is soluble iff $p=2$ or $p\equiv 1\,(4)$.*

COROLLARY 5. *If $n=\prod_p p^{e_p}$ is an integer such that e_p is even whenever $p\equiv 3\,(4)$ then $n=x^2+y^2$ has solutions.*

THEOREM 6. *The converse holds.*

PROOF. Consider the ring $\mathcal{O}=\mathbb{Z}[i]=\mathbb{Z}\oplus\mathbb{Z}i$. Let $z\mapsto\bar{z}$ be the non-trivial Galois automorphism of $\mathbb{Q}(i)$. Then $Nz=z\bar{z}$ is a multiplicative map $\mathcal{O}\to\mathcal{O}$ (product of two multiplicative maps), which is the formula 0.4.1. Now let $\pi\in\mathcal{O}$be a prime divisor of some rational prime p. Then $N\pi|Np=p^2$ so $N\pi\in\left\{1,p,p^2\right\}$. But $N\pi\neq 1$ (not a unit). If $N\pi=p^2$ then $N(\frac{p}{\pi})=1$ so $\pi\sim p$ and p is a prime. If $N\pi=p$ then $p=\pi\bar{\pi}$ must be the prime factorization of p, and $p=x^2+y^2$ where $\pi=x+iy$.

(1) $p\equiv 3\,(4)$. Then $p\sim\pi$ is a prime of cO since:
   (a) It is not a sum of two squares mod 4, hence not in $\mathbb{Z}$, and we are in the first case.
   (b) The map $\mathbb{F}_p[x]\to\mathcal{O}/p\mathcal{O}$ given by mapping $\mathbb{F}_p$ to $\mathbb{Z}/p\mathbb{Z}$ and x to $i+p\mathcal{O}$ factors through the field $\mathbb{F}_{p^2}\simeq\mathbb{F}_p[x]/(x^2+1)$, of the same cardinality, so $\mathcal{O}/p\mathcal{O}$ is a field. Thus (p) is a prime ideal so p is prime.

(2) If $p\equiv 1\,(4)$ then it is not prime in $\mathcal{O}$, hence there is π such that $p=N\pi$.
   (a) The order of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ is divisible by p, hence it has a solution to $x^2\equiv -1\,(p)$. If a is the solution then $p|(1+ai)(1-ai)$ but it divides neither. It follows that p isn't prime in $\mathcal{O}$.
   (b) The ring $\mathcal{O}/p\mathcal{O}$ contains four solutions to $x^2=-1$ (both $\pm a+p\mathcal{O}$ and $\pm i+p\mathcal{O}$) so it isn't a field.

(3) If $p=2$ then $p=(1+i)(1-i)=-i(1+i)^2$ since $(1+i)\sim(1-i)$.
   - Note that if $p\equiv 1\,(4)$ and $p=x^2+y^2$ then $x\pm iy$ are non-associate primes, since the only units in $\mathbb{Z}[i]$ are $\pm 1,\pm i$ but if $x-iy=i^a(x+iy)$ then either $x+iy$ is totally real, totally complex, or $|x|=|y|$ and all cases are impossible.

□

Summary.

- Every prime p of $\mathbb{Z}$ is either inert, split or ramified (only finitely many primes of the latter kind)
- Remarks about Chebotarev density.
- This classification covers all primes of $\mathbb{Z}[i]$ since if π is a prime then π divides the non-unit $N\pi \in \mathbb{Z}$ and hence one of its prime factors, so $\pi | p$ for some rational prime p.

0.4.3. Remark. Let $K = \mathbb{Q}(\sqrt{-3})$. Then $\mathbb{Z}[\sqrt{-3}]$ is a subring like above, but in it 2 is prime (norm too small to have proper divisors) and $2|(1+\sqrt{-3})(1-\sqrt{-3})$ without 2 dividing any of the factors. Nevertheless set $\omega = \frac{-1+\sqrt{-3}}{2}$. Then $K = \mathbb{Q}(\omega)$ and in $\mathbb{Z}[\omega] = \mathbb{Z} \oplus \mathbb{Z}[\omega]$ there's unique factorization (this is a ring since $\omega^2 + \omega + 1 = 0$).

0.5. Fermat's Last Theorem (Lecture 2)

0.5.1. Lamé's mistake. Let x, y, z be a primitive solution to $x^p + y^p = z^p$ where p is an odd prime.

We can equivalently write this as

$$z^p = (x-y)\prod_{j=1}^{p-1}\left(x - \zeta^j y\right)$$

where ζ is a primitive pth root of unity. It's therefore natural to work in the ring $\mathcal{O} = \mathbb{Z}[\zeta]$ of cyclotomic integers (when $p = 4$ this is $\mathbb{Z}[i]$, when $p = 3$ this is $\mathbb{Z}[\omega]$). Let ρ be a common divisor of $x - \zeta^j y, x - \zeta^k y$. It then divides $(\zeta^j - \zeta^k)y$ and $(\zeta^{-j} - \zeta^{-k})x$. For any $j \not\equiv k\,(p)$, $\zeta^j - \zeta^k = \zeta^j(1-\zeta^{k-j}) = \zeta^j \frac{1-\zeta^{k-j}}{1-\zeta}(1-\zeta)$ so ρ divides $(1-\zeta)x, (1-\zeta)y$. Since x, y are relatively prime we have $\rho | \pi = 1 - \zeta$ which is a prime element since $\pi^{p-1} \times (\text{unit}) = \prod_{j=1}^{p-1}(1-\zeta^j) = \Phi(1) = p$ where $\Phi(x) = \frac{x^p-1}{x-1}$ is the pth cyclotomic polynomial.

Case 1. p divides none of x, y, z. Then the $(x - \zeta^j y)$ are pairwise relatively prime (including $j = 0$) so there is $\varepsilon \in \mathcal{O}^\times$, $t \in \mathcal{O}$ such that

$$x - \zeta y = \varepsilon t^p\,.$$

If τ denotes complex conjugation we then have

$$x - \zeta^{-1} y = \tau(\varepsilon)\tau(t)^p\,.$$

Now, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ we have $\left|\sigma\frac{\tau(\varepsilon)}{\varepsilon}\right| = \left|\frac{\tau(\sigma(\varepsilon))}{\sigma(\varepsilon)}\right| = 1$ since the Galois group is commutative. It follows that $\frac{\tau(\varepsilon)}{\varepsilon}$ is a root of unity, hence of the form ζ^{-r} for some r. Also, for any $t \in \mathcal{O}$, there is $a \in \mathbb{Z}$ such that $t \equiv a\,(\pi)$. Since $t^p - a^p \equiv (t-a)^p\,(p)$ and since $p | \pi^{p-1} | \pi^p$ we have $t^p \equiv a^p\,(p)$ and hence $\tau(t)^p \equiv a^p \equiv t^p\,(p)$. Thus

$$x - \zeta^{-1} y = \zeta^{-r}\varepsilon\tau(t)^p \equiv \zeta^{-r}(x - \zeta y)\,(p)\,.$$

If $\zeta^r = 1$ this implies $(\zeta - \zeta^{-1})y \equiv 0\,(p)$ so $p|(1-\zeta)y$, so $\pi^{p-2}|y$. But this would force $p|y$ which isn't the case. Otherwise, we have for some $1 \le r \le p-1$,

$$\zeta^{r-1}(\zeta x - y) \equiv x - \zeta y\,(p)\,,$$

which we can rewrite as

$$(1-\pi)^{r-1}(x-y-\pi x)-(x-y+\pi y)\equiv 0\,(p)\,.$$

Expanding in a power series in π, if $2\le r\le p-2$ the highest-order term is $x\pi^r$ and we must have $p|x$ which is impossible. For $r=1$, $r=p-1$ one can derive a similar contradiction.

Case 2. $p|z$. Now π divides each of the $x-\zeta^j y$ (also $x-y$), and the $\frac{x-\zeta^j y}{1-\zeta}$ are pairwise relatively prime. We thus have

$$\left(\frac{z}{\pi}\right)^p=\prod_{j=0}^{p-1}\frac{x-\zeta^j y}{\pi}$$

where the factors on the right are relatively prime. It follows that for some $\varepsilon_j\in\mathcal{O}^\times$ and $t_j\in\mathcal{O}$,

$$x-\zeta^j y=\varepsilon_j\pi t_j^p$$

furthermore, the t_j are relatively prime. Now the $x-\zeta^j y$ where $j\neq 0$ are all divisible by π exactly once (since they are all conjugate, and their differences are divisible exactly once), so $\pi\nmid t_j$ for $j\neq 0$ and $\pi\mid t_0$ since $p|z$.

CHAPTER 1

Number Fields and Algebraic Integers

DEFINITION 7. A (global) *number field* is a finite extension of $\mathbb{Q}$.

Fix a number field K and set $n = [K : \mathbb{Q}]$.

1.1. Algebraic Integers (Lecture 3)

DEFINITION 8. An element $\alpha \in K$ is said to be an *algebraic integer* if $p(\alpha) = 0$ for some monic polynomial $p \in \mathbb{Z}[x]$. The set of algebraic integers in K is denoted $\mathcal{O}_K$ and called the "ring of integers" or the "maximal order".

LEMMA 9. *$\alpha \in K$ is an algebraic integer iff its minimal polynomial is in $\mathbb{Z}[x]$.*

PROOF. One direction is immediate. For the other, let $p \in \mathbb{Z}[x]$ be monic such that $p(\alpha) = 0$ and let $m \in \mathbb{Q}[x]$ be the minimal polynomial. Then m is an irreducible factor of p in $\mathbb{Q}[x]$, but by Gauss's Lemma every such divisor is in $\mathbb{Z}[x]$. □

EXAMPLE 10. $K = \mathbb{Q}$. The minimal polynomial of α is $x - \alpha$ so $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. This is the "rational root theorem".

EXAMPLE 11. $K = \mathbb{Q}(i)$. The minimal polynomial of $a + bi$ is $(x - a - bi)(x - a + bi) = (x-a)^2 + b^2 = x - (2a)x + (a^2 + b^2)$. This is $\mathbb{Z}[x]$ iff $2a, a^2 + b^2 \in \mathbb{Z}$. Thus $a \in \frac{1}{2}\mathbb{Z}$. If $a \in \mathbb{Z}$ then $b \in \mathbb{Q}$, $b^2 \in \mathbb{Z}$ so $b \in \mathbb{Z}$. If $a \notin \mathbb{Z}$ then $(2a)^2 + (2b)^2 \in 4\mathbb{Z}$ where $2a$ is an odd integer. This forces $(2b)^2$ to be an integer, hence $2b$ to be an integer, but then $(2b)^2$ is $0, 1 \bmod 4$ which is impossible since $(2a)^2 \equiv 1\,(4)$. Thus $a + bi$ is algebraic iff $a, b \in \mathbb{Z}$.

REMARK 12. Note that $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of K.

LEMMA 13. *$\beta \in \mathcal{O}_K$ iff $\mathbb{Z}[\beta]$ is a finitely generated Abelian group iff there is a finitely generated Abelian group $M \subset K$ such that $\beta M \subset M$.*

PROOF. If $\beta \in \mathcal{O}_K$ then $\mathbb{Z}[\beta] = \mathbb{Z} \oplus \mathbb{Z}\beta \oplus \cdots \oplus \mathbb{Z}\beta^{n-1}$ where β has degree n. The last claim implies the first by Cayley–Hamilton. □

THEOREM 14. *Let $\alpha, \beta \in K$ be algebraic integers. Then so are $\alpha \pm \beta$, $\alpha\beta$.*

PROOF. Suppose that $\alpha M \subset M$, $\beta N \subset N$, where $M = \sum_{i=1}^{r} \mathbb{Z}x_i$, $N = \sum_{j=1}^{s} \mathbb{Z}y_j$. Then $MN = \sum_{i,j} \mathbb{Z}x_i y_j$ is invariant by α, β hence by $\mathbb{Z}[\alpha, \beta]$ which contains the requisite elements. □

COROLLARY 15. *$\mathcal{O}_K$ is a subring of K. If $\alpha \in \mathcal{O}_K$ then:*

(1) Every Galois conjugate of α is integral over $\mathbb{Q}$;
(2) The minimal polynomial of α over $\mathbb{Q}$ is monic and belongs to $\mathbb{Z}[x]$;
(3) $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha), N_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}$ and,
(4) $\alpha \in \mathcal{O}_K^{\times}$ iff $N_{\mathbb{Q}}^{K}\alpha \in \mathbb{Z}^{\times} = \{\pm 1\}$.

PROOF. (1) Let L be a normal extension containing K. Then $\mathcal{O}_L \cap K = \mathcal{O}_K$ by definition, and every conjugate of α satisfies the same polynomials that α does.

(2) The minimal polynomial of α is $\prod_{\mu \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})} (x - \mu\alpha) = \prod_{\sigma \in \mathrm{Hom}(\mathbb{Q}(\alpha), L)} (x - \sigma\alpha) \in \mathcal{O}_L[x] \cap \mathbb{Q}[x] = \mathbb{Z}[x]$ since $\mathcal{O}_L$ is a ring.

(3) now follows by taking specific coefficients.

(4) Exercise. □

LEMMA 16. *Let $\alpha \in K$. Then there is $m \in \mathbb{Z}$ so that $m\alpha \in \mathcal{O}_K$.*

PROOF. Let $f = \sum_{i=0}^{d} a_i x^i \in \mathbb{Q}[x]$ be the (monic) minimal polynomial of α. Then $\sum_{i=0}^{d} m^{d-i} a_i (m\alpha)^i = 0$. If m is large enough then $m^{d-i} a_i \in \mathbb{Z}$ for all $0 \leq i < d$. □

COROLLARY 17. *There exists a basis of K consisting of elements of $\mathcal{O}_K$.*

LEMMA 18. *The quadratic form $(x, y) \mapsto \mathrm{Tr}(xy)$ is non-degenerate.*

PROOF. $\mathrm{Tr}(x \cdot x^{-1}) = n$. □

PROPOSITION 19. *There exist a $\mathbb{Q}$-basis $\{\omega_i^*\}_{i=1}^n \subset K$ so that $\mathcal{O}_K \subset \oplus_i \mathbb{Z}\omega_i^*$.*

PROOF. Take $\{\omega_i^*\}$ be the basis dual to a basis contained in $\mathcal{O}_K$ w.r.t. the trace form. □

CONCLUSION 20. The $\mathbb{Z}$-module $\mathcal{O}_K$ embeds in $\mathbb{Z}^n$ and contains a copy of $\mathbb{Z}^n$.

THEOREM 21. *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

PROOF. Classification of finitely generated Abelian groups. □

1.2. The absolute discriminant (skipped)

Fix a number field K, and let $n = [K : \mathbb{Q}]$

DEFINITION 22. A ($\mathbb{Z}$-)*lattice* in K is a subgroup $L = \oplus_{i=1}^n \mathbb{Z}\omega_i$ where $\{\omega_i\}_{i=1}^n$ is a Q-basis of K.

Let $\{\sigma_j\}_{j=1}^n$ be an enumeration of $\mathrm{Hom}(K, \overline{\mathbb{Q}})$.

LEMMA 23. *Given $\{\omega_i\}_{i=1}^n \subset K$, let A be the matrix where $A_{ij} = \sigma_j(\omega_i)$. Let B be the matrix where $B_{ij} = \mathrm{Tr}_{\mathbb{Q}}^K \omega_i\omega_j$ ("the Gram matrix of the quadratic space $\left(\oplus_{i=1}^n \mathbb{Z}\omega_i, \mathrm{Tr}_{\mathbb{Q}}^K\right)$"). Then $(\det A)^2 = \det B$.*

PROOF. $B = AA^{\mathrm{t}}$ since $\mathrm{Tr}_Q^K(x) = \sum_j \sigma_j(x)$. □

LEMMA 24. *Let $K = \mathbb{Q}(\alpha)$, and let $\omega_i = \alpha^{i-1}$. Then $\det B = \Delta(f)$ where $f \in \mathbb{Q}[x]$ is the minimal polynomial of α.*

PROOF. $\det A = \prod_{i<j} (\omega_i - \omega_j)$ by the Vandermonde determinant, and $\Delta(f) = \prod_{i<j} (\omega_i - \omega_j)^2$. □

LEMMA 25. *$\gamma \in M_n(\mathbb{Q})$, and let A', B' be the associated matrices. Then $\det B' = (\det \gamma)^2 \det B$.*

PROOF. $B' = \gamma B \gamma^{\mathrm{t}}$. □

COROLLARY 26. *$\det B \neq 0$ iff $\{\omega_i\}$ is a $\mathbb{Q}$-basis.*

PROOF. Any sequence has a unique representation as $\omega_i = \sum_j \gamma_{ij}\alpha^{j-1}$ $K = \mathbb{Q}(\alpha)$ and $\gamma_{ij} \in \mathbb{Q}$. Then $\det B = (\det\gamma)^2 \Delta(f)$ where $\Delta(f) \neq 0$ and $\{\omega_i\}$ is a basis iff $\gamma \in \mathrm{GL}_n(\mathbb{Q})$ iff $\det\gamma \neq 0$. □

COROLLARY 27. *If* $\det B \neq 0$ *it only depends on the lattice generated by the* $\{\omega_i\}_{i=1}^n$ *and will be denoted* $d_{K/\mathbb{Q}}(L)$.

PROOF. If $\{\omega_i\}, \left\{\omega_j'\right\}$ generate the same lattice they are related by a matrix in $\mathrm{GL}_n(\mathbb{Z})$ whose squared determinant is therefore 1. □

PROPOSITION 28. *Let* $L_1 \subset L_2$ *be two lattices. Then* $d_{K/\mathbb{Q}}(L_1) = [L_2 : L_1]^2 d_{K/\mathbb{Q}}(L_2)$.

PROOF. Gaussian elimination. □

LEMMA 29. *Let* $L \subset \mathcal{O}_K$ *be a lattice. Then* $d_{K/\mathbb{Q}}(L) \in \mathbb{Z} \setminus \{0\}$

PROOF. The associated matrix B consists of integers. □

DEFINITION 30. The *absolute discriminant* of K is the number $d_K = d_{K/\mathbb{Q}}(\mathcal{O}_K)$.

REMARK 31. Suppose that $L \subset \mathcal{O}_K$ is a lattice and $d_{K/\mathbb{Q}}(L) = d = e^2 f$ with f squarefree. Since $d_{K/\mathbb{Q}}(L) = d_K [\mathcal{O}_K : L]^2$ it follows that $[\mathcal{O}_K : L] \,|e$ and hence that $L \subset \mathcal{O}_K \subset \frac{1}{e}L$, which reduces the problem of finding $\mathcal{O}_K$ to checking a coset representative for each element of $\frac{1}{e}L/L$ to see if it is integral.

For a starting point let $K = \mathbb{Q}(\alpha)$ where $\alpha \in \mathcal{O}_K$. Then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$.

EXAMPLE 32. Let $K = \mathbb{Q}(\sqrt{d})$ with d squarefree. Then $d_{K/\mathbb{Q}}\left(\mathbb{Z} \oplus \mathbb{Z}\left[\sqrt{d}\right]\right) = \det\begin{pmatrix} \mathrm{Tr}\,1 & \mathrm{Tr}\sqrt{d} \\ \mathrm{Tr}\sqrt{d} & \mathrm{Tr}\,d \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d$. It follows that

$$d_K = \begin{cases} d & d \equiv 1\,(4) \\ 4d & d \equiv 2,3\,(4) \end{cases}$$

Integers of the form are called *fundamental discriminants.*

1.3. Unique factorization (Lectures 4,5)

Fix a number field K of degree n. We will study the ideals in $\mathcal{O}_K$.

DEFINITION 33 (Warm-up). Let I, J be ideals of a ring R. Then $IJ = \left\{\sum_{i=1}^k a_i b_i \mid a_i \in I,\, b_j \in J\right\}$ is the ideal generated by all products ab with $a \in A$, $b \in B$.

EXERCISE 34. This turns the set of ideals into a monoid.

CONVENTION. *For this section, "ideal" always means a non-zero ideal (but includes the whole ring). A "prime" of* $\mathcal{O}_K$ *always means a prime ideal, not a prime element. We say "rational prime" to mean a prime number* $p \in \mathbb{Z}$.

PROPOSITION 35. *(Ideals of* $\mathcal{O}_K$*) Fix a proper ideal* $\mathfrak{a} \lhd \mathcal{O}_K$.

(1) $\mathfrak{a} \cap \mathbb{Z}$ *is a non-zero proper ideal of* $\mathbb{Z}$.

(2) $[\mathcal{O}_K : \mathfrak{a}] < \infty$.

(3) $\mathfrak{a}$ *is finitely generated. In fact,* $\operatorname{rank}_{\mathbb{Z}} \mathfrak{a} = n$.
(4) If $\mathfrak{a}$ *is prime then it is maximal, and* $\mathfrak{a} \cap \mathbb{Z} = (p)$ *for a prime number* p.

PROOF. Exercise. □

DEFINITION 36. The *norm* of an ideal is $N\mathfrak{a} \stackrel{\text{def}}{=} [\mathcal{O}_K : \mathfrak{a}] = \#(\mathcal{O}_K/\mathfrak{a})$.

DEFINITION 37. Say that a prime $\mathfrak{p} \lhd \mathcal{O}_K$ *lies above* $(p) \lhd \mathbb{Z}$ if $\mathfrak{p} \cap \mathbb{Z} = (p)$.

REMARK 38. Conversely, it is clear that for any rational prime p, $p\mathcal{O}_K$ is a proper ideal of $\mathcal{O}_K$, hence that there exist primes lying above (p). In the case of an extension L/K of number fields, the argument above still shows that every prime of L (that is, of $\mathcal{O}_L$) lies above a prime of K. The converse is not as easy – see Proposition 52

We will now develop a theory of unique factorization in $\mathcal{O}_K$. The result is due to Kummer, the proof due to Dedekind.

As motivation, consider the following inductive proof that every integer is a product of irreducibles: let $a \geq 1$ be minimal among those which are not products of primes. Then $a \geq 2$; let $p = \min\{b \mid 2 \leq b, b|a\}$. Then p is irreducible (any factors would divide n also and be smaller). By construction $\frac{n}{p} < n$ so it is a product of primes. Now multiply both sides by p. Replacing a with an ideal $\mathfrak{a}$, we replace p with a maximal ideal $\mathfrak{p}$ containing $\mathfrak{a}$. One issue now is constructing an ideal $\mathfrak{p}^{-1}\mathfrak{a}$ such that $\mathfrak{p}\left(\mathfrak{p}^{-1}\mathfrak{a}\right) = \mathfrak{a}$, but the real difficulty is in showing that $\mathfrak{p}^{-1}\mathfrak{a}$ is "smaller" that $\mathfrak{a}$ in the appropriate sense (its index in $\mathcal{O}_K$ is smaller) so that the inductive argument can run.

DEFINITION 39. An $\mathcal{O}_K$-submodule $\mathfrak{a} \subset K$ is a *fractional ideal* if there is $\alpha \in K^\times$ so that $\alpha\mathfrak{a} \subset \mathcal{O}_K$.

Given fractional ideals $\mathfrak{a}, \mathfrak{b}$ let $\mathfrak{ab}$ be the module generated by all products xy, $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. This is also a fractional ideal. Multiplication of fractional ideals is commutative and associative, and has the unit $(1) = \mathcal{O}_K$. We call a fractional ideal *invertible* if it is invertible in this commutative monoid (we will later show that this is a group).

LEMMA 40. *Every proper ideal of* $\mathcal{O}_K$ *contains a product of primes.*

PROOF. Let $\mathfrak{a}$ be a maximal counterexample. It is not prime so there are $x, y \in \mathcal{O}_K \setminus \mathfrak{a}$ with $xy \in \mathfrak{a}$. Then $(\mathfrak{a}, x)(\mathfrak{a}, y) = \mathfrak{a}$, a contradiction. □

PROPOSITION 41. *Let* $\mathfrak{p} \lhd \mathcal{O}_K$ *be prime. Then* $\mathfrak{p}^{-1} \stackrel{def}{=} \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}_K\}$ *is a fractional ideal properly containing* $\mathcal{O}_K$. *In particular,* $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

PROOF. Let $p \in \mathbb{Z}$ be the prime lying below $\mathfrak{p}$. Let $x, y \in \mathfrak{p}^{-1}$ and $\alpha \in \mathcal{O}_K$. First, $(\alpha x + y)\mathfrak{p} \subset x\mathfrak{p} + y\mathfrak{p} \subset \mathcal{O}_K + \mathcal{O}_K = \mathcal{O}_K$. Second, if $x \in \mathfrak{p}^{-1}$ then $xp \in x\mathfrak{p} \subset \mathcal{O}_K$ so $p\mathfrak{p}^{-1} \subset \mathcal{O}_K$. $\mathfrak{p}^{-1} \supset \mathcal{O}_K$ by definition of ideal, and the real issue (as noted above) is to see that $\mathfrak{p}^{-1} \neq \mathcal{O}_K$. For this note that the ideal $p\mathcal{O}_K$ contains a product of prime ideals. Let $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ be a minimal such product. Since $\mathfrak{p}$ contains this product, it contains one factor, and hence equal to it (all primes are maximal). Let $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus p\mathcal{O}_K$ (this exists by minimality of r). Then $a\mathfrak{p} \subset p\mathcal{O}_K$ so $\frac{a}{p}\mathfrak{p} \subset \mathcal{O}_K$ but $\frac{a}{p} \notin \mathcal{O}_K$. Finally, $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}_K$. Since $\mathfrak{p}\mathfrak{p}^{-1}$ is an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$ and $\mathfrak{p}$ is a maximal ideal one side must be an equality. If $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ held then every $y \in \mathfrak{p}^{-1}$ would preserve the finitely generated $\mathbb{Z}$-module $\mathfrak{p}$ and hence be integral, a contradiction. □

THEOREM 42. *All ideals of $\mathcal{O}_K$ are invertible; every ideal can be uniquely written in the form $\prod_{i=1}^r \mathfrak{p}_i^{e_i}$ with $\mathfrak{p}_i$ prime and $e_i \in \mathbb{Z}_{>0}$. $\mathfrak{a}|\mathfrak{b}$ in the monoid of ideals iff $\mathfrak{b} \subset \mathfrak{a}$.*

PROOF. First, let $\mathfrak{a} \lhd \mathcal{O}_K$ be a proper ideal and let $\mathfrak{a} \subset \mathfrak{p} \lhd \mathcal{O}_K$ be a maximal ideal. Then $\mathfrak{p}^{-1}\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$ and $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$ since $\mathfrak{p}^{-1} \not\subset \mathcal{O}_K$.

Now let $\mathfrak{a} \lhd \mathcal{O}_K$ be maximal among the ideal without representation as a product of primes. Then $\mathfrak{p}^{-1}\mathfrak{a}$ can be written as such a product, and hence so can $\mathfrak{a}$. If $\mathfrak{a} = \prod_i \mathfrak{p}_i$ then $\mathfrak{a}\prod_i \mathfrak{p}_i^{-1} = \mathcal{O}_K$ so $\mathfrak{a}$ is invertible. For uniqueness let $\prod_{i=1}^r \mathfrak{p}_i = \prod_{j=1}^t \mathfrak{q}_j$. Then $\mathfrak{p}_r$ contains the product on the left, hence the product on the right, hence equal to one of the factors. Multiplying by $\mathfrak{p}_r^{-1}$ the claim follows by induction on r.

Finally, $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ then certainly $\mathfrak{b} \subset \mathfrak{a}$. Conversely, if $\mathfrak{b} \subset \mathfrak{a}$ then $\mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_K$. □

COROLLARY 43. *Every fractional ideal is invertible, so that the fractional ideals form a group. Every element of this group has a unique representation in the form $\prod_{i=1}^r \mathfrak{p}_i^{e_i}$ with $e_i \in \mathbb{Z} \setminus \{0\}$.*

DEFINITION 44. Call a fractional ideal *principal* if it is of the form $\alpha\mathcal{O}_K$ for some $\alpha \in K^\times$. Say that two fractional ideals $\mathfrak{a}, \mathfrak{b}$ are *in the same class* if $\mathfrak{a}\mathfrak{b}^{-1}$ is principal (note that every fractional ideal is in the same class as an ideal by definition). The principal fractional ideals form a subgroup of the group of fractional ideals. The *class group* of K is the quotient $\mathrm{Cl}(K)$ of the group of ideals by the group of principal ideals. It measures the failure of unique factorization.

THEOREM 45 (Dedekind). $\mathrm{Cl}(K)$ *is a finite group. Its order is denoted h_K and called the* class number *of K.*

This is an immediate Corollay of Theorem 189 of Section 4.3.

REMARK 46. Every prime ideal contains irreducible elements (an element of minimal norm must be irreducible) but if it contains a prime element the ideal is principal since non-zero prime ideals are maximal.

REMARK 47 (Hilbert Classfield + Chebotarev's Density Theorem). $\lim_{x\to\infty} \frac{\#\{\mathfrak{p}|N\mathfrak{p}\leq x, \mathfrak{p} \text{ principal}\}}{\#\{\mathfrak{p}|N\mathfrak{p}\leq x\}} = \frac{1}{h_K}$.

1.4. Primes in extensions (Lectures 6,7,8)

Fix a finite extension L/K of number fields and a prime $\mathfrak{p} \lhd \mathcal{O}_K$.

1.4.1. Residue field extensions and ramification (Lecture 6).

LEMMA 48. *Let $\mathfrak{P}$ be a prime of L. Then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime of K, and $\mathfrak{P}$ contains no other prime of K.*

PROOF. Exercise. □

DEFINITION 49. In the setting above we say that $\mathfrak{P}$ *lies above* $\mathfrak{p}$ and write $\mathfrak{P}|\mathfrak{p}$.

In the setting of Definition 49, the $\mathcal{O}_K$-module $\mathcal{O}_L/\mathfrak{P}$ is annihilated by $\mathfrak{p}$, so is in fact a $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$-module. In other word, the finite field $k_\mathfrak{P}$ is an extension of the finite field $k_\mathfrak{p}$.

DEFINITION 50. The number $q_\mathfrak{p} = \#\mathcal{O}_K/\mathfrak{p}$ is called the residue field size. $f(\mathfrak{P}/\mathfrak{p}) \stackrel{\text{def}}{=} \left[k_\mathfrak{P} : k_\mathfrak{p}\right] = \dim_{k_\mathfrak{p}} k_\mathfrak{P}$ is called the *residue index* or the *inertial degree.*

LEMMA 51. *Let $\mathfrak{p}$ be a prime of K. Then $\mathfrak{P}|\mathfrak{p}$ iff $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$.*

PROOF. Exercise. □

PROPOSITION 52. *$\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$. In particular, $\{\mathfrak{P} \lhd \mathcal{O}_L \mid \mathfrak{P}|\mathfrak{p}\}$ is non-empty and finite.*

PROOF. Exercise. □

DEFINITION 53. Let $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ be the factorization of $\mathfrak{p}\mathcal{O}_L$. We write $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$ and call this number the *ramification index* or the *ramification degree*. We also write $f_i = f(\mathfrak{P}_i/\mathfrak{p})$ for the residue index.

LEMMA 54. *Let $\mathfrak{P} \lhd \mathcal{O}_L$ be prime. Then for all $e \geq 1$, $\mathcal{O}_L/\mathfrak{P}^e$ is a dvr – a local ring and a PID.*

PROOF. The ideals of $\mathcal{O}_L/\mathfrak{P}^e$ correspond to the ideals of $\mathcal{O}_L$ containing $\mathfrak{P}^e$, which by unique factorization are $\mathfrak{P}^j$ for $1 \leq j \leq e$. Let $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, and let $\bar{\pi}$ be its image mod $\mathfrak{P}^e$. Then the image of $\mathfrak{P}^j$ is $(\bar{\pi})^j$. □

THEOREM 55. $n = \sum_{i=1}^{g} e_i f_i$.

PROOF. We calculate the dimension of the $k_\mathfrak{p}$-vector space $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ in two different ways. First, since $\mathfrak{P}_i$ are maximal ideals, we have $\mathfrak{P}_i + \mathfrak{P}_j = (1)$ for all j. It follows that $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = (1)$ (Exercise). Also, $\mathfrak{p}\mathcal{O}_L = \cap_{i=1}^{g} \mathfrak{P}_i^{e_i}$ (they have the same prime factorization). By the CRT, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \oplus_{i=1}^{g} \mathcal{O}_L/\mathfrak{P}_i^{e_i}$. Now $\mathcal{O}_L/\mathfrak{P}_i^{e_i} \simeq \mathcal{O}_L/\mathfrak{P}_i \oplus_{j=1}^{e_i-1} \mathfrak{P}^j/\mathfrak{P}^{j+1}$ and by Lemma 54 multiplication by $\bar{\pi}^j$ gives gives a vector space isomorphism $\mathcal{O}_L/\mathfrak{P}_i \to \mathfrak{P}^j/\mathfrak{P}^{j+1}$, so $\dim_{k_\mathfrak{p}} \mathcal{O}_L/\mathfrak{P}_i^{e_i} = e_i f_i$.

In the other direction, if $K = \mathbb{Q}$ then $\mathcal{O}_L/p\mathcal{O}_L \simeq \mathbb{Z}^n/p\mathbb{Z}^n \simeq (\mathbb{Z}/p\mathbb{Z})^n$ and the proof is over. Unfortunately, in general $\mathcal{O}_L$ is not a free $\mathcal{O}_K$-module and we need to work harder. Specifically, we may localize at $\mathfrak{p}$ first. $\mathcal{O}_{K,\mathfrak{p}}$ is a PID (same proof as for $\mathcal{O}_L/\mathfrak{P}^e$), and $\mathcal{O}_L[S^{-1}]$ ($S = \mathcal{O}_K \setminus \mathfrak{p}$) is a torsion-free module, hence free. Since K is a further localization, it follows that $\mathcal{O}_L[S^{-1}] \simeq \mathcal{O}_{K,\mathfrak{p}}^n$ for $n = [L:K]$. Finally, $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_L[S^{-1}]/\mathfrak{p}\mathcal{O}_L[S^{-1}]$ as $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \simeq k_\mathfrak{p}$-modules. □

1.4.2. Explicit factorization (Lecture 7).

THEOREM 56. *Suppose $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, and let $f \in \mathcal{O}_K[x]$ be the minimal polynomial of α over K. For a prime $\mathfrak{p} \lhd \mathcal{O}_K$ Let $\bar{f} = \prod_{i=1}^{r} \bar{P}_i^{e_i}$ be the factorization of the image of f in $k_\mathfrak{p}[x]$ into irreducibles. Then there are r primes of L lying above $\mathfrak{p}$, and $f(\mathfrak{P}_i/\mathfrak{p}) = \deg \bar{P}_i$ and $e(\mathfrak{P}_i/\mathfrak{p}) = e_i$.*

PROOF. We have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}_K[x]/(f,\mathfrak{p}) \simeq k_\mathfrak{p}[x]/\left(\bar{f}\right) \simeq \bigoplus_{i=1}^{r} k_\mathfrak{p}[x]/\left(\bar{P}_i^{e_i}\right).$$

It follows that there are r ideals of $\mathcal{O}_L$ in the factorization of $\mathfrak{p}$, with $\mathcal{O}_L/\mathfrak{P}_i \simeq k_\mathfrak{p}[x]/(\bar{P}_i)$ hence $f(\mathfrak{P}_i/\mathfrak{p}) = \deg \bar{P}_i$. Also, $\prod_{i=1}^{r} \mathfrak{P}_i^{e_i} \subset \mathfrak{p}\mathcal{O}_L$ (in the quotient the LHS maps to zero) but this holds for no smaller exponents, so we have found the e_i. □

EXAMPLE 57. In $K = \mathbb{Q}(\sqrt{-5})$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ with minimal polynomial x^2+5. Mod 2 this factors as $(x+1)^2$ so 2 ramifies. To find generators for the prime we want to take the inverse image of the ideal $(x+1)/\left((x+1)^2\right)$ in $\mathbb{F}_2[x]/\left((x+1)^2\right)$, so the ideal will be $\left(2, 1+\sqrt{-5}\right)$.

Mod 3 this factors as $(x+1)(x-1)$ so the two ideals will be $\left(3, \pm 1+\sqrt{-5}\right)$.

REMARK 58. In case where $\mathcal{O}_L$ is not of this form localize at $\mathfrak{p}$ first.

Furthermore, if $[\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ is prime to p (the rational prime under $\mathfrak{p}$) then there is no need to localize since these two rings have the same localization.

1.4.3. Galois extensions (Lecture 8). We assume now that L/K is Galois, with Galois group $G = \mathrm{Gal}(L:K)$. It is clear that G acts on the set of primes $\{\mathfrak{P}_i\}_{i=1}^{g}$ lying over $\mathfrak{p}$.

PROPOSITION 59. *G acts transitively on the primes above $\mathfrak{p}$.*

PROOF. Suppose that $\mathfrak{P}'$ is not in the G-orbit of $\mathfrak{P}$. By the CRT there exists $x \in \mathcal{O}_L$ such that $x \in \mathfrak{P}'$ but $x \notin (\sigma\mathfrak{P})$ for all $\sigma \in G$. It follows that $\sigma x \notin \mathfrak{P}$ for all $\sigma \in G$, and since $\mathfrak{P}$ is prime we have $N_K^L x \notin \mathfrak{P}$. But $N_K^L x \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p} \subset \mathfrak{P}$, a contradiction. □

COROLLARY 60. *All primes above $\mathfrak{p}$ have the same residual degree and ramification index, and we have $efr = n$.*

DEFINITION 61. *The decomposition group at $\mathfrak{P}$ is the subgroup $G_{\mathfrak{P}} = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$.*

Note that the action of $\sigma \in \mathfrak{P}$ preserves congruence mod $\mathfrak{P}$, and hence descends to an action on $k_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$, fixing $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{P}$. In other words, there is a natural homomorphism

$$G_{\mathfrak{P}} \to \mathrm{Gal}\left(k_{\mathfrak{P}} : k_{\mathfrak{p}}\right).$$

LEMMA 62. *Let $K \subset E \subset L$ be the fixed field of $G_{\mathfrak{P}}$. Then $\mathfrak{P}$ is the unique ideal of $\mathcal{O}_L$ lying above $\mathfrak{P} \cap \mathcal{O}_E$, and the injection $\mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_E/\mathfrak{P} \cap \mathcal{O}_E$ is an isomorphism.*

PROOF. $G_{\mathfrak{P}} = \mathrm{Gal}(L:E)$ acts transitively on the set of primes lying above $\mathfrak{P} \cap \mathcal{O}_E$; this set includes the fixed point $\mathfrak{P}$. Finally, let $\alpha \in \mathcal{O}_E$. There is $\beta \in \mathcal{O}_E$ such that $\beta \equiv \alpha\,(\mathfrak{P} \cap \mathcal{O}_E)$ and $\beta \equiv 1\ (\sigma\mathfrak{P} \cap \mathcal{O}_E)$ for all $\sigma \in G \setminus G_{\mathfrak{P}}$ (note that $\sigma\mathfrak{P}$ does not lie over $\mathfrak{P} \cap \mathcal{O}_E$ in that case). Then $N_K^E \beta \in \mathcal{O}_K$ and $N_K^E \beta \equiv \alpha\,(\mathfrak{P})$. It follows that $N_K^E \beta \equiv \alpha\,(\mathfrak{P} \cap \mathcal{O}_E)$. □

PROPOSITION 63. *This map $G_{\mathfrak{P}} \to \mathrm{Gal}\left(k_{\mathfrak{P}} : k_{\mathfrak{p}}\right)$ is surjective.*

PROOF. WLOG may replace K with E, $\mathfrak{p}$ with $\mathfrak{P} \cap \mathcal{O}_E$ (same residue field) so may assume there is a unique prime of L over $\mathfrak{p}$, and that $G_{\mathfrak{P}} = G$. Let $\alpha \in \mathcal{O}_L$ project to $\bar{\alpha} \in k_{\mathfrak{P}}$ generating the extension, and let $f \in K[x]$ be the minimal polynomial of α. Then every root of f is an algebraic integer, so $f \in \mathcal{O}_K[x]$ and f splits in $\mathcal{O}_L[x]$ by normality. It follows that $\bar{f}$ splits in $k_{\mathfrak{P}}[x]$. Let $\bar{\sigma} \in \mathrm{Gal}\left(k_{\mathfrak{P}} : k_{\mathfrak{p}}\right)$. Then $\bar{\sigma}\bar{\alpha}$ is also a root of $\bar{f}$, and hence of the form $\bar{\beta}$ for a root there exists $\sigma \in \mathrm{Gal}(L/K)$ such that σ □

DEFINITION 64. The kernel of this map is called the *inertia subgroup I*. Any element of $G_{\mathfrak{P}}$ projecting to the generator of $\mathrm{Gal}\left(k_{\mathfrak{P}} : k_{\mathfrak{p}}\right)$ (given by $x \mapsto x^{q_{\mathfrak{p}}}$) is called a *Frobenius element* and is denoted

Note the following interpretation: $\sigma \in G_{\mathfrak{P}}$ iff $x \equiv y\,(\mathfrak{P})$ implies $\sigma x \equiv \sigma y\,(\mathfrak{P})$. In addition, $\sigma \in I_{\mathfrak{P}}$ iff $\sigma x \equiv x\,(\mathfrak{P})$ and σ is a Frobenius element iff $\sigma x \equiv x^{q_{\mathfrak{p}}}\,(\mathfrak{P})$.

.

CHAPTER 2

Local fields

2.1. Valuations and absolute values

Fix a field F.

2.1.1. Definitions; basic properties (Lecture 9).

DEFINITION 65. A *valuation* is a map $v\colon F \to \mathbb{R}\cup\{\infty\}$ such that:
(1) $v(xy) = v(x)+v(y)$
(2) $v(x)+v(y) \geq \min\{v(x), v(y)\}$
(3) $v^{-1}(\infty) = \{0\}$.

EXAMPLE 66. (Valuations)
(1) $F = \mathbb{Q}$, $v_p\left(p^r \frac{a}{b}\right) = r$ where $p \nmid ab$.
(2) $F = K(t)$ (K a field), $p \in K[t]$ irreducible, $v_p\left(p^r \frac{a}{b}\right) = r$ where $p \nmid ab$.
(3) $F = K(t)$, $v_\infty\left(\frac{a}{b}\right) = \deg b - \deg a$.

DEFINITION 67. An *absolute value* on F is a map $|\cdot| : F \to \mathbb{R}_{\geq 0}$ such that:
(1) $|xy| = |x|\,|y|$
(2) $|x+y| \leq |x| + |y|$
(3) $|x| = 0$ iff $x = 0$.

Further, call the absolute value *trivial* if $|F^\times| = \{1\}$, *ultrametric* or *non-archimedean* if $|x+y| \leq \max\{|x|, |y|\}$.

Note that $|1| = |1|^2$ but $|1| \neq 0$ so $|1| = 1$.

EXAMPLE 68. Let v be a valuation on F, and let $q > 1$. Then $|x|_v = q^{-v(x)}$ is a non-archimedean absolute value. On $\mathbb{Q}$ we let $|x|_p = p^{-v_p(x)}$ so that $|p^r|_p = \frac{1}{p^r}$.

PROPOSITION 69 (Product formula). *Let $x \in \mathbb{Q}^\times$. Then $|x|_\infty \cdot \prod_p |x|_p = 1$.*

LEMMA 70. *Let $|\cdot|$ be an absolute value on F. Then $|\cdot|$ is non-archimedean iff it is bounded on the set $\{n\cdot 1_F \mid n \in \mathbb{Z}_{\geq 1}\}$, and this is implied by $|n\cdot 1_F| \leq 1$ for some $n \geq 2$.*

PROOF. If $|\cdot|$ is non-archimedean then $|n\cdot 1_F| = |\sum_{i=1}^n 1_F| \leq \max\{|1_F|\} = 1$. Conversely, suppose that $|n\cdot 1_F| \leq M$ for all n. Then for any $x, y \in F$ we have

$$\begin{aligned} |x+y|^n &= \left|\sum_{k+l=n} \binom{n}{k} x^k y^l\right| \leq \sum_{k+l=n} \left|\binom{n}{k}\right| (\max\{|x|, |y|\})^n \\ &\leq (n+1)M(\max\{|x|, |y|\})^n \end{aligned}$$

and the claim follows by taking nth roots and letting $n \to \infty$.

Finally, suppose that $|b| \leq 1$ for some $b \geq 2$. let $A = \{0, 1, \ldots, b-1\}$ and let $M = \max_{a \in A} |a|$. Writing any $n \in \mathbb{N}$ to base b we have $n = \sum_{i \leq \log_b n} a_i b^i$ where $a_i \in A$. It follows that $|n| \leq C(1 + \log_b n)$ for some C. Then $|n| \leq C(1 + d \log_b n)^{1/d}$ for all d, and taking $d \to \infty$ we find $|n| \leq 1$. □

COROLLARY 71. *Every absolute value on a field of positive characteristic is non-archimedean.*

Given an absolute value $|\cdot|$ on F, we have an associated metric $d(x,y) = |x-y|$ (check). This is ultrametric iff $|\cdot|$ is non-archimedean.

DEFINITION 72. Two absolute values are *equivalent* if they define the same topology on F.

LEMMA 73 (Snowflake). *If $|\cdot|$ is an absolute value then $|\cdot|^\lambda$ is an absolute value for all $0 < \lambda \leq 1$ (and sometimes for other values too).*

PROOF. Check. □

LEMMA 74. *Let $|\cdot|_1, |\cdot|_2$ be non-trivial and define the same topology. Then they are equivalent iff $|\cdot|_1 = |\cdot|_2^\lambda$ for some $\lambda > 0$.*

PROOF. Sufficiency is clear. For necessity note that $x^n \to 0$ in $(F, |\cdot|)$ iff $|x| < 1$. In particular, the sets $\{x \mid |x| < 1\}, \{x \mid |x| > 1\}, \{x \mid |x| = 1\}$ only depend on the topology induced by $|\cdot|$. Now choose some $a \in F$ satisfying $|a|_1 > 1$. Then $|a|_2 > 1$ and there is a uniqueλ such that $|a|_1 = |a|_2^\lambda$. Let $b \in F^\times$ be another such that $|b|_1 > 1$, and suppose that $|b|_1 > |b|_2^\lambda$. For any $\varepsilon > 0$ we can find arbitrarily large m, n such that $|b|_2^n \leq |a|_2^m \leq |b|_2^n (1+\varepsilon)$. Then $1 \leq \left|\frac{a^m}{b^n}\right|_2 \leq (1+\varepsilon)$ while $\left|\frac{a^m}{b^n}\right|_1 = \left|\frac{a^m}{b^n}\right|_2^\lambda \cdot \left(\frac{|b|_2^\lambda}{|b|_1}\right)^n \leq (1+\varepsilon)^\lambda \left(\frac{|b|_2^\lambda}{|b|_1}\right)^n$. For n large enough this is less than 1, a contradiction. Similar argument if $|b|_1 < |b|_2^\lambda$. □

DEFINITION 75. $|F|$ will denote the set of equivalence classes of non-trivial absolute values of F.

THEOREM 76 (Ostrowski). $|\mathbb{Q}| = \left\{|\cdot|_p\right\}_{p \leq \infty}$.

PROOF. See Problem Set 4. □

REMARK 77. We see that the purely metric notion of "absolute value" contains information about the arithmetic of $\mathbb{Q}$.

THEOREM 78 (Weak approximation [Generalized CRT]; Artin–Whaples). *Let $\{|\cdot|_i\}_{i=1}^n$ be pairwise inequivalent non-trivial absolute values on a field F. Let $\underline{x} \in F^n$ and let $\varepsilon > 0$. Then there is $y \in F$ such that $|y - x_i|_i < \varepsilon$.*

PROOF. We first construct for each $2 \leq k \leq n$ some $z_1 \in F$ such that $|z_1|_1 > 1$ and $|z_1|_j < 1$ for $2 \leq j \leq k$. When $k = 2$ this is just the inequivalence of the valuations; suppose that we have z_1 like this. If $|z|_{k+1} < 1$ then we are done. If $|z|_{k+1} \geq 1$ choose w such that $|w|_1 > 1$ and $|w|_{k+1} < 1$. If $|z|_{k+1} = 1$ then for all $s \geq 1$, $|z^s w|_1 > 1$, $|z^s w|_{k+1} < 1$, and if s is large enough then also $|z^s w|_j < 1$ if $2 \leq j \leq k$. If $|z|_{k+1} > 1$ consider $\frac{z^s w}{1+z^s}$. For s large this has small $|\cdot|_j$-value while the $|\cdot|_1, |\cdot|_{k+1}$-values tend to those of w.

It follows that there are z_i such that $|z_i|_i > 1$ and $|z_i|_j < 1$ if $j \neq i$. Now let $w_i = \frac{z_i^s}{\sum_{j=1}^n z_j^s}$. Then $\sum_{i=1}^n w_i = 1$ and $\lim_{s \to \infty} |w_i|_j = \delta_{ij}$. It follows that for for any $\varepsilon > 0$ there is s large enough such

that $\left|w_i - \delta_{ij}\right|_j < \varepsilon$. Now given $\underline{x} \in F$ let $y = \sum_{i=1}^n w_i x_i$. Then $\left|y - x_j\right|_j = \left|\sum_{i=1}^n \left(w_i - \delta_{ij}\right) x_i\right|_j \leq \varepsilon \sum_{i=1}^n \left|x_i\right|_j$. □

REMARK 79. Note the parallel with the proof of the CRT, and the fact this this is non-arithmetic – holds for any field.

2.1.2. Completion – $\mathbb{Q}_p$ (Lecture 10).

LEMMA 80. *Let $(X, d_X), (Y, d_Y)$ be metric spaces with Y complete, and let $f\colon X^n \to Y$ be* uniformly continuous on every ball. Then there is a unique continuous function $\hat{f}\colon \hat{X}^n \to Y$ extending f, and $\hat{f}$ is also uniformly continuous on balls.

PROOF. Uniqueness is clear since X^n is dense in $\hat{X}^n$. For existence for $1 \leq i \leq n$ let $\left(x_j^i\right)_{j=1}^{\infty} \subset X$ be a Cauchy sequence. Let R be such that $d_X\left(x_j^i, x_1^i\right) \leq R$ for all i, j. Then since f is uniformly continuous on $\left\{\underline{x} \in X^d \mid \max_i d_X\left(x^i, x_1^i\right) \leq R\right\}$, $\left(f\left(\underline{x}_j\right)\right)_{j=1}^{\infty}$ is a Cauchy sequence in Y. Letting $\underline{x}_j$ be the join of two Cauchy sequences with the same limit shows that $\lim_{j\to\infty} f\left(\underline{x}_j\right)$ only depends on the limit of the $\underline{x}_j$, giving the desired extension. Furthermore, every ball in $\hat{X}^d$ is contained in a ball with center in X^d. □

COROLLARY 81. *Let $|\cdot|_v$ be an absolute value on F. Then the field operations and the absolute value on F extend uniquely to the completion F_v, giving it the structure of a topological field, complete with respect to the extension of the absolute value (which will have the same notation).*

EXAMPLE 82. The completions of $\mathbb{Q}$ will be denoted $\mathbb{Q}_p$ and $\mathbb{Q}_\infty = \mathbb{R}$.

LEMMA 83 (Student's dream). *Let F be a field complete wrt a non-archimedean absolute value $|\cdot|$. Let $(a_n)_{n\geq 1} \subset F$ be a sequence. Then the series $\sum_{n=0}^{\infty} a_n$ converges in K iff* $\lim_{n\to\infty} a_n = 0$.

PROOF. Exercise (PS3) □

DEFINITION 84. $\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \mid |x|_p \leq 1\right\}$.

LEMMA 85 ($\mathbb{Z}_p$). *(1) $\mathbb{Z}_p$ is an open (hence closed) subring of $\mathbb{Q}_p$.*
(2) $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.
(3) The map $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}_p/p^k\mathbb{Z}_p$ is an isomorphism.
(4) Every element of $\mathbb{Z}_p$ can be uniquely represented in the form $\sum_{j=0}^{\infty} a_j p^j$ where $a_j \in \{0, \ldots, p-1\}$ (or any set of representatives of $\mathbb{Z}/p\mathbb{Z}$).
(5) $\mathbb{Z}_p$ is compact.

PROOF. (1) is true for any ultrametric absolute value. For (2) given $x \in \mathbb{Z}_p$ suppose that $\left|p^k \frac{a}{b} - x\right|_p \leq p^{-r}$ for some $r \geq 0$. Then $p^{-k} = \left|p^k \frac{a}{b}\right|_p \leq \max\left\{\left|p^k \frac{a}{b} - x\right|_p, |x|_p\right\} \leq 1$ so $k \geq 0$. Now let $\bar{b} \in \mathbb{Z}$ be an inverse to b mod p^r. Then $p^k a\bar{b} \in \mathbb{Z}$ and

$$\begin{aligned}
\left|p^k a\bar{b} - x\right|_p &\leq \max\left\{\left|p^k a\bar{b} - p^k \frac{a}{b}\right|_p, \left|p^k \frac{a}{b} - x\right|_p\right\} \\
&= \max\left\{p^{-k}\left|1 - b\bar{b}\right|_p, p^{-r}\right\} \\
&\leq \max\left\{p^{-k-r}, p^{-r}\right\} = p^{-r}.
\end{aligned}$$

Note that our purely metric construction "knows about modular arithmetic".

Picture - 1. All balls in $\mathbb{Q}_p$ are open since the set of distances are discrete. All sets $a+p^k\mathbb{Z}_p$ are balls, so are open. Let $x \neq y \in \mathbb{Z}_p$. Then $|x-y| = p^{-(k-1)}$ for some $k \geq 1$ at which point $x \not\equiv y\,(p^k\mathbb{Z}_p)$. Now $y+p^k\mathbb{Z}_p$ and $\bigsqcup_{a \not\equiv x\,(p^k)} a+p^k\mathbb{Z}_p$ are disjoint and cover Zp. It follows that x, y are in different connected components of $\mathbb{Z}_p$ - that it is *totally disconnected*. But it is not discrete. We now prove the next part.

(3) $\mathbb{Z}_p$ is open in $\mathbb{Q}_p$, so $p^k\mathbb{Z}_p$ is open in $\mathbb{Z}_p$ and the quotient $\mathbb{Z}_p/p^k\mathbb{Z}_p$ is therefore discrete. Now $\mathbb{Z} \cap p^k\mathbb{Z}_p = p^k\mathbb{Z}$ (exercise) so the injection $\mathbb{Z} \to \mathbb{Z}_p$ gives an injection $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}_p/p^k\mathbb{Z}$ with dense image, hence an isomorphism.

Picture - 2. $\mathbb{Z}_3$ is the disjoint union of $3\mathbb{Z}_3, 1+3\mathbb{Z}_3, 2+3\mathbb{Z}_3$. Each of those is a further union, for example $3\mathbb{Z}_3 = 9\mathbb{Z}_3 \sqcup 3+9\mathbb{Z}_3 \sqcup 6+9\mathbb{Z}_3$ and $2+3\mathbb{Z}_3 = 2+9\mathbb{Z}_3 \sqcup 5+9\mathbb{Z}_3 \sqcup 8+9\mathbb{Z}_3$, $5+9\mathbb{Z}_3 = 5+27\mathbb{Z}_3 \sqcup 14+27\mathbb{Z}_3 \sqcup 23+27\mathbb{Z}_3$. Get a $(p+1)$-regular rooted tree, rooted at Zp. Every element of $\mathbb{Z}_p$ corresponds to an *infinite path* in the tree (equivalently, a point on the boundary). Given a point get a path (reduce mod p^k successively) and given a path take representatives of the classes mod p^k, which is a Cauchy sequence [and any two clearly have the same limit]). Not obvious in this picture which paths correspond to elements of Z, of course.

(4) Let $A \subset \mathbb{Z}$ be a set of representatives for $\mathbb{Z}/p\mathbb{Z}$ and let $f\colon A^{\mathbb{N}} \to \mathbb{Z}_p$ be the map $f(\underline{a}) = \sum_{j=0}^{\infty} a_j p^j$. We show the map is a homeomorphism. By Lemma 83, each such series converges in $\mathbb{Z}_p$ (it is a closed subset of Qp, hence complete) so f is well-defined; for continuity note that the inverse image of $a+p^k\mathbb{Z}_p$ only depends on the first k coordinates in $A^{\mathbb{N}}$. For injectivity suppose that $\left(a'_j\right)_{j\geq 0}$ is a second sequence, and that j_0 is the first time they disagree. Then $\left(\sum_{j=0}^{\infty} a_j p^j\right) - \left(\sum_{j=0}^{\infty} a'_j p^j\right) = p^{j_0}(a_{j_0} - a'_{j_0}) + p^{j_0+1}\sum_{j>j_0}\left(a_j - a'_j\right)p^j$. Since $p \nmid (a_{j_0} - a'_{j_0})$ we have $\left|\left(\sum_{j=0}^{\infty} a_j p^j\right) - \left(\sum_{j=0}^{\infty} a'_j p^j\right)\right|_p = p^{-j_0} > 0$ and the sums are distinct. For surjectivity use the "path in the tree" picture, or use the density of $\mathbb{Z}_{\geq 0}$ and the fact (exercise) that those have representations as finite power series.

(5) $A^{\mathbb{N}}$ is compact by Tychonoff so $\mathbb{Z}_p$ is compact. In fact, the compactness shows that f is a closed map hence a homeomorphism. Conceretely, we prove Bolzano–Weierstraß: Every sequence has subsequence which stablizes mod p^k, so applying a diagonal argument every sequence has a subsequence which for each mk eventually stablizes mod p^k. But such a sequence is Cauchy and hence converges (our space is complete). Alternatively, note that for each radius p^{-k} we can cover $\mathbb{Z}_p$ by p^k balls of radius p^{-k} indexed by $\mathbb{Z}/p^k\mathbb{Z}_p$. □

COROLLARY 86. *$\mathbb{Z}_p$ is a maximal compact subring of $\mathbb{Q}_p$; the topology of $\mathbb{Q}_p$ is generated by the open sets $p^r\mathbb{Z}_p$.*

PROOF. On any compact subring we have $|\cdot|$ is bounded. But if $|x| > 1$ then $|x^n| \to \infty$, so any compact subring is contained in $\mathbb{Z}_p$. □

2.2. Complete fields (Lectures 11-13)

From now on we suppose that F is complete wrt the non-trivial absolute value $|\cdot|$.

2.2.1. Finite-dimensional subspaces are closed. (Just state the result). Consider a TVS V over F.

LEMMA 87. *Let $0 \in U \subset V$ be a neighbourhood of zero. Then there is a neighbourhood $0 \in U' \subset U$ such that $xU' \subset U'$ whenever $|x| \leq 1$ (we say that U' is* balanced*).*

PROOF. The set $\{(x,v) \in F \times V \mid xv \in U\}$ is open, and hence contains a subset of the form $B_F(0,r) \times U_1$ where U_1 is a neighbourhood of zero and $r > 0$. Let $x \in F$ be such that $|x| > \frac{1}{r}$ (this exists since the absolute value is non-trivial). Then $x \cdot B_F(0,r) = B_F(0,|x|r) \supset B_F(0,1)$, $U_2 = x^{-1}U_1$ is open, and $B_F(0,1)U_2 \subset xB_F(0,r)x^{-1}U_1 \subset U$. Finally, $U' = B_F(0,1)U_2 = \cup_{|x|\leq 1} xU_2$ is open, $B_F(0,1)$-invariant and contained in U. □

LEMMA 88. *Let $W \subset V$ be a complete subspace. Then it is closed.*

PROOF. Let I be a directed set and let $\{w_i\}_{i\in I}$ be a net in W converging to $v \in V$. Then $\{w_i\}_{i\in I}$ is a Cauchy net, so it converges in W by assumption. Then V is Hausdorff this means that $v \in W$. □

LEMMA 89. *Let V be a TVS over F. Then every 1-dimensional subspace of V is linearly homeomorphic to F, in particular complete and closed.*

PROOF. Let $v \in V$ be non-zero. The map $f(x) = xv$ is continuous by definition of TVS, and it is enough to check that it is open.. Since V is Hausdorff there is an open neighbourhood $0 \in U \subset V$ not containing v. Let $0 \in U' \subset U$ be a balanced neighbourhood contained in it. Then $\{\alpha \in F \mid \alpha v \in U'\}$ is $B_F(0,1)$-invariant and does not contain 1. It is therefore contained in $B_F(0,1)$, and it follows that $\{\alpha v \mid |\alpha| \leq 1\} \supset U' \cap Fv$, in other words that $f(B_F(0,1))$ contains a neighbourhood of $f(0)$. By translation and rescaling it follows that $f(B_F(x,r))$ contains a neighbourhood of $f(x)$, and it is now clear that f is open. □

THEOREM 90 (Finite-dimensional spaces over complete fields). *Let F be a field complete with respect to the non-trivial absolute value $|\cdot|$. Let V be a finite-dimensional TVS over F. Then V is linearly homeomorphic to $F^{\dim V}$. In particular, any finite-dimensional subspace of an F-TVS is complete, hence closed.*

PROOF. Induction on $\dim V$; we already know the case $\dim V = 1$. Suppose that $\dim V = n+1$ with basis $\{v_i\}_{i=1}^{n+1}$. Let $W_1 = \mathrm{Span}_F\{v_i\}_{i=1}^{n}$, $W_2 = \mathrm{Span}_F\{v_{n+1}\}$. Then by induction W_1, W_2 are linearly homeomorphic to F^n, F respectively hence complete and closed in V. Let $f\colon F^{n+1} \to V$ be he map $f(\underline{x}) = \sum_{i=1}^{n+1} x_i v_i$. This is a continuous isomorphism of vector space, and we want to construct a continuous inverse. For this note that the linear isomorphism $V \to (V/W_1) \times (V/W_2)$ is continuous since these are closed subspaces. By induction again we have isomorphisms $V/W_1 \simeq F$ and $V/W_2 \simeq F^n$, and hence also a continuous linear isomorphism $V \to F^{n+1}$. To make this inverse to the original one it is enough to compose with an appropriate automorphism of F^{n+1}, and all of those are continuous. □

COROLLARY 91. *Let L/F be an algebraic extension. Then there is at most one absolute value on L extending that of F.*

PROOF. Any $x \in L$ then generates a finite-dimensional vector space $K(x)$. The restrictions of any two absolute values from L to $K(x)$ will give $K(x)$ two topologies as a K-vector space which much coincide, so they are equivalent on $K(x)$. But they agree on K, so they are the same valuation. □

COROLLARY 92. *Let L/F be a finite extension of fields, and let $|\cdot|_w$ be an absolute value of L whose restriction to F, $|\cdot|_v$, is non-trivial. Then L_w is an algebraic extension of F_v. In fact, $[L_w : F_v] \leq [L : F]$.*

PROOF. Consider L_w as an F_v-vector space. Then the subspace $L \cdot F_v$ is finite-dimensional, hence closed. By the density of L we have $L_w = L \cdot F_v$. □

2.2.2. Extension of valuations. Let K be a field equipped with a (non-trivial) non-archimedean absolute value $|\cdot|$.

LEMMA 93. *Let $\mathcal{O} = \{x \in K \mid |x| \leq 1\}$, $\mathfrak{p} = \{x \in K \mid |x| < 1\}$.*

(1) $\mathcal{O}$ is a subring of K, in fact the maximal bounded subring.
(2) K is the field of fractions of $\mathcal{O}$, which is integrally closed.
(3) $\mathfrak{p}$ is an ideal of $\mathcal{O}$.
(4) $\mathcal{O}^\times = \{x \in K \mid |x| = 1\} = \mathcal{O} \setminus \mathfrak{p}$. In particular, $\mathfrak{p}$ is the unique maximal ideal of $\mathcal{O}$.

PROOF. PS3, □

NOTATION 94. We call $\mathcal{O}$ the *maximal bounded subring* or the *valuation ring*, $\mathfrak{p} = \{x \in K \mid |x| < 1\}$, $\kappa = \mathcal{O}/\mathfrak{p}$ the *residue field*. For $a \in \mathcal{O}$ we write $\bar{a}$ for its image in κ.

Suppose now that K is *complete*.
For a polynomial $f = \sum_{i=0}^{d} a_i x^i \in K[x]$ write $|f| = \max_i |a_i|$. Call $f \in \mathcal{O}[x]$ *primitive* if $|f| = 1$, that is if $\bar{f} \neq 0$.

PROPOSITION 95 (Hensel's Lemma). *Let $f \in \mathcal{O}[x]$.*

(1) Suppose that for some $\alpha \in \mathcal{O}$, $|f(\alpha)| < |f'(\alpha)|^2$. Then there is $\beta \in \mathcal{O}$ such that $f(\beta) = 0$ and $|\alpha - \beta| \leq \left|\frac{f(\alpha)}{f'(\alpha)^2}\right| < 1$.
(2) Suppose that $\bar{f} \neq 0$ and that $\bar{f} = \bar{g}\bar{h}$ in $\kappa[x]$ where $\bar{g}, \bar{h}$ are relatively prime. Then there are $g, h \in \mathcal{O}[x]$ lifting $\bar{g}, \bar{h}$ such that $\deg g = \deg \bar{g}$ and $f = gh$.

PROOF. (1) Note that for $f \in \mathcal{O}[x]$, $\alpha, \beta \in \mathcal{O}$ we have $|f(\alpha) - f(\beta)| \leq |\alpha - \beta|$. In particular, if $|\alpha - \beta| < |f'(\alpha)|$ then $|f'(\alpha) - f'(\beta)| < |f'(\alpha)|$ so $|f'(\beta)| = |f'(\alpha)| > 0$. Also, we have $f'(\alpha) \in \mathcal{O}$ so $f(x) - f(\alpha) - f'(\alpha)(x - \alpha) \in \mathcal{O}[x]$ and it follows that there is $g(x) \in \mathcal{O}[x]$ such that

$$f(x) = f(\alpha) + f'(\alpha)(x - \alpha) + g(x)(x - \alpha)^2 .$$

Now set $c = \left|\frac{f(\alpha)}{f'(\alpha)^2}\right| < 1$ and define a sequence by $\alpha_0 = \alpha$, $\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$. Suppose by induction that $|f'(\alpha_n)| = |f'(\alpha)|$, $\left|\frac{f(\alpha_n)}{f'(\alpha_n)^2}\right| \leq c^{2^n}$. Then $\alpha_n, \alpha_{n+1} \in \mathcal{O}$. Using a Taylor expansion for $f'(x)$, there is $\gamma \in \mathcal{O}$ such that

$$\begin{aligned} \left|f'(\alpha_{n+1}) - f'(\alpha_n)\right| &= |\gamma(\alpha_{n+1} - \alpha_n)| \\ &\leq \left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right| < \left|f'(\alpha_n)\right| . \end{aligned}$$

It follows that $|f'(\alpha_{n+1})| = |f'(\alpha)|$. Now using a Taylor expansion for $f(x)$ there is $\gamma \in \mathcal{O}$ such that

$$\begin{aligned}\left|\frac{f(\alpha_{n+1})}{f'(\alpha_{n+1})^2}\right| &= \left|\frac{f(\alpha_n)+f'(\alpha_n)(\alpha_{n+1}-\alpha_n)+\gamma(\alpha_{n+1}-\alpha_n)^2}{f'(\alpha_{n+1})^2}\right| \\ &\leq \left|\frac{f(\alpha_n)^2}{f'(\alpha_n)^4}\right| \leq \left(c^{2^n}\right)^2.\end{aligned}$$

It follows that $\alpha_{n+1}-\alpha_n \to 0$ and hence that $\beta = \lim_{n\to\infty}\alpha_n$ exists. It is clear that $f(\beta)=0$. Also, $|\alpha_{n+1}-\alpha_n| = \left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right| \leq c^{2^n} \leq c$ so by induction $|\alpha_n - \alpha| \leq c$ and $|\beta-\alpha| \leq c$.

(2) $d = \deg(f)$, $k = \deg(\bar{g})$, and let g_0, h_0 be a preimages of $\bar{g}, \bar{h}$ of the same degree as the latter ones. Suppose that for some $\pi \in \mathfrak{p}$ we have constructed p_i, q_i with $\deg p_i < k$, $\deg q_i \leq d-k$ such that for $g_n = g_0 + \sum_{i=1}^n \pi^i p_i$ and $h_n = h_0 + \sum_{i=1}^n \pi^i q_i$ $f \equiv g_n h_n \left(\pi^{n+1}\mathcal{O}\right)$ (thus, we need π to divide every coefficient of $f - g_0 h_0$). Then for any p_{n+1}, q_{n+1} we have

$$\begin{aligned}f - g_{n+1}h_{n+1} &= (f-g_nh_n) - \pi^{n+1}(g_nq_{n+1}+h_np_{n+1}) - \pi^{2n+2}p_{n+1}q_{n+1} \\ &\equiv (f-g_nh_n) - \pi^{n+1}\left(g_0q_{n+1}+g_0p_{n+1}\right)\left(\pi^{n+2}\mathcal{O}\right)\end{aligned}$$

and thus

$$\pi^{-(n+1)}\left[f-g_{n+1}h_{n+1}\right] \equiv \pi^{-(n+1)}\left[f-g_nh_n\right] - \left(g_0q_{n+1}+h_0p_{n+1}\right)(\pi\mathcal{O}).$$

Our goal is then to find p_{n+1}, q_{n+1} such that

$$\left(g_0q_{n+1}+h_0p_{n+1}\right) \equiv \pi^{-(n+1)}\left[f-g_nh_n\right](\pi\mathcal{O}).$$

Let $f_n = \pi^{-(n+1)}(f-g_nh_n) \in \mathcal{O}[x]$. Since $\bar{g}, \bar{h}$ are relatively prime, we could have fixed $a, b \in \mathcal{O}[x]$ such that $\bar{a}\bar{g}+\bar{b}\bar{h}=1$. Now if π divides the coefficients of $ag_0+bh_0-1 \in \mathfrak{p}[x]$ we have $g_0(af_n)+h_0(bf_n) \equiv f_n(\pi\mathcal{O})$. The highest coefficient of g_0 is a unit (it has the same degree mod $\mathfrak{p}$) so we can divide with remainder $bf_n = qg_0 + p_{n+1}$ where $\deg p_{n+1} < \deg g_0 = k$. Then we also have

$$g_0(af_n+h_0q)+h_0p_{n+1} \equiv f_n(\pi\mathcal{O}).$$

Define q_{n+1} by omitting from (af_n+h_0q) any coefficient divisible by π. Then

$$g_0q_{n+1}+h_0p_{n+1} \equiv f_n(\pi\mathcal{O}).$$

Also, since the leading coefficient of g_0 is a unit, and since $\deg(h_0p_{n+1}) < d$, $\deg f_n \leq d$ we must have $\deg q_{n+1} \leq d-k$. □

COROLLARY 96. *Let $f \in K[x]$ be irreducible and satisfy $a_0a_d \neq 0$. Then $|f| = \max\{|a_0|, |a_d|\}$.*

PROOF. Multiply by a constant to make $f \in \mathcal{O}[x]$ and $|f|=1$. If $a_0, a_d \in \mathfrak{p}$ write $\bar{f} = x^r\bar{h}$ for some $\bar{h}$ non-vanishing at $0 \in \kappa$. Then $r>0$ since $a_0 \in \mathfrak{p}$ and $r<d$ (otherwise a_d would be a unit), so we can lift x^r to a factor of f of degree r in $\mathcal{O}[x]$, a contradiction. □

COROLLARY 97. *Let $f \in K[x]$ be irreducible. Suppose that $a_d = 1$ and $a_0 \in \mathcal{O}$. Then $f \in \mathcal{O}[x]$.*

THEOREM 98. *Let K be complete with respect to a non-trivial non-archimedean absolute value and let L/K be an algebraic extension of degree n. Then $|\alpha| \stackrel{def}{=} \left|N_K^L(\alpha)\right|^{1/n}$ defines an absolute value on L which extends that of K.*

PROOF. This is clearly multiplicative. Let $\alpha \in L^\times$ satisfy $N_K^L \alpha \in \mathcal{O}_K$. Let $f \in K[x]$ be the minimal polynomial of α. Then $N_K^L \alpha = (f(0))^{[L:K]/\deg f}$ so $|f(0)| \leq 1$. It follows that $f \in \mathcal{O}_K[x]$ so α is integral over $\mathcal{O}_K$. Conversely, if α is integral then clearly $N_K^L \alpha \in \mathcal{O}_K$. It follows that $\{\alpha \in L \mid |\alpha| \leq 1\}$ is a subring of L. In particular, if $|\alpha| \leq 1$ then $|1+\alpha| \leq 1$. Now let $\alpha, \beta \in L^\times$ and suppose that $|\alpha| \leq |\beta|$. Then $\left|\frac{\alpha}{\beta}\right| \leq 1$ so $\left|1+\frac{\alpha}{\beta}\right| \leq 1$ so $|\alpha+\beta| \leq |\beta|$. □

COROLLARY 99. *The absolute value extends uniquely to any algebraic extension of F.*

2.2.3. Digression. Noting the last proof, it's natural to define an absolute value with slightly different axioms, replacing the triangle inequality with $\exists C : |x+y| \leq C \max\{|x|, |y|\}$. Equivalently, one assumes that $C = \sup\{|1+x| \mid |x| \leq 1\} < \infty$. This is strong enough to define convergence with all the usual properties, hence completion. One advantage is that now $|\cdot|^\lambda$ is an absolute value for all $\lambda > 0$. Note that in most cases checking $|xy| = |x|\,|y|$ is easy, and behaviour under addition is the difficult part.

One setting where this arises:

THEOREM 100. *Let K be a non-discrete locally compact field. Then one of the following holds:*

(1) K is isomorphic to a finite extension of R.
(2) K is isomorphic to a finite extension of $\mathbb{Q}_p$ for some rational prime p.
(3) K is isomorphic to $\mathbb{F}_q((t))$ for some prime power q.

SKETCH OF PROOF. Let μ be a Haar measure on $(K,+)$. Then for any $a \in K^\times$, $E \mapsto \mu(aE)$ is a Haar measure also, so there is $|a| \in \mathbb{R}^\times_{>0}$ such that $\mu(aE) = |a|\,\mu(E)$. This also holds for $a = 0$ with $|0| = 0$. This is clearly multiplicative and non-zero for $a \neq 0$. Next one checks that $|\cdot|$ is continuous, and that $\{x \mid |x| \leq 1\}$ is compact. It follows that there is C as in the modified definition. In the non-archimedean case (absolute value bounded on $\mathbb{Z}$), looking at $\left|(1+x)^N\right|$ now shows that $C = 1$ so we have an ultrametric. In characteristic zero our field now contains some $\mathbb{Q}_p$ or $\mathbb{R}$ by Ostrowski, and is finite-dimensional over $\mathbb{Q}_p$ since it is locally compact. In finite charactersitic one shows that the field of constants is the residue field.

For details see □

2.3. Ramification

Fix a field K complete with respect to a non-archimedean absolute value $|\cdot|_v$. Equip every algebraic extension with the unique absolute value extending this one.

For an algebraic extension L/K of degree n let $|\cdot|_w$ be the absolute value, $\mathcal{O}_L$ be the valuation ring, $\mathfrak{p}_L$ the prime, λ the residue field.

2.3.1. Ramification index and residue degree.

DEFINITION 101. For a finite extension L/K set $e(L/K) = [v(L^\times) : v(K^\times)]$ and $f(L/K) = [\lambda : \kappa]$.

PROPOSITION 102. *$n \geq ef$ and if $|\cdot|_v$ is discrete then we have equality.*

PROOF. Let $\{\omega_i\}_{i=1}^f \subset \mathcal{O}_L$ reduce mod $\mathfrak{P}$ to a basis of λ over κ. Let $\left\{\Pi_j\right\}_{j=0}^{e-1} \subset \mathcal{O}_L$ be such that $\left|\Pi_j\right|_w$ are coset representatives. Suppose that for some $x_{ij} \in K$ we have

$$\sum_{i,j} x_{ij} \omega_i \Pi_j = 0\,.$$

Let $s_j = \sum_i x_{ij}\omega_i$. Suppose not all the x_{ij} here are zero. For each j we rescale s_j by an element of $K^\times$ so that all the $\{x_{ij}\}_{i=1}^f \subset \mathcal{O}_K$ but that not all are in $\mathfrak{p}$. Call the resulting sum s'_j. Then $s'_j \in \mathcal{O}_L$ but reducing mod $\mathfrak{p}_L$ not all cofficients are zero in κ, so $s'_j \notin \mathfrak{p}_L$ by the choice of $\bar{\omega}_i$. It follows that $s'_j \in \mathcal{O}_L^\times$ so $\left|s'_j\right| = 1$, at which point $\left|s_j\right| \in |K^\times|$. Now in the sum $\sum_j s_j \Pi_j = 0$ two non-zero summands must have the same absolute value, which is a contradiction.

Suppose now that v is discrete and let $\Pi_j = \Pi^j$ where Π is a uniformizer. Then $M = \oplus_{ij}\mathcal{O}_K\omega_i\Pi_j \subset \mathcal{O}_L$. We will show equality. Let $N = \oplus_i \mathcal{O}_K\omega_i$. Then $N + \Pi\mathcal{O}_L = \mathcal{O}_L$since ω_i are a generating set for $\mathcal{O}_L/\Pi\mathcal{O}_L$ as an $\mathcal{O}_K$-module. Iterating we find

$$\mathcal{O}_L = N + \Pi(N + \Pi(\cdots)) = \sum_{j=0}^{e-1} \Pi^j N + \Pi^e\mathcal{O}_L = M + \Pi^e\mathcal{O}_L = M + \varpi\mathcal{O}_L\,.$$

It now follows by induction that

$$\mathcal{O}_L = M + \varpi^k\mathcal{O}_L$$

for all $k \geq 1$. But then M is dense in $\mathcal{O}_L$ ($\varpi^k\mathcal{O}_L$ is a basis of neighbourhoods of the identity!). On the other hand since $\mathcal{O}_K$ is closed in K, $M \simeq \mathcal{O}_K^{ef}$ is closed in its K-span, which is a K-subspace of L, hence closed. It follows that M is closed in L, so $M = \mathcal{O}_L$. □

REMARK 103. This gives an alternative proof of the claim from chapter 1.

2.3.2. Unramified extensions.

DEFINITION 104. A finite extension L/K is *unramified* if $\lambda : \kappa$ is separable and $[\lambda : \kappa] = [L : K]$. An infinite extension is unramified if every finite subextension is unramified.

LEMMA 105. *Let $L/M/K$ be a tower of extensions with $[L : K]$ finite. Then L/K is unramified iff both of $L/M, M/K$ are.*

PROOF. First, λ/κ is separable iff μ/κ and λ/μ are. Since $f \leq n$ we have

$$[\lambda : \kappa] = [\lambda : \mu]\,[\mu : \kappa] \leq [L : M]\,[M : K] = [L : K]\,.$$

If L/K is unramified then the equality $[\lambda : \kappa] = [L : K]$ forces equality throughout. If $L/M, M/K$ are unramified then we have equality throughout and $[\lambda : \kappa] = [L : K]$. □

PROPOSITION 106. *Inside a fixed algebraic closure $\bar{K}$ let L/K be unramified, M/K any extension. Then LM/M is unramified.*

PROOF. Enough to consider the case of L finite. Then $\lambda = \kappa(\bar{\alpha})$ for some $\alpha \in \mathcal{O}_L$. Let $f \in \mathcal{O}_K$ be the minimal polynomial of α. Then $\bar{f} \in \kappa[x]$ is monic, and $\bar{f}(\bar{\alpha}) = 0$ $[\lambda : \kappa] \leq \deg \bar{f} \leq \deg f \leq [L : K] = [\lambda : \kappa]$. It follows that $\bar{f}$ is the minimal polynomial of $\bar{\alpha}$, in particular it is irreducible. Also, $\deg f = [L : K]$ so $L = K(\alpha)$. Now let $g \in \mathcal{O}_M[x]$ be the minimal polynomial of α over M. Then $\bar{g} \in \mu[x]$ is separable (it divides $\bar{f}$) and hence irreducible (if it factored then the factors would be relatively prime and then by Hensel's Lemma we could lift this to a factorization of g). It follows that $[M(\alpha) : M] = [\mu(\bar{\alpha}) : \mu] \leq [M(\alpha) : M]$ and hence we have equality. □

COROLLARY 107. *Let $L/M/K$ be a tower of algebraic extensions. Then L/K is unramified iff both of $L/M, M/K$ are.*

PROOF. PS4 □

THEOREM 108. *The compositum of unramified extensions is unramified.*

DEFINITION 109. The maximal unramified subextension *of L/K is the compositum T of all unramified subextensions of L/K. In particular, we let K^{ur} denote the maximal unramified subextension of $\bar{K}/K$, that is the compositum of all unramified extensions of K.*

PROPOSITION 110. *Let T/K be the maximal unramified subextension of L/K. Then τ is the separable closure of κ in λ, and T, K have the same value groups.*

PROOF. We have $e = 1$ in every finite subextension of T/K, so the value groups are the same. Now let $\bar{\alpha} \in \lambda$ be separable over κ, and let $f \in \mathcal{O}_K[x]$ be a monic lift of its minimal polynomial $\bar{f}$. Then f is irreducible by Hensel's Lemma, and $\bar{f}(\bar{\alpha}) = 0$ while $\bar{f}'(\bar{\alpha}) \neq 0$ since $\bar{f}$ is separable. It follows from Hensel's Lemma again that f has a root $\alpha \in L$ lifting $\bar{\alpha}$. Then $K(\alpha)$ is unramified over K since $[K(\alpha) : K] = \deg f = \deg \bar{f} = [\kappa(\bar{\alpha}) : \kappa]$. □

2.3.3. Ramification. Suppose now that κ is prefect and that the absolute value $|\cdot|_K$ is discrete.

DEFINITION 111. Say that L/K is *totally ramified* if it has no unramified subextensions.

Say that L/K is *tamely ramified* if it is totally ramified and every finite subextension has order prime to $p = \mathrm{char}(\kappa)$.

PROPOSITION 112. *Let L/K be totally ramified and finite. Then the minimal polynomial of a uniformizer $\Pi \in \mathfrak{p}_L$ is an Eisenstein polynomial and $L = K(\Pi)$. Conversely, such a polynomial is irreducible and generates a totally ramified extension.*

DEFINITION 113. $f \in \mathcal{O}_K[x]$ is an *Eisenstein* polynomial if it is monic, if $\bar{f} = x^e$ where $e = \deg(f)$ and if $f(0) \in \mathfrak{p}_K \setminus \mathfrak{p}_K^2$.

PROOF. Suppose $[L : K] = e$ and that $[K(\Pi) : K] = d|e$. Every conjugate of Π has the same absolute value, so all the coefficients are in the prime ideal. The first coefficient is the product of the conjugates, so up to units is equal to Π^d. But this coefficient is in $K^\times$, so its absolute value is an integer power of Π^e. It follows that $e|d$ so $e = d$ and the constant coefficient of the minimal polynomial is ϖ up to units.

For the converse let $f \in \mathcal{O}_K[x]$ be an Eisenstein polynomial of degree e, and let $L = K(\Pi)$ where Π is a root of f. Say $f(x) = \sum_{i=0}^{e} a_i x^i$ with $a_e = 1$ and $a_i \in \mathfrak{p}_K$ for $i < e$. Now for $i < e \left|a_i \Pi^i\right| < |\Pi|^i$. If $|\Pi| \geq 1$ were true then $|\Pi|^i \leq |\Pi|^e$ would hold, so that $|f(\Pi)| = |\Pi|^e > 0$, which is impossible. Thus $|\Pi| < 1$. Now for $1 \leq i \leq e-1$, $\left|a_i \Pi^i\right| < |a_i| \leq |a_0|$. Since $f(\Pi) = 0$ it follows that $|\Pi^e| = |a_0|$, and since $|K^\times|$ is generated by $|a_0|$ this means that $e\,(K(\Pi) : K) \geq e$. We thus have:

$$e \leq e\,(K(\Pi) : K) \leq [K(\Pi) : K] \leq \deg f = e\,.$$

It follows that we have equality throughout. That $[K(\Pi) : K] = \deg f$ shows that f is irreducible; that $e\,(K(\Pi) : K) = [K(\Pi) : K]$ shows that the extension is totally ramified.

Then $|\Pi| = \left|N_K^L \Pi\right|^{1/e} = |\varpi|^{1/e}$ by assumption, so $e(L/K) = e = [L : K]$. □

THEOREM 114. *$\mathbb{Q}_p$ has at most finitely many extensions of a given degree.*

PROOF. There's a unique unramified extension of any degree (PS5), so enough to count totally ramified extensions.

First, let f be a fixed Eisenstein polynomial with root α generating a field $K = \mathbb{Q}_p(\alpha)$. Then $f'(\alpha) \neq 0$ (f is irreducible and separable). If g is close to f then $g(\alpha), g'(\alpha) \in \mathcal{O}_K$ are close

to $f(\alpha), f'(\alpha)$. In particular, in a neighbourhood of f we have $\left|\frac{g(\alpha)}{(g'(\alpha))^2}\right| < 1$. Then by Hensel's Lemma g has a root in K so (g being an Eisenstein polynomial hence irreducible) f, g determine the same extension.

It follows that every Eisenstein polynomial has a neighbourhood determining the same extension. But the set of Eisenstein polynomials is compact! □

2.4. Places of number fields

We can now recover the results of Section 1.4 using the technology of completion instead of localization.

2.4.1. Extension of absolute values for non-complete fields.

LEMMA 115. *Let L/K be an extension of fields, and let w be an absolute value on L, trivial on K. Then w is trivial on the algebraic closure of K in L.*

PROOF. Let $|\cdot|$ be an absolute value of L, trivial on K. Then $|\cdot|$ is non-archimedean. Choose $\alpha \in L$ such that $|\alpha| > 1$ and let $f(x) = \sum_{i=0}^{d} a_i x^i \in K[x]$ be its monic minimal polynomial. Then for $i < d$ we have $\left|a_i \alpha^i\right| = |\alpha|^i < |\alpha|^d$ and hence $|f(\alpha)| = |\alpha|^d > 0$. It follows that α is transcendental over K. □

DEFINITION 116. Let L/K be an algebraic extension of fields. Let $w \in |L|$, $v \in |K|$. We say that *w extends v* (or *lies above v*) and write $w|v$ if the restriction of w to K is equivalent to v (note that the restriction is an absolute value).

From now on fix a finite extension of fields L/K and a place v of K.

LEMMA 117. *There is a natural bijection between $\{w \in |L| \mid w|v\}$ and $\mathrm{Hom}(L, \bar{K}_v)/\mathrm{Gal}(K_v)$.*

PROOF. v has a unique extension to $\bar{K}_v$, which is therefore Galois-invariant. This gives a map $\mathrm{Hom}_K(L, \bar{K}_v)/\mathrm{Gal}(K_v) \to \{w \in |L| \mid w|v\}$. For surjectivity let L_w be the completion of L under an absolute value. Then the compositum $L \cdot K_v \subset L_w$ is a finite-dimensional K_v-subspace, hence closed. The density of L in L_w now shows that $L_w = LK_v$ and in particular that it is finite over K_v. We therefore have an embedding $L_w \hookrightarrow \bar{K}_v$ and the pullback absolute value must be w by uniqueness. For injectivity let $K \subset L, L' \subset \bar{K}_v$ be two subfields which are finite over K and suppose we have an isometric K-homomorphism $\sigma\colon L \to L'$. Then σ extends to an isometry of the topological closures of L, L' in $\bar{K}_v$. These closures are subfields containing K_v and the extension is still a field isomorphism. Extend this isomorphism to an automorphism of $\bar{K}_v$ to obtain an element of the Galois group conjugating the two subfields. □

COROLLARY 118. *Suppose $L = K(\alpha)$ with minimal polynomial $f \in K[x]$. Then the places of L lying above v are in bijection with the irreducible divisors of f in $K_v[x]$.*

PROOF. $\mathrm{Hom}_K(L, \bar{K}_v)$ is in bijection with the irreducible factors. Moreover, the absolute values are obtained by finding roots of f in $\bar{K}_v$ and pulling back the absolute value. □

REMARK 119. This is a new proof of 56, in a form suitable for primes dividing the discrminant of α.

EXAMPLE 120. Let K be a number field, v an archimedean place, L/K a finite extension. Suppose $L = K(\alpha)$. If $K_v \simeq \mathbb{C}$ then $K_w \simeq \mathbb{C}$ for all $w|v$; α has $n = [L:K]$ K_v-embeddings in $\mathbb{C}$ so there are n places, all complex. If $K_v \simeq \mathbb{R}$ then the min poly f factors into some linear and some quadratic factors, so there are both real and complex places. Finally, we see that if K has r real places and s complex places then $r+2s = [K:\mathbb{Q}]$ (complex places come in pairs since the roots of real polynomials come in complex conjugate pairs). Note that for archimedean places it is normal to talk about real and complex *embeddings* rather than "places over R".

EXAMPLE 121. Let $K = \mathbb{Q}, L = \mathbb{Q}\left(\sqrt[3]{2}\right)$, with minimal polynomial $f(x) = x^3 - 2$.

- Over $\mathbb{Q}_\infty = \mathbb{R}$, f factors as $\left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}\right)$ with the latter factor irreducible. Thus three embeddings in C, but only two places since complex conjugate embeddings give the same absolute value.
- Over $\mathbb{Q}_2$, f is Eisentein hence irreducible. Thus there is a unique place $w_2|2$ and the extension is totally (but tamely) ramifield
- Over $\mathbb{Q}_3$, $f \equiv (x-2)^3\,(3)$. We have $f(2) = 3\cdot 2$, $f'(2) = 3\cdot 4$ so Hensel's Lemma does not apply, and indeed f has no root mod 9. In fact, $g(y) = f(y-1) = y^3 - 3y^2 + 3y - 3$ is Eisenstein, so again only only place and the extension is totally (and strongly) ramified.
- Over $\mathbb{Q}_5$, we reduce mod 5 to get $\bar{f} = (x-3)(x^2+3x+4)$ where the second factor is irred (no root) and rel prime to the linear factor, so by Hensel's Lemma f factors in $\mathbb{Q}_5[x]$ as a product $f_1 f_2$ with f_1 linear, f_2 quadratic. Thus two places over 5, one with completion isomorphic to $\mathbb{Q}_5$, the other to a quadratic extension. In fact, to the unramfied extension: since $\bar{f}_2$ is irred, we have $f\left(L_{w_5^2} : \mathbb{Q}_5\right) \geq \deg \bar{f}_2 = 2 = \left[L_{w_5^2} : \mathbb{Q}_5\right]$.
- Over Qp, $p \geq 5$ $\bar{f}'(x) = 3x^2$ is relatively prime to $\bar{f}$, so by Hensel's Lemma f factors as $f = \prod_i f_i$ where $\bar{f} = \prod_i \bar{f}_i$ and the $\bar{f}_i$ are irred and distinct. It follows that the places over p correspond to the f_i and they are all unramified since again $f\left(L_{w_p^i} : \mathbb{Q}_p\right) \geq \deg \bar{f}_i = \deg f_i = \left[L_{w_p^i} : \mathbb{Q}_p\right]$.
  - If $p \equiv 1\,(3)$ then $\mathbb{Z}/p\mathbb{Z}$ has cube roots of unity, so $\bar{f}$ is either irred (p inert) or splits to linear factors (*p splits completely*).
  - f splits iff f has a root mod p, that is iff 2 is a cube in $\mathbb{Z}/p\mathbb{Z}$. Let $p = \pi\bar{\pi}$ in the Eisenstein integesr $\mathbb{Z}[\omega]$. Then $f(\pi : p) = 1$ ($efg = 2$ and $g = 2$) so $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega] \simeq \mathbb{Z}/p\mathbb{Z}$ and thus we need to decide if $\left(\frac{2}{\pi}\right)_3 = 1$ and by cubic reciprocity this is $\left(\frac{\pi}{2}\right)_3$ if we choose π to be primary ($\pi \equiv \pm 2\,(3)$). Now 2 is prime in $\mathbb{Z}[\omega]$, so $\mathbb{Z}[\omega]/2\mathbb{Z}[\omega] \simeq \mathbb{F}_4$, and the cubes there are just the identity. Thus $\left(\frac{2}{\pi}\right)_3 = 1$ iff $\pi \equiv 1\,(2)$. Writing $p = a^2 + 3b^2$ where $a, b \in \mathbb{Z}$ (take the norm of π) p is primary if
  - If $p \equiv 2\,(3)$ then $x \mapsto x^3$is an automorphism of $(\mathbb{Z}/p\mathbb{Z})^\times$. In particular, $\bar{f}$ has a root. This root is unique since there are no cube roots of unity, so f splits as a product of a linear factor and a quadratic factor.

Retunring to the general case, for each $w|v$ we have a K_v-algebra hom $K_v \otimes_K L \to L_w$. We therefore have a K_v-algebra homomorphism $K_v \otimes_K L \to \prod_{w|v} L_w$.

THEOREM 122. *If L/K is separable, this is an isomorphism.*

PROOF. Say $L = K(\alpha)$ with minimal polynomial $f \in K[x]$. Let $f = \prod_w f_w$ be the factorization of f in $K_v[x]$. Then by the CRT $\prod_w L_w = \prod_w (K_v[x]/(f_w)) = K_v[x]/fK_v[x] = K_v \otimes_K (K[x]/fK[x])$. □

COROLLARY 123 (Reproof of Theorem 55). *If L/K is separable we have $[L:K] = \sum_{w|v} [L_w : K_v] = \sum_{w|v} e(w|v) f(w|v)$*

.

COROLLARY 124. *If L/K is separable we have for all $v \in |K|$ and $\beta \in L$ that $\mathrm{Tr}_K^L \beta = \sum_{w|v} \mathrm{Tr}_{K_v}^{L_w} \beta$ and $N_K^L \beta = \prod_{w|v} N_{K_w}^{L_w} \beta$.*

PROOF. $\mathrm{Tr}_K^L \beta$ let $M_\beta \in \mathrm{End}_{K\text{-vsp}}(L)$ and $M_\beta^v \in \mathrm{End}_{K_v\text{-vsp}}(K_v \otimes L)$ be multiplication by β. Then $M_\beta^v = 1 \otimes M_\beta$ so $\mathrm{Tr} M_\beta = \mathrm{Tr} M_\beta^v$. But under the decomposition $K_v \otimes L \simeq \oplus_w L_w$ each L_w is M_β^v-invariant, so

$$\mathrm{Tr} M_\beta^v = \sum_{w|v} \mathrm{Tr}\left(M_\beta^v \restriction_{L_w}\right) = \sum_{w|v} \mathrm{Tr}_{K_v}^{L_w} \beta\,.$$

□

2.4.2. Galois extensions.

PROPOSITION 125 (Reproof of 59). *Suppose L/K is finite and Galois. Then $G = \mathrm{Gal}(L/K)$ acts transitively on the places above v.*

PROOF. Suppose not. Then there are two disjoint orbits. By weak approximation (Theorem 78) can find $\alpha \in L$ such that $|x|_w < 1$ in one orbit, but $|x|_w > 1$ in the other orbit. Taking norms we get a contradiction. □

DEFINITION 126. The *decomposition group* is $G_w = \mathrm{Stab}_G(w)$. If v is non-archimedean we also have the *inertia subgroup* $I_w = \mathrm{Ker}(G_w \to \mathrm{Aut}(\lambda_w : \kappa_v)) = \{\sigma \in G_w \mid \sigma x \equiv x (\mathfrak{P}_w)\}$.

LEMMA 127. *L_w/K_v is Galois with Galois group G_w.*

PROOF. Let $L = K(\alpha)$ with minimal polynomial f. Then $L_w = L \cdot K_v = K_v(\alpha)$ so the extension L_w/K_v is a splitting field for the separable polynomial f hence Galois. Let $f_w \in K_v[x]$ be the irreducible factor of f such that $L_w \simeq K_v[x]/(f_w)$ and suppose without loss of generality that α is a root of f_w. Then $G_w = \{\sigma \in G \mid f_w(\sigma\alpha) = 0\}$ so that $|G_w| = \deg f_w = [L_w : K_v]$ and hence $G_w \simeq \mathrm{Gal}(L_w : K_v)$. □

LEMMA 128. *Let L_w/K_v be a Galois extension of complete non-archimedean fields. Then the extension λ_w/κ_v of residue fields is normal and the map $\mathrm{Gal}(L_w : K_v) \to \mathrm{Aut}(\lambda_w : \kappa_v)$ is surjective.*

PROOF. Given $\bar{\alpha} \in \lambda_w$ let $\alpha \in \mathcal{O}_w$ be any preimage, and let $f \in K_v[x]$ be its minimal polynomial. Then f splits in L_w since the extension is Galois, its reduction $\bar{f}$ splits in λ_w, so finally the minimal polynomial of $\bar{\alpha}$ splits. □

2.4.3. Places of number fields.

DEFINITION 129. Let F be a number field. Call a place of F *infinite* if it is archimedean (equivalently, lies over the archimedean place of $\mathbb{Q}$), *finite* otherise (it if lies over a non-archimedean place of$\mathbb{Q}$). Write $|F|_\infty$, $|F|_\mathrm{f}$ for the two sets of places.

PROPOSITION 130. *Let F be a number field. Then*

(1) $|F|_\infty = \mathrm{Hom}(F,\mathbb{C})/\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

(2) $|F|_f = \left\{ |\cdot|_{\mathfrak{p}} \mid \mathfrak{p} \lhd \mathcal{O}_F \text{ prime} \right\}$.

PROOF. (1) This is Lemma 117.

(2) Let $\mathfrak{p} \lhd \mathcal{O}_F$ be prime, and for $x \in \mathcal{O}_F$ let $v_{\mathfrak{p}}(x) = e$ where $\mathfrak{p}^e \| x\mathcal{O}_F$. This is clearly a valuation, and the valuations corresponding to distinct primes are inequivalent: if x belongs to one prime but not the other then x^n will behave differently.

Conversely, let $|\cdot|_v$ be a non-archimdean absolute value on F, normalized so that the restriction to $\mathbb{Q}$is $|\cdot|_p$ for some p. Let $\alpha \in F$ have $|\alpha|_v > 1$ and let $f \in \mathbb{Z}[x]$ be monic, of degree d. Then $|f(\alpha)|_v = |\alpha|_v^d > 0$ so $\alpha \notin \mathcal{O}_F$. It follows that $|x|_v \leq 1$ for all $x \in \mathcal{O}_F$ and hence that $\mathfrak{p} = \{x \in \mathcal{O}_F \mid |x|_v < 1\}$ is a prime ideal of $\mathcal{O}_F$. Since $|p|_v = |p|_p < 1$ we have $p \in \mathfrak{p}$ so $\mathfrak{p}|p$. Let $|\cdot|_{\mathfrak{p}}$ be the absolute value corresponding to this ideal, normalized the same way. Then the two absolute values agree on p and on the complement $\mathcal{O}_F \setminus \mathfrak{p}$, hence on the invertible elements of the localization $(\mathcal{O}_F)_{\mathfrak{p}}$. But that ring is a local PID, so it is now enough to check that they agree on a generator of the maximal ideal. For this note that (up to units of the localization) p is a power of that generator, and the absolute values agree on p. □

LEMMA 131. *Let v be a finite place of F, corresponding to the prime $\mathfrak{p} \lhd \mathcal{O}_F$. Then $\mathcal{O}_F$ is dense in the valuation ring $\mathcal{O}_v \subset F_v$ and $\mathfrak{p}$ is dense in the prime ideal $\mathfrak{p}_v \lhd \mathcal{O}_v$. More generally for a fractional ideal $\mathfrak{a}$ of F of order e at $\mathfrak{p}$ its closure in F_v is $\mathfrak{p}_v^e$. Conversely, $\mathfrak{p}_v^e \cap \mathcal{O}_F = \mathfrak{p}^e$.*

PROOF. The closure of $\mathfrak{a}$ in L_w is $\mathcal{O}$-invariant, hence $\mathcal{O}_w$ invariant. Also, if $\mathfrak{a} \subset \alpha\mathcal{O}_L$ then its closure is contained in $\alpha\mathcal{O}_w$. It is therefore a fractional ideal, so we have $\overline{\mathfrak{a}} = \mathfrak{P}_w^{e'}$ for some $e' \in \mathbb{Z}$ and we need to show $e = e'$.

We have already checked that the closure of $\mathfrak{P}$ is $\mathfrak{P}_w$ and that $\mathfrak{P}$

The claim is invariant under multiplication by elements of $L^\times$ (including the rational prime p below $\mathfrak{P}$), so we may assume $\mathfrak{a}$ is an ideal of $\mathcal{O}_L$. From $\mathfrak{a} \subset \mathfrak{P}^e$ we get $\overline{\mathfrak{a}} \subset \mathfrak{P}_w^e$ that is $e' \geq e$. Conversely, $\mathfrak{a} \subset \overline{\mathfrak{a}} \cap \mathcal{O}_L$

The argument above shows that $\mathcal{O}_F \subset \mathcal{O}_v$ and $\mathfrak{p} \subset \mathfrak{p}_v$. To get the density it's enough to approximate $x \in F$ such that $|x|_v \leq 1$ by elements of $\mathcal{O}_F$. By hypothesis the prime factorization of the principal fractional ideal (x) has $\mathfrak{p}$ to a positive power. In other words, there is an ideal $\mathfrak{a}$ prime to $\mathfrak{p}$ such that $(x)\,\mathfrak{a} \subset \mathcal{O}_F$. Since $\mathfrak{p} \nmid \mathfrak{a}$ there is $\alpha \in \mathfrak{a}$ which is not in $frakp$. By the choice $\alpha \in \mathfrak{a}$ we have $\alpha x \in OF$. Since α is prime to $frakp$, it is prime to $\mathfrak{p}^k$ for each k, so that $(\alpha) + \mathfrak{p}^k = (1)$. Then for each k there is $\bar{\alpha} \in \mathcal{O}_F$ such that $\alpha\bar{\alpha} \equiv 1\ (\mathfrak{p}^k)$ and then $\bar{\alpha}\alpha x \in \mathcal{O}_F$ satisfies

$$v_{\mathfrak{p}}(\alpha\bar{\alpha}x - x) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(\alpha\bar{\alpha} - 1) \geq k$$

(recall that $v_{\mathfrak{p}}(x) \geq 0$ by hypothesis). Letting $k \to \infty$ these elements approximate x to arbitrary precision with respect to $|\cdot|_v$. Finally, if $|x|_v < 1$ then by the ultrametric property we have $|\alpha\bar{\alpha}x| < 1$ once k is large enough so elements of $\mathfrak{p}_v$ can be approximated by elements of $frakp$. □

Next, we reconcile our notions of residue degree and ramification index.

LEMMA 132. *Let L/K be an extension of number fields of degree n. Let $v \in |K|$, $w \in |L|$ be non-archimedean places such that $w|v$. Then $e(L_w/K_v) = e(\mathfrak{P}/\mathfrak{p})$ and $f(L_w/K_v) = f(\mathfrak{P}/\mathfrak{p})$.*

PROOF. Lemma 131 shows that $\mathcal{O}_{K_v}/\mathfrak{p}_v \simeq \mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_{L_w}/\mathfrak{P}_w \simeq \mathcal{O}_L/\mathfrak{P}$ in compatible fashions. For the ramification indices localize at $\mathfrak{p}$, $\mathfrak{P}$first. This does not change the ramification index,

and now after localization we have $(\mathfrak{P})^e = \mathfrak{p}$ and that both ideals are principal, so there is nothing to prove. □

For the final claim we introduce a new normalization of the absolute values.

DEFINITION 133. Fix a place w of the number field F, and write $|\cdot|_v$ for an absolute value in the class of v which restricts to the absolute value $|\cdot|_p$ on $\mathbb{Q}$ (perhaps $p = \infty$). We then write $\|\cdot\|_v$ for the absolute value $\|\cdot\|_v = |\cdot|_v^{[F_v:\mathbb{Q}_p]}$.

LEMMA 134. *For an infinite place v associated to an embedding $\varphi\colon F \to \mathbb{C}$, we have $\|x\|_v = |\varphi(x)|_{\mathbb{R}}$ if φ is real, $\|x\|_v = \varphi(x)\overline{\varphi(x)}$ if φ is complex. For a finite place v associated to the prime $\mathfrak{p} \lhd \mathcal{O}_F$ let $q_v = \#\kappa_v = [\mathcal{O}_v : \mathfrak{p}_v]$ be the size of the residue field. Then*

$$\|x\|_v = q_v^{-v_{\mathfrak{p}}((x))}.$$

PROOF. The claims for infinite places are immediate. For finite places let F_v be a finite extension of Qp. Then

$$\|x\|_v' = q_v^{-v(x)}$$

is an absolute value on F_v equivalent to the absolute value $|\cdot|_v$ extending that of Qp. To see the power relating the two it's enough to consider the case $x = p$. In that case $v(p) = e$ where e is the ramification index (for which $p\mathcal{O}_v = \mathfrak{p}_v^e$) and certainly $q_v = p^f$ where f is the residue degree. It follows that

$$\|p\|_v' = p^{-ef} = |p|_v^{-[F_v:\mathbb{Q}_p]} = \|p\|_v$$

and hence

$$\|x\|_v' = \|x\|_v$$

for all x. □

PROPOSITION 135 (Product formula). *For all $x \in F^\times$,*

$$\prod_{v \in |F|} \|x\|_v = 1.$$

PROOF. The claim for $F = \mathbb{Q}$ is an exercise in unique factorization (see PS3). Recall now that if $v \in |F|$ restricts to the p-adic absolute value on $\mathbb{Q}$ (perhaps $p = \infty$) then $|x|_v = \left|N_{\mathbb{Q}_p}^{F_v} x\right|_p^{1/[F_v:\mathbb{Q}_p]}$ (that's Theorem 98), in which case

$$\|x\|_v = \left|N_{\mathbb{Q}_p}^{F_v} x\right|_p.$$

But then

$$\prod_{v|p} \|x\|_v = \prod_{v|p} \left|N_{\mathbb{Q}_p}^{F_v} x\right|_p = \left|\prod_{v|p} N_{\mathbb{Q}_p}^{F_v} x\right|_p = \left|N_{\mathbb{Q}}^{F} x\right|_p$$

by Corollary 124. We therefore have

$$\prod_v \|x\|_v = \prod_{p \le \infty} \prod_{v|p} \|x\|_v = \prod_{p \le \infty} \left|N_{\mathbb{Q}}^{F} x\right|_p = 1$$

by the product formula for $\mathbb{Q}$. □

CHAPTER 3

Different, Discriminant and ramification

Let K be either a number field or a field complete with respect to a discrete absolute value. Let $\mathcal{O}_K$ be the ring of integers in the first case, the valuation ring in the second. Let L be a finite separable extension of K, $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L (which is the valuation ring in the second case).

In this section we develop two invariants of this extension; an ideal of $\mathcal{O}_L$ called the (relative) *different* and an ideal of $\mathcal{O}_K$called the (relative) *discriminant*. These encode the ramification of the extension: a prime $\mathfrak{P} \lhd \mathcal{O}_L$ divides the different iff $e(\mathfrak{P} : \mathfrak{P} \cap \mathcal{O}_K) > 1$, while $\mathfrak{p} \lhd \mathcal{O}_K$divides the discrminant iff there is $\mathfrak{P}|\mathfrak{p}$ a prime of $\mathcal{O}_L$ such that $e(\mathfrak{P} : \mathfrak{p}) > 1$.

3.1. The trace form and duality (1 hour, 8/3/2013)

3.1.1. Analytic motivation. Recall that (basic Fourier analysis on the circle)

$$L^2(\mathbb{R}/\mathbb{Z}) = \hat{\bigoplus_{k\in\mathbb{Z}}} \mathbb{C} e_k$$

where $e_k(x) = e^{2\pi i k x}$. This underlines much of classical analytic number theory.

Now let K be a number field. Then $K_\infty = \prod_{v|\infty} K_v$ is an R-algebra with $\dim_{\mathbb{R}} K_\infty = \sum_{v|\infty} f(K_v : \mathbb{R}) = n$ where $n = [K : \mathbb{Q}]$. The product embedding $\mathcal{O}_K \hookrightarrow K_\infty$ has discrete image, since any non-zero element of $\mathcal{O}_K$ has norm in $\mathbb{Z} \setminus \{0\}$ whereas $N_{\mathbb{R}}^{K_\infty}$ is continuous.

EXAMPLE 136. $\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R} \times \mathbb{R}$. $\sqrt{2}$ on the left is a formal symbol whose only property is that it squares to 2, but in $\mathbb{R}$ there are two genuinely distinct roots of 2 (one is positive, the other negative), so two embeddings in $\mathbb{R}$. The image is discrete since if $a + b\sqrt{2}, a - b\sqrt{2}$ are both close to 0 in $\mathbb{R}$ for $a, b \in \mathbb{Z}$ not then the norm $a^2 - 2b^2$ would be an integer close to zero, so that $a = b = 0$. Alternatively, recover a, b from linear combinations.

It follows that $\mathcal{O}_K$ is a discrete subgroup of K_∞. Since $\mathrm{rk}_{\mathbb{Z}} \mathcal{O}_K = n = [K : \mathbb{Q}]$ (see xxx), $\mathcal{O}_K$is cocompact.

EXERCISE. For $k = (k_v)_{v|\infty}, x = (x_v)_{v|\infty} \in K_\infty$ define $e_k(x) = \exp\left(2\pi i \sum_{v|\infty} \mathrm{Tr}_{\mathbb{R}}^{K_v} k_v x_v\right)$. Now that if k, x are images of $k, x \in K$ then $e_k(x) = \exp(2\pi i \mathrm{Tr}_{\mathbb{Q}}^K(kx))$ (see Corollary 124). It now follows (for general k) that e_k is $\mathcal{O}_K$-periodic iff $\mathrm{Tr}_{\mathbb{Q}}^K(kx) \in \mathbb{Z}$ for all $x \in \mathcal{O}_K$. In other words, characters of $K_\infty/\mathcal{O}_K$ are parametrised by the dual lattice $\mathcal{O}_K^*$.

$$L^2\left(K_\infty/\mathcal{O}_K\right) \simeq \hat{\bigoplus_{k\in\mathbb{Z}}} \mathbb{C} e_k$$

3.1.2. The trace form. The trace form $(x,y) = \mathrm{Tr}_K^L(xy)$ is a non-degenerate bilinear form on L, and so gives an idenfication of L with its dual K-vector space (for its first use in the course, see Proposition 19). From now on write simply Tr unless we need to specify the field.

DEFINITION 137. Let $\Lambda \subset L$ be an $\mathcal{O}_K$-submodule. We define the *dual* of Λ to be $\Lambda^* = \left\{x \in L \mid \mathrm{Tr}_K^L(x\Lambda) \subset \mathcal{O}_K\right\}$.

Note that Λ^* is always an $\mathcal{O}_K$-submodule of L.

LEMMA 138. *Let $\{\omega_i\}_{i=1}^n$ be a K-basis for L, and let $\{\omega_i^*\}_{i=1}^n$ be the dual basis with respect to the trace form. Then*

$$\left(\bigoplus_{i=1}^n \mathcal{O}_K\omega_i\right)^* = \bigoplus_{i=1}^n \mathcal{O}_K\omega_i^*.$$

PROOF. Let $\Lambda = \bigoplus_{i=1}^n \mathcal{O}_K\omega_i$. Since $\mathrm{Tr}_K^L(\omega_i\omega_j) \in \mathbb{Z}$ for all i, $\omega_j \in \Lambda^*$. Conversely, let $\sum_{j=1}^n a_j\omega_j^* \in \Lambda^*$ where $a_i \in K$. Then $a_j = \mathrm{Tr}_K^L\left(\omega_i\sum_{j=1}^n a_j\omega_j^*\right) \in \mathcal{O}_K$. □

COROLLARY 139. *The dual of a fractional ideal is a fractional ideal.*

PROOF. First note that $\mathcal{O}_L \subset \mathcal{O}_L^*$ and that if $\alpha \in L^\times$ then $(\alpha L)^* = \alpha^{-1}L^*$ (so that we may freely replace $\mathfrak{a}$ with $\alpha\mathfrak{a}$ without loss of generality). Now let $\mathfrak{a}$ be a fractional ideal of L. Then if $x \in \mathfrak{a}^*$and $\alpha \in L$ we have $\mathrm{Tr}_K^L(\alpha x\mathfrak{a}) = \mathrm{Tr}_K^L(\alpha x\mathfrak{a}) = \mathrm{Tr}_K^L(x\mathfrak{a}) \in \mathfrak{a}^*$ so $\mathfrak{a}^*$ is an $\mathcal{O}_L$-module. If $\mathfrak{a} \subset \mathcal{O}_L$ then $\mathfrak{a}^* \supset \mathcal{O}_L^* \supset \mathcal{O}_L$ so it is non-zero. Finally, let $\alpha \in \mathfrak{a}$be non-zero and let $\{\omega_i\}_{i=1}^n$ be a K-basis of L contained in $\mathcal{O}_K$. Then $\mathfrak{a} \supset \alpha\mathcal{O}_L \supset \oplus_{i=1}^n \mathcal{O}_K(\alpha\omega_i)$. Then by the Lemma $\mathfrak{a}^* \subset \oplus_{i=1}^n \mathcal{O}_K\alpha^{-1}\omega_i^*$. Let $m \in \mathbb{Z}\setminus\{0\}$ be such that $m\omega_i \in \mathcal{O}_L$ for all i, at which point we see that $(m\alpha)\mathfrak{a}^* \subset \mathcal{O}_L$so $\mathfrak{a}^*$ is indeed a fractional ideal. □

3.2. The different

3.2.1. Definition; first properties (Lecture 22).

DEFINITION 140. The *complementary module* (or *inverse relative different*) of L/K is the fractional ideal $\mathcal{C}_{L/K} \stackrel{\text{def}}{=} \mathcal{O}_L'$. The *relative different* of the extension is then the ideal $\mathcal{D}_{L/K} \stackrel{\text{def}}{=} \mathcal{C}_{L/K}^{-1}$.

REMARK 141. We saw in the proof of Corollary 139 that $\mathcal{O}_L \subset \mathcal{C}_{L/K}$ so $\mathcal{C}_{L/K}^{-1}$ is an ideal.

LEMMA 142. *The dual of the fractional ideal $\mathfrak{a}$ is the fractional ideal $\mathcal{C}_{L/K}\mathfrak{a}^{-1}$.*

PROOF. We clearly have $\mathrm{Tr}_K^L\left(\mathfrak{a}\mathcal{C}_{L/K}\mathfrak{a}^{-1}\right) = \mathrm{Tr}_K^L\left(\mathcal{C}_{L/K}\right) = \mathcal{O}_K$ so $\mathcal{C}_{L/K}\mathfrak{a}^{-1} \subset \mathfrak{a}^*$. Conversely, $\mathrm{Tr}\left(\mathcal{O}_K\mathfrak{a}\mathfrak{a}^*\right) \subset \mathcal{O}_K$ by definition so $\mathfrak{a}\mathfrak{a}^* \subset \mathcal{C}_{L/K}$ and hence $\mathfrak{a}^* \subset \mathcal{C}_{L/K}\mathfrak{a}^{-1}$ □

LEMMA 143 (Different in towers). *Let $M/L/K$ be a tower. Then $\mathcal{D}_{M/K} = \mathcal{D}_{L/K}\mathcal{D}_{M/L}$.*

PROOF. We have $\mathrm{Tr}_K^M\left(\mathcal{C}_{L/K}\mathcal{C}_{M/L}\mathcal{O}_M\right) = \mathrm{Tr}_K^L\mathrm{Tr}_M^K\left(\mathcal{C}_{L/K}\mathcal{C}_{M/L}\mathcal{O}_M\right) = \mathrm{Tr}_K^L\left(\mathcal{C}_{L/K}\,\mathrm{Tr}_M^K\left(\mathcal{C}_{M/L}\mathcal{O}_M\right)\right) \subset \mathrm{Tr}_K^L\left(\mathcal{C}_{L/K}\mathcal{O}_L\right) \subset \mathcal{O}_K$ so $\mathcal{C}_{L/K}\mathcal{C}_{M/L} \subset \mathcal{C}_{M/K}$.

Conversely, since $\mathcal{O}_L\mathcal{O}_M = \mathcal{O}_M$, $\mathrm{Tr}_K^L\left(\mathcal{O}_L\,\mathrm{Tr}_L^M\left(\mathcal{C}_{M/K}\mathcal{O}_M\right)\right) = \mathrm{Tr}_K^M\left(\mathcal{C}_{M/K}\mathcal{O}_M\right) \subset \mathcal{O}_K$ so $\mathrm{Tr}_L^M\left(\mathcal{C}_{M/K}\mathcal{O}_M\right) \subset \mathcal{C}_{L/K}$. Thus $\mathrm{Tr}_L^M\left(\mathcal{C}_{L/K}^{-1}\mathcal{C}_{M/K}\mathcal{O}_M\right) \subset \mathcal{O}_L$ and hence $\mathcal{C}_{L/K}^{-1}\mathcal{C}_{M/K} \subset \mathcal{C}_{M/L}$ and $\mathcal{C}_{M/K} \subset \mathcal{C}_{L/K}\mathcal{C}_{M/L}$. □

We now calculate another dual basis, giving us a bound on the different.

PROPOSITION 144. *Let $L = K(\alpha)$ be a separable extension of degree n. Define $b_i \in L$ by $\frac{f(x)}{x-\alpha} = \sum_{i=0}^{n-1} b_i x^i$ where $f \in K[x]$ is the minimal polynomial of α. Then the basis dual to $\{\alpha^i\}_{i=0}^{n-1}$ is $\left\{\frac{b_i}{f'(\alpha)}\right\}_{i=0}^{n-1}$. If, in addition, $\alpha \in \mathcal{O}_L$then $\mathcal{O}_K[\alpha]^* = \frac{1}{f'(\alpha)}\mathcal{O}_K[\alpha]$.*

PROOF. Let $g(x) = \frac{f(x)}{x-\alpha}$, and let β be a root of f. Then $g(\beta) = \begin{cases} f'(\beta) & \beta = \alpha \\ 0 & \beta \neq \alpha \end{cases}$. Now let $\{\alpha_i\}_{i=1}^n$ be the roots of f in a splitting field consider the polynomial

$$h_r(X) = \sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)}.$$

By the observation we have $h_r(\alpha_j) = \alpha_j^r$ so if $0 \leq r \leq n-1$, $h_r(X) - X^r$ is a polynomial of degree at most $n-1$ with n roots. It follows that $h_r(X) = X^r$. Writing $h_r(X) = \mathrm{Tr}_K^L \frac{f(X)}{X-\alpha} \frac{\alpha^r}{f'(\alpha)}$ we see that $\mathrm{Tr} \frac{b_i}{f'(\alpha)} \alpha^r = \delta_{ir}$.

Now suppose that $f(x) = \sum_{i=0}^n a_i x^i$ where $a_i \in \mathcal{O}_K$ and $a_n = 1$. Then $(x-\alpha)\sum_{i=0}^{n-1} b_i x^i = \sum_{i=0}^n a_i x^i$ is equivalent to $b_i - \alpha b_{i+1} = a_{i+1}$ (set $b_{-1} = b_n = 0$). Thus $b_{n-1} = 1$ and it follows by induction that all $b_i \in \mathcal{O}_K[\alpha]$. Conversely, starting from $1 = b_{n-1}$ again suppose by induction that $\alpha^i \in \mathrm{Span}_{\mathcal{O}_K}\left\{b^j\right\}_{n-1-i \leq j \leq n-1}$. Since $\alpha b_j = b_{j-1} - a_j b_{n-1}$ it follows that $\alpha^{i+1} \in \mathrm{Span}_{\mathcal{O}_K}\left\{b^j\right\}_{n-1-i-1 \leq j \leq n-1}$ and we are done. □

COROLLARY 145. *Let $L = K(\alpha)$ where $\alpha \in \mathcal{O}_L$, and let $f \in \mathcal{O}_K[x]$ be the minimal polynomial of α. Then $\mathcal{D}_{L/K}$ divides $f'(\alpha)\mathcal{O}_L$.*

PROOF. We have $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$ so $\mathcal{C}_{L/K} \subset \mathcal{O}_K[\alpha]^* = \frac{1}{f'(\alpha)}\mathcal{O}_K[\alpha] \subset \frac{1}{f'(\alpha)}\mathcal{O}_L$. It follows that $\mathcal{D}_{L/K} \supset f'(\alpha)\mathcal{O}_L$ as claimed. □

FACT 146. *$\mathcal{D}_{L/K}$ is the GCD of all the ideals $f'(\alpha)$ where α ranges over all integral generators of L.*

COROLLARY 147. *Let L/K be an unramified extension of local fields. Then $\mathcal{D}_{L/K} = (1)$.*

PROOF. Let $\alpha \in \mathcal{O}_L$be such that $\lambda = \kappa(\bar{\alpha})$, and let f be its minimal polynomial. Then $\bar{f}$ is the minimal polynomial of $\bar{\alpha}$. By definition of separability $\bar{f}'(\bar{\alpha}) \neq 0$ and it follows that $f'(\alpha) \in \mathcal{O}_L^\times$. □

3.2.2. Local-to-global (Lecture 23).

DEFINITION 148. For a finite set $S \subset |L|_{\mathrm{f}}$ the set of S-integers is $\mathcal{O}_L^S = \{x \in L \mid \forall w \in |L|_{\mathrm{f}} \setminus S : |x|_w \leq 1\}$. Also set $L_S = \prod_{w \in S} L_w$.

LEMMA 149. *let S be as above. Then $\mathcal{O}_L^S$ is dense in $L_S = \prod_{w \in S} L_w$.*

PROPOSITION 150. *Let K be a number field, and let w be a finite place of L corresponding to the prime ideal $\mathfrak{P} \lhd \mathcal{O}_L$ and lying over the place v of K. Then the exponent of $\mathfrak{P}$ in $\mathcal{D}_{L/K}$ is the exponent of $\mathfrak{P}_w$ in $\mathcal{D}_{L_w/K_v}$.*

PROOF. By Lemma 131 it is enough to show that the closure of $\mathcal{C}_{L/K}$ in L_w (which is a fractional ideal) is $\mathcal{C}_{L_w/K_v}$. In one direction let $x \in \mathcal{C}_{L/K}$ and let $y \in \mathcal{O}_{L_w}$. By Lemma 149 there is $z \in \mathcal{O}_L^S$ such that z is sufficiently w-close to y (see below) and z is w'-close to 0 for all $w'|v$ other than w. Then z is everywhere integral so $z \in \mathcal{O}_L$. We thus have $\mathrm{Tr}_K^L(xz) \in \mathcal{O}_K \subset \mathcal{O}_{K_v}$. But

$$\mathrm{Tr}_K^L(xz) = \mathrm{Tr}_{K_v}^{L_w}(xz) + \sum_{\substack{w'|v \\ w' \neq v}} \mathrm{Tr}_{K_v}^{L_{w'}}(xz).$$

By assumption $z \in \mathcal{O}_{L_{w'}}$ so $\mathrm{Tr}_{K_v}^{L_{w'}}(xz) \in \mathcal{O}_{K_v}$ for all w'. It follows that $\mathrm{Tr}_{K_v}^{L_w}(xz) \in \mathcal{O}_{K_v}$ and hence that $\mathrm{Tr}_{K_v}^{L_w}(xy) = \mathrm{Tr}_{K_v}^{L_w}(xz) + \mathrm{Tr}_{K_v}^{L_w}(x(y-z)) \in \mathcal{O}_{K_v}$ as long as $|y-z|_w |x|_w \leq 1$.

Conversely, let $x \in \mathcal{C}_{L_w/K_v}$ and let $z \in \mathcal{O}_L^S$ be w-close to x and w'-close to 0 for all $w'|v$ other than w. Then for $y \in \mathcal{O}_L$ we have $z, y \in \mathcal{O}_{L_{w'}}$ for all w' so $\mathrm{Tr}_{K_v}^{L_{w'}}(zy) \in \mathcal{O}_{K_v}$. Also, $\mathrm{Tr}_{K_v}^{L_w}(zy) = \mathrm{Tr}_{K_v}^{L_w}((z-x)y) + \mathrm{Tr}_{K_v}^{L_w}(xy) \in \mathcal{O}_{K_v}$ as long as $|z-x|_w \leq 1$. It follows that $\mathrm{Tr}_K^L(zy)$ is v-integral. It is also v' integral for all other finite places of K since both z, y are integral for any $w'|v'$. Thus $\mathrm{Tr}_K^L(zy) \in \mathcal{O}_K$ and $z \in \mathcal{C}_{L/K}$. □

3.2.3. The different and ramification (Lecture 23 continued).

PROPOSITION 151. *Let L_w/K_v be an extension of complete fields with discrete valuations and perfect residue fields, and let e be the ramification index. Then $\mathfrak{P}_w^{e-1}$ divides $\mathcal{D}_{L_w/K_v}$, exactly if the extension is at most tamely ramified. If the ramification is wild then $\mathfrak{P}_w^e$ divides $\mathcal{D}_{L_w/K_v}$.*

PROOF. By multiplicativity in towers and Corollary 147 we may assume that the extension is totally ramified, hence of the form $L_w = K_v(\Pi)$ where Π satisfies an Eisenstein polynomial: $f(\Pi) = \Pi^e + \sum_{i=0}^{e-1} a_i \Pi^i = 0$ where $a_i \in \mathfrak{p}_v$, a_0 a uniformizer of K_v.

We begin with the identity $\mathcal{O}_{L_w} = \mathcal{O}_{K_v}[\Pi]$. In problem 9 of Problem Set 4 it is shown that for any set $A \subset \mathcal{O}_{L_w}$ of representatives for the residue field λ_w, $\mathcal{O}_{L_w} = \left\{\sum_{i=0}^{\infty} a_i \Pi^i \mid a_i \in A\right\}$. Under the hypothesis that the extension is totally ramified, L_w and K_v have the same residue field, so we may choose $A \subset \mathcal{O}_{K_v}$, which shows that $\mathcal{O}_{K_v}[\Pi]$ is dense in $\mathcal{O}_{L_w}$. But $\mathcal{O}_{K_v}[\Pi] \simeq (\mathcal{O}_{K_v})^e$ is compact, so equal to its closure.

Finally, by Proposition 144 we have $\mathcal{D}_{L_w/K_v} = \left(e\Pi^{e-1} + \sum_{i=1}^{e-1} i a_i \Pi^{i-1}\right) \mathcal{O}_{L_w}$. Since $\Pi^e | a_i$ we see see that $\mathcal{D}_{L_w/K} = \left(\Pi^{e-1}\right)$ if e is prime to p. If $p|e$ then $\Pi^e | \mathcal{D}_{L_w/K_v}$. □

We now summarize the discussion so far.

THEOREM 152. *Let L/K be a finite extension of number fields. For each prime $\mathfrak{P} \lhd \mathcal{O}_L$, say lying over $\mathfrak{p} \lhd \mathcal{O}_K$, we have $v_{\mathfrak{P}}\left(\mathcal{D}_{L/K}\right) \geq e(\mathfrak{P}/\mathfrak{p}) - 1$ with equality unless the extension is wildly ramified at $\mathfrak{P}$, at which point the inequality is strict. In particular*

(1) $\mathfrak{P} \mid \mathcal{D}_{L/K}$ iff $\mathfrak{P}$ is ramified.
(2) There are finitely many ramified primes.

PROOF. The first claim is the Proposition; the last claim follows from Corollary 145. □

3.3. The Discriminant

3.3.1. General extensions of fields. Let L/K be a finite separable extension of fields. Let $\Omega = \{\omega_i\}_{i=1}^n \subset L$ be a K-basis, let $\{\sigma_j\}_{i=1}^n = \mathrm{Hom}_K(L, \bar{K})$, and set

$$D_{L/K}(\Omega) = \left(\det\left(\sigma_j \omega_i\right)_{i,j}\right)^2 .$$

This is independent of the ordering of the basis and the set of embeddings. It is therefore $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-invariant and hence an element of K (we will verify momentarily that it is non-zero).

Let $A \in M_n(\bar{K})$ be the matrix $a_{ij} = \sigma_j(\omega_i)$. Then $D_{L/K}(\Omega) = (\det(A))^2$. Suppose $\Omega' = \{\omega'_k\}_{k=1}^n$ is another basis associated to the matrix B where $b_{kj} = \sigma_j \omega'_k$, and let $S \in \mathrm{GL}_n(K)$ be the change-of-basis matrix given by $\omega_i = \sum_k s_{ik}\omega'_k$. Then

$$a_{ij} = \sigma_j \omega_i = \sigma_j \left(\sum_k s_{ik}\omega'_k\right) = \sum_k s_{ik}\sigma_j \omega'_k = \sum_k s_{ik} b_{kj} ,$$

in other words

$$A = SB .$$

In particular,

$$D_{L/K}(\Omega) = (\det S)^2 D_{L/K}(\Omega')$$

and (once we prove $D_{L/K}(\Omega) \neq 0$) we can define a discrimimant $D_{L/K} \in K^\times / (K^\times)^2$. We also note that if the two bases generate the same R-module for a subring $R \subset K$ then $\det(S) \in R^\times$ so we can associate to free R-module generated by the basis a discriminant in $K^\times / (R^\times)^2$.

EXERCISE 153 (PS6). For $\beta \in L^\times$ we have

$$D_{L/K}(\beta\Omega) = \left(N_K^L \beta\right)^2 D_{L/K}(\Omega)$$

LEMMA 154. *Let Ω, Ω' be two bases with associated matrices. Then $(AB^t)_{ik} = \mathrm{Tr}_K^L\left(\omega_i \omega'_k\right)$. In particular, leeting Ω' be the dual basis with respect to the trace form (always non-degenerate on a separable extension) we have $AB^\times = I_n$ so A is always invertible, and letting $\Omega' = \Omega$ instead gives*

$$D_{L/K}(\Omega) = \det\left(\mathrm{Tr}_K^L(\omega_i \omega_j)\right) .$$

We also relate our discriminant to a different point-of-view.

LEMMA 155. *Suppose that $L = K(\alpha)$ and let $\{\alpha_j\}_{j=1}^n \subset \bar{K}$ be the Galois conjugates of α (=the roots of its minimal polynomial). Then for the basis $\omega_i = \alpha^i$ ($0 \leq i \leq n-1$) we have*

$$D_{L/K}(\Omega) = \prod_{j<k} \left(\alpha_j - \alpha_k\right)^2 = \Delta(f)$$

where $f = \prod_{j=1}^n \left(x - \alpha_j\right)$ is the minimal polynomial of α.

PROOF. Let $\alpha_j = \sigma_j(\alpha)$. Then $a_{ij} = \sigma_j(\alpha^i) = \alpha_j^i$ so by the Vandermonde determinant,

$$\det(A) = \prod_{j<k} \left(\alpha_j - \alpha_k\right)$$

and the claim follows. □

3.3.2. Number fields and p-adic fields. Assume now that L, K are either number fields or fields complete with respect to a discrete valuation.

LEMMA-DEFINITION 156. *Let $\mathfrak{a} \subset L$ be a fractional ideal. Then the $\mathcal{O}_K$-submodule K generated by $\left\{D_{L/K}(\Omega) \mid \Omega \subset \mathfrak{a} \text{ is a } K\text{-basis of } L\right\}$ (denoted henceforth $D_{L/K}(\mathfrak{a})$) is a fractional ideal, to be called the (relative) discriminant of fraka.*

PROOF. If $\Omega \subset \mathcal{O}_L$ then $\mathrm{Tr}_K^L\left(\omega_i\omega_j\right) \in \mathcal{O}_K$ so that $D_{L/K}(\Omega) \in \mathcal{O}_K \setminus \{0\}$, and we see that for any non-zero $\mathfrak{a} \lhd \mathcal{O}_L$, $D_{L/K}(\mathfrak{a})$ is a non-zero ideal in $\mathcal{O}_K$. For general fractional ideals it remains to observe that $D_{L/K}(\beta\mathfrak{a}) = \left(N_K^L(\beta)\right)^2 D_{L/K}(\mathfrak{a})$ follows from Exercise 153. □

REMARK 157. By definition $\mathfrak{a} \subset \mathfrak{b}$ implies $D_{L/K}(\mathfrak{a}) \subset D_{L/K}(\mathfrak{b})$, that is $\mathfrak{b}|\mathfrak{a} \Rightarrow D_{L/K}(\mathfrak{b})|D_{L/K}(\mathfrak{a})$.

EXERCISE 158 (PS6). Suppose $\mathfrak{a} = \oplus_{i=1}^n \mathcal{O}_K\omega_i$ happens to be a free OK-module (e.g. because $\mathcal{O}_K$ is a PID). Then $D_{L/K}(\mathfrak{a}) = \left(D_{L/K}(\Omega)\right)$.

DEFINITION 159. The *relative discriminant* of L/K is the ideal $D_{L/K} = D_{L/K}(\mathcal{O}_L)$.

COROLLARY 160. *Let $\alpha \in \mathcal{O}_L$ be such that $L = K(\alpha)$. Then $D_{L/K} \mid (\Delta(f))$ where $f \in \mathcal{O}_K[x]$ is the minimal polynomial of α.*

PROPOSITION 161 (local-to-global). *Let L/K be an extension of number fields and let $v \in |K|_f$. Then the closure of $D_{L/K}$ in $\mathcal{O}_v$ is $\prod_{w|v} D_{L_w/K_v}$.*

PROOF. We first verify that in the identification

$$L \otimes_K K_v \simeq \bigoplus_{w|v} L_w$$

the closure of $\mathcal{O}_L$ (under the diagonal embedding) is $\overline{\mathcal{O}_L} = \bigoplus_{w|v} \mathcal{O}_{L_w}$. Indeed the closure of $\mathcal{O}_L$in each L_w is $\mathcal{O}_{L_w}$ so we just need to show surjectivity. For this use that $\mathcal{O}_L^S$ is dense in $\bigoplus_{w|v} L_w$ where $S = \{w : w|v\}$. But any element of $\mathcal{O}_L^S$ can be approximated by an element of $\mathcal{O}_L$ modulu a large power of the product of primes in S.

Now if $\Omega_w \subset \mathcal{O}_{L_w}$ are K_v-bases of th L_w let $\Omega = \cup_{w|v}\Omega_w$ be the resulting K_v-basis of $\bigoplus_{w|v} L_w$ and let Ω' consists of elements of $\mathcal{O}_L$ approximating those of Ω. Then they are linearly independent (determinant is continuous) and $D_{L/K}(\Omega')$ is close to

$$\prod_{w|v} D_{L_w/K_v}(\Omega_w) .$$

It follows that the closure of $D_{L/K}$ contains $\prod_{w|v} D_{L_w/K_v}$.

Conversely, let $\Omega \subset \mathcal{O}_L$ be any K-basis of L. We need to show that $D_{L/K}(\Omega) \in \prod_{w|v} D_{L_w/K_v}$. For this note that its image in $L \otimes_K K_v \simeq \bigoplus_{w|v} L_w$ is a K_v-basis, and the claim follows from the following: □

LEMMA 162. *Let $A \in M_n(K_v)$. Then there is $g \in \mathrm{GL}_n(\mathcal{O}_{K_v})$ such that gA is diagonal. Equivalently, in a finite-dimentional K_v-vectorspace V given two bases $\Omega = \{\omega_i\}_{i=1}^n$ and $\Omega' = \left\{\omega_j'\right\}_{j=1}^n$ there is $g \in \mathrm{GL}_n(\mathcal{O}_{K_v})$ such that $\sum_j g_{ij}\omega_j' = \varpi_v^{d_i}\omega_i$.*

PROOF. Do Gaussian elimination, selecting as a pivot in each column an element of maximal absolute value. □

THEOREM 163 (Different and discriminant). $D_{L/K} = N_K^L \mathcal{D}_{L/K}$.

PROOF. Localizing and completing it is enough to consider the case where L, K are complete wrt discrete valuations. Since $\mathcal{O}_K$ is a PID we have

$$\mathcal{O}_L = \bigoplus_{i=1}^{n} \mathcal{O}_K \omega_i$$

for a basis Ω which means both that $D_{L/K} = \left(D_{L/K}(\Omega)\right)$ and that the complementary module is $\mathcal{C}_{L/K} = \bigoplus_{i=1}^{n} \mathcal{O}_K \omega_i^*$ where $\Omega^* = \{\omega_i^*\}$ is the basis dual to Ω.

We now compute the discriminant of the complementary module in two different ways. On the one hand, by Lemma 154 we have $D_{L/K}(\Omega) D_{L/K}(\Omega^*) = 1$ (the relevant matrices are inverse!). On the other hand, $\mathcal{C}_{L/K}$ is a principal fractional ideal, say of the form $\left(\beta^{-1}\right)$ for $\beta \in OL$. Then $D_{L/K}\left(\mathcal{C}_{L/K}\right) = N_K^L(\beta^{-1})^2 D_{L/K}$. Combining both identities we get

$$D_{L/K}^{-1} = \left(N_K^L \mathcal{D}_{L/K}\right)^{-2} D_{L/K},$$

that is

$$\left(D_{L/K}\right)^2 = \left(N_K^L \mathcal{D}_{L/K}\right)^2.$$

Since the group of fractional ideals is torsion-free the claim follows. □

COROLLARY 164. *In a tower $M : L : K$, $D_{M/K} = D_{L/K}^{[M:L]} N_K^L D_{M/L}$.*

3.3.3. On calculating the discriminat. When $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, $D_{L/K} = D(\alpha) = \prod_{i<j} \left(\alpha_i - \alpha_j\right)^2 = D(f)$ where f is the minimal polynomial of α and α_i are the conjugates. We note that in special cases this can be calculated explicitely.

Indeed, $D(f)$ is a symmetric polynomial in the roots, hence a polynomial in the coefficients of f. This polynomial is homogenous of degree $n(n-1)$ in the roots, so if f is a fewnominal explicit formulas can be written down. For example:

PROPOSITION 165 (Discriminant formulas).

(1) Let $f(x) = x^n + b$. Then $D(f) = (-1)^{\frac{n(n-1)}{2}} n^n \cdot b^{n-1}$.
(2) Let $f(x) = x^n + ax + b$. Then

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \left[n^n b^{n-1} + (-1)^{n-1}(n-1)^{(n-1)} a^n\right].$$

REMARK 166. Note that the only homogenous polynomials of degree $n(n-1)$ in the roots have the form $c_1 b^{n-1} + c_2 a^n$ so it remained to find the coefficients.

PROOF. PS6 □

COROLLARY 167. $D(x^3 + ax + b) = -\left[4a^3 + 27b^2\right]$

3.4. Example: Cyclotomic fields

Let ζ_n be a primitive root of unity of order n. Then $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$, hence Galois. There is an injection $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ from the action on the primitive roots of unity, hence the extension is Abelian and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq \phi(n)$ (Euler Totient).

3.4.1. $K = \mathbb{Q}(\zeta_n)$**;** $n = p^r$**,** p **prime.**

PROPOSITION 168. $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = p^{r-1}(p-1) = \phi(p^r)$*, the extension is ramified only over* p *where it is totally ramified and* $\pi = 1 - \zeta_{p^r}$ *is a prime element.*

PROOF. Approach 1: Let $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \sum_{j=0}^{p-1} X^{jp^{r-1}}$. Then $\zeta_{p^r} - 1$ is a root of $\Phi_{p^r}(Y+1)$ which is Eisenstein at p.

Approach 2: $\frac{1-\zeta_{p^r}^k}{1-\zeta_{p^r}} = \sum_{j=0}^{k-1} \zeta_{p^r}^j \in \mathbb{Z}[\zeta_{p^r}]$. If $(p,k) = 1$ then $\zeta_{p^r}^k$ is also a primtive root of unity and therefore $\left(\frac{1-\zeta_{p^r}^k}{1-\zeta_{p^r}}\right)^{-1} \in \mathbb{Z}[\zeta_{p^r}^k] = \mathbb{Z}[\zeta_{p^r}]$. It follows that these ratios are all units ("*cyclotomic units*") and hence that $1-\zeta_{p^r}^k$ are all associate in $\mathbb{Z}[\zeta_{p^r}]$. In particular, $\pi^{\varphi(p^r)} \sim \prod_{k\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(1-\zeta_{p^r}^k\right) = \Phi_{p^r}(1) = p$. It follows that the ramification index of (π) is at least $\phi(p^r)$, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(p^r)$, and the extension is totally ramified at p, with a unique prime π over it.

Since ζ_n satisfies $x^n - 1$ whose derivative is nx^{n-1}, the only ramified prime is p. □

LEMMA 169. *The ring of integers of* $\mathbb{Q}(\zeta_n)$ *is* $\mathbb{Z}[\zeta_n]$.

PROOF. Consider the orders $\mathcal{O} = \mathbb{Z}[\zeta_n] \subset \mathcal{O}_K$. Now $\mathcal{O}_K/\pi\mathcal{O}_K = \mathbb{Z}/p\mathbb{Z}$ since the extension is totally ramified. It follows that $\mathcal{O}_K = \mathbb{Z} + \pi\mathcal{O}_K = \mathcal{O} + \pi\mathcal{O}_K$. Multiplying by π we see that $\pi\mathcal{O}_K = \pi\mathcal{O} + \pi^2\mathcal{O}_K$ so $\mathcal{O}_K = \mathcal{O} + \pi\mathcal{O} + \pi^2\mathcal{O}_K = \mathcal{O} + \pi^2\mathcal{O}_K$. Continuing by induction we see that $\mathcal{O}_K = \mathcal{O} + \pi^k\mathcal{O}_K$ for all k.

Approach 1: Since $D(\mathcal{O})$ is a power of p, $[\mathcal{O}_K : \mathcal{O}]$ is a power of p. Therefore if we pass to the π-adic completion, this index will remain the same. But taking $k \to \infty$, shows that the π-adic completions are the same.

Approach 2: We have $\mathcal{O}_K = \mathcal{O} + p^k\mathcal{O}_K$ for all k since p^k is a power of π up to a unit. Since $[\mathcal{O}_K : \mathcal{O}]$ is a power of p, for k large enough we have $p^k\mathcal{O}_K \subset \mathcal{O}$. □

COROLLARY 170. *The discrmimant of* $\mathbb{Q}(\zeta_n)$ *is* $\pm p^{p^{r-1}(rp-r-1)}$.

PROOF. PS6 □

3.4.2. $K = \mathbb{Q}(\zeta_n)$**;** $n = \prod_{i=1}^s p_i^{r_i}$**.** Since $(X^n-1)' = nX^{n-1}$, the different divides n and hence only primes dividing n might ramify. Since the extension contains $\mathbb{Q}(\zeta_{p_i})$, we see that all the p_i do ramify.

Let $K_i = \mathbb{Q}\left(\zeta_{p_1^{r_1}}, \ldots, \zeta_{p_i^{r_i}}\right)$, $K = K_s$ ($K_0 = \mathbb{Q}$). Then for $1 \le i \le s$, p_i is unramified in K_{i-1}, so the ramification index of p_i in K_i/K_{i-1} is the same as in $K_i/\mathbb{Q}$ which is at least that of $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$, which is totally ramified at p. It follows that $[K_i : K_{i-1}] = \phi(p_i^{r_i})$ and hence that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ for all n.

THEOREM 171. $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

PROOF. Using the same induction scheme, suppose that $p^r \| n$ and let $n = p^r m$. Then the ring of integers of $M = \mathbb{Q}(\zeta_m)$ is $\mathcal{O}_M = \mathbb{Z}[\zeta_m]$. The rational prime p is unramified there, splitting as a product $p\mathcal{O}_M = \prod_j \mathfrak{p}_j$. The polynomial $\Phi_{p^r}(Y+1)$ has constant term p and we see $\Phi_{p^r}(Y+1)$ is Eisenstein over all the $\mathfrak{p}_j$ (in particular, irreducible). For each j we have a unique prime $\mathfrak{P}_j$ of $\mathcal{O}_K$ above $\mathfrak{p}_j$. Now $\pi | p$ so π is a product of the $\mathfrak{P}_j$. From $(\pi)^e = (p)$ we get that $\pi = \prod_j \mathfrak{P}_j$ and hence

that

$$\mathcal{O}_K/\pi\mathcal{O}_K = \prod_j \mathcal{O}_K/\mathfrak{P}_j = \prod_j \mathcal{O}_M/\mathfrak{p}_j = \mathcal{O}_M/p\mathcal{O}_M\,.$$

The argument now proceeds as before. □

PROPOSITION 172. $|D_K| = \left(\prod_{p^r \| n} p^{\frac{rp-r-1}{p-1}}\right)^{\phi(n)} = \frac{n^{\phi(n)}}{\prod_{p|n} p^{\frac{\phi(n)}{p-1}}}$.

PROOF. PS6 □

What about the sign?

LEMMA 173 (Brill). *Let K be a number field. Then the sign of D_K is $(-1)^s$ where s is the number of complex places.*

PROOF. Fix an integral basis $\{\omega_i\}_{i=1}^n$, $n = [K:\mathbb{Q}]$. Let $A_{ij} = \sigma_j(\omega_i)$ where $\{\sigma_j\}_{j=1}^n = \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$. Then $\bar{A}$ is obtained by exchanging σ_j with $\bar{\sigma}_j$, which involves exchanging s columns. It follows that $\det\bar{A} = (-1)^s \det A$. It follows that $D_K = (\det A)^2 = (-1)^s |\det A|^2$. □

3.5. Everywhere unramified extensions

LEMMA 174. *Let K be a field, $f \in K[x]$. Let $\Delta = \Delta(f)$. Then any splitting field of f contains $K(\sqrt{\Delta})$.*

PROOF. Let $\{\alpha_i\}_{i=1}^n$ be the roots of f in a splitting field L. Then $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)^2$ so $\sqrt{\Delta} = \prod_{i<j}(\alpha_i - \alpha_j) \in L$. □

LEMMA 175. *Let $f \in \mathbb{Z}[x]$ be monic. Let L be the splitting field of f. Suppose that $\Delta = \Delta(f)$ is squarefree and let $K = \mathbb{Q}(\sqrt{\Delta})$. Then L/K is everywhere unramified.*

CHAPTER 4

Geometry of Numbers

4.1. Lattices in $\mathbb{R}^n$

DEFINITION 176. A *lattice* $\Lambda < \mathbb{R}^n$ is discrete and cocompat subgroup, equivalently a free $\mathbb{Z}$-submodule generating by a basis.

LEMMA 177. *The two definitions are equivalent.*

COROLLARY 178. *(Of the proof of the Lemma) Let* $\Lambda = \oplus_i \mathbb{Z}\underline{v}_i$. *Then* $\mathcal{F} = \{\sum_{i=1}^n a_i \underline{v}_i \mid a_i \in [0,1]\}$ *is a bounded fundamental domain.*

DEFINITION 179. The covolume *of* Λ *is* $\mathrm{vol}(\mathcal{F}) = \det(\cdots \underline{v}_i \cdots) = \sqrt{\det\left(\left\langle \underline{v}_i, \underline{v}_j \right\rangle\right)_{i,j}}$.

PROPOSITION 180. $\#\{\underline{\lambda} \in \Lambda \cap B(\underline{0}, R)\} \sim \frac{\mathrm{vol}\, B(R)}{\mathrm{vol}(\mathcal{F})}$.

PROOF. The set $\bigcup_{\underline{\lambda} \in \Lambda \cap B(\underline{0},R)} (\mathcal{F} + \underline{\lambda})$ has volume $\#\{\underline{\lambda} \in \Lambda \cap B(\underline{0}, R)\} \mathrm{vol}(\mathcal{F})$ and its symmetric difference with $B(R)$ is contained in a spherical shell of radius R and constant thickness, hence has volume $O(R^{-1} \mathrm{vol}(B(R)))$. □

COROLLARY 181. $\mathrm{vol}(\mathcal{F})$ *is indpendent of the choice of* $\mathcal{F}$, *and will be denoted* $\mathrm{vol}(\mathbb{R}^n/\Lambda)$ *or* $\mathrm{covol}(\Lambda)$.

THEOREM 182 (Minkowski). *Let* $\Lambda < \mathbb{R}^n$ *be a lattice (discrete and cocompat subgroup, equivalently a free* $\mathbb{Z}$*-submodule generating by a basis). Let* $X \subset \mathbb{R}^n$ *be convex, bounded and symmetic aboud the origin. Suppose that* $\mathrm{vol}(X) \geq 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$. *Then there is* $\underline{0} \neq \underline{\lambda} \in X \cap \Lambda$.

PROOF. Suppose first that $\mathrm{vol}(X) > 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$. Assume by contradiction that $X \cap \Lambda = \{\underline{0}\}$. Then all translates of $\frac{1}{2}X$ are disjoint: if there are $\underline{x}, \underline{y} \in X$ and a non-zero $\underline{\lambda} \in \Lambda$ such that $\frac{1}{2}\underline{x} = \frac{1}{2}\underline{y} + \underline{\lambda}$ then $\underline{\lambda} = \frac{1}{2}\underline{x} + \frac{1}{2}(-\underline{y}) \in X$ by assumption. Now let $r = \mathrm{diam}(\mathcal{F})$. Then for all $R > 0$,

$$\bigcup_{\underline{\lambda} \in \Lambda \cap B(\underline{0},R)} \left(\frac{1}{2}X + \underline{\lambda}\right) \subset B(\underline{0}, R + r).$$

Since the union on the left is disjoint, we have

$$\#\{\underline{\lambda} \in \Lambda \cap B(\underline{0}, R)\} \frac{\mathrm{vol}(X)}{2^n} \leq \mathrm{vol}(B_{\mathbb{R}^n}(R + r)).$$

But $\#\{\underline{\lambda} \in \Lambda \cap B(\underline{0}, R)\} \sim \frac{\mathrm{vol}\, B(R)}{\mathrm{vol}(\mathbb{R}^n/\Lambda)}$ and $\mathrm{vol}(B(R + r)) \sim \mathrm{vol}(B(R))$. It follows that, as $R \to \infty$,

$$\frac{\mathrm{vol}(X)}{2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)} \mathrm{vol}(B(R)) \leq (1 + o(1)) \mathrm{vol}(B(R))$$

which is impossible.

Now suppose that $\mathrm{vol}(X) = 2^n \mathrm{vol}(\mathbb{R}^n/\Lambda)$. The set of lattice points in $N_1(X) = X + B(\underline{0},1)$ is discrete and compact, hence finite. In particular there is $\varepsilon > 0$ such that $\Lambda \cap X = \Lambda \cap N_\varepsilon(X) \neq \{\underline{0}\}$ and we are done. □

4.2. Discriminant bounds

LEMMA 183. *For a number field K the image of $\mathcal{O}_K$ in K_∞ is a lattice of covolume $2^{-s}\sqrt{|d_K|}$.*

REMARK 184. The lemma implicitely depends on the choice of inner product on K_∞ made in its proof.

PROOF. Let $T \subset \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$ be a set of representatives for the infinite places of K, say $T = T_{\mathbb{R}} \sqcup T_{\mathbb{C}}$, and let $\iota\colon K \to K_\infty = \prod_{\tau\in T} K_\tau$ be the embedding. We have seen (Theorem 122) that ι induces an isomorphism $K \otimes_{\mathbb{Q}} \mathbb{Q}_\infty \to K_\infty$, and in particular ι maps every $\mathbb{Q}$-basis of K to an $\mathbb{R}$-basis of K_∞. Since $\mathcal{O}_K$ is the $\mathbb{Z}$-span of an integral basis, it follows that its image is a lattice in K_∞. On K_∞ we take the Hermitian product $\langle (x_\tau),(y_\tau)\rangle = \sum_{i=1}^n x_\tau \bar{y}_\tau$. Then for $\omega_i, \omega_j \in \mathcal{O}_K$ we have $\langle \iota(\omega_i), \iota(\omega_j)\rangle = \sum_{\tau\in T} \tau(\omega_i)\bar{\tau}(\omega_j)$. □

THEOREM 185. *Let K be a number field. There are at most finitely many extensions of degree n having a given discriminant.*

PROOF. Can easily reduce to the case $K = \mathbb{Q}$ and counting extensions L such that $i \in L$ (the discriminant of $L(i)$ diffes by a constant). Thus we are counting totally complex L. Fix an infinite place v_0 and let

$$X = \left\{ (x_v) \in L_\infty \mid |\Im x_{v_0}| \leq C\sqrt{|D|},\, |\Re x_{v_0}| < 1,\, |x_v| < 1\, v \neq v_0 \right\}.$$

This is convex, symmetric about the origin, and has volume $C'\sqrt{D}$ where C' depends only on C, n. Choosing C depending on n we can ensure the volume is more than $2^n 2^{-n/2}\sqrt{|D|} \geq 2^n \mathrm{vol}(L_\infty/\mathcal{O}_L)$ and it follows that there is $\alpha \in \mathcal{O}_L \cap X$. Then from $N_{\mathbb{Q}}^L(\alpha) \geq 1$ it follows that $|\alpha|_{v_0} > 1$. Hence $\Im \alpha_{v_0} \neq 0$ and all conjugates of α are distinct, so $L = \mathbb{Q}(\alpha)$. But this means that the coefficients of the min poly are bounded in terms of D, α. □

THEOREM 186. $|d_K|^{1/2} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2}$.

PROOF. Let

$$X_t = \left\{ (x_v) \in K_\infty \mid \sum_{v|\infty} |x_v| \leq t \right\}.$$

A calculation shows $\mathrm{vol}(X_t) = 2^r(2\pi)^s \frac{t^n}{n!}$. For $t^n = n!\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ one has $\mathrm{vol}(X_t) = 2^n 2^{-s}\sqrt{|d_K|}$ and hence X_t contains a non-zero lattice point α. Since

$$1 \leq \left|N_{\mathbb{Q}}^K(\alpha)\right| = \prod_{v|\infty} |\alpha|_v \leq \frac{1}{n^n}\left(\sum_v |\alpha|_v\right)^n = \frac{t^n}{n^n}$$

the bound follows. □

COROLLARY 187 (Hermite). *There are finitely many extensions of bounded disciminant.*

-

COROLLARY 188 (Minkowski). *$\mathbb{Q}$ has no unramified extensions.*

PROOF. By Stirling's formula, $n! \leq \sqrt{2\pi n}\frac{n^n}{e^n}e^{\frac{1}{12n}}$, we have $|d_k| \geq \frac{1}{2\pi n}\left(\frac{\pi e^2}{4}\right)^n e^{-1/6n}$, which grows exponentially with n. For $n=2$ we see $|d_K|^{1/2} \geq \frac{\pi}{2} > 1$ so $d_K > 1$. □

4.3. Finiteness of the class group

A variant of the above proof will give:

THEOREM 189. *Let $C_K = \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$. Then every ideal class contains a representative of norm at most $C_K^{-1}|d_K|^{1/2}$.*

PROOF. Let $\mathfrak{a} \lhd \mathcal{O}_K$. Since $N\mathfrak{a} = [\mathcal{O}_K : \mathfrak{a}]$, the image of $\mathfrak{a}$ in K_∞ is a lattice of covolume $N\mathfrak{a}2^{-s}|d_K|^{1/2}$. As in the proof of Theorem 186 there is non-zero $\alpha \in \mathfrak{a}$ such $\sum_{v|\infty}|\alpha|_v \leq t$ where $t^n = n!\left(\frac{4}{\pi}\right)^s N\mathfrak{a}\sqrt{|d_K|}$, and again we have

$$\left|N_{\mathbb{Q}}^K(\alpha)\right| \leq \frac{t^n}{n^n} = C_K N\mathfrak{a}\,|d_K|^{1/2}\,.$$

Let $\mathfrak{b}$ be the ideal such that $(\alpha) = \mathfrak{a}\mathfrak{b}$. Then $\left|N_{\mathbb{Q}}^K(\alpha)\right| = N(\alpha) = N\mathfrak{a}N\mathfrak{b}$ so

$$N\mathfrak{b} \leq C_K\,|d_K|^{1/2}\,.$$

Note that $\mathfrak{b}$ is in the class of $\mathfrak{a}^{-1}$. □

4.4. The Unit Theorem

Let K be a number field. We restrict the injection $\mathcal{O}_K \hookrightarrow K_\infty$ to the units $\mathcal{O}_K^\times$, and take absolute values. We obtain a multiplicative map

$$\begin{aligned}\mathcal{O}_K^\times &\to \prod_{v|\infty}\mathbb{R}_{>0}^\times\\ \varepsilon &\mapsto (\|\varepsilon\|_v)_{v|\infty}\,.\end{aligned}$$

It is natural to compose with the logarithm function and obtain a map

$$\begin{aligned}\log\colon \mathcal{O}_K^\times &\to \mathbb{R}^{r+s}\\ \varepsilon &\mapsto (\log\|\varepsilon\|_v)_{v|\infty}\,.\end{aligned}$$

In view of the product formula $\prod_v\|\varepsilon\|_v = 1$, we have for $\varepsilon \in \mathcal{O}_K^\times$ that $\sum_{v|\infty}\log\|\varepsilon\|_v = 0$. Thus the image of $\mathcal{O}_K^\times$ lies in the obvious hyperplane.

LEMMA 190. *The image of $\mathcal{O}_K^\times$ in $\mathbb{R}^{r+s}$ is discrete.*

PROOF. Suppose $\|\varepsilon\|_v \leq 2$ for all v. This bounds the coefficients of the polynomial $\prod_{\sigma\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})}(x-\sigma(\alpha))$, which are rational integers. It follows that a neighbourhood of the identity in $\prod_v\mathbb{R}_{>0}^\times$ contains only finitely many elements of the image. □

COROLLARY 191. *The image of* log *is isomorphic to $\mathbb{Z}^t$ for some $t \leq r+s-1$.*

LEMMA 192 (Kronecker). *Let $\alpha \in \mathcal{O}_{\overline{\mathbb{Q}}}$ be non-zero and have all its conjugates in the unit disc. Then z is a root of unity.*

PROOF. Let $K=\mathbb{Q}(\alpha)$, $n=[K:\mathbb{Q}]$. Then for every $\beta\in OK$, $f_\beta(x)=\prod_{\sigma\in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})}(x-\sigma(\beta))\in \mathbb{Z}[x]$. If., furthermore, $|\sigma(\beta)|\leq 1$ for all σ then the coefficients of f_β are $O_n(1)$. It follows that there are only finitely many such β. But $\left\{\alpha^k\right\}_{k\geq 1}$ all have this property. By the pigeon-hole principle $\alpha^k=\alpha^\ell$ for some $k\neq l$ so α is a root of unity. □

COROLLARY 193. *The kernel of* log *consists of the roots of unity.*

It follows that $\mathcal{O}_K^\times\simeq \mu_n\times\mathbb{Z}^t$.

THEOREM 194. $\mathcal{O}_K^\times\simeq \mu_n\times\mathbb{Z}^{r+s-1}$.

EXAMPLE 195. Some cases

(1) $K=\mathbb{Q}$, $r=1$, $s=0$, $\mathbb{Z}^\times=\{\pm 1\}$.
(2) $K=\mathbb{Q}(\sqrt{-d})$, $r=0$, $s=1$, $\mathcal{O}_K^\times$ is the group of roots of unity (see PS1 for classification)
(3) $K=\mathbb{Q}(\sqrt{2})$. $r=2$, $s=0$, $\mathcal{O}_K^\times=\left\{\pm\left(1+\sqrt{2}\right)^n\right\}_{n\in\mathbb{Z}}$.
(4) $K=\mathbb{Q}(\sqrt{d})$, Pell's equation.
(5) $K=\mathbb{Q}(\sqrt[3]{2})$, $r=1$, $s=1$, $\mathcal{O}_K^\times=\left\{\pm\left(1-\sqrt[3]{2}\right)^n\right\}_{n\in\mathbb{Z}}$.

LEMMA 196. *For each $v_0|\infty$ there is $\varepsilon\in\mathcal{O}_K^\times$ such that $|\varepsilon|_v<1$ for all infinite $v\neq v_0$.*

PROOF. Fix $M>2^{-s}\sqrt{|d_K|}$. Identifying $K_\infty=\mathbb{R}^n$, consider the rectangle $X_\varepsilon=\left[M\varepsilon^{-(n-1)},M\varepsilon^{-(n-1)}\right]\times[-\varepsilon,\varepsilon]^{n-1}$ of volume 2^nM. For all ε we have $X_\varepsilon\cap\mathcal{O}_K\neq\{0\}$. The norm of $\alpha\in X_\varepsilon\cap\mathcal{O}_K$ is a rational integer, bounded in terms of M. In particular, there are at most finitely many norms occuring. There are finitely many ideals of a given norm, so the set of ideals (α) occuring is finite. In particular, there is an infinite sequence α_i such that $\alpha_i\in X_{\varepsilon_i}$ with $\varepsilon_i\to 0$ and (α_i) all equal. Then $\alpha_i\alpha_j^{-1}$ is a unit for all i. Furthermore, fixing j and letting $i\to\infty$ gives the desired unit. □

LEMMA 197. *Let $X=\left(x_{ij}\right)\in M_n(\mathbb{R})$ be a matrix with $x_{ij}<0$ for $i\neq j$, $x_{ii}>0$. Suppose that $X\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix}=\underline{0}$. Then* $\mathrm{rk}X\geq n-1$.

PROOF. Suppose the first $r=n-1$ columns are dependent, say $\sum_{j=1}^r c_jx_{ij}=0$ holds for all i where the c_j are not all zero. Wlog suppose that $c_1>0$ is largest in absolute value among the c_j. Then $x_{11}=-\sum_{j=2}^n x_{1,j}\geq-\sum_{j=2}^r x_{1,j}$. Multiplying by c_1 we find

$$c_1x_{11}\geq-\sum_{j=2}^r c_1x_{1,j}\geq-\sum_{j=2}^r c_jx_{1,j}\,,$$

with strict inequality unless the c_j are all equal. So unless the c_j are all equal we have

$$\sum_{j=1}^r c_jx_{1,j}>0\,,$$

a contradiction. But if all the c_j are equal and positive then

$$\sum_{j=1}^r c_jx_{n,j}>0\,,$$

a contradiction. □

DEFINITION 198. The *regulator* of K, denoted R_K, is the covolume of $\mathcal{O}_K^\times$ in the hyperplane $\mathbb{R}^{r+s-1}$. Equivalently,

$$R_K = |\det(\log|u_i|_v)|$$

where v runs over the infinite places and u_i runs over a basis for $\mathcal{O}_K^\times$ modulu the roots of unity.

CHAPTER 5

Analytic Theory: L-functions

5.1. Counting via complex analysis: Smooth cutoffs and Dirichlet Series

In this section we'll answer problems like: how many ideals (prime ideals) are there of norm at most X?

REMARK 199. Note that due to units, counting integers of norm at most X doesn't make sense. Counting integers modulu units amounts to counting principal ideals, and the techniques we'll discuss apply to that case as well.

5.1.1. Smooth cutoffs. Let $(a_n)_{n\geq 1}$ be any sequence. We'd like to estimate the summatory function $\sum_{n\leq x} a_n$ (say, count integers, or primes). We can express this in different ways:

$$\sum_{n\leq X} a_n = \sum_{n\geq 1} a_n \mathbb{1}_{[0,X]}(n) = \sum_{n\geq 1} a_n \mathbb{1}_{[0,1]}\left(\frac{n}{X}\right).$$

It is now natural to spectrally expand the cutoff function using, that is use Fourier analysis. But the *sharp cutoff* above is badly discountinuous, and hence behaves badly under Fourier expansion. This is the cause of much technical difficulties. Instead, we shall use *smooth cutoffs*, replacing $\mathbb{1}_{[0,1]}(x)$ with a smooth function, usually compactly supported. If $a_n \geq 0$ we can obtain lower and upper bounds by choosing $\varphi \equiv 1$ on $[0,1-h]$, supported in $[0,1+h]$, with h chosen in terms of X (to optimize the error term). In many cases one can simplify the analysis by *dyadic* counting: letting φ approximate the characteristic function of $[1,2]$ and then summing dyadically.

5.1.2. The Mellin transform.

DEFINITION 200. The *Mellin transform* of a function φ defined on $\mathbb{R}^\times_{>0} = (0,\infty)$ is $\tilde{\varphi}(s) = \int_0^\infty \varphi(x) x^s \frac{\mathrm{d}x}{x}$.

Note that $\frac{\mathrm{d}x}{x}$ is the Haar measure of $\mathbb{R}^\times_{>0}$.

REMARK 201. Under the isom $\exp\colon \mathbb{R}^+ \to \mathbb{R}^\times_{>0}$ this is the usual Fourier transform.

LEMMA 202. *If $\varphi \in C_c((0,\infty))$ then $\tilde{\varphi}(s)$ is entire. If $\varphi(s)$ decays at infinity at least at some polynomial rate then $\tilde{\varphi}$ is holomorhic in some right half-plane.*

FACT 203. *Let φ be reasonable. Then for σ large enough (for proof see later discussion of Fourier inversion),*

$$\varphi(x) = \frac{1}{2\pi i}\int_{(\sigma)} \tilde{\varphi}(s) x^{-s} \frac{\mathrm{d}s}{s}. \tag{5.1.1}$$

5.1.3. Counting. Let $\varphi(x)$ be a smooth bump function. We'd like to estimate the *smooth sum* $\sum_{n\geq 1} a_n \varphi\left(\frac{n}{X}\right)$. Using the Mellin inversion formula (5.1.1)

$$\begin{aligned}\sum_{n\geq 1} a_n \varphi\left(\frac{n}{X}\right) &= \frac{1}{2\pi i}\sum_{n\geq 1} a_n \int_{(\sigma)} \left(\frac{n}{X}\right)^{-s} \tilde{\varphi}(s)\frac{\mathrm{d}s}{s} \\ &= \frac{1}{2\pi i}\int_{(\sigma)} D(s)\tilde{\varphi}(s)X^s\frac{\mathrm{d}s}{s}.\end{aligned}$$

where $D(s) = \sum_{n\geq 1} a_n n^{-s}$ is the associated Dirichlet series. We can justify the exchange of summation and integration when σ is large enough so that $D(s)$ converges absolutely and $\tilde{\varphi}(s)$ decays by the smoothness of φ. Now suppose that $\tilde{\varphi}(s)$ and $D(s)$ continue meromorphically to the left. We can then shift the contour, gaining since the term X^s (with constant absolute value X^σ) will become smaller. We can do this as long as $D(s)$ *grows polynomially in vertical strips.* When we do this we will pick up contribution from poles. The conclusion is:

$$\sum_{n\geq 1} a_n \varphi\left(\frac{n}{X}\right) = \sum_{\sigma'<\Re\rho<\sigma} X^\rho \operatorname{Res}_{s=\rho}\left(D(s)\tilde{\varphi}(s)\frac{1}{s}\right) + \frac{1}{2\pi i}\int_{(\sigma')} D(s)\tilde{\varphi}(s)X^s\frac{\mathrm{d}s}{s}.$$

Taking φ compactly supported away from 0,$\tilde{\varphi}$ is entire (and decays in the vertical direction) and we can write this as

$$\sum_{n\geq 1} a_n \varphi\left(\frac{n}{X}\right) = \sum_{\sigma'<\Re\rho<\sigma} \tilde{\varphi}(\rho)X^\rho \operatorname{Res}_{s=\rho}\left(D(s)\frac{1}{s}\right) + O\left(X^{\sigma'}\right)$$

5.1.4. Example: Counting integers. Consider first the case where $a_n = 1$ so that $\sum_{n\leq x} a_n$ is simply $[x]$. Then $D(s) = \sum_{n\geq 1} n^{-s} = \zeta(s)$ continues to $\mathbb{C}$ with only a simple pole at $s = 1$ (where the residue is 1). We get

$$\sum_{n=1}^{\infty} \varphi\left(\frac{n}{X}\right) = \tilde{\varphi}(1) - \tilde{\varphi}(0)\zeta(0) + \text{small}.$$

Note that $\tilde{\varphi}(1) = \int_0^\infty \varphi(x)\,\mathrm{d}x$, as expected.

5.1.5. Example: Counting integers mod 4. Let $\chi_4(n) = \begin{cases} 1 & n\equiv 1\,(4) \\ -1 & n\equiv -1\,(4) \\ 0 & 2|n \end{cases}$, $I_4(n) = \begin{cases} 1 & n \text{ odd} \\ 0 & n \text{ even} \end{cases}$.

Then

$$\begin{aligned}\frac{I_4+\chi_4}{2}(n) &= \begin{cases} 1 & n\equiv 1\,(4) \\ 0 & \text{otherwise} \end{cases} \\ \frac{I_4-\chi_4}{2}(n) &= \begin{cases} 1 & n\equiv -1\,(4) \\ 0 & \text{otherwise} \end{cases}.\end{aligned}$$

What is $\sum_{n\geq 1} I_4(n)n^{-s}$? For this note that

$$\sum_{\text{even } n\geq 1} n^{-s} = \sum_{m\geq 1} (2m)^{-s} = 2^{-s}\zeta(s)$$

so that

$$\sum_{n=1}^{\infty} I_4(n)n^{-s} = \left(1-2^{-s}\right)\zeta(s)\,.$$

It follows that the counts we want can be done using the Dirichlet series

$$D(s) = \frac{1}{2}\left(\left(1-2^{-s}\right)\zeta(s) \pm L(s;\chi_4)\right)$$

where $L(s;\chi_4) = \sum_{n\geq 1}\chi_4(n)n^{-s}$ is Dirichlet's L-function. The latter function continues to an entire function (no poles!) so we find

$$\sum_{n\equiv\pm 1\,(4)} \varphi\left(\frac{n}{X}\right) = \frac{1}{2}\left(\frac{1}{2}\tilde{\varphi}(1)X \pm \tilde{\varphi}(0)L(0;\chi_4)\right) + \text{small}$$

(note that $1-2^{-0}=0$). In other words, about a quarter of all integers are in the relevant residue class.

5.1.6. Counting primes: Riemann's Zeta function and Dirichlet's L-function. This is the key idea of Riemann's 1859 memoir. Start with Euler's observation that (in the region of absolute convergence)

$$\zeta(s) = \prod_p \left(1-p^{-s}\right)^{-1}$$

(note that the pole at $s=1$ already shows there are infinitely many primes). It follows that

$$-\frac{\zeta'}{\zeta}(s) = \sum_n \Lambda(n)n^{-s}$$

where $\Lambda(n) = \begin{cases}\log p & n = p^e \\ 0 & \text{otherwise}\end{cases}$ is the von Mangoldt function. The continuation of the Riemann zetafunction applies to its logarithmic derivative again. The poles of the logarithmic derivatives are at the zeros and poles of the function, and the residue is the order of zero/pole, so we get the *explicit formula*

$$\sum_{n=1}^{\infty}\Lambda(n)\varphi\left(\frac{n}{X}\right) = \tilde{\varphi}(1)X - \sum_{\zeta(\rho)=0}\tilde{\varphi}(\rho)\frac{X^{\rho}}{\rho} + \text{small}\,.$$

Problem of course is bounding contribution from t1he zeroes. Note that there are infinitely many, so need to be careful, but the vertical decay of $\tilde{\varphi}$ ensures absolute convergence. On the *Riemann hypothesis* that $\Re(\rho) = \frac{1}{2}$ we get $\sum_{p\leq x}\log p = x + O(\sqrt{x}\log x)$.

5.1.7. Primes congruent to ± 1 mod 4. A *Dirichlet Series* is a series of the form $D(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. These are generating series for arithmetical functions, where multiplication of series corresponds to Dirichlet convolution of arithmetical functions.

LEMMA 204. *$D(s)$ converges somewhere iff $\{a_n\}$ grows at most polynomially. In that case the region of absolute convergence is a half-plane (either open or closed). The domain of convergence is an open half-plane, with the convergence uniform in any properly contained half-plane.*

Similarly, note that $\chi_4(mn) = \chi_4(m)\chi_4(n)$ and that $|\chi_4(n)| \leq 1$ for all n, from which it is easy to show that $L(s;\chi_4)$ converges absolutely for $\Re(s) > 1$ and that in that region we have the absolutely convergent Euler product representation

$$L(s;\chi_4) = \prod_p \left(1 - \chi_4(p)p^{-s}\right)^{-1}$$

and hence

,

$$-\frac{L'(s;\chi_4)}{L(s;\chi_4)} = \sum_{n=1}^{\infty} \Lambda(n)\chi_4(n)n^{-s}$$

so that

$$\sum_{n=1}^{\infty} \Lambda(n)\varphi\left(\frac{n}{X}\right) = \sum_{\rho} \mathrm{Res}_{s=\rho}\left[-\frac{\zeta'(s)}{\zeta(s)}\right]\frac{\tilde{\varphi}(\rho)}{\rho}X^{\rho} - \frac{\zeta'(0)}{\zeta(0)}\tilde{\varphi}(0)$$

and

$$\begin{aligned}\sum_{n\equiv\pm 1\,(4)} \Lambda(n)\varphi\left(\frac{n}{X}\right) &= \frac{1}{2}\left[\sum_{\rho} \mathrm{Res}_{s=\rho}\left[-\frac{\zeta'(s)}{\zeta(s)}\right]\frac{\tilde{\varphi}(\rho)}{\rho}X^{\rho} - \frac{\zeta'(0)}{\zeta(0)}\tilde{\varphi}(0)\right] \\ &\pm \frac{1}{2}\left[\sum_{\rho} \mathrm{Res}_{s=\rho}\left[-\frac{L'(s;\chi_4)}{L(s;\chi_4)}\right]\frac{\tilde{\varphi}(\rho)}{\rho}X^{\rho} - \frac{L'(0;\chi_4)}{L(0;\chi_4)}\tilde{\varphi}(0)\right].\end{aligned}$$

Using the argument principle as before gives

$$\sum_{n\equiv\pm 1\,(4)} \Lambda(n)\varphi\left(\frac{n}{X}\right) = \frac{1}{2}\tilde{\varphi}(1)X - \frac{1}{2}\sum_{\zeta(\rho)=0}\frac{\tilde{\varphi}(\rho)}{\rho}X^{\rho} \mp \frac{1}{2}\sum_{L(\rho;\chi_4)=0}\frac{\tilde{\varphi}(\rho)}{\rho}X^{\rho} - \frac{1}{2}\frac{\zeta'(0)}{\zeta(0)}\tilde{\varphi}(0) \mp \frac{1}{2}\frac{L'(0;\chi_4)}{L(0;\chi_4)}\tilde{\varphi}(0).$$

By estimating the terms invovling the roots (using the decay of $\tilde{\varphi}$) it is possible to deduce

THEOREM 205 (PNT; de la Valee-Pussin, Hadamard). $\sum_{n=1}^{\infty}\Lambda(n)\varphi\left(\frac{n}{X}\right) \sim \tilde{\varphi}(1)X$.

THEOREM 206 (PNT in AP; de la Valee-Pussin, Hadamard). *If* $(a,q) = 1$ *then* $\sum_{n\equiv a\,(q)}\Lambda(n)\varphi\left(\frac{n}{X}\right) \sim \frac{1}{\phi(q)}\tilde{\varphi}(1)X$.

5.2. Fourier Analysis and Poisson Sum

5.2.1. Analysis on $\mathbb{R}/\mathbb{Z}$. For $f \in C^{\infty}(\mathbb{R}/\mathbb{Z})$ and $k \in \mathbb{Z}$ let

$$\hat{f}(k) = \int_{\mathbb{R}/\mathbb{Z}} f(x)e^{-2\pi ikx}\,\mathrm{d}x.$$

Then (integration by parts) $\hat{f}(k)$ decay faster than any polynomial and it follows that

$$\sum_{k\in\mathbb{Z}} \hat{f}(k)e^{2\pi ikx}$$

and all its derivatives converge uniformly. In fact we have the *Fourier Inversion Formula*

$$f(x) = \sum_{k\in\mathbb{Z}} \hat{f}(k)e^{2\pi ikx}$$

with convergence in $C^{\infty}(\mathbb{R}/\mathbb{Z})$.

Letting $e(z) = e^{2\pi iz}$ denote the standard characters, we note that the Fourier variables k actually vary in the *dual lattice* $\mathbb{Z}^*$. For example, if f is defined on $r\mathbb{Z}$ then the Fourier variables vary in $k \in \frac{1}{r}\mathbb{Z}$.

5.2.2. Analysis on $\mathbb{R}^n/\Lambda$. Now let $\Lambda < \mathbb{R}^n$ be a lattice, and let $\Lambda^* = \left\{k \in (\mathbb{R}^n)^* \mid \forall x \in \Lambda : k \cdot x \in \mathbb{Z}\right\}$ be the dual lattice. Again for $f \in C^\infty(\mathbb{R}^n/\Lambda)$ we define the Fourier coefficients by

$$\hat{f}(k) = \frac{1}{\operatorname{vol}(\mathbb{R}^n/\Lambda)} \int_{\mathbb{R}^n/\Lambda} f(x) e(-kx)\,\mathrm{d}x$$

and then again the coefficients decay faster than any polynomial and we have Fourier inversion as

$$f(x) = \sum_{k \in \Lambda^*} \hat{f}(k) e(kx).$$

One proof is to handle $\mathbb{R}^n/\mathbb{Z}^n = (\mathbb{R}/\mathbb{Z})^n$ using the density of $(C^\infty(\mathbb{R}/\mathbb{Z})^{\otimes n}$ in $C^\infty(\mathbb{R}^n/\mathbb{Z}^n)$ and then apply an automorphism to get the theory for a geenral lattice.

5.2.3. Poisson sum. Call $f \in C^\infty(\mathbb{R}^n)$ a *Schwartz function* if f and all its derivatives decay faster than any power law. Write $\mathcal{S}(\mathbb{R}^n)$ for the set of such functions. For $f \in \mathcal{S}(\mathbb{R}^n)$ and $k \in (\mathbb{R}^n)^*$ set

$$\hat{f}(k) = \int_{\mathbb{R}^n} f(x) e(-kx)\,\mathrm{d}x.$$

Smoothness of f implies (via integrating by parts) that the $\hat{f}$ decay. Decay of f implies (by differentiating under the integral sign) that $\hat{f}$ are differentiable. Combining the arguments shows that $\hat{f} \in \mathcal{S}\left((\mathbb{R}^n)^*\right)$. In fact Fourier inversion holds here but we won't need this.

For $\varphi \in \mathcal{S}(\mathbb{R}^n)$ and a lattice $\Lambda < \mathbb{R}^n$ set $\Phi(x) = \sum_{\lambda \in \Lambda} \varphi(x+\lambda)$. This series (and all its derivatives) converges uniformly so $\Phi \in C^\infty(\mathbb{R}^n/\Lambda)$. We may therefore apply Fourier inversion to get

$$\Phi(x) = \sum_{k \in \Lambda^*} \hat{\Phi}(k) e(kx).$$

Now set $x = 0$ to get

$$\sum_{x \in \Lambda} \varphi(x) = \sum_{k \in \Lambda^*} \hat{\Phi}(k).$$

To compute the terms on the right, let $\mathcal{F} \subset \mathbb{R}^n$ be a compact fundamental domain for Λ. Then

$$\begin{aligned}
\hat{\Phi}(k) &= \frac{1}{\operatorname{vol}(\mathbb{R}^n/\Lambda)} \int_{\mathbb{R}^n/\Lambda} \Phi(x) e(-kx)\,\mathrm{d}x \\
&= \frac{1}{\operatorname{vol}(\mathbb{R}^n/\Lambda)} \int_{\mathcal{F}} \left(\sum_{\lambda \in \Lambda} \varphi(x+\lambda) \right) e(-kx)\,\mathrm{d}x \\
&= \frac{1}{\operatorname{vol}(\mathbb{R}^n/\Lambda)} \int_{\mathcal{F}} \left(\sum_{\lambda \in \Lambda} \varphi(x+\lambda) e\left(-k(x+\lambda)\right) \right) \mathrm{d}x
\end{aligned}$$

since $k \in \Lambda^*$. We now exchange summation and integration (justified by putting absolute values and redoing the calculation below) so

$$\begin{aligned}\hat{\Phi}(k) &= \frac{1}{\mathrm{vol}\,(\mathbb{R}^n/\Lambda)} \sum_{\lambda\in\Lambda} \int_{\mathcal{F}} \varphi(x+\lambda) e\,(-k(x+\lambda))\,\mathrm{d}x \\ &= \frac{1}{\mathrm{vol}\,(\mathbb{R}^n/\Lambda)} \sum_{\lambda\in\Lambda} \int_{\mathcal{F}+\lambda} \varphi(x) e\,(-kx)\,\mathrm{d}x \\ &= \frac{1}{\mathrm{vol}\,(\mathbb{R}^n/\Lambda)} \int_{\mathbb{R}^n} \varphi(x) e\,(-kx)\,\mathrm{d}x \\ &= \frac{1}{\mathrm{vol}\,(\mathbb{R}^n/\Lambda)} \hat{\varphi}(k)\,.\end{aligned}$$

We have proved

PROPOSITION 207 (Poisson Summation Formua). *For $\varphi \in \mathcal{S}(\mathbb{R}^n)$ and a lattice $\Lambda < \mathbb{R}^n$,*

$$\sum_{x\in\Lambda} \varphi(x) = \frac{1}{\mathrm{vol}\,(\mathbb{R}^n/\Lambda)} \sum_{k\in\Lambda^*} \hat{\varphi}(k)\,.$$

5.3. Analytical continuation of the Riemann zetafunction

For $\varphi(x) \in \mathcal{S}(\mathbb{R})$ and $r > 0$ set $\varphi(r\mathbb{Z}) \stackrel{\mathrm{def}}{=} \sum_{n\neq 0} \varphi(rn) = (\sum_{x\in r\mathbb{Z}} \varphi(x)) - \varphi(0)$. Now define the *zeta-integral*

$$Z(\varphi; s) = \int_0^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r}\,.$$

REMARK 208. Note that we may assume wlog that $\Phi(r)$ is even, so we may consider this an integral on $\mathbb{R}^\times/\mathbb{Z}^\times$.

LEMMA 209. *The sum defining $\varphi(r\mathbb{Z})$ converges locally uniformly absolutely (in particular this function is continuous), decays faster than any polynomial as $r \to \infty$ and satisfies $\varphi(r\mathbb{Z}) = O(r^{-1})$.*

PROOF. Let N be even, and let C be such that$|\varphi(x)| \leq \frac{C}{1+x^N}$ for all $x \in \mathbb{R}$. Then

$$\begin{aligned}\left|\sum_{n=1}^\infty \varphi(rn)\right| &\leq \int_0^\infty \frac{C}{1+(rx)^N}\,\mathrm{d}x \\ &= \left(\int_0^\infty \frac{C\,\mathrm{d}x}{1+x^N}\right) r^{-N}\,.\end{aligned}$$

It follows that the sum conveges absolutely for $|r| \geq r_0$ and that it decays faster than any polynomial. For r small break the sum up into $|n| \leq r^{-1}$ and $|n| > r^{-1}$. □

PROPOSITION 210. *The zeta-integrals converge uniformly absolutely for $\Re(s) \geq \sigma > 1$.*

PROOF. We have $\int_0^1 |\varphi(r\mathbb{Z}) r^s| \frac{dr}{r} \ll \int_0^1 r^{-1} r^\sigma \frac{dr}{r} = \sigma - 1$ since $\sigma - 2 > -1$, and $\int_1^\infty |\varphi(r\mathbb{Z}) r^s| \frac{dr}{r} \ll \int_1^\infty r^{-N} r^\sigma \frac{dr}{r} = N - \sigma$ if $N > \sigma$. □

Now for $\Re s > 1$ we have:

$$\begin{aligned} Z(\varphi;s) &= \int_0^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r} \\ & \int_1^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r} + \int_0^1 \left[\sum_{n\in\mathbb{Z}} \varphi(rn)\right] r^s \frac{dr}{r} - \varphi(0)\int_0^1 r^s \frac{dr}{r} \\ & \int_1^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r} - \frac{\varphi(0)}{s} + \int_0^1 \left[\sum_{n\in\mathbb{Z}} \hat{\varphi}(r^{-1}n)\right] r^s \frac{dr}{r} \\ & \int_1^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r} - \frac{\varphi(0)}{s} + \int_1^\infty \left[\sum_{n\in\mathbb{Z}} \hat{\varphi}(rn)\right] r^{1-s} \frac{dr}{r} \\ & \int_1^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r} - \frac{\varphi(0)}{s} + \int_1^\infty \hat{\varphi}(r\mathbb{Z}) r^{1-s} \frac{dr}{r} - \frac{\hat{\varphi}(0)}{1-s}. \end{aligned}$$

The proof of the Proposition shows that $\int_1^\infty \varphi(r\mathbb{Z}) r^s \frac{dr}{r}$ defines an entire function. We have thus shown:

PROPOSITION 211. *For all $\varphi \in \mathcal{S}(\mathbb{R})$, $Z(\varphi;s)$ extends to a meromorphic function with poles at most at $s = 0, 1$ and satisfies the* functional equation

$$Z(\varphi;s) = Z(\hat{\varphi};1-s).$$

Suppose now that φ is even. Then for $\Re(s) > 1$,

$$\begin{aligned} Z(\varphi;s) &= 2\int_0^\infty \left[\sum_{n=1}^\infty \varphi(rn)\right] r^s \frac{dr}{r} \\ &= 2\sum_{n=1}^\infty \int_0^\infty \varphi(rn) r^s \frac{dr}{r} \\ &= 2\left(\int_0^\infty \varphi(r) r^s \frac{dr}{r}\right)\left[\sum_{n=1}^\infty n^{-s}\right]. \end{aligned}$$

Choose first $\varphi \in C_c^\infty\left(\mathbb{R}_{>0}^\times\right)$. Then $\int_0^\infty \varphi(r) r^s \frac{dr}{r}$ converges for all s and hence defines an entire function. It follows that

$$\sum_{n=1}^\infty n^{-s} = \frac{Z(\varphi;s)}{2\int_0^\infty \varphi(r) r^s \frac{dr}{r}}$$

gives a meromorphic continuation of $\zeta(s)$.

Next, make the specific choice $\varphi(x) = e^{-\pi x^2}$. In this case $2\int_0^\infty \varphi(r) r^s \frac{dr}{r} = 2\int_0^\infty e^{-\pi r^2} r^s \frac{dr}{r} = \int_0^\infty e^{-t} \left(\frac{t}{\pi}\right)^{\frac{s-1}{2}} \pi^{-\frac{1}{2}} \frac{dt}{\sqrt{t}} = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$. Writing $\xi(s) = Z(e^{-\pi x^2};s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ we find that $\xi(s)$ extends to an entire function with poles at $s = 0, 1$ where the residues are $-1, 1$ respectively. Since $\hat{\varphi} = \varphi$ we also obtain the *functional equation*

$$\xi(s) = \xi(1-s).$$

Finally, since $\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$ is everywhere non-vanishing and has a simple pole at $s = 0$, $\zeta(s)$ has a pole at $s = 1$. From the formula above we see that $Z(\varphi;s)$ is *bounded in vertical strips* (away from the poles), so in particular this holds for the completed zetafunction $\xi(s)$.

5.4. The Dedekind Zetafunction

5.4.1. Preliminaries. Fix a number field K of degree $n = [K : \mathbb{Q}]$. Suppose K has r_1 (resp. r_2) real (resp. complex) places so that $r_1 + 2r_2 = n$.

Let $K_\infty = \bigoplus_{v|\infty} K_v$ be the archimedean completion in which $\mathcal{O}_K$ is a lattice. Write $\mathcal{C}_{K/\mathbb{Q}}$ for the complementary module, d_K for the absolute discriminant and write V for the covolume $\mathrm{vol}(K_\infty/\mathcal{O}_K) = 2^{-r_2}\sqrt{|d_K|}$ as computed in Lemma 183.

Let $K_\infty^1 = \{r \in K_\infty^\times \mid \|r\| = 1\}$, and note that K_∞^1 contains the image of the units $\mathcal{O}_K^\times$. Recalling the map $\log\colon K_\infty^\times \to \mathbb{R}^{r_1+r_2}$ from Section 4.4 we showed there that $\log\left(\mathcal{O}_K^\times\right)$ is a lattice hyperplane $\log\left(K_\infty^1\right)$, and defined the *regulator* R_K to be the covolume $\mathrm{vol}\left(\log\left(K_\infty^1\right)/\log\left(\mathcal{O}_K^\times\right)\right)$. Since $\mathrm{Ker}\log = \left\{(r_v)_{v|\infty} \mid \forall v : |r_v| = 1\right\} \simeq \{\pm 1\}^{r_1}(\mathbb{R}/2\pi\mathbb{Z})^{r_2}$ is compact we see that $K_\infty^1/\mathcal{O}_K^\times$ is compact as well.

We now record two volume computations we shall need later:

LEMMA 212. *Let $\mathfrak{c} \subset K$ be a fractional ideal. Then* $\mathrm{vol}(K_\infty/\mathfrak{c}) = N\mathfrak{c}\cdot V = 2^{-r_2}N\mathfrak{c}\sqrt{|d_K|}$.

LEMMA 213. $\mathrm{vol}\left(K_\infty^1/\mathcal{O}_K\right) = \frac{1}{w}2^{r_1}(2\pi)^{r_2}R_K$ *where* $w = \#\left(\mathcal{O}_K^\times\right)_{tors}$ *is the numebr of roots of unity in K.*

PROOF. We verified in Corollary 193 that $\mathrm{Ker}\log \cap \mathcal{O}_K^\times$ is exactly the group of roots of unity. □

5.4.2. Absolute convergence.

DEFINITION 214. The *Dedekind zetafunction of K* is

$$\zeta_K(s) = \sum_{\mathfrak{a}\lhd\mathcal{O}_K} (N\mathfrak{a})^{-s}.$$

LEMMA 215 (Euler product). *The series above converges absolutely in the half-plane $\Re(s) > 1$ where we also have*

$$\zeta_K(s) = \prod_{\mathfrak{p}\ prime} \left(1 - N\mathfrak{p}^{-s}\right)^{-1}.$$

PROOF. Taking the logarithm, we need to study

$$\sum_{v<\infty}\sum_{m=1}^{\infty}\frac{1}{m}q_v^{-ms}.$$

Now for each rational prime p there are at most $n = [K : \mathbb{Q}]$ primes $\mathfrak{p}|p$ and these have $q_v = p^{f_v}$. It follows that

$$\left|\sum_{v<\infty}\sum_{m=1}^{\infty}\frac{1}{m}q_v^{-ms}\right| \leq n\sum_{p<\infty}\sum_{m=1}^{\infty}\frac{1}{m}p^{-m\sigma}$$

which converges for $\sigma > 1$. We conclude that $\sum_{v<\infty}\sum_{m=1}^{\infty}\frac{1}{m}q_v^{-ms}$ converges absoltuely for $\Re(s) > 1$; exponentiating it follows that the Euler product converges for $\Re(s) > 1$ and using unique factorization it follows that the Dedekind zetarfunction converges as well.

More generally, let $\chi\colon \mathrm{Cl}(K) \to \mathbb{C}^\times$be a character of the class group. We will then consider the L-function

$$L(s;\chi) = \sum_{\mathfrak{a}\lhd\mathcal{O}_K}\chi(\mathfrak{a})(N\mathfrak{a})^{-s}$$

which by the same reasoning converges absolutely in $\Re(s) > 1$ and admits the Euler product

$$L(s;\chi) = \prod_{\mathfrak{p}<\infty} \left(1 - \chi(\mathfrak{p}) N\mathfrak{p}^{-s}\right)^{-1}.$$

□

5.4.3. Analytical continuation: single ideal class. For an ideal class $\mathcal{I}$ let

$$\zeta_K(s;\mathcal{I}) = \sum_{\mathfrak{a}\in\mathcal{C}} N\mathfrak{a}^{-s}.$$

Fix a representative $\mathfrak{c} \lhd \mathcal{O}_K$ of the inverse class. Then for each $\mathfrak{a} \in \mathcal{C}$, $\mathfrak{a}\mathfrak{c}$ is a principal ideal represented by an element $\alpha \in \mathfrak{c}$, and the converse also holds modulu units. It follows that

$$\zeta_K(s;\mathcal{I}) = \sum_{\alpha\in(\mathfrak{c}\setminus\{0\})/\mathcal{O}_K^\times} \left(N\left(\alpha\mathfrak{c}^{-1}\right)\right)^{-s}$$

or equivalently

$$N\mathfrak{c}^{-s}\zeta_K(s;\mathcal{I}) = \sum_{\alpha\in(\mathfrak{c}\setminus\{0\})/\mathcal{O}_K^\times} (N\alpha)^{-s}.$$

Now let $\varphi \in \mathcal{S}(K_\infty)$ be a test function. For $r \in K_\infty^\times$ and a fractional ideal $\mathfrak{c}$ we set

$$\varphi(r\mathfrak{c}) = \sum_{\alpha\in\mathfrak{c}} \varphi(r\alpha)$$

(multiplication in K_∞!). Note that for any $\varepsilon \in \mathcal{O}_K^\times$ we have $\varphi(\varepsilon r\mathfrak{c}) = \varphi\left(r(\varepsilon\mathfrak{c})\right) = \varphi(r\mathfrak{c})$. It follows that the function $r \mapsto \varphi(r\mathfrak{c})$ is in fact defined on $\mathcal{O}_K^\times\backslash K_\infty^\times$ and we set

$$Z(s;\mathfrak{c};\varphi) = \int_{\mathcal{O}_K^\times\backslash K_\infty^\times} \varphi\left(r\mathfrak{c}\right) \|r\|^s d^\times r.$$

Note that replacing $\varphi(x)$ with $\varphi(\varepsilon x)$ with $|\varepsilon_v|_v = 1$ for all v does not change the integral, so after averaging we may assume that $\varphi(x)$ only depends on the vector of absolute values $(|x_v|_v)_{v|\infty}$.

DEFINITION 216. For $\varphi \in \mathcal{S}(K_\infty)$ and $s \in \mathbb{C}$ write $\tilde{\varphi}(s) = \int_{K_\infty^\times} \varphi(r) \|r\|^s d^\times r$.

Note that this converges if $\Re(s) > 1$ (then $\|r\|^s d^\times r = \|r\|^{s-1} \mathrm{d}r$ and the difference between $K_\infty^\times$ and K_∞ is a set of measure zero) and that for $\varphi \in C_c^\infty(K_\infty^\times)$ the function $\tilde{\varphi}(s)$ is entire.

LEMMA 217. *The zeta-integral above converges absolutely for $\Re(s) > 1$ where we have*

$$Z(s;\mathfrak{c};\varphi) = (N\mathfrak{c})^{-s}\, \zeta\left(s;\mathcal{I}\right) \tilde{\varphi}(s).$$

PROOF. It suffices to consider the case of φ real-valued and non-negative and s positive and real, where we may change the order of summation and integration to get:

$$\begin{aligned} Z(s;\mathfrak{c};\varphi) &= \int_{\mathcal{O}_K^\times\backslash K_\infty^\times} \varphi(r\mathfrak{c})\,\|r\|^s\,d^\times r \\ &= \int_{\mathcal{O}_K^\times\backslash K_\infty^\times} \sum_{\alpha\in\mathfrak{c}\backslash\{0\}} \varphi(r\alpha)\,\|r\|^s\,d^\times r \\ &= \sum_{\alpha\in\mathfrak{c}\backslash\{0\}} \int_{\mathcal{O}_K^\times\backslash K_\infty^\times} \varphi(r\alpha)\,\|r\|^s\,d^\times r \\ &= \sum_{\alpha\in\mathfrak{c}\backslash\{0\}/\mathcal{O}_K^\times} \int_{K_\infty^\times} \varphi(r\alpha)\,\|r\|^s\,d^\times r \\ &= \sum_{\alpha\in\mathfrak{c}\backslash\{0\}/\mathcal{O}_K^\times} |N\alpha|^{-s} \int_{K_\infty^\times} \varphi(r\alpha)\,\|r\alpha\|^s\,d^\times r \\ &= (N\mathfrak{c})^{-s}\,\zeta(s;\mathcal{I}) \int_{K_\infty^\times} \varphi(r)\,\|r\|^s\,d^\times r. \end{aligned}$$

Finally, the set of non-invertible points in K_∞ has measure zero, so we have

$$\int_{K_\infty^\times} \varphi(r)\,\|r\|^s\,d^\times r = \int_{K_\infty} \varphi(r)\,\|r\|^{s-1}\,\mathrm{d}r$$

which converges absoltuely for $\Re(s) > 1$. □

For the analytical continuation we investigate the domain of integration with more care. We have $\mathcal{O}_K^\times\backslash K_\infty^\times \simeq \left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\times\mathbb{R}_{>0}$ so the only asymptotics for $\varphi(r\mathfrak{c})$ are in terms of $\|r\|$, with rapid decay as $\|r\|\to\infty$. Accordingly we split the domain according to whether $\|r\|$ is at least 1 or at most 1. The rapid decay immediately gives:

LEMMA 218. *Let $A = \{x\in K_\infty^\times \mid \|x\|\geq 1\}/\mathcal{O}_K^\times \subset K_\infty^\times/\mathcal{O}_K^\times$. Then the partial integral*

$$\int_A \varphi(r\mathfrak{c})\,\|r\|^s\,d^\times r$$

converges absolutely for all $s\in\mathbb{C}$, where it defines an entire function which si boudned in vertical strips.

PROPOSITION 219. *In the domain of absolute convergence we have*

$$\begin{aligned} Z(s;\mathfrak{c};\varphi) &= \int_A \varphi(r\mathfrak{c})\,\|r\|^s\,d^\times r + \frac{1}{N\mathfrak{c}\cdot V}\int_A \hat{\varphi}\left(r\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\|r\|^{1-s}\,d^\times r \\ &\quad -\varphi(0)\,\mathrm{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{s} - \frac{\hat{\varphi}(0)}{N\mathfrak{c}\cdot V}\,\mathrm{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{1-s}. \end{aligned}$$

COROLLARY 220. *$Z(s;\mathfrak{c};\varphi)$ extends to a meromorphic function on $\mathbb{C}$ bounded in vertical strips, having at most simple poles at $s=0,1$ with residues as determined above and (for even φ) satisfies the functional equation*

$$Z(s;\mathfrak{c};\varphi) = Z\left(s;\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}};\hat{\varphi}\right)$$

PROOF. All the claims except for the functional equation are clear. For the last we apply the Proposition to the right-hand-side to get

$$\begin{aligned} Z(1-s;\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}};\hat{\varphi}) &= \int_A \hat{\varphi}\left(r\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\|r\|^{1-s}d^\times r + \frac{1}{N\left(\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\cdot V}\int_A \varphi\left(r\mathfrak{c}\mathcal{C}_{K/\mathbb{Q}}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\|r\|^{s}d^\times r \\ &\quad -\hat{\varphi}(0)\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{1-s} - \frac{\varphi(0)}{N\left(\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\cdot V}\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{s}. \end{aligned}$$

Noting that $N\mathfrak{c}^{-1} = \frac{1}{N\mathfrak{c}}$ and that $\frac{1}{N(\mathcal{C}_{K/\mathbb{Q}})} = N(\mathcal{D}_{K/\mathbb{Q}}) = |d_K| = 2^{2s_2}V^2$ by Theorem 163 we get:

$$\begin{aligned} & Z(1-s;\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}};\hat{\varphi}) \\ 2^{-2r_2}\frac{1}{N\mathfrak{c}\cdot V}Z(1-s;\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}};\hat{\varphi}) &= \int_A \varphi\left(r\mathfrak{c}\mathcal{C}_{K/\mathbb{Q}}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\|r\|^{s}d^\times r + \frac{1}{}\int_A \hat{\varphi}\left(r\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\|r\|^{1-s}d^\times r \\ &\quad -\hat{\varphi}(0)\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{1-s} - \frac{\varphi(0)}{N\left(\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\cdot V}\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{s}. \end{aligned}$$

□

PROOF OF PROPOSITION 219. Let A^{c} be the complement $\{x \in K_\infty^\times \mid \|x\| \le 1\}$. Then

$$Z(s;\mathfrak{c};\varphi) = \int_A \varphi(r\mathfrak{c})\|r\|^s d^\times r + \int_{A^{\mathrm{c}}} \varphi(r\mathfrak{c})\|r\|^s d^\times r,$$

and we need to deal with the second integral. Completing the sum to the whole lattice we have $\varphi(r\mathfrak{c}) = \sum_{\lambda\in r\mathfrak{c}}\varphi(\lambda) - \varphi(0)$, and we would like to apply Poisson sum for which we need to determine the lattice dual to $r\mathfrak{c}$. By Lemma 142 the lattice dual to $\mathfrak{c}$ is $\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}$ so the lattice dual to $r\mathfrak{c}$ is $r^{-1}\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}$ and we conclude that:

$$\varphi(r\mathfrak{c}) = \frac{1}{\operatorname{vol}(K_\infty/r\mathfrak{c})}\hat{\varphi}\left(r^{-1}\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right) - \varphi(0) + \frac{1}{\operatorname{vol}(K_\infty/r\mathfrak{c})}\hat{\varphi}(0).$$

□

Integrating on A^{c} we have:

$$\int_{A^{\mathrm{c}}} \varphi(0)\|r\|^s d^\times r = \varphi(0)\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\int_0^1 r^s d^\times r = \varphi(0)\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{s}$$

and

$$\begin{aligned} \int_{A^{\mathrm{c}}} \frac{\hat{\varphi}(0)}{\operatorname{vol}(K_\infty/r\mathfrak{c})}\|r\|^s d^\times r &= \frac{\hat{\varphi}(0)}{N\mathfrak{c}\cdot V}\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\int_0^1 r^{s-1}d^\times r \\ &= \frac{\hat{\varphi}(0)}{N\mathfrak{c}\cdot V}\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{s-1} \end{aligned}$$

and hence

$$\begin{aligned} \int_{A^{\mathrm{c}}} \varphi(r\mathfrak{c})\|r\|^s d^\times r &= \frac{1}{N\mathfrak{c}\cdot V}\int_{A^{\mathrm{c}}} \hat{\varphi}\left(r^{-1}\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right)\|r\|^{s-1}d^\times r \\ &\quad -\varphi(0)\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{s} - \frac{\hat{\varphi}(0)}{N\mathfrak{c}\cdot V}\operatorname{vol}\left(\mathcal{O}_K^\times\backslash K_\infty^1\right)\frac{1}{1-s}. \end{aligned}$$

As before, changing variables $r \to r^{-1}$ gives finally:

$$\begin{aligned} Z(s;\mathfrak{c};\varphi) &= \int_A \varphi(r\mathfrak{c}) \|r\|^s d^\times r + \frac{1}{N\mathfrak{c}\cdot V} \int_A \hat{\varphi}\left(r\mathfrak{c}^{-1}\mathcal{C}_{K/\mathbb{Q}}\right) \|r\|^{1-s} d^\times r \\ &\quad -\varphi(0)\,\mathrm{vol}\left(\mathcal{O}_K^\times \backslash K_\infty^1\right) \frac{1}{s} - \frac{\hat{\varphi}(0)}{N\mathfrak{c}\cdot V}\,\mathrm{vol}\left(\mathcal{O}_K^\times \backslash K_\infty^1\right) \frac{1}{1-s}. \end{aligned}$$

COROLLARY 221. *$\zeta(s;\mathfrak{c})$ extends meromorphically as well.*

PROOF. For any $\varphi \in C_c^\infty(K_\infty^\times)$ the transform $\tilde{\varphi}(s)$ is entire, and we can choose it to be non-vanishing at any specific s. □

THEOREM 222. *$L(s;\chi)$ continues meromorhpically to $\mathbb{C}$, holomorphically unless $\chi = \chi_0$, with the functional equation ...*

Bibliography